CAPITAL UNIVERSITY OF SCIENCE AND
TECHNOLOGY, ISLAMABAD

Cryptographic Schemes Based on Enhanced Matrix Power Function

by

Saadia Noor

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

in the

Faculty of Computing
Department of Mathematics

2019

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

CERTIFICATE OF APPROVAL

Cryptographic Schemes Based on Enhanced Matrix Power Function

by

Saadia Noor

(MMT171008)

THESIS EXAMINING COMMITTEE

S. No.	Examiner	Name	Organization
(a)	External Examiner	Dr. Tariq Shah	QAU, Islamabad
(b)	Internal Examiner	Mr. Qamar Mahmood	CUST, Islamabad
(c)	Supervisor	Dr. Rashid Ali	CUST, Islamabad

Dr. Rashid Ali
Thesis Supervisor
May, 2019

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

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

Author's Declaration

I, **Saadia Noor** hereby state that my M.Phil thesis titled "**Cryptographic Schemes Based on Enhanced Matrix Power Function**" 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.

(Saadia Noor)

MMT171008

Plagiarism Undertaking

I solemnly declare that research work presented in this thesis titled **"Cryptographic Schemes based on Enhanced Matrix Power Function"** 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.

(Saadia Noor)

MMT171008

Acknowledgements

First of all, I would like to thank **Almighty Allah** for His countless blessings 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 gratitude to my kind supervisor **Dr. Rashid Ali** for his constant motivation. He was always there whenever I found any problem. I really appreciate his efforts and guidance throughout my thesis and proud to be a student of such kind supervisor.

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. Dur-e-Shehwar** and **Dr. Samina Rashid** for conveying the excellent lectures.

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

I am thankful to all of my family members for becoming a bulwark of patience and support during my research work. However, my deepest gratitude is reserved for my Parents for their earnest prayers, unconditional love and unflinching support in completing my degree program. They supported and encouraged me throughout my life.

I would like to thank all of my friends Mehwish Sehar, Sumaira BiBi, Sania Mehmood, Saba Noureen and Sundas Iqbal for supporting me during degree programs. Also I would like to thank all my seniors for guiding me during my research journey. Especially, I would like to thank my Husband for motivating me during research work.

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

(Saadia Noor)

MMT171008

Abstract

A new enhanced matrix power function (MPF) is presented for the construction of cryptographic primitives and an Asymmetric Cipher in non-commutative cryptography. As stated in previously published papers, a matrix power function is an action of two matrices powering some base matrix on the left and right. The inversion equations of MPF, analogous to the MPF problem, are derived and have some structural similarity with equations of classical multivariate quadratic (MQ) problem. The matrix power function problem seems to be more complicated unlike the MQ problem, as its equations are not defined over the field, but are represented as leftright action of two matrices defined over the platform semi-groups and in particular, over the Galois Field $GF(p^q)$. The main results are: (1) the proposal of key exchange protocol based on nonsymmetric and noncommuting algebraic structures, *i.e* $GF(p^q)$. (2) the algebraic structures are proposed for the construction of asymmetric cipher based on matrix power function. (3) the presentation of preliminary security analysis. These results allow us to consider that the enhanced MPF can be a candidate one-way function (OWF), since the effective (polynomial-time) inversion algorithm for it is not yet known. Detailed examples of the application of the proposed Matrix power function for the Key Agreement Protocol (KAP) and an Asymmetric Cipher are presented. Since the direct MPF value is computed adequately, the proposed MPF is suitable for the realization of cryptographic protocols in devices with restricted computation resources.

Contents

List of Figures

List of Tables

Abbreviations

DH	Diffie Hellman
DLP	Discrete Logrithm Problem
CSP	Conjugacy Search Problem
OWF	One Way Function
PKA	Public Key Authority
CA	Certificate Authority
MPF	Matrix Power Function
MITM	Man In The Middle
MATE	Man At The End

Symbols

M	Plaintext or Message
C	Ciphertext
E	Encryption Algorithm
D	Decryption Algorithm
P_R	Private Key
P_U	Public Key
$\mathbb{G}$	Group
$\mathbb{Z}$	Set of Integers
$\mathbb{R}$	Set of Real Numbers
$\mathbb{Q}$	Rational Numbers
$\mathbb{C}$	Complex Numbers
$\mathbb{Z}_p$	Finite Field Of Order Prime p

Chapter 1

Introduction

There is a major need of secure channel for wireless networking and secret communication for decades, since the advancement of communication technology is influencing the development of more reliable authentic cryptosystems. Over 2000 years, shift ciphers based on alphabets have been used. Later on many ciphers were introduced for sending codes or secret messages. For example, mono alphabetical cipher, playfair cipher, four square cipher, hill ciphers of different orders, etc. With the passage of time resistance to these cryptosystems has been introduced and there has been numerous attacks applicable on them.

Cryptography [1] actually gives us tools to conceal the sensitive information and transmit it confidentially over the susceptible communication channel. For this purpose cryptography gives us basic structure known as cryptosystem. This system has five major constituents named as plaintext, encryption algorithm, decryption algorithm, ciphertext and key.

Purpose of cryptography [2] is not only encryption and decryption but to provide safety for information and data. Cryptography gives data confidentiality, authenticity, availability and integrity.

There are two major classification of cryptography based on key administration known as Symmetric key cryptography [3] and Asymmetric key cryptography [3]. In Symmetric key cryptography, only one key is handed over to both the parties to scramble or unscramble the data but the main issue with this technique is

key distribution when there are large number of participants in one protocol. If this key is disclosed communications get compromised. Examples of symmetric key cryptography involves DES systems [4] and AES systems [5]. To overcome the significant key issue in symmetric key cryptography, In 1976, Asymmetric key cryptography was introduced by Diffie-Hellman [6]. This idea brought revolution in cryptosystems and resolved the key distribution issues. Asymmetric key cryptography operates with pair of keys. In Asymmetric key cryptography, encryption and decryption is performed by two different keys, so that knowledge of encryption key is not exactly equal to knowledge of decryption key. Hence, the security of the cryptosystem is not compromised. Examples of Asymmetric key cryptography involves ElGamal [7], RSA [8], Elliptic curve cryptography (ECC) [9], etc.

Recent technologies affecting the advancement of cryptographic protocols are Internet Of Things(IOT) [10] and Quantum computers [11]. The resistance to quantum cryptanalysis became important after the proposal of polynomial time quantum cryptanalysis by Peter W. Shor [12]. For conventional cryptographic primitives named as Diffie-Hellman, RSA, ECC cryptosystems the security to quantum crytanalysis became more challenging.

The creation of One Way Functions (OWF)[13] is a modern trend these days and its security relies on Non-acceptance Polynomial time NP hard problems [14].

NP problem is easy to confirm that proposed solution is true but its difficult to be assured that its the only true solution that exists. For example, the given set $\{-8, -4, -2, 1, 5, 8\}$ sums upto to zero. Is there any other non empty subset that sums upto zero? and the answer to this is yes, *i.e* $\{-4, -2, 1, 5\}$.

Effective cryptanalysis algorithms that can solve NP problems [14] are not known yet. Therefore cryptosystems based on one way functions is a noteable part of quantum cryptography. Many cryptographic primitives that can resist quantum crptanalysis has been created such as lattice based cryptography. One of them is one way function based on multivariate quadratic problem (MQ) [15] which has been proved to be NP complete [16] and NP hard [17]. Said OWF has some connection with the proposed one way function based on enhanced matrix power function (MPF) problem. Additional drift for constructing primitives in post

quantum cryptography is of using algebra based non-commutative structures. In [18], author suggested this theme.

The focal aim for these swings was administration towards the use of non commutative [19] groups like "braid groups, Thompson groups, polycyclic groups, Grigorchuk groups, matrix groups, etc".

An entralling proposal based on non-commutative groups was presented by Anshel-Goldfield in [19]. In this book, author designed key exchanging based on commutator equality by introducing the notion of algebraic eraser.

Anyhow, nearly these perspectives were cryptanalyzed and their shortcomings were proclaimed.

Variety of corresponding papers can be found following from year 2017, but they utilize non-commutative group in their own ways like using structures having non symmetry, problems based on group rings like Learning With Errors (LWE) [20]. It can be seen that not only non-commutative structures but also non symmetric structures are employed. Idea of using matrix power function in cryptography was initiated by Sakalauskas in [21]. In [22], a captivating new enhanced matrix power function was proposed as a continuation of above said publications in this field. Initially, the Matrix power function was launched in [21] for establishing symmetric cipher. The further implementations for asymmetric primitives constructions were performed in [23–26].

1.1 Current Research

In this dissertation, a new key exchanging scheme is proposed on the basis of enhanced matrix power function and also a new and modified version of an asymmetric cipher based on matrix power function is introduced.

The focal aim of this research is to establish a matrix power function having algebraic structure that is non-commutative and non-symmetric. This can be assummed that it will be more resistance to quantum cryptanalysis [27]. Since it is better than that algebra based structures which have some kind of periodicity and symmetry. This proposal is different from other non commutating algebraic

structures.

The following tasks are performed in this research.

1. The construction of enhanced matrix power function is based on extended Galois field and finite field because of its large key space and enhanced security.

2. Using the MPF, we have proposed a new key exchange scheme based on discrete log problem.

3. The construction of new and modified version of an asymmetric cipher based on matrix power function with Galois field in its platform is proposed.

4. We have developed codes and algorithms using computer algebra software "ApCoCoA" [28] for effective computations.

The rest of the dissertation is compiled as follows:

In **Chapter 1**, we have discussed the idea of cryptography and introduced our thesis.

In **Chapter 2**, we have given the basic definition and concepts of algebra and cryptography to enlighten the idea that is going to be presented in the succeeding chapters. In the form of sections, the brief description of the cryptography, cryptanalysis, basic notions of Matrix power function, Public key authority and Diffie-Hellman key exchange protocol is discussed.

In **Chapter 3**, we have four sections. First section is about the general overview of enhanced matrix power function with some definitions and properties. In second section we have proposed an algorithm for key exchanging based on matrix power function using Galois field $GF(p^q)$ and general linear group $GL(Z_p)$. Third section deals with the toy example with artificially small matrix order to explain this idea. Also there are two illustrative examples and their calculations are carried out with the help of Computer algebra system "ApCoCoA".

In **Chapter 4**, we have reviewed an article named as " New Asymmetric cipher of non-commuting cryptography class based on matrix power function by Eligijus Sakalauskas, Aleksejus Mihalkovich published in 2014" [23]. We have inquired and

reviewed the calculation performed in this paper and also in the light of this paper, we have proposed a modified version of this scheme using Galois fields. Also there are two examples to demonstrate the proposed Asymmetric cipher. All the calculation are performed with the help of Computer algebra system "ApCoCoA".

Chapter 2

Preliminaries

In this chapter some basic definitions from cryptography and key management are presented. Furthermore, some basic definitions from algebra are also highlighted for further assistance.

2.1 Cryptography

Cryptography is the science of secure communication between two parties in the presence of malicious entity over the public channel. More specifically, cryptography [3] is about the construction and analysis of protocols that block hackers from accessing secret messages. This entire process of secure communication is carried out by the help of a system named as cryptosystem. This system consists of five components named as plaintext, ciphertext, encryption algorithm, decryption algorithm and the key. Plaintext is the original message where as the encrypted message is called ciphertext. The plaintext is concealed by ciphertext via the encryption algorithm. The ciphertext is then retrieved back to plaintext by the receiver or an authenticated person via the decryption algorithm. Both sender and receiver use a secret key to encrypt the original message. The whole security of this cryptosystem is based on the key security, otherwise the secrecy is compromised.

2.1.1 Purposes of Cryptography

Cryptography not only secure the messages, but also elevates physical world issues that need inviolability of data. In current era, the main purposes [2] of cryptography are as under:

- **Confidentiality:** Confidentiality comes up with two embedded qualities, *i.e* data confidentiality and privacy.
    a. **Data Confidentiality:** Disclosure or non-availability of personal or privileged information to adversaries is guaranteed.
    b. **Privacy:** Authority is to be assured to oneself that data associated to them will not be compromised.
- **Integrity:** Integrity involves:
    a. **Data Integrity:** There is assurity that the data is reconstructed merely in a legitimate way.
    b. **System Integrity:** A guaranteed system that fulfills the propose ideas in an unaffected manner, that is free from illegal exploitation.
- **Authenticity:** The competency to recognize the individuals that are communicating with each other and also the source of the data.
- **Availability:** The accessibility of schemes to certified owners according to their requirements.

2.1.2 Classification of Cryptography

There are two major classification of cryptography based on key dissemination known as Symmetric Key and Asymmetric Key Cryptography.

- Symmetric Key Cryptography
- Asymmetric Key Cryptography

2.1.2.1 Symmetric Key Cryptography

Since 1976 before the development of modern cryptographic schemes, symmetric key cryptography [29] is used over public networks for transmission of secret messages. The other name for this technique is public key cryptography. In this technique, both encryption and decryption are done by same and only one key. A protocol for typical Symmetric key cryptography is shown in Figure 2.1 in which both participants are using a common key K for data encryption and decryption which is concealed from attackers. (DES) Data Encryption Standard [3], (AES)

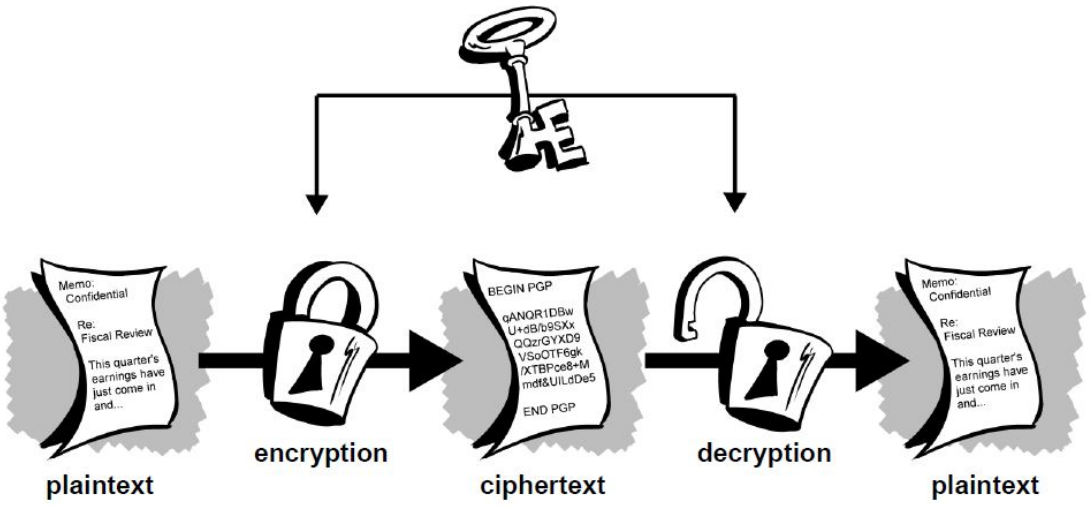

Figure 2.1: Symmetric key Cryptography.

Advanced Encryption Standard [5] and Blowfish [30] are the examples of Symmetric key cryptography. Disadvantages of this cryptosystem include key management and security issues. Symmetric encryption techniques may be classified as either block cipher or stream cipher. Block cipher performs encryption and decryption on a fixed length block of data and gives common block of ciphertext at a time while stream cipher perform encryption and decryption on one byte of plaintext at a time.

2.1.2.2 Asymmetric Key Cryptography

In 1976, Whitfield Diffie and Martin Hellman [6] proposed the great idea of asymmetric key cryptography to reduce the issue of key security. Their belief was based

on one-way trapdoor function which is used in transmission of keys between the two parties. Its base is mathematical function preferably than the substitution and permutation. In Asymmetric key cryptography, private and public keys are used in encryption and decryption of data, actually these keys are not identical but somehow large enough to be paired together. Private key is stored secret while public one is publicaly available. The public key of one entity is used to encrypt message while the other one uses his private key for decryption. The main components for public key encryption [18] are as follows in Figure 2.2. The plaintext

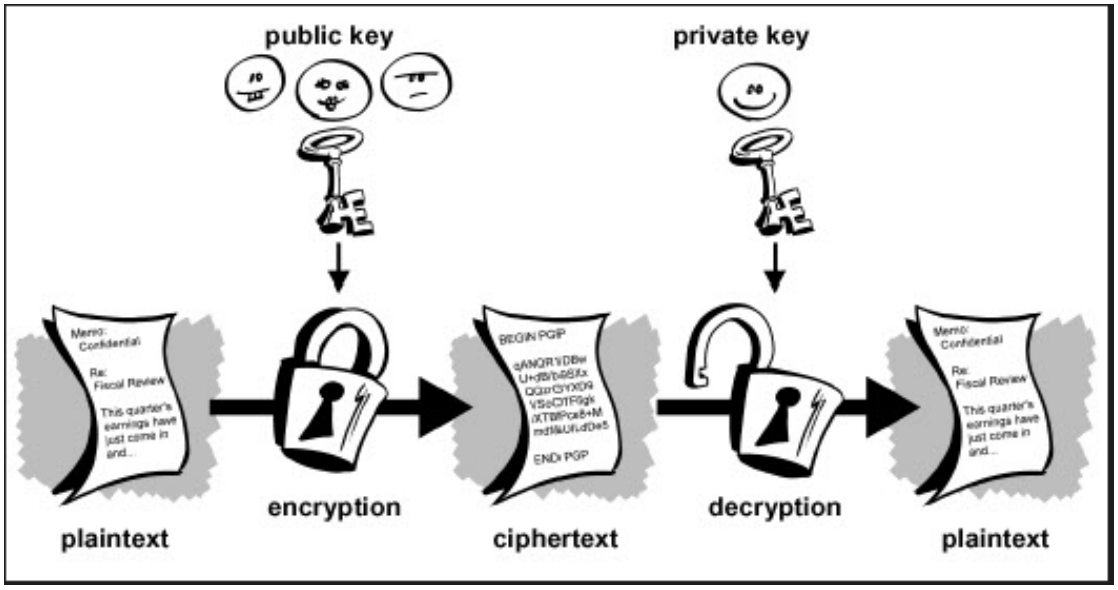

Figure 2.2: Asymmetric Key Cryptography.

(M) is encrypted with the help of encryption algorithm (E) and public key (PU) of the recipient and coverted in ciphertext (C), after receiving the ciphertext, recipient will use his own private key (PR) and will decrypt the encoded message via decryption algorithm. The structure is given below:

$$C = E(P_U, M) \tag{2.1}$$

$$M = D(P_R, C). \tag{2.2}$$

Examples for Asymmetric key cryptography [31] are RSA cryptosystem [8], ElGamal cryptosystem [7] and Elliptic curve cryptosystem [9].

2.2 Cryptanalysis

The operation used to crack a system or communication is called an attack [32] on that system. The main aim of attack is to recover the secret key K and not only the message.

Cryptanalysts is the person who execute this attack and the process of this whole attack is known as cryptanalysis [33]. It can be said that a cryptanalyst does cryptanalysis when there is some weakness in the cryptosystems. Either confidentiality, integrity, authenticity or availability of the crypstosystem is compromised [34]. There are two general approaches of cryptanalytic attacks such as total-break attacks and single break attacks.

• **Total-break Attacks**

In this approach [35], attacker's main aim is to unveil the secret key or to model another fake key so that he can decrypt the system successfully.

• **Single-break Attacks**

In this approach, attacker attempts to retrieve plaintext by using the available knowledge on public forum.

There are many known cryptographic attacks [36] one can found in the literature, some of them are discussed here.

2.2.1 Ciphertext Only Attacks

In this category, attacker has the knowledge of encrypted text and the encryption technique and he tries to reveal the original text. Either with the help of occurrence of frequency of characters or any other [37].

2.2.2 Known Plaintext Attacks

In this category, attacker has the apprehension of some of the ciphertext as well as its corresponding plaintext. On this basis, he attempts to recover the key or makes a logical algorithm to decode any further ciphertexts [38].

2.2.3 Chosen Plaintext Attacks

In this category, attacker arbitrarily selects plaintext according to his own preferences and tries to obtain ciphertext. Using the combination of these two he attempts to recover key [34].

2.2.4 Chosen Ciphertext Attacks

In this category, attacker chooses ciphertext [39] according to his wish and tries to obtain corresponding plaintext and tries to acquire as much information as he can to obtain the secret key successfully [40].

2.2.5 Man In The Middle Attacks (MITM)

In this category, attacker sits in between the two secretly communicating parties and gets a hold over communication from both the transmitter and recipient ends. To perform this man in the middle attack [41], attacker first chooses two fake keys and then start the transmission with first party using his one key and when he establish this channel with first party, he gets the encrypted information and decrypt this with his own keys. Then he encrypts or altered the received message using his keys and transmits this to second party, when second party approaches him and establish communication he dercypts their encrypted information using his keys. In this way one can interrupt the whole communication by hiding its real identity from both ends and compromise the security of the system.

2.2.6 Man At The Ends Attacks (MATE)

One of the form of active attack in security of a communication channel found is a Man at the end attack [42], which is somewhat similar to man in the middle attack. As in this attack, the malicious entity has a control over device which allows him to amend or remove the message sent from one side of communication

channel. As the adversary is a human, therefore has much abilities of a human mind. Although attacker has sanction and limitless access to the gadget and this results in all security protections to go in vain for a specific period of time.
Timing has a great role in this attack as attacker must have to reciprocate and establish the traffic of messages before the legitimate one. The need for a timing advantage make this attack more difficult to be implemented, as it demands a beneficent position in the network like internet backbone.

2.2.7 Brute Force Attacks

In this category, attacker attempts every feasible key in order to guess the original message from encrypted one. With larger key extent, this attack [43] can be made invalid .

2.3 Mathematical Background

In this section we will present some elementary definitions from algebra that will be used throughout the thesis.

Definition 2.3.1 (Groups)
The nonempty set $\mathbb{G}$ of elements that satisfies the following axioms under the binary operation $*$ is called a group and is represented by $(\mathbb{G}, *)$ [44].

G1. **Closure Property:** Binary operation $*$ is closed, *i.e.* $s * t \in \mathbb{G}$ for all $s, t \in \mathbb{G}$.

G2. **Associativity:** $(s * t) * u = s * (t * u)$ for all $s, t, u \in \mathbb{G}$.

G3. **Existence of Identities:** There exists an element $i \in \mathbb{G}$ such that $s * i = i * s = s$ for all $s \in \mathbb{G}$. Here i is the identity of set $\mathbb{G}$.

G4. **Existence of Inverses:** For each element $t \in \mathbb{G}$, $\exists\ t' \in \mathbb{G}$ such that $t * t' = t' * t = i$. Here i is the identity of $\mathbb{G}$.

Example 2.3.2 Some examples of groups are given below.

i. Set of complex number $\mathbb{C}$, real numbers $\mathbb{R}$, rational numbers $\mathbb{Q}$, and integers $\mathbb{Z}$ are all group under binary operation addition " $+$ ".

ii. Set of real numbers $\mathbb{R}/\{0\}$, rational number $\mathbb{Q}/\{0\}$ and complex number $\mathbb{C}/\{0\}$ are groups under binary operation multiplication " $\cdot$ ".

iii. Let $\mathbb{Z}_w = \{0, 1, 2, ...w-1\}$ and $w > 0$ and $w \in \mathbb{Z}$ is group under the binary operation defined by addition modulo v that is $x * y = (x + y) \bmod w$.

iv. Set of integers $\mathbb{Z}$ does not form a group under multiplication due to absence of multiplicative inverses (Inverse of 3 is $\frac{1}{3}$ however $\frac{1}{3} \notin \mathbb{Z}$).

v. The set of all $n \times n$ matrices $A = [a_{ij}]$, with complex coordinates, denoted by $M_n(C)$ is a group under multiplication.

Definition 2.3.3 (Abelian Group)

A group $\mathbb{G}$ is called abelian group [44] if it satisfies the commutative law under the same binary operation that is for all $s, t \in \mathbb{G} \Rightarrow s * t = t * s$.

Example 2.3.4 Some examples of abelian groups are given below.

i. Set of rational numbers $\mathbb{Q}$, real numbers $\mathbb{R}$ and integers $\mathbb{Z}$ under addition are abelian groups.

ii. Set of rational numbers $\mathbb{Q}$, romplex numbers $\mathbb{C}$ and real numbers $\mathbb{R}$ without zero are abelian groups under multiplication.

iii. Special Linear Group is characterized as $SL(Q) = \{\mathbb{Q} \in \mathbb{T}(q, q) | det(\mathbb{Q}) = 1\}$ where $T(q, q)$ is matrix of order $q \times q$ is a group under matrix multiplication. It is non abelian group as matrices do not commute in general.

Definition 2.3.5 (Ring)

The **Ring** [44] denoted by $(R, +, .)$ is the set of elements embedded with two binary operations addition "$+$" and multiplication "$\cdot$" that satisfies the following axioms:

R1. $(R, +)$ is an abelian group.

R2. $(R, \cdot)$ is monoid.

R3. Left and right distributive laws of multiplication with respect to addition holds in R.

Example 2.3.6 Some examples of ring are given below.

i. Set of integers $\mathbb{Z}$ under addition " $+$ " and multiplication " $\cdot$ " is a ring.

ii. Let $\mathbb{Z}_p = \{0, 1, 2, ...p-1\}$ and $p > 0$ and $p \in \mathbb{Z}$ is a ring under addition and multiplication modulo p.

iii. The set of all $n \times n$ matrices with real entries under the usual matrix addition and multiplication forms a ring.

Definition 2.3.7 (Field)

The set $(F, +, \cdot)$ together with binary operations " $+$ " and " $\cdot$ " is called field F [45], if the following properties holds.

F1. F is abelian under addition.

F2. F forms an abelian group under multiplication (only nonzero elements).

F3. Multiplication is distributed over addition in F.

Example 2.3.8 Some examples of field are given below.

i. Real numbers $\mathbb{R}$ and rational numbers $\mathbb{Q}$ forms field under addition and multiplication.

ii. For every prime p, set of integers $\mathbb{Z}_p$ under mod p is a field.

iii. The set of all $n \times n$ matrices with entries of real numbers under the traditional matrix addition and multiplication forms a field.

Definition 2.3.9 (Extension Field)

Let F and S be two fields then F is the extension field [45] of S, denoted by F/T, if T is the subfield of F under the restricted operations of S.

Example 2.3.10 Some examples of extension fields are given below.

i. The field of complex numbers is the extension field of the field of real numbers, denoted by $\mathbb{C}/\mathbb{R}$.

ii. Let $p(u) = u^2 + 1 \in \mathbb{Z}_3(u)$ then there exist the extension field T of $\mathbb{Z}_3$ such that $T = \mathbb{Z}_3(u)/u^2 + 1$.
The field $\mathbb{Z}_3(u)/u^2{+}1$ is represented as $\{0, 1, 2, u, u{+}1, u{+}2, 2u, 2u{+}1, 2u{+}2\}$, which is the set of all polynomials in u of degree less than 2 with coefficients from $\mathbb{Z}_3$
Note that $(u^2 + 1) + (u^2 + 1) = 0$ this implies that $u^2 + 1 = 0$ so $u^2 = -1 = 2$. Therefore, in T there exist the polynomials that are irreducible in mod $(u^2 + 1)$.

2.4 Galois Field

A finite field [47] named as Galois field was first proposed by the French mathematician Evariste Galois in 1830. Galois field [48] is a finite field with order as a prime or extended. Let p be a prime number, a finite field with p elements denoted by $GF(p)$ or $\mathbb{Z}_p$, consists of set of integers $Z_p = \{0, 1, 2, \cdots, p-1\}$ with arithmetic operations modulo p. As p is prime, so gcd(p,s)=1 for each $s \in \mathbb{Z}_p$ that is p is relatively prime to every element of $\mathbb{Z}_p$.

Definition 2.4.1 (Polynomial Over $GF(p)$)
The given expression having 'x' as a variable is a polynomial $f(x)$ over $GF(p)$.

$$F(x) = a_i x^i + a_{i-1} x^{i-1} + \cdots + a_1 x + a_0 \qquad \text{for all} \quad i = 0, 1, \cdots, n.$$

where the coefficients a_i are taken from $GF(p)$.

Definition 2.4.2 (Irreducible Polynomial)
A polynomial $m(x)$ of degree q is said to be irreducible [49] if it cannot be decomposed as $m(x) = g(x)h(x)$ with polynomials $g(x)$ and $h(x)$ of degree less than q, otherwise it is known as reducible polynomial. For example, $x^6{+}x^5{+}x^4{+}x^3{+}x^2{+}x$

is reducible polynomial over $GF(2^2)$, and x^3+x^2+x, x^3+1 are irreducible polynomials over $GF(2^2)$.

2.5 Extended Galois Field $GF(p^q)$

An extension of a field to prime order is called an Extended finite field $GF(p^q)$ [50] with q a positive integer number, where $GF(p^q)$ is the set of all polynomials over $GF(p)$ of degree less than q and coefficients from $GF(p)$. In the examples below, we will represent some elements from Galois fields in tablular form.

Example 2.5.1 Elements of $GF(2^8)$

The elements in $GF(2^8)$ [51] are polynomials having degrees less than 8, with coefficients in $GF(2) = \{0,1\}$ reduced under polynomial modulo by using an irreducible polynomial of degree 8. It consist of 256 different elements with 8-bits binary representation. All the elements of $GF(2^8)$ are shown in the Table 2.1.

Decimal	Polynomial	Binary
0	0	00000000
1	1	00000001
2	β	00000010
3	$\beta+1$	00000011
4	β^2	00000100
5	β^2+1	00000101
6	$\beta^2+\beta$	00000110
7	$\beta^2+\beta+1$	00000111
8	β^3	00001000
9	β^3+1	00001001
10	$\beta^3+\beta$	00001010
.	.	.
255	$\beta^7+\beta^6+\beta^5+\beta^4+\beta^3+\beta^2+\beta+1$	11111111

Table 2.1: Elements of Galois Field $GF(2^8)$

Example 2.5.2 Elements of $GF(2^{10})$

The elements of $GF(2^{10})$ are polynomials having degrees less than 10, with coefficients in $GF(2) = \{0,1\}$ reduced under polynomial modulo by using an irreducible

polynomial of degree 10. It consist of 1024 different elements with 10-bits binary representation. All the elements of $GF(2^{10})$ are shown in the Table 2.2.

Decimal	Polynomial	Binary
0	0	0000000000
1	1	0000000001
2	β	0000000010
3	$\beta + 1$	0000000011
4	β^2	0000000100
5	$\beta^2 + 1$	0000000101
6	$\beta^2 + \beta$	0000000110
7	$\beta^2 + \beta + 1$	0000000111
8	β^3	0000001000
9	$\beta^3 + 1$	0000001001
10	$\beta^3 + \beta$	0000001010
.	.	.
.	.	.
1024	$\beta^9 + \beta^8 + \beta^7 + \beta^6 + \beta^5 + \beta^4 + \beta^3 + \beta^2 + \beta + 1$	1111111111

Table 2.2: Elements of Galois Field $GF(2^{10})$

2.6 Multiplicative Inverses in Galois Field

As the elements of Galois Fields are represented by polynomials so we need to find their inverses too. For this we use Extended Euclidean Algorithm [52] to find inverse of any polynomial in Galois field $GF(p^q)$. We can find the multiplicative inverse of any polynomial $r(x) \in GF(p^q)$ modulo an irreducible polynomial $m(x)$ when $\gcd(r(x), m(x))= 1$ with the help of underlying algorithm. $r(x) \mod m(x)$ is as follows:

Algorithm 2.6.1 (Extended Euclidean Inverse Algorithm)

Input: A polynomial $r(x)$ and an irreducible polynomial $m(x)$.

Output: $r^{-1}(x) \mod m(x)$.

1. Boot six polynomials $A_i(x)$ and $B_i(x)$ for $i = 1, 2, 3$ as

   $(A_1(x), A_2(x), A_3(x)) = (1, 0, m(x))$

   $(B_1(x), B_2(x), B_3(x)) = (0, 1, r(x))$

2. If $B_3(x) = 0$, return $A_3(x)$=gcd$(r(x), m(x))$; no inverse of $r(x)$ exist in mod $m(x)$

3. If $B_3(x) = 1$ then return $B_3(x)$=gcd$(r(x), m(x))$ and $B_2(x) = r^{-1}(x) \mod m(x)$

4. Now divide $A_3(x)$ with $B_3(x)$ also find the quotient $Q(x)$ when $A_3(x)$ is divided by $B_3(x)$.

5. Set $(T_i(x) = (A_i(x) - Q(x).B_i(x))$; $i = 1, 2, 3$.

6. Set $(A_1(x), A_2(x), A_3(x)) = (B_1(x), B_2(x), B_3(x))$

7. Set $(B_1(x), B_2(x), B_3(x)) = (T_1(x), T_2(x), T_3(x))$

8. Goto step number 2.

2.6.1 Diffie-Hellman Key Exchange Protocol(DH)

Initially, the concept of public key protocols was given by Ralph Merkle afterwards Diffie and Martin Hellman proposed this idea [6]. DH is used to exchange keys safely over the public network. This key sharing not only support two parties but more than that. DH is highly useful primitive because shared secret key can be helpful to establish a session key secretly that is used in number of different symmetric cryptosystems.

The Diffie-Hellman Key exchange protocol is briefed in following Figure 2.3.

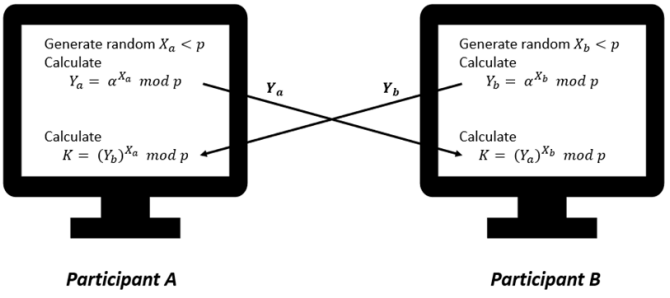

Figure 2.3: Diffie-Hellman Key exchange protocol.

Key agreement protocol between two users is as follows:

• User A generates $x_a < q$ at random, and calculates $Y_a = \beta^{x_a} \bmod q$ and sends it to user B.

• User B generates $x_b < q$ at random, and calculates $Y_b = \beta^{x_b} \bmod q$ and sends it to user A. Also calculates secret shared key as $K = (Y_a)^{x_b} \bmod q$.

• User A calculates secret shared key as $K = (Y_b)^{x_a} \bmod q$.

Definition 2.6.2 (Discrete Logrithm Problem (DLP))

Suppose we have an expression a^k, and we need to find k when a and a^k is given. This is known as discrete log problem. The discrete log problem [53] is usually known as hard problem because it is quite impossible to determine. Also it is to be noted that small order of group can easily be attacked using brute force attack but still its difficult for large order groups.

Definition 2.6.3 (Conjugacy Search Problem (CSP))

For the given elements u, v in a noncommutative group $\mathbb{G}$, the problem of determining the conjugator $w \in \mathbb{G}$ such that $u^w = w^{-1}uw = v$ is known as conjugacy search problem (CSP).

Definition 2.6.4 (Carmichael Number)

Robert Carmichael gave the idea of Carmichael number. A Carmichael number [54] is a composite number which verifies the congruence relation $b^{m-1} \equiv 1 \pmod{m}$ for all integers b that are relatively prime to m, in modular arithmetic.

The function associated with these numbers are called Carmichael function and its values are given by the following formula

$$\lambda(n) = \text{ lcm } [(p_i - 1)p_i^{(\alpha_i - 1)}]_i$$

where $p_i^{(\alpha_i)}$ are prime integers.

Definition 2.6.5 (Carmichael Theorem)

If s and m are co-prime numbers so that the greatest common divisor

$\gcd(s, m) = 1$, then $s^{\lambda(m)} = 1(\bmod m)$, where λ is the Carmichael function.

2.7 Public Key Authority (PKA)

Distribution of public keys is a challenging task. By securing the control over distribution of keys from directory we can achieve stronger security for distribution. It should have the properties of directory, that means this situation suppose that a focal authority keeps an effective directory of members public keys. This demand that users know the public key of the directory. Users then negotiate with directory to acquire any desired public key securely, for this there should be immediate access to the directory whenever keys are required. The protocol for public key authority is briefed in following Figure 2.4.

Protocol between two users and public key authority is as follows:

(1) Initiator A sends requests for the public key of user B at some recorded time to the public key authority.

(2) The authority then encrypt the public key of the other desired user B along with the request and request time of A with the help of their own private key.

(3) Initiator A then sends the encrypted message to the responder B, and that message consists of identity of A along with the specific number N_1. Encryption of this message is done by the public key of B, which can only be decrypted by the private key of B.

(4) Responder B sends requests for the public key of user A at some recorded time to the public key authority.

(5) The authority then encrypt the public key of the desired user A along with the request and request time of B with the help of their own private key.

(6) Responder B then sends the encrypted message having N_1 and N_2 to the initiator A. Encryption of this message is done by the public key of A, which can only be decrypted by the A's private key.

(7) Initiator responds back with encrypted message having N_2 that is encrypted by public key of B.

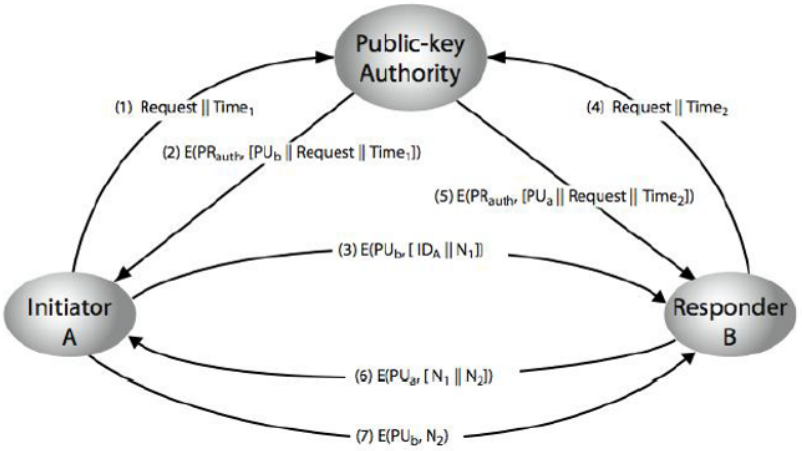

Figure 2.4: Public Key Authority.

2.8 Public Key Certificates (PKC)

Real time access to the public key authority is sometimes difficult, so overcome this issue and maintaining the secrecy certificates are issued that are as authentic as the keys acquired directly from concerned authority. This certificate holds identity and other information like validity period, usage rights etc. to public key of the corresponding user with all constituents signed by a reliable Public Key or Certificate Authority (CA). Anyone can verify this who has the knowledge of authority's public key or by the attached trusted signature. The X.509 standard is the universally accepted scheme for public key certificates. The protocol for public key certificates is briefed in following Figure 2.5.
Requirements for Public Key Certificates is as follows:

i. Owner's name and public key of any certificate can easily be obtained.

ii. Verification of the certificate by certificate authority that it is not counterfeited.

iii. Certificate authority (CA) has only the authority to create or update any certificate.

iv. Validity of the desired certificate can be verified by any participant [55].

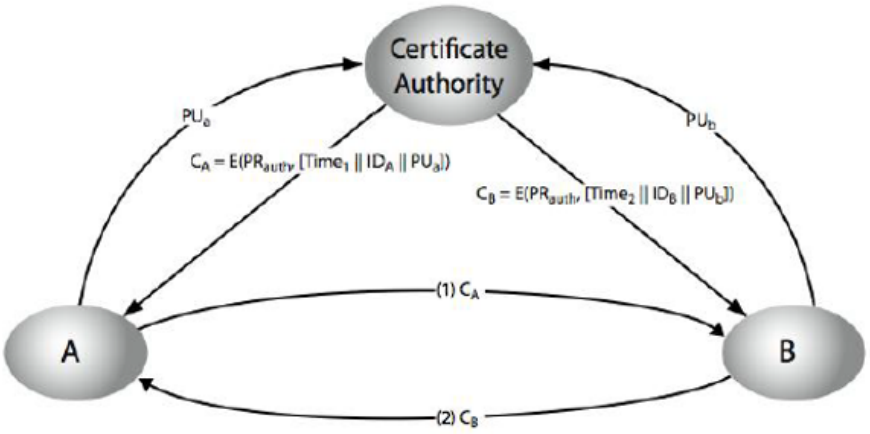

Figure 2.5: Certificate Authority.

2.9 Toeplitz Matrices

"A matrix in which each declining diagonal from left to right is constant is called a Toeplitz matrix [56] 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 we have

$$T_{i,j} = T_{i+1,j+1} = a_{i-j}.$$

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

$$T = \begin{bmatrix} a_0 & a_1 & a_2 & a_3 & a_4 \\ a_5 & a_0 & a_1 & a_2 & a_3 \\ a_6 & a_5 & a_0 & a_1 & a_2 \\ a_7 & a_6 & a_5 & a_0 & a_1 \\ a_8 & a_7 & a_6 & a_5 & a_0 \end{bmatrix}.$$

2.9.1 Circulant Matrices

"A circulant matrix [57] is a special kind of Toeplitz matrix where each row vector is shifted by one element to the right relative to the preceding row vector, enclosing

cyclically, *i.e* every row is a circular shift of the first row".

When an additional property, *i.e* $a_i = a_{i+n}$ is added to Toeplitz matrix, it becomes a circulant matrix. For example: A 5×5 circulant matrix is as follows.

$$C = \begin{bmatrix} a_0 & a_1 & a_2 & a_3 & a_4 \\ a_4 & a_0 & a_1 & a_2 & a_3 \\ a_3 & a_4 & a_0 & a_1 & a_2 \\ a_2 & a_3 & a_4 & a_0 & a_1 \\ a_1 & a_2 & a_3 & a_4 & a_0 \end{bmatrix}.$$

2.9.2 Properties of Circulant Matrices

Circulant matrices and the eigenvectors gives us magnificent efficient algorithms named as fast Fourier transform (FFTs) [58], that play a pivotal role in computational science and engineering.

i. The circulant matrices [59] hold a surprising property that is the eigenvectors of circulant matrices are always the same. The eigenvalues are different for each matrix, but since we know the eigenvectors we can easily diagonalize them.

ii. 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 [52], cryptography [3], simulations [60], digital signal processing [61] etc.

iii. The eigenvectors can be written as a primitive root of unity.

$$\omega_n = e^{\frac{2\pi i}{n}}$$

The quantity ω_n has the very special property that $\omega_n^n = e^{2\pi i} = 1 = \omega_n^0$, but no smaller power equals 1. Therefore, $\omega_n^{j+n} = \omega_n^j \omega_n^n = \omega_n^j$ that is the exponents of ω are periodic.

2.10 Matrix Power Function (MPF)

A function that determines a matrix which is obtained by powering a given matrix by two numerical matrices on left and right side is known as matrix power function. It is some kind of similar to multiplication of a matrix by two matrices on both sides, respectively. The matrix having matrices as a power is named as based matrix while the the matrices that are in powers are known as power matrices. Generally, the base matrix is defined over the multiplicative semigroup S and power matrices over the numerical semiring R. The base matrices and power matrices are taken from matrix semigroups M_S and M_R respectively.

Definition 2.10.1 (Left Sided MPF)
This left sided MPF is given by a matrix W powered by another matrix X on the left, with value equal to some matrix $A = \{a_{ij}\}$. The formation is as follows:

$$ {}^{X}W = A, \qquad \{a_{ij}\} = \prod_{k=1}^{m} w_{jk}^{x_{ik}} \tag{2.3} $$

If X, W are matrices of order 2, then ${}^{X}W$ is computed as follows:

$$ \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} \begin{bmatrix} w_{11} & w_{12} \\ w_{21} & w_{22} \end{bmatrix} = \begin{bmatrix} w_{11}^{x_{11}}.w_{21}^{x_{12}} & w_{12}^{x_{11}}.w_{22}^{x_{12}} \\ w_{11}^{x_{21}}.w_{21}^{x_{22}} & w_{12}^{x_{21}}.w_{22}^{x_{22}} \end{bmatrix} $$

Example 2.10.2 If X, W are in $M_2(\mathbb{F})$ as

$$ X = \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix}, W = \begin{bmatrix} 4 & 2 \\ 1 & 6 \end{bmatrix} \text{ then} $$

$$ {}^{X}W = \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix} \begin{bmatrix} 4 & 2 \\ 1 & 6 \end{bmatrix} = \begin{bmatrix} 64 & 48 \\ 16 & 144 \end{bmatrix} $$

Definition 2.10.3 (Right Sided MPF)

This right sided MPF is given by a matrix W powered by another matrix Y on the right, with value equal to some matrix $B = \{b_{ij}\}$. The formation is as follows:

$$W^Y = B, \qquad \{b_{ij}\} = \prod_{k=1}^{m} w_{ik}^{y_{kj}} \tag{2.4}$$

If W, Y are matrices of order 2, then W^Y is computed as follows:

$$\begin{bmatrix} w_{11} & w_{12} \\ w_{21} & w_{22} \end{bmatrix} \begin{bmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{bmatrix} = \begin{bmatrix} w_{11}^{y_{11}}.w_{12}^{y_{21}} & w_{11}^{y_{21}}.w_{12}^{y_{22}} \\ w_{21}^{y_{11}}.w_{22}^{y_{21}} & w_{21}^{y_{21}}.w_{22}^{y_{22}} \end{bmatrix}$$

Example 2.10.4 If W, Y are in $M_2(\mathbb{F})$ as

$$W = \begin{bmatrix} 4 & 2 \\ 1 & 6 \end{bmatrix}, Y = \begin{bmatrix} 2 & 3 \\ 3 & 1 \end{bmatrix} \text{ then}$$

$$W^Y = \begin{bmatrix} 4 & 2 \\ 1 & 6 \end{bmatrix} \begin{bmatrix} 2 & 3 \\ 3 & 1 \end{bmatrix} = \begin{bmatrix} 128 & 128 \\ 216 & 6 \end{bmatrix}$$

Definition 2.10.5 (Two Sided MPF)

The two sided MPF is given by a matrix W powered by two matrices, X on the left and Y on the right, with value equal to some matrix $C = \{c_{ij}\}$. The formation is as follows:

$${}^X W^Y = C, \qquad \{c_{ij}\} = \prod_{k=1}^{m} \prod_{\ell=1}^{m} w_{k\ell}^{x_{ik}.y_{\ell j}} \tag{2.5}$$

If X, W, Y are matrices of order 2, then ${}^X W^Y$ is computed as follows:

$$\begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} \begin{bmatrix} w_{11} & w_{12} \\ w_{21} & w_{22} \end{bmatrix} \begin{bmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{bmatrix}$$

$$= \begin{bmatrix} w_{11}^{x_{11}y_{11}}.w_{21}^{x_{12}y_{11}}.w_{12}^{x_{11}y_{21}}.w_{22}^{x_{12}y_{21}} & w_{11}^{x_{11}y_{12}}.w_{21}^{x_{12}y_{12}}.w_{12}^{x_{11}y_{22}}.w_{22}^{x_{12}y_{22}} \\ w_{11}^{x_{21}y_{11}}.w_{21}^{x_{22}y_{11}}.w_{12}^{x_{21}y_{21}}.w_{22}^{x_{22}y_{21}} & w_{11}^{x_{21}y_{12}}.w_{21}^{x_{22}y_{12}}.w_{12}^{x_{21}y_{22}}.w_{22}^{x_{22}y_{21}} \end{bmatrix}$$

Example 2.10.6 If X, W, Y are in $M_2(\mathbb{F})$ as

$$X = \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix}, W = \begin{bmatrix} 4 & 2 \\ 1 & 6 \end{bmatrix}, Y = \begin{bmatrix} 2 & 3 \\ 3 & 1 \end{bmatrix}$$

$$\text{then } {}^{X}W^{Y} = \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix} \begin{bmatrix} 4 & 2 \\ 1 & 6 \end{bmatrix} \begin{bmatrix} 2 & 3 \\ 3 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 64 & 48 \\ 16 & 144 \end{bmatrix} \begin{bmatrix} 2 & 3 \\ 3 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 452984832 & 12582912 \\ 764411904 & 589824 \end{bmatrix}$$

Definition 2.10.7 (One Way Function (OWF))

A function [13] that gives value at every input but its inversion is considered to be hard.

Definition 2.10.8 (Matrix Multivariate Quadratic (MQ) Problem)

[15] Consider that a matrix Q is described over some cyclic group A given that the generator of the group is a. A discrete logarithm ld_a having base as generator of $E = {}^{X}Q_{Y}$ can be related to E, Q to get

$$ld_a E = ld_a^X Q^Y = X ld_a Q Y = XHY,$$

where ld_aE and ld_aQ implies, $H = ld_aQ$. So, assume that H and ld_aE are specified, finding the unknown matrices X and Y is referred as matrix MQ problem. This problem resembles the popular NP-complete problem and named as multivariate quadratic (MQ) problem. "Matrix MQ problem is a candidate one way function", which is proved in [62–64] with the help of conjectures as the inversion of this problem is associated with the NP complete solutions of popular MQ problems over any field.

Chapter 3

Cryptographic Primitive Construction Based on Enhanced Matrix Power Function

In this chapter, we have proposed a new scheme whose theme is taken from Eligijus Sakalausas research article named as " Enhanced Matrix Power Function for Cryptographic Primitive Construction" [22]. In this scheme, we have replaced base matrix with polynomial matrix from Galois Field and powering matrices with matrices from general linear group. Also we have used computer algebra system "ApCoCoA" [28] to solve the key protocol algorithm used here.

3.1 Properties of Matrix Power Function

Matrix power function is associated with following properties.

Property 1. One sided associativity holds in matrix power function (left-right respectively). If the following identity is true.

$$ {}^{Y}({}^{X}W) = {}^{(XY)}W = {}^{XY}W \tag{3.1} $$

$$(W^X)^Y = W^{(XY)} = W^{XY} \tag{3.2}$$

Property 2. Two sided associativity holds in matrix power function. If the following identity is true.

$$({}^X W)^Y = {}^X(W^Y) = {}^X W^Y \tag{3.3}$$

Definition 3.1.1

A matrix power function is considered as associative if it holds both one-sided and two-sided associativity.

Definition 3.1.2

The computation of immediate value for matrix power function is to search matrix C in equation 2.5, when matrices W, X and Y are given.

Definition 3.1.3

The computation of reverse value for matrix power function is to search for matrices X and Y in equation 2.5, when matrices W and C are given.

Conjecture 3.1.4 The construction of cryptographic protocol based on MPF has the following necessary conditions.

1. It holds associative law.
2. Matrices X and Y are taken as circulant matrices because circulant matrices holds commutative property. So for any circulant matrices U and V.

$$UX = XU, \tag{3.4}$$

$$YV = VY \tag{3.5}$$

3. MPF satisfies the following clauses.
   - ***i.*** The computation of direct MPF value is computationally easy.
   - ***ii.*** Without the knowledge of polynomial time algorithm, the MPF problem is polynomially identical to a certain hard problem.

Conjecture 3.1.5 Since problems based on MPF are polynomially equivalent to the particular sort of generalized multivariate(MQ) problems [15] that are assumed to be hard. So it can be observed as a potential candidate of one way function for the cryptographic primitive construction.

Conjecture 3.1.6 For constructing key agreement protocol (KAP), MPF is considered as a candidate one way function.

1. The computation of direct MPF value is algorithmically effective.
   Whereas, the computation of direct MPF value is to search matrix C in equation 2.5 , when matrices W, X and Y are given.

2. The computation of Inverse MPF value is infeasible.
   Whereas, the computation of inverse MPF value is to search for matrices X and Y in equation 2.5, when matrices W and C are given.

3. The MPF is associative.

4. The MPF problem is hard according Conjecture 2.

3.2 The Proposed Construction of Cryptographic Primitive

Diverse cryptosystems are designed using key agreement protocols, like ElGamal cryptosystem is based on Diffie and Hellman key exchange protocol. Now, we relate the primitive construction of cryptosystem based on enhanced matrix power function that can be used in public key cryptosystems having polynomials over non-commutative Rings [65]. For designing the public key cryptosystem we utilized variation of Diffie Hellman key exchange protocol.

Algorithm 3.2.1 (Certification) Suppose that Alice and Bob wants secure communication channel in the presence of adversaries, for this they need a common secret key K to proceed further. But there may be intruders that interrupt their message traffic, so firstly both the parties will coordinate with the authorized

certificate authority to confirm the identity of each other. The certificates will be obtained by following these steps:

1. Alice wants to get her public key certified, she will send her public key to authority.
2. Certificate authority then respond back with certificate C_A which is encrypted by private key of authority having identity of A, authorized public key of A and the request time of Alice.
3. Meanwhile, Bob also sends his public key to authority.
4. Certificate authority then respond back with certificate C_B which is encrypted by private key of authority having identity of B, authorized public key of B and the request time of Bob.
5. Alice now share her certificate C_A with Bob.
6. Bob also shares his certificate C_B with Alice.

In this way, there establish an authorized way to begin key agreement protocol.

Algorithm 3.2.2 (Key Agreement Protocol) The construction of the key agreement protocol (KAP) is described as follows.
Input: $W \in GF(p^q)$ as a public matrix and four secret circulant matrices X, Y, U and V belonging to general linear group $GL(n, \mathbb{Z}_p)$.
Output: Common session key K.
Key generation: Key will be generated by following these steps.

1. At random, Alice chooses two secret circulant matrices $X, Y \in GL(n, \mathbb{Z}_p)$, and then calculate the MPF value and transmits it to Bob.

$$A = {}^{X}W^{Y}$$

2. Similarly, at random Bob chooses two secret circulant matrices $U, V \in GL(n, \mathbb{Z}_p)$ to calculate the MPF value and transmits it to Alice.

$$B = {}^{U}W^{V}$$

3. Now Alice will calculate the same secret shared key as

$$K_A = {}^{X}({}^{U}W^{V})^{Y} \tag{3.6}$$

4. Then, Bob will calculate the same secret shared key as

$$K_B = {}^{U}({}^{X}W^{Y})^{V} \tag{3.7}$$

5. Secret session key K for the both the paticipants is same.

$$K_A = K = K_B$$

We have used general linear group of matrices of finite order over the finite field $GL(n, \mathbb{Z}_p)$ for implementing this scheme, as the convolution of the proposed scheme depends upon conjugacy search problem(CSP) and discrete log problem (DLP).

Correctness: The correctness of the above protocol can be realized as follows: From equation 3.6 we have,

$$K_A = {}^{X}({}^{U}W^{V})^{Y} = {}^{XU}W^{VY} \tag{3.8}$$

Using equations 3.3, 3.4 and 3.5 in 3.8 , we get,

$$\begin{aligned} K_A &= {}^{UX}W^{YV} \\ &= {}^{U}({}^{X}W^{Y})^{V} \\ &= K_B \end{aligned}$$

Hence ,

$$K_A = K_B = K$$

The key agreement protocol is briefed in following Figure 3.1.

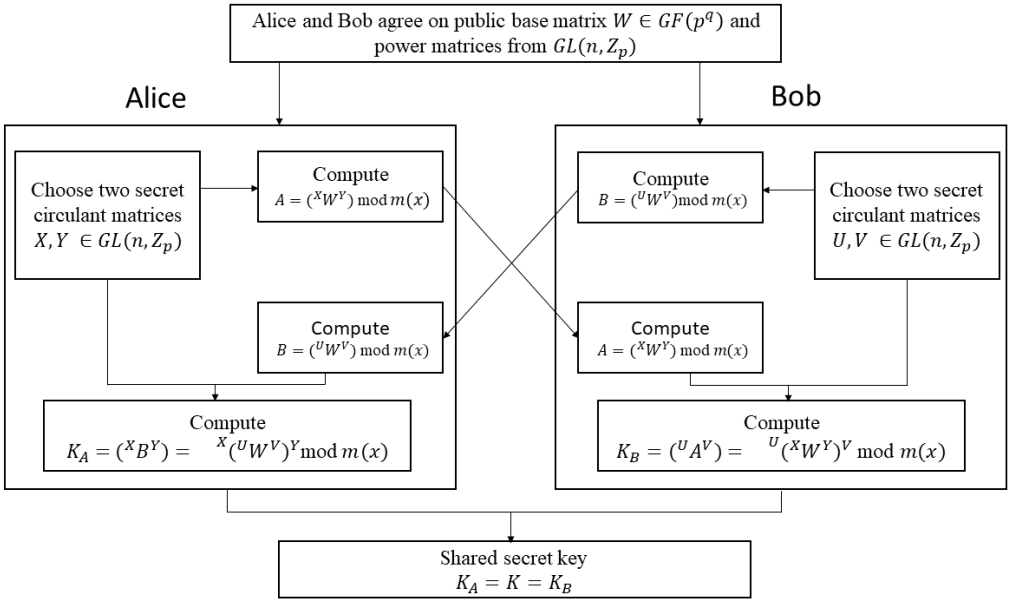

Figure 3.1: Key exchange protocol.

Example 3.2.3 Let there be two parties named as Alice and Bob, who wants to communicate securely over a public platform. They both agree on following parameters to be obvious.

Public Parameter:

i. The base matrix W will be of order 2 over the Galois field $GF(2^2)$. As we are doing our computations in Galois field and we know that operations in this field are done under certain modulo. Here we take irreducible polynomial as $m(x) = x^2 + x + 1$. All the calculations will be performed under mod $(m(x))$.

$$W = \begin{bmatrix} x & 1 \\ x+1 & x+1 \end{bmatrix} \in GF(2, 2^2)$$

ii. Their secret matrices will be circulant matrices over $GL(2, \mathbb{Z}_7)$, that is General linear group of matrices of order 2 and elements will be from $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$.

Using the algorithm given above, example follows through these steps.

Step 1. Alice chooses two secret circulant matrices [57] at random whose elements

are taken from general linear group $\mathbb{Z}_7$.

$$X = \begin{bmatrix} 3 & 6 \\ 6 & 3 \end{bmatrix} \text{ and } Y = \begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix}$$

and then she calculates ${}^{X}W^{Y}$ as follows.

$$\begin{aligned} {}^{X}W^{Y} &= \begin{bmatrix} 3 & 6 \\ 6 & 3 \end{bmatrix} \begin{bmatrix} x & 1 \\ x+1 & x+1 \end{bmatrix} \begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix} \\ &= \begin{bmatrix} x^3(x+1)^6 & (x+1)^6 \\ x^6(x+1)^3 & (x+1)^3 \end{bmatrix} \begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix} \\ &= \begin{bmatrix} x^3(x+1)^{30} & x^{12}(x+1)^{30} \\ x^6(x+1)^{15} & x^{24}(x+1)^{15} \end{bmatrix} \\ &= \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \bmod (x^2+x+1) \end{aligned}$$

and send this to Bob.

Step 2. Now, Bob chooses two secret circulant matrices at random whose elements are taken from general linear group $GL(2, \mathbb{Z}_7)$ as

$$U = \begin{bmatrix} 5 & 2 \\ 2 & 5 \end{bmatrix} \text{ and } V = \begin{bmatrix} 6 & 1 \\ 1 & 6 \end{bmatrix}$$

and then calculates ${}^{U}W^{V}$ as follows.

$$
\begin{aligned}
{}^{U}W^{V} &= \begin{bmatrix} 5 & 2 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} x & 1 \\ x+1 & x+1 \end{bmatrix} \begin{bmatrix} 6 & 1 \\ 1 & 6 \end{bmatrix} \\
&= \begin{bmatrix} x^5(x+1)^2 & (x+1)^2 \\ x^2(x+1)^5 & (x+1)^5 \end{bmatrix} \begin{bmatrix} 6 & 1 \\ 1 & 6 \end{bmatrix} \\
&= \begin{bmatrix} x^{30}(x+1)^{14} & x^5(x+1)^{14} \\ x^{12}(x+1)^{35} & x^2(x+1)^{35} \end{bmatrix} \\
&= \begin{bmatrix} x & 1 \\ x & 1 \end{bmatrix} \bmod (x^2+x+1)
\end{aligned}
$$

and send this to Alice.

Step 3. After getting ${}^{U}W^{V}$, Alice calculates her secret shared key K_A as

$$
\begin{aligned}
K_A &= {}^{X}\ ({}^{U}W^{V})^{Y} \\
&= \begin{bmatrix} 3 & 6 \\ 6 & 3 \end{bmatrix} \begin{bmatrix} x & 1 \\ x & 1 \end{bmatrix} \begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix} \\
&= \begin{bmatrix} x^9 & 1 \\ x^9 & 1 \end{bmatrix} \begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix} \\
&= \begin{bmatrix} x^9 & x^{36} \\ x^9 & x^{36} \end{bmatrix} \\
&= \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \bmod (x^2+x+1)
\end{aligned}
$$

Step 4. After getting ${}^{X}W^{Y}$, Bob calculates his secret shared key K_B as

$$\begin{aligned} K_B &= {}^{U}({}^{X}W^{Y})^{V} \\ &= \begin{bmatrix} 5 & 2 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 6 & 1 \\ 1 & 6 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \bmod (x^2 + x + 1) \end{aligned}$$

Step 5. It can be seen that shared secret key computed by both the participants is same.

$$K_A = K_B = K$$

Example 3.2.4 There are two parties in our protocol named as "Hen" and "Ben". Both the parties consent on public parameters as

i. The base matrix W will be of order 3 and is taken from the Galois field $GF(2^2)$.

$$W = \begin{bmatrix} x & 1 & x \\ 1 & x & x+1 \\ x+1 & 1 & x+1 \end{bmatrix} \in GF(3, 2^2)$$

ii. Their secret matrices will be circulant matrices and from $GL(3, \mathbb{Z}_5)$, that is General linear group of matrices of order 3 and elements will be from $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.

As we are doing our computations in Galois field and we know that operations in this field are done under certain modulo. Here we take irreducible polynomial as $m(x) = x^2 + x + 1$. All the calculations will be performed under $mod(m(x))$. The computations performed below are carried out with the help of computer algebra

software "ApCoCoA". Protocol between two parties is as follows.

Step 1. Hen chooses two secret circulant matrices at random from $GL(3, \mathbb{Z}_5)$.

$$X = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix} \text{ and } Y = \begin{bmatrix} 1 & 2 & 1 \\ 1 & 1 & 2 \\ 2 & 1 & 1 \end{bmatrix}$$

and calculates ${}^{X}W^{Y}$ as

$$\begin{aligned} {}^{X}W^{Y} &= \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix} \begin{bmatrix} x & 1 & x \\ 1 & x & x+1 \\ x+1 & 1 & x+1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 1 \\ 1 & 1 & 2 \\ 2 & 1 & 1 \end{bmatrix} \\ &= \begin{bmatrix} x & 1 & x \\ x+1 & 1 & 1 \\ 1 & 1 & x+1 \end{bmatrix} \bmod (x^2+x+1) \end{aligned}$$

and sends it to the Ben.

Step 2. Now, Ben chooses two secret circulant matrices at random from $GL(3, \mathbb{Z}_5)$ to compute ${}^{U}W^{V}$.

$$U = \begin{bmatrix} 2 & 2 & 1 \\ 1 & 2 & 2 \\ 2 & 1 & 2 \end{bmatrix} \text{ and } V = \begin{bmatrix} 3 & 2 & 2 \\ 2 & 3 & 2 \\ 2 & 2 & 3 \end{bmatrix}$$

$${}^{U}W^{V} = \begin{bmatrix} 2 & 2 & 1 \\ 1 & 2 & 2 \\ 2 & 1 & 2 \end{bmatrix} \begin{bmatrix} x & 1 & x \\ 1 & x & x+1 \\ x+1 & 1 & x+1 \end{bmatrix} \begin{bmatrix} 3 & 2 & 2 \\ 2 & 3 & 2 \\ 2 & 2 & 3 \end{bmatrix}$$

$$= \begin{bmatrix} x+1 & 1 & 1 \\ x & x & x+1 \\ 1 & x & x+1 \end{bmatrix} \bmod (x^2+x+1)$$

and sends it to the Hen.

Step 3. After getting ${}^{U}W^{V}$, Hen will calculate his secret shared key K_A as

$$K_A = {}^{X}({}^{U}W^{V})^{Y} = \begin{bmatrix} x+1 & x+1 & 1 \\ x & x+1 & x \\ 1 & x+1 & x+1 \end{bmatrix}$$

Step 4. Meanwhile, after getting ${}^{X}W^{Y}$, Ben will calculate his secret shared key K_B as

$$K_B = {}^{U}({}^{X}W^{Y})^{V} = \begin{bmatrix} x+1 & x+1 & 1 \\ x & x+1 & x \\ 1 & x+1 & x+1 \end{bmatrix}$$

Step 5. It is clear that the secret shred key obtained by both the parties is same.

$$K_A = K = K_B$$

Example 3.2.5 Let there be two parties, for key exchange protocol both agrees on the following public parameters.

i. The base matrix W will be of order 4 over the Galois field $GF(2^3)$. As we are doing our computations in galois field and we know that operations in this field are done under certain modulo. Here we take irreducible polynomial as $m(x) = x^3 + x + 1$. All the calculations will be performed under $mod(m(x))$. The computations performed below are carried out with the help of computer

algebra software "ApCoCoA".

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

ii. Their secret matrices will be circulant matrices over $GL(4, \mathbb{Z}_{11})$, that is General linear group of matrices of order 4 and elements will be from $\mathbb{Z}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

Key sharing between two parties is followed as.

Step 1. First person chooses two secret circulant matrices at random from $GL(4, \mathbb{Z}_{11})$.

$$X = \begin{bmatrix} 5 & 3 & 2 & 6 \\ 6 & 5 & 3 & 2 \\ 2 & 6 & 5 & 3 \\ 3 & 2 & 6 & 5 \end{bmatrix} \text{ and } Y = \begin{bmatrix} 7 & 6 & 1 & 4 \\ 4 & 7 & 6 & 1 \\ 1 & 4 & 7 & 6 \\ 6 & 1 & 4 & 7 \end{bmatrix}$$

to calculate ${}^{X}W^{Y}$, which is as follows

$${}^{X}W^{Y} = \begin{bmatrix} 5 & 3 & 2 & 6 \\ 6 & 5 & 3 & 2 \\ 2 & 6 & 5 & 3 \\ 3 & 2 & 6 & 5 \end{bmatrix} \begin{bmatrix} x^4+x^3+1 & x^4+x^3+x^2 & x^2+1 & x^4+x^3 \\ x^7+x^6 & x^7+x^5 & x^4+x^3+1 & x^2+x \\ x^4+x^2+1 & x^3+x^2+x & x^6+x^4+1 & x+1 \\ x^3+1 & x^2+1 & x^5+x^3+x & x^7+x^6+x^4 \end{bmatrix} \begin{bmatrix} 7 & 6 & 1 & 4 \\ 4 & 7 & 6 & 1 \\ 1 & 4 & 7 & 6 \\ 6 & 1 & 4 & 7 \end{bmatrix}$$

$$= [S_i] \; mod(x^8 + x^4 + x^3 + x + 1) \qquad \text{for} \;\; i = 1, 2, 3, 4.$$

where S_i, represents columns of matrix ${}^{X}W^{Y}$ that are given below[1].

$$S_1 = \begin{bmatrix} x^7+x^4+x^3+x+1 \\ x^6+x^2+x \\ x^7+x^6+x^3+x^2+1 \\ x^5+x^4+x+1 \end{bmatrix}$$

$$S_2 = \begin{bmatrix} x^7+x^5+x^3+1 \\ x^6+x^2+x \\ x^6+x^3+x+1 \\ x^7+x^6+x^4+x^2+1 \end{bmatrix}$$

$$S_3 = \begin{bmatrix} x^7+x^5+x^4+x^2 \\ x^7+x^6+x^5+x^4+1 \\ x^6+x^5+x^3+x^2+x+1 \\ x^6+x^4+x^3 \end{bmatrix}$$

$$S_4 = \begin{bmatrix} x^6+x^4+x \\ x^6+x^2+x \\ x^5+x^4+x^2+x \\ x^6+x^5+x+1 \end{bmatrix}$$

and sends this to second person.

Step 2. Second person chooses two secret circulant matrices at random from $GL(4, \mathbb{Z}_{11})$.

$$U = \begin{bmatrix} 9 & 6 & 7 & 8 \\ 8 & 9 & 6 & 7 \\ 7 & 8 & 9 & 6 \\ 6 & 7 & 8 & 9 \end{bmatrix} \text{ and } V = \begin{bmatrix} 1 & 1 & 5 & 2 \\ 2 & 1 & 1 & 5 \\ 5 & 2 & 1 & 1 \\ 1 & 5 & 2 & 1 \end{bmatrix}$$

[1]We use this representation because matrix is big in size.

to calculate ${}^{U}W^{V}$, which is as follows

$$
{}^{U}W^{V} = \begin{bmatrix} 9 & 6 & 7 & 8 \\ 8 & 9 & 6 & 7 \\ 7 & 8 & 9 & 6 \\ 6 & 7 & 8 & 9 \end{bmatrix} \begin{bmatrix} x^4+x^3+1 & x^4+x^3+x^2 & x^2+1 & x^4+x^3 \\ x^7+x^6 & x^7+x^5 & x^4+x^3+1 & x^2+x \\ x^4+x^2+1 & x^3+x^2+x & x^6+x^4+1 & x+1 \\ x^3+1 & x^2+1 & x^5+x^3+x & x^7+x^6+x^4 \end{bmatrix} \begin{bmatrix} 1 & 1 & 5 & 2 \\ 2 & 1 & 1 & 5 \\ 5 & 2 & 1 & 1 \\ 1 & 5 & 2 & 1 \end{bmatrix}
$$

$$
= [S_i] \mod (x^8+x^4+x^3+x+1) \qquad \text{for } i = 1,2,3,4.
$$

where S_i, represents columns of matrix ${}^{U}W^{V}$ that are given below.

$$
S_1 = \begin{bmatrix} x^6+x^5+x^2+x \\ x^7+x^3+1 \\ x^5+x^3+x^2+1 \\ x^7+x^6+x^5+x^3+x^2+1 \end{bmatrix}
$$

$$
S_2 = \begin{bmatrix} x^7+x^6+x^4+x^2+x \\ x^7+x^6+x^4+x^2 \\ x^4+x+1 \\ x^7+x^6+x^2+1 \end{bmatrix}
$$

$$
S_3 = \begin{bmatrix} x^7+x^6+x^4+x^3+x^2 \\ x^7+x^6+x^5+x^4+x+1 \\ x^7+x^4+x^2+1 \\ x^5+x^4+x \end{bmatrix}
$$

$$
S_4 = \begin{bmatrix} x^7+x^6+x \\ x^6+x^5+x^4+x^2+x \\ x^2+x+1 \\ x^5+x \end{bmatrix}
$$

and sends its to the first person.

Step 3. Secret shared key of first person is same as secret shared key of second person.

$$
\begin{aligned}
K_A &= {}^{X}({}^{U}W^{V})^{Y} = K \\
K_B &= {}^{U}({}^{X}W^{Y})^{V} = K \\
K &= [S_i] \mod (x^8 + x^4 + x^3 + x + 1) \qquad \text{for } i = 1, 2, 3, 4.
\end{aligned}
$$

where S_i, represents columns of matrix K that are given below.

$$
S_1 = \begin{bmatrix} x^4 + x^2 + x \\ x^7 + x^5 + x^4 + x^2 \\ x^5 + x^4 + x^2 + 1 \\ x^6 + x^5 + x^2 \end{bmatrix}
$$

$$
S_2 = \begin{bmatrix} x^5 + x^4 + x^2 + x + 1 \\ x^6 + x^3 + x + 1 \\ x^7 + x^6 + x^4 + x^2 + 1 \\ x^7 + x^6 + x^5 + x^4 + x^3 + x + 1 \end{bmatrix}
$$

$$
S_3 = \begin{bmatrix} x^7 + x^3 + x^2 \\ x^5 + x^3 \\ x^6 + x^5 + x^3 + x^2 + x + 1 \\ x^6 + x^5 + x^4 + x^3 + x \end{bmatrix}
$$

$$
S_4 = \begin{bmatrix} x^5 + x^2 + x \\ x^6 + x^5 + x^3 + x^2 + x \\ x^7 + x^6 + x^4 + x^3 + 1 \\ x^7 + x^6 + x^5 + x^2 + 1 \end{bmatrix}
$$

3.2.1 Computational Cost

The brief inspection of the complexity of our key exchange protocol is as follows: As the traditional methods for multiplication/inversion of matrices defined over Z_{p^q} takes about $\mathcal{O}(n^w q^2 \log^2 p)$ bit operations, whereas for the product of two

square matrices, a well known algorithm requires $\mathcal{O}(n^w)Z_{p^q}$ operations and each Z_{p^q} operation needs $\mathcal{O}(q^2 \log^2 p)$ bit operations. Consider the rank of a $3n^2 \times 2n^2$ coefficient matrix W is t. We have $0 < t \leq 2n^2$ by utilizing the Gaussian elimination method. If $r = 2n^2$, the matrix has rank $N = 0$. So, the complexity of our algorithm is concluded in the following Table 3.1.

Computational cost	Explanation
$\mathcal{O}(2n^2p^q)$	Discrete logarithms of two matrices
$\mathcal{O}(3n^2.(2n^2)^{w-1}q^2 \log^2 p)$	$3n^2$ equations in $2n^2$ variables
$\mathcal{O}(3n^2(2n^2 - r)^{w-1}q^2 \log^2 p)$	A linear combination of solution space
$\mathcal{O}(n^w q^2 \log^2 p)$	one time inversion

Table 3.1: Compuatational cost of Key agreement protocol

Hence, the total bit complexity of our protocol is $\mathcal{O}(n^{2w}q^2 \log^2 p)$.

3.3 Security Analysis

With the advancement of communication technology, there is large increase in data vulnerability due to diffusive attacks.

Idea of using enhanced matrix power function is initiated by Sakalauskas in [22]. We have used the enhanced matrix power function for the construction of our scheme as MPF is a candidate one-way function (OWF), since the effective (polynomial time) inversion algorithm for it is not yet known. By getting the idea and structure of protocol from the said paper we have proposed a key exchange protocol based on enhanced matrix power function using platform of semi-groups. In particular, we have used extended Galois field $GF(n, p^q)$ in base matrices and general linear group $GL(n, \mathbb{Z}_p)$ in its exponents on both sides which results in comp-lex algebraic structure that cannot be attacked easily.

3.3.1 Brute Force Attack

If we choose 60 decimal digits as order of prime p and polynomial with degree greater than 10 in the Galois field $GF(p^q)$, we can acquire a secure protocol, so that the brute force attack will become infeasible. The public and private matrices should have $(2^n - 1)$ form of order, so that it become a Mersenne prime.

3.3.2 Algebraic Attack

Algebraic attack is a cryptanalytic technique based on solution of system by reducing the whole system in the form of equations. If an adversary is observing the protocol he has the knowledge of public parameters (M_L, M_R, A, B, Q), where $A = {}^{X}Q^{Y}$ and $B = {}^{U}Q^{V}$, then he have to search for the pair of secret keys of both the participants, so that he can solve the following equations.

$$A = {}^{X}Q^{Y},$$
$$XM_L = M_L X,$$
$$YM_R = M_R Y.$$

So, If an attacker obtains the matrices $\widetilde{X}$ and $\widetilde{Y}$ that satisfies the given equations then attack is feasible.

Hence, to enhance the security and complexity of discrete log Problem, we present this Key exchange scheme having Galois field $GF(p^q)$ as platform semi-rings and when an adversary wants to attack this protocol by means of this attack, he has to solve complex pattern of algebraic structures powering algebraic structures which is quite impossible to be implemented.

Now we will illustrate the above mentioned attack by mounting it on our Example 3.2.3.

Example 3.3.1 Consider the key exchange protocol presented in Example 3.2.3, the public parameters are

• The base matrix W of order 2 over the Galois field $GF(2^2)$, whose irreducible

polynomial is $m(x) = x^2 + x + 1$.

$$W = \begin{bmatrix} x & 1 \\ x+1 & x+1 \end{bmatrix} \in GF(2, 2^2)$$

• Secret matrices will be over $GL(2, \mathbb{Z}_7)$, that is General linear group of matrices of order 2 and elements will be from $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$.

We want to find the secret matrices X and Y using all the known public information. In order to mount the above stated algebraic attack, we start by assuming the unknown matrices as

$$X = \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} \text{ and } Y = \begin{bmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{bmatrix}.$$

Now if the attacker gets access to or hack ${}^{X}W^{Y}$ given in Example 3.2.3 as

$${}^{X}W^{Y} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \bmod (x^2 + x + 1)$$

Putting X and Y in the above equation, we get

$$\begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} \begin{bmatrix} x & 1 \\ x+1 & x+1 \end{bmatrix} \begin{bmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \bmod (x^2 + x + 1)$$

$$\begin{bmatrix} x^{x_{11}}(x+1)^{x_{12}} & (x+1)^{x_{12}} \\ x^{x_{21}}(x+1)^{x_{22}} & (x+1)^{x_{22}} \end{bmatrix} \begin{bmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \bmod (x^2 + x + 1)$$

$$\begin{bmatrix} x^{x_{11}y_{11}}(x+1)^{x_{12}y_{11}+x_{12}y_{21}} & x^{x_{11}y_{12}}(x+1)^{x_{12}y_{12}+x_{12}y_{22}} \\ x^{x_{21}y_{11}}(x+1)^{x_{22}y_{11}+x_{22}y_{21}} & x^{x_{21}y_{12}}(x+1)^{x_{22}y_{12}+x_{22}y_{22}} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \bmod (x^2 + x + 1)$$

He get the following system of equations,

$$x^{x_{11}y_{11}}(x+1)^{x_{12}y_{11}+x_{12}y_{21}} = 1 \bmod (x^2+x+1)$$
$$x^{x_{11}y_{12}}(x+1)^{x_{12}y_{12}+x_{12}y_{22}} = 1 \bmod (x^2+x+1)$$
$$x^{x_{21}y_{11}}(x+1)^{x_{22}y_{11}+x_{22}y_{21}} = 1 \bmod (x^2+x+1)$$
$$x^{x_{21}y_{12}}(x+1)^{x_{22}y_{12}+x_{22}y_{22}} = 1 \bmod (x^2+x+1)$$

The attacker now has to solve four discrete logrithm problem in $GF(2^2)$. Which is clearly not feasible. If somehow he become able to correctly guess all the exponents, then he will have to find 8 unknowns from 4 equations. Hence the system is undetermined and may give infinitely many solutions and it will be impossible for attacker to obtain the secret session key by mounting the linear algebraic attack.

3.3.3 Man In The Middle Attack (MITM)

As far as simple Key generation scheme is concerned, this is vulnerable to be intercepted from middle, but as we have introduced public key certificate based algorithm where authentication of the keys is required, we can prevent this attack. When both the parties get the authenticated Public key certificated from authorized Certificate authority then no middle man can impersonate and disturb the communication network.
Also we can overcome this attack with the help of digital signature, one can extend this work and apply the digital signatures over the proposed key protocol.

3.3.4 Man At The Ends Attack (MATE)

Man at the end (MATE) attack is unnoticed generally in security analysis by analysts because it is strenous to model, examine and assess typically [66]. There are various versions of MATE attack that depends on the physical framework of compromised device. For a specific person, altering attack can be implemented in which attacker alters the integrity of software [67]. In reverse engineering attack, the adversary trace the entitlement from the device software and then alters

the privacy right of retailor [68]. Likewise, in cloning attack an advarsary may fabricates and publish the duplicate of software by violating the ownership [69]. Sometimes an attacker may attack by making his own codes using the publicly exposed codes to deceit any anti-virus software [70].

Although MATE attacks are difficult to examine and model but there are various techniques to secure our device, like digital asset protection, software protection, hardware protection and hardware based software protection. For additinal consideration on core protection framework against the MATE attack, we refer to [42].

Chapter 4

An Improved Asymmetric Cipher Based on Matrix Power Function

In this chapter, we will review the asymmetric cipher proposed by Sakalauskas, E. and Mihalkovich, A. in [23], named as "New Asymmetric Cipher of Non-Commuting Cryptography Class Based on Matrix Power Function". This cipher corresponds to the category of intensively emerging non-commuting cryptography because of expected resistance to probable quantum cryptanalysis [11]. Furthermore, we have extended this work by proposing a modified version of this scheme by using the platform of Galois Field.

4.1 The Proposed Asymmetric Cipher

To design this public key cryptosystem, authors utilized a finite ring defined on integers $\mathbb{Z}_n = \{0, 1, 2....., n-1\}$ and performed all the calculations under modulo n. All the operations performed here are associative and commuting in general. $\mathbb{Z}_n^*$ is used to denote the multiplication group of integers that are relatively prime to n in $\mathbb{Z}_n$. The order of this group is determined by $\phi(n)$ which is Euler's totient. Also Authors have suggested the matrix power function for constructing this cipher, as matrix power function is a candidate one way function and it fulfills

the conjectures given in chapter 3. As the set $\mathbb{Z}_n^*$ is multiplicative group and we need powering elements, for this authors referred the Carmichael's theorem that sates that for any element $a \in \mathbb{Z}_n^*$, the element a^x has power x from $\mathbb{Z}_{\lambda(n)}$, means $x \in \mathbb{Z}_{\lambda(n)}$ given that $\lambda(n)$ is the Carmichael function. Carmichael function is defined as the smallest positive integer λ, which satisfies the identity $a^\lambda = 1 \bmod n$ for all a co-prime with n. Also $\mathbb{Z}_{\lambda(n)}$ is determined by the value of n.

Remark 4.1.1 According to authors, Alice should choose non singular matrix as her secret power matrix. But in this said article there is the matrix X taken clearly singular as given below, which results in the ambiguity of the solution presented in this paper.

$$X = \begin{bmatrix} 3 & 0 & 3 \\ 3 & 3 & 3 \\ 2 & 3 & 2 \end{bmatrix}, |X| = 0$$

The general scheme as proposed in [23] is explained and computed as follows.

Algorithm 4.1.2 (Proposed Cipher)

Let there be two participants Alice and Bob. The protocol is carried as Bob wants to send coded message M to Alice. He will encrypt that M with the help of Alice's public key, and Alice will decrypt that with the help of her own private key. As we are working in matrices so our proposed M will be in the form of matrix of order m with entries encoded in binary numbers. Also matrices used to obtain key matrix are all non-commuting. The construction is explained below.

Public Parameters:

(i) Let Q be the public base matrix selected randomly from matrix semigroup M_S.

(ii) Let Z_1 and Z_2 be two non-commutative public matrices selected randomly from matrix ring M_R

Alice will now select a non singular secret matrix X in M_R and computes a secret matrix U with the help of secret polynomial P_U chosen at random. Matrix U is computed as $U = P_U(Z_1).P_U(Z_2)$ which is a product of polynomials of Z_1 and Z_2. Alice has a pair of private key $PrK_A = (X, U)$ and her public key contains triplet of matrices $PuK_A = (A_1, A_2, E)$.

where

$$A_1 = XZ_1X^{-1} \tag{4.1}$$

$$A_2 = XZ_2X^{-1} \tag{4.2}$$

$$E = {}^{X}Q^{U} \tag{4.3}$$

Encryption: With the help of Alice's public keys, Bob performs the encryption in the following way.

1. Bob selects a non singular matrix Y at random from M_R.

2. He then computes a secret matrix V with the help of secret polynomial P_V chosen at random. Matrix V is computed as

$$V = P_V(Z_1).P_V(Z_2) \tag{4.4}$$

Also by using Alice's public matrices A_1 and A_2, he computes a matrix W.

$$P_V(A_1).P_V(A_2) = XVX^{-1} = W \tag{4.5}$$

3. He then takes matrix E and raise it to the power matrix $W = XVX^{-1}$ on the left to obtain ${}^{XV}Q^{U}$ as $WX = XV$. Also he use his secret power matrix Y and raise the matrix ${}^{XV}Q^{U}$ by Y on the right and the resulting matrix will be the key matrix K,

$$K = {}^{W}E^{Y} = {}^{XV}Q^{UY} \tag{4.6}$$

which is used for encrypting the message M and the computation of cipher-text C.

4. Now, Bob computes the ciphertext C as $C = K \oplus M$. where $\oplus$ is carried out as bitwise sum modulo 2 of all the corresponding entries of matrices K and M.

For example:

$3 \oplus 10$ means $0011 \oplus 1010$ which is equals to 1001 means 9. So bitwise sum modulo 2 of 3 and 10 is 9.

5. Bob will compute his three public matrices (B_1, B_2, F),

where

$$B_1 = Y^{-1} Z_1 Y,$$

$$B_2 = Y^{-1} Z_2 Y$$

$$F = {}^{V} Q^{Y}$$

and send this to Alice altogether with ciphertext C.

Decryption: With the help of Bob's public keys and her own private keys, Alice performs the decryption in the following way.

1. By using public matrices (B_1, B_2) of Bob, Alice computes

$$Y^{-1}UY = P_U(B_1).P_U(B_2),$$

where $U = P_U(Z_1).P_U(Z_2)$.

2. She then takes the public matrix F of Bob, and raise it to the power matrix X on left and $Y^{-1}UY$ to the right, which results in same matrix as key matrix K.

$$K = {}^{X} F^{Y^{-1}UY} = {}^{XV} Q^{UY} \tag{4.7}$$

3. Alice can decrypt the ciphertext C by using encryption key K as follows.

$$M = K \oplus C = K \oplus K \oplus M. \tag{4.8}$$

Correctness: The correctness of the above mentioned Asymmetric cipher can be identified with the help of following demonstration.

From equation 4.5, we have

$$P_V(A_1).P_V(A_2) = XVX^{-1} = W \tag{4.9}$$

Let us consider a random polynomial $P_V(x) = ax^2 + bx$, by using this polynomial along with equations 4.1, 4.2 in $P_V(A_1)$ and $P_V(A_2)$, we get

$$\begin{aligned}
P_V(A_1) &= P_V(XZ_1X^{-1}) \\
&= a(XZ_1X^{-1})^2 + b(XZ_1X^{-1}) \\
&= a(XZ_1X^{-1}XZ_1X^{-1}) + b(XZ_1X^{-1}) \\
&= a(XZ_1Z_1X^{-1}) + b(XZ_1X^{-1}) \\
&= a(XZ_1^2X^{-1}) + b(XZ_1X^{-1}) \\
&= X(aZ_1^2X^{-1} + bZ_1X^{-1}) \\
&= X(aZ_1^2 + bZ_1)X^{-1} \\
&= XP_V(Z_1)X^{-1} \\
P_V(A_2) &= P_V(XZ_2X^{-1}) \\
&= a(XZ_2X^{-1})^2 + b(XZ_2X^{-1}) \\
&= a(XZ_2X^{-1}XZ_2X^{-1}) + b(XZ_2X^{-1}) \\
&= a(XZ_2Z_2X^{-1}) + b(XZ_2X^{-1}) \\
&= a(XZ_2^2X^{-1}) + b(XZ_2X^{-1}) \\
&= X(aZ_2^2X^{-1} + bZ_2X^{-1}) \\
&= X(aZ_2^2 + bZ_2)X^{-1} \\
&= XP_V(Z_2)X^{-1}
\end{aligned}$$

By putting these values in left hand side of 4.5, we have

$$\begin{aligned}
P_V(A_1).P_V(A_2) &= \{XP_V(Z_1)X^{-1}\}.\{XP_V(Z_2)X^{-1}\} \\
&= XP_V(Z_1)X^{-1}XP_V(Z_2)X^{-1} \\
&= XP_V(Z_1)P_V(Z_2)X^{-1}
\end{aligned}$$

Using equation 4.4 in above equation, we get

$$P_V(A_1).P_V(A_2) = XVX^{-1}$$

Also from 4.5, we have

$$XVX^{-1} = W$$

By multiplying X on L.H.S of the above equation and using cancellation law, we have

$$XVX^{-1}X = WX$$
$$XV = WX$$

Hence this completes the proof.

Remark 4.1.3 To compute the given in example of the article [23], let us consider an illustrative example by taking another random non-singular matrix X and all the other parameters as per article.

$$X = \begin{bmatrix} 3 & 0 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 2 \end{bmatrix}, |X| = 1 \neq 0.$$

Example 4.1.4 Alice and Bob agree on a public platform group defined over

$$S = \mathbb{Z}^*{}_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}.$$

Since $a^4 = 1 \; \forall \; a \in Z^*{}_{15}$ and the power ring is defined over $\mathbb{R} = \mathbb{Z}_4$. Note that all the base matrices are taken from platform group under modulo 15 and all the power matrices are taken from power ring under modulo 4.

Setup: Alice and Bob consent on public matrix Q to be base matrix and two non-commuting matrices Z_1 and Z_2 to be power matrices.

$$Q = \begin{bmatrix} 2 & 7 & 13 \\ 8 & 2 & 7 \\ 13 & 7 & 8 \end{bmatrix}, Z_1 = \begin{bmatrix} 3 & 3 & 1 \\ 3 & 2 & 2 \\ 0 & 0 & 3 \end{bmatrix}, Z_2 = \begin{bmatrix} 3 & 3 & 0 \\ 0 & 1 & 1 \\ 3 & 3 & 3 \end{bmatrix}$$

Let us suppose that Alice's secret non singular power matrix is

$$X = \begin{bmatrix} 3 & 0 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 2 \end{bmatrix}, |X| = 1 \neq 0.$$

Alice choose a secret polynomial $P_U(x) = x^2 + 3x$ and calculates the secret power matrix U as

$$\begin{aligned} U &= P_U(Z_1).P_U(Z_2) \\ &= \begin{bmatrix} 27 & 24 & 15 \\ 24 & 19 & 19 \\ 0 & 0 & 18 \end{bmatrix} \begin{bmatrix} 18 & 21 & 3 \\ 3 & 7 & 7 \\ 27 & 30 & 21 \end{bmatrix} \\ &= \begin{bmatrix} 963 & 1185 & 564 \\ 1002 & 1207 & 604 \\ 486 & 540 & 378 \end{bmatrix} \\ &= \begin{bmatrix} 3 & 1 & 0 \\ 2 & 3 & 0 \\ 2 & 0 & 2 \end{bmatrix} \bmod 4 \end{aligned}$$

She calculates matrix E as

$$
\begin{aligned}
E &= {}^{X}Q^{U} \\
&= \begin{bmatrix} 3 & 0 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 2 \end{bmatrix} \begin{bmatrix} 2 & 7 & 13 \\ 8 & 2 & 7 \\ 13 & 7 & 8 \end{bmatrix} \begin{bmatrix} 3 & 1 & 0 \\ 2 & 3 & 0 \\ 2 & 0 & 2 \end{bmatrix} \\
&= \begin{bmatrix} 11 & 14 & 1 \\ 1 & 14 & 1 \\ 8 & 4 & 4 \end{bmatrix} \bmod 15
\end{aligned}
$$

To compute her public matrices, she has to calculate inverse of X by using $X^{-1} = Adj(X)/det(X)$. Firstly she will find $det(X) = 9 = 1 \bmod 4$, calculates its inverse by using extended euclidean algorithm 2.6.1. As $(1)^{-1} \bmod 4 = 1$ and multiply inverse of $det(X)$ with $Adj(X)$ to get the inverse of X as

$$
X^{-1} = \begin{bmatrix} 0 & 1 & 1 \\ 2 & 0 & 3 \\ 3 & 3 & 3 \end{bmatrix}
$$

Alice public matrices A_1 and A_2 are computed as follows.

$$
\begin{aligned}
A_1 &= XZ_1X^{-1} \\
&= \begin{bmatrix} 3 & 0 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 2 \end{bmatrix} \begin{bmatrix} 3 & 3 & 1 \\ 3 & 2 & 2 \\ 0 & 0 & 3 \end{bmatrix} \begin{bmatrix} 0 & 1 & 1 \\ 2 & 0 & 3 \\ 3 & 3 & 3 \end{bmatrix} \\
&= \begin{bmatrix} 54 & 45 & 72 \\ 55 & 45 & 78 \\ 66 & 57 & 93 \end{bmatrix}
\end{aligned}
$$

$$= \begin{bmatrix} 2 & 1 & 0 \\ 3 & 1 & 2 \\ 2 & 1 & 1 \end{bmatrix} \bmod 4$$

$$A_2 = XZ_2X^{-1}$$

$$= \begin{bmatrix} 3 & 0 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 2 \end{bmatrix} \begin{bmatrix} 3 & 3 & 0 \\ 0 & 1 & 1 \\ 3 & 3 & 3 \end{bmatrix} \begin{bmatrix} 0 & 1 & 1 \\ 2 & 0 & 3 \\ 3 & 3 & 3 \end{bmatrix}$$

$$= \begin{bmatrix} 63 & 45 & 99 \\ 53 & 36 & 84 \\ 57 & 39 & 84 \end{bmatrix}$$

$$= \begin{bmatrix} 3 & 1 & 3 \\ 1 & 0 & 0 \\ 1 & 3 & 0 \end{bmatrix} \bmod 4$$

Alice public key is $PuK_A = (A_1, A_2, E)$ and her private key is $PrK_A = (X, U)$.

Encryption: Let Bob wants to send encrypted message to Alice. Since all the base matrices are taken from $Z*_{15}$ under modulo 15, therefore the elements of message matrix M will be coded under 4 bits. So $M = \{m_{ij}\}$, where $m_{ij} \in Z_{16}$.

$$M = \begin{bmatrix} 10 & 8 & 3 \\ 13 & 2 & 12 \\ 14 & 2 & 3 \end{bmatrix}$$

Bob performs encryption with the help of Alice's public key PuK_A.

He selects his secret non-singular power matrix Y as

$$Y = \begin{bmatrix} 0 & 1 & 3 \\ 1 & 2 & 1 \\ 3 & 0 & 2 \end{bmatrix}$$

Bob choose a secret polynomial $P_V(x) = 2x^2+x$ and calculates the power matrices V and W as

$$\begin{aligned} V &= P_V(Z_1).P_V(Z_2) \\ &= \begin{bmatrix} 39 & 33 & 25 \\ 33 & 28 & 28 \\ 0 & 0 & 21 \end{bmatrix} \begin{bmatrix} 21 & 27 & 6 \\ 6 & 9 & 9 \\ 39 & 45 & 27 \end{bmatrix} \\ &= \begin{bmatrix} 1992 & 2475 & 1206 \\ 1953 & 2403 & 1206 \\ 819 & 945 & 567 \end{bmatrix} \\ &= \begin{bmatrix} 0 & 3 & 2 \\ 1 & 3 & 2 \\ 3 & 1 & 3 \end{bmatrix} \bmod 4 \\ W &= P_V(A_1).P_V(A_2) \\ &= \begin{bmatrix} 16 & 7 & 4 \\ 29 & 13 & 10 \\ 20 & 9 & 7 \end{bmatrix} \begin{bmatrix} 29 & 25 & 21 \\ 7 & 2 & 6 \\ 13 & 5 & 6 \end{bmatrix} \\ &= \begin{bmatrix} 565 & 434 & 402 \\ 1062 & 801 & 747 \\ 734 & 553 & 516 \end{bmatrix} \end{aligned}$$

$$= \begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 3 \\ 2 & 1 & 0 \end{bmatrix} \bmod 4$$

He then calculates key matrix as

$$K = {}^{W}E^{Y} = {}^{XV}Q^{UY}$$

$$= \begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 3 \\ 2 & 1 & 0 \end{bmatrix} \begin{bmatrix} 11 & 14 & 1 \\ 1 & 14 & 1 \\ 8 & 4 & 4 \end{bmatrix} \begin{bmatrix} 0 & 1 & 3 \\ 1 & 2 & 1 \\ 3 & 0 & 2 \end{bmatrix}$$

$$= \begin{bmatrix} 14 & 14 & 1 \\ 14 & 2 & 13 \\ 14 & 1 & 14 \end{bmatrix} \bmod 15$$

Message encrypted in ciphertext as the bit-wise sum modulo 2 of all the corresponding entries of K and M.

$$C = K \oplus M$$

$$= \begin{bmatrix} 14 & 14 & 1 \\ 14 & 2 & 13 \\ 14 & 1 & 14 \end{bmatrix} \oplus \begin{bmatrix} 10 & 8 & 3 \\ 13 & 2 & 12 \\ 14 & 2 & 3 \end{bmatrix}$$

$$= \begin{bmatrix} 4 & 6 & 2 \\ 3 & 0 & 1 \\ 0 & 3 & 13 \end{bmatrix}$$

To compute her public matrices, he has to calculate inverse of Y by using $Y^{-1} = Adj(Y)/det(Y)$. Firstly he will find $det(Y) = -17 = 3 \bmod 4$, calculates its inverse by using extended euclidean algorithm 2.6.1 as $(3)^{-1} \bmod 4 = 3$ and multiply

inverse of $det(Y)$ with $Adj(Y)$ to get the inverse of Y as

$$Y^{-1} = \begin{bmatrix} 0 & 2 & 1 \\ 3 & 1 & 1 \\ 2 & 1 & 1 \end{bmatrix}$$

He calculates his public power matrices (B_1, B_2, F) as follows.

$$\begin{aligned} B_1 &= Y^{-1} Z_1 Y \\ &= \begin{bmatrix} 0 & 2 & 1 \\ 3 & 1 & 1 \\ 2 & 1 & 1 \end{bmatrix} \begin{bmatrix} 3 & 3 & 1 \\ 3 & 2 & 2 \\ 0 & 0 & 3 \end{bmatrix} \begin{bmatrix} 0 & 1 & 3 \\ 1 & 2 & 1 \\ 3 & 0 & 2 \end{bmatrix} \\ &= \begin{bmatrix} 25 & 14 & 36 \\ 35 & 34 & 63 \\ 29 & 25 & 49 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 2 & 0 \\ 3 & 2 & 3 \\ 1 & 1 & 1 \end{bmatrix} \bmod 4 \\ B_2 &= Y^{-1} Z_2 Y \\ &= \begin{bmatrix} 0 & 2 & 1 \\ 3 & 1 & 1 \\ 2 & 1 & 1 \end{bmatrix} \begin{bmatrix} 3 & 3 & 0 \\ 0 & 1 & 1 \\ 3 & 3 & 3 \end{bmatrix} \begin{bmatrix} 0 & 1 & 3 \\ 1 & 2 & 1 \\ 3 & 0 & 2 \end{bmatrix} \\ &= \begin{bmatrix} 20 & 13 & 24 \\ 25 & 38 & 57 \\ 22 & 29 & 45 \end{bmatrix} \end{aligned}$$

$$= \begin{bmatrix} 0 & 1 & 0 \\ 1 & 2 & 1 \\ 2 & 1 & 1 \end{bmatrix} \bmod 4$$

$$F = {}^{V}Q^{Y}$$

$$= \begin{bmatrix} 0 & 3 & 2 \\ 1 & 3 & 2 \\ 3 & 1 & 3 \end{bmatrix} \begin{bmatrix} 2 & 7 & 13 \\ 8 & 2 & 7 \\ 13 & 7 & 8 \end{bmatrix} \begin{bmatrix} 0 & 1 & 3 \\ 1 & 2 & 1 \\ 3 & 0 & 2 \end{bmatrix}$$

$$= \begin{bmatrix} 11 & 2 & 1 \\ 14 & 1 & 14 \\ 1 & 7 & 14 \end{bmatrix} \bmod 15$$

Bob sends his public triplet keys (B_1, B_2, F) along with ciphertext C to Alice.

Decryption: Alice will now decrypt the message in following steps.

Alice will use her secret polynomial $P_U(x)$ and evaluates the power matrix $Y^{-1}UY$.

$$Y^{-1}UY = P_U(B_1).P_U(B_2)$$

$$= \begin{bmatrix} 10 & 12 & 6 \\ 21 & 19 & 18 \\ 8 & 8 & 7 \end{bmatrix} \begin{bmatrix} 1 & 5 & 1 \\ 7 & 12 & 6 \\ 9 & 8 & 5 \end{bmatrix}$$

$$= \begin{bmatrix} 148 & 242 & 112 \\ 316 & 477 & 225 \\ 127 & 192 & 91 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 2 & 0 \\ 0 & 1 & 1 \\ 3 & 0 & 3 \end{bmatrix} \bmod 4$$

Alice calculate the key matrix as

$$K = {}^{X}F^{Y^{-1}UY} = {}^{XV}Q^{UY}$$

$${}^{X}F^{Y^{-1}UY} = \begin{bmatrix} 3 & 0 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 2 \end{bmatrix} \begin{bmatrix} 11 & 2 & 1 \\ 14 & 1 & 14 \\ 1 & 7 & 14 \end{bmatrix} \begin{bmatrix} 0 & 2 & 0 \\ 0 & 1 & 1 \\ 3 & 0 & 3 \end{bmatrix}$$

$$= \begin{bmatrix} 14 & 14 & 1 \\ 14 & 2 & 13 \\ 14 & 1 & 14 \end{bmatrix} \bmod 15$$

Alice will now decrypt the original message M.

$$M = C \oplus K$$

$$= \begin{bmatrix} 4 & 6 & 2 \\ 3 & 0 & 1 \\ 0 & 3 & 13 \end{bmatrix} \oplus \begin{bmatrix} 14 & 14 & 1 \\ 14 & 2 & 13 \\ 14 & 1 & 14 \end{bmatrix}$$

$$= \begin{bmatrix} 10 & 8 & 3 \\ 13 & 2 & 12 \\ 14 & 2 & 3 \end{bmatrix}$$

4.2 An Improved Asymmetric Cipher

In this section, we will propose and explore a new and improved version of the cryptosystem described above. To design the more secure cipher, we have used General linear group of matrices over Galois Field $GF(p^q)$ alongwith the matrix power function. We have chosen our platform group as Galois Field $GF(p^q)$ that engage computational difficulty of the discrete log problem (DLP) and conjugacy

search problem (CSP). The overall scheme is explained with the help of examples. The key generation and the encryption decryption computations are carried out with the help of the computer algebra system ApCoCoA [28].

4.2.1 Suggested Parameters of the Improved Cipher

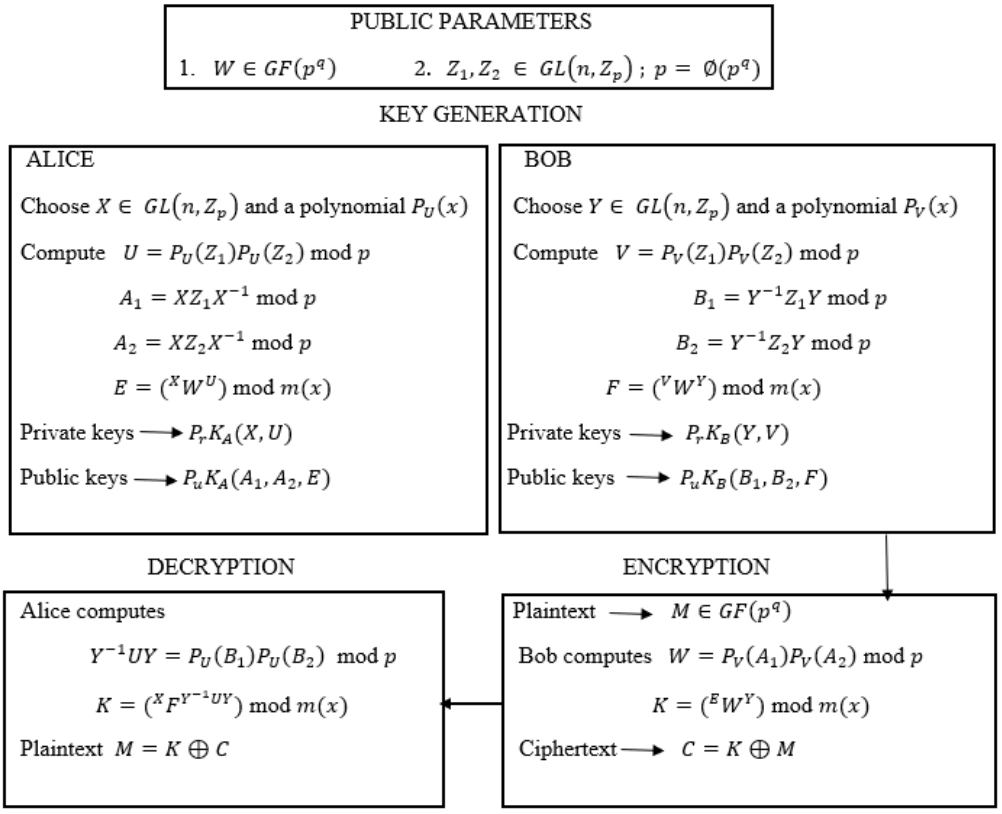

Figure 4.1: Asymmetric Cipher.

The algorithm of asymmetric cipher based on matrix power function is briefed in the above Figure 4.1.

In [23] authors suggested "The use of $GL(n, \mathbb{Z}_p)$ for implementing proposed scheme, where $GL(n, Z_p)$ is general linear group of matrices of order n over the finite field $\mathbb{Z}_p$". To enhance the security of cipher one needs to enlarge the key space, for this reason we have proposed this modification and have enlarge the key space and message space by using $GF(p^q)$ as the extension of $GF(p)$. We have used Galois Field $GF(p^q)$ as our platform and all the base matrices are taken from this

field. All the operations performed here are associative and commuting by default. According to the theme of matrix power function, we have to take power matrices from the matrix ring whose order is the totient of the chosen Galois field's order.

4.2.2 Illustrative Examples

In this subsection, we will explain the modified and improved version of asymmetric cipher based on matrix power function with the help of examples.
Let us consider some examples to demonstrate our proposed scheme.

Example 4.2.1 Alice and Bob agree on a public platform group defined over extended Galois field $GF(2^8)$. As in this field we need an irreducible polynomial to perform addition and multiplication. So let us take $m(x) = (x^8 + x^4 + x^3 + x + 1)$. All the calculation followed in base matrices will be executed under the modulo $(m(x))$. Let us consider the order of matrices will be 2.
Since order of our Galois field is 256 and the power ring should be defined over the totient of the order of Galois field. Hence, powering matrix will be taken from the General linear group $GL(2, \mathbb{Z}_{255})$. Reductions of all the powering matrix will be under mod 255.
Setup: Alice and Bob consent on public matrix Q to be base matrix and two non-commuting matrices Z_1 and Z_2 to be power matrices.

$$Q = \begin{bmatrix} x^6 + x^5 + x^4 & x^3 + x^2 + 1 \\ x^7 + 1 & x^2 + x \end{bmatrix} \in GL(2; GF(2^8)),$$

$$Z_1 = \begin{bmatrix} 175 & 2 \\ 15 & 200 \end{bmatrix} \text{ and } Z_2 = \begin{bmatrix} 213 & 74 \\ 6 & 109 \end{bmatrix} \in GL(2; \mathbb{Z}_{256})$$

Let us suppose that Alice's secret non singular power matrix is

$$X = \begin{bmatrix} 98 & 35 \\ 201 & 161 \end{bmatrix}$$

Alice choose a secret polynomial $P_U(x) = x^2 + 2x$ and calculates the secret power matrix U as

$$\begin{aligned} U &= P_U(Z_1).P_U(Z_2) \\ &= \begin{bmatrix} 31005 & 754 \\ 5655 & 40430 \end{bmatrix} \begin{bmatrix} 46239 & 23976 \\ 1944 & 12543 \end{bmatrix} \\ &= \begin{bmatrix} 141 & 117 \\ 30 & 105 \end{bmatrix} \bmod 255 \end{aligned}$$

She calculates matrix E as

$$\begin{aligned} E &= {}^{X}Q^{U} \\ &= \begin{bmatrix} 98 & 35 \\ 201 & 161 \end{bmatrix} \begin{bmatrix} x^6 + x^5 + x^4 & x^3 + x^2 + 1 \\ x^7 + 1 & x^2 + x \end{bmatrix} \begin{bmatrix} 141 & 117 \\ 30 & 105 \end{bmatrix} \\ &= \begin{bmatrix} x^6 + x^2 & x^7 + x^6 + x^4 + x^3 + x + 1 \\ x^7 + x^4 + x^3 + x^2 & x^7 + x^6 + x^5 + x^4 + x + 1 \end{bmatrix} \bmod (m(x)) \end{aligned}$$

To compute her public matrices, she has to calculate inverse of X by using $X^{-1} = Adj(X)/det(X)$. Firstly she will find $det(X) = 73 \bmod 255$, calculates its inverse by using extended euclidean algorithm 2.6.1. As $(73)^{-1} \bmod 255 = 7$ and multiply inverse of $det(X)$ with $Adj(X)$ to get the inverse of X as

$$X^{-1} = \begin{bmatrix} 107 & 10 \\ 123 & 176 \end{bmatrix}$$

Alice public matrices A_1 and A_2 are computed as follows.

$$\begin{aligned} A_1 &= XZ_1X^{-1} \\ &= \begin{bmatrix} 98 & 35 \\ 201 & 161 \end{bmatrix} \begin{bmatrix} 175 & 2 \\ 15 & 200 \end{bmatrix} \begin{bmatrix} 107 & 10 \\ 123 & 176 \end{bmatrix} \end{aligned}$$

$$= \begin{bmatrix} 148 & 201 \\ 186 & 227 \end{bmatrix} \bmod 255$$

$$A_2 = XZ_2X^{-1}$$

$$= \begin{bmatrix} 98 & 35 \\ 201 & 161 \end{bmatrix} \begin{bmatrix} 213 & 74 \\ 6 & 109 \end{bmatrix} \begin{bmatrix} 107 & 10 \\ 123 & 176 \end{bmatrix}$$

$$= \begin{bmatrix} 54 & 57 \\ 87 & 13 \end{bmatrix} \bmod 255$$

Alice's public keys are $PuK_A = (A_1, A_2, E)$ and her private keys are $PrK_A = (X, U)$.

Encryption: Let Bob wants to send encrypted message to Alice. Since all the base matrices are taken from $GF(2^8)$ under modulo $m(x) = (x^8 + x^4 + x^3 + x + 1)$, therefore the elements of message matrix M will be coded under 8 bits. So $M = \{m_{ij}\}$, where $m_{ij} \in GL(2, 2^8)$.

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

Bob performs encryption with the help of Alice's public key PuK_A.

He selects his secret non-singular power matrix Y as

$$Y = \begin{bmatrix} 117 & 223 \\ 97 & 121 \end{bmatrix}$$

Bob choose a secret polynomial $P_V(x) = 3x^2 + x$ and calculates the power matrices V and W as

$$V = P_V(Z_1).P_V(Z_2)$$

$$= \begin{bmatrix} 92140 & 2252 \\ 16890 & 120290 \end{bmatrix} \begin{bmatrix} 137652 & 71558 \\ 5802 & 37084 \end{bmatrix}$$

$$= \begin{bmatrix} 159 & 73 \\ 0 & 65 \end{bmatrix} \bmod 255$$

$$W = P_V(A_1).P_V(A_2)$$

$$= \begin{bmatrix} 178018 & 226326 \\ 209436 & 266972 \end{bmatrix} \begin{bmatrix} 23679 & 11514 \\ 17574 & 15397 \end{bmatrix}$$

$$= \begin{bmatrix} 111 & 234 \\ 162 & 113 \end{bmatrix} \bmod 255$$

He then calculates key matrix as

$$K = {}^{W}E^{Y} = {}^{XV}Q^{UY}$$

$$K = \begin{bmatrix} 111 & 234 \\ 162 & 113 \end{bmatrix} \begin{bmatrix} x^6 + x^2 & x^7 + x^6 + x^4 + x^3 + x + 1 \\ x^7 + x^4 + x^3 + x^2 & x^7 + x^6 + x^5 + x^4 + x + 1 \end{bmatrix} \begin{bmatrix} 117 & 223 \\ 97 & 121 \end{bmatrix}$$

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

Message encrypted in ciphertext as the bit-wise sum modulo 2 of all the corresponding entries of K and M.

$$C = K \oplus M$$

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

$$= \begin{bmatrix} 10101110 & 01100110 \\ 10100011 & 01000000 \end{bmatrix} \oplus \begin{bmatrix} 00100101 & 00011010 \\ 11000000 & 11000100 \end{bmatrix}$$

$$= \begin{bmatrix} 10001011 & 01111100 \\ 01100011 & 10000100 \end{bmatrix}$$

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

To compute his public matrices, he has to calculate inverse of Y by using $Y^{-1} = Adj(Y)/det(Y)$. Firstly he will find $det(Y) = 176 \bmod 255$, calculates its inverse by using extended euclidean algorithm 2.6.1 as $(176)^{-1} \bmod 255 = 71$ and multiply inverse of $det(Y)$ with $Adj(Y)$ to get the inverse of Y as

$$Y^{-1} = \begin{bmatrix} 176 & 232 \\ 253 & 147 \end{bmatrix}$$

He calculates his public power matrices (B_1, B_2, F) as follows.

$$B_1 = Y^{-1} Z_1 Y$$

$$= \begin{bmatrix} 176 & 232 \\ 253 & 147 \end{bmatrix} \begin{bmatrix} 175 & 2 \\ 15 & 200 \end{bmatrix} \begin{bmatrix} 117 & 223 \\ 97 & 121 \end{bmatrix}$$

$$= \begin{bmatrix} 144 & 122 \\ 32 & 231 \end{bmatrix} \bmod 255$$

$$B_2 = Y^{-1} Z_2 Y$$

$$= \begin{bmatrix} 176 & 232 \\ 253 & 147 \end{bmatrix} \begin{bmatrix} 213 & 74 \\ 6 & 109 \end{bmatrix} \begin{bmatrix} 117 & 223 \\ 97 & 121 \end{bmatrix}$$

$$= \begin{bmatrix} 164 & 92 \\ 242 & 158 \end{bmatrix} \bmod 255$$

$$F = {}^{V}Q^{Y}$$

$$= \begin{bmatrix} 159 & 73 \\ 0 & 65 \end{bmatrix} \begin{bmatrix} x^6+x^5+x^4 & x^3+x^2+1 \\ x^7+1 & x^2+x \end{bmatrix} \begin{bmatrix} 117 & 223 \\ 97 & 121 \end{bmatrix}$$

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

Bob sends his public triplet keys (B_1, B_2, F) along with ciphertext C to Alice.

Decryption: Alice will now decrypt the message in following steps.

Alice will use her secret polynomial $P_U(x)$ and evaluates the power matrix $Y^{-1}UY$.

$$Y^{-1}UY = P_U(B_1).P_U(B_2)$$

$$= \begin{bmatrix} 24928 & 45994 \\ 12064 & 57727 \end{bmatrix} \begin{bmatrix} 49488 & 29808 \\ 78408 & 47544 \end{bmatrix}$$

$$= \begin{bmatrix} 246 & 150 \\ 93 & 0 \end{bmatrix} \bmod 255$$

Alice calculate the key matrix K and decrypts the original message M as,

$$K = {}^{X}F^{Y^{-1}UY} = {}^{XV}Q^{UY}$$

$${}^{X}F^{Y^{-1}UY} = \begin{bmatrix} 98 & 35 \\ 201 & 161 \end{bmatrix} \begin{bmatrix} x^7+x^5+x^4+x & x^5+x^3+1 \\ x^7+x^5+x^4+x^3+x^2+1 & x^6+x^5+x^2+x \end{bmatrix} \begin{bmatrix} 246 & 150 \\ 93 & 0 \end{bmatrix}$$

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

$$M = C \oplus K$$

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

$$= \begin{bmatrix} 10001011 & 01111100 \\ 01100011 & 10000100 \end{bmatrix} \oplus \begin{bmatrix} 10101110 & 01100110 \\ 10100011 & 01000000 \end{bmatrix}$$

$$= \begin{bmatrix} 00100101 & 00011010 \\ 11000000 & 11000100 \end{bmatrix}$$

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

Hence, the obtained mesaage is same as sended by the Bob.

Example 4.2.2 Let us take another example of the given scheme using matrices of order 3. Two participants, let us say A and B agree on a public platform group defined over extended galois field $GF(2^3)$. As in this field we need an irreducible polynomial to perform addition and multiplication. So let us take $m(x) = (x^3+x+1)$. All the calculation followed in base matrices will be executed under the modulo $(m(x))$. Let us consider the order of matrices will be 3.
Since order of our Galois field is 8 and the power ring should be defined over the totient of the order of Galois field. Hence, powering matrix will be taken from the General linear group $GL(3, GF(2^3))$. Reductions of all the powering matrix will be under mod 7.

Setup: Both the participants A and B consent on public matrix Q to be base matrix and two non-commuting matrices Z_1 and Z_2 to be power matrices.

$$Q = \begin{bmatrix} x^2+1 & x & 1 \\ x^2+x & x+1 & x^2 \\ x & x^2+x+1 & 1 \end{bmatrix} \in GL(3; GF(2^3),$$

$$Z_1 = \begin{bmatrix} 5 & 2 & 3 \\ 4 & 4 & 5 \\ 1 & 0 & 2 \end{bmatrix} \text{ and } Z_2 = \begin{bmatrix} 2 & 1 & 6 \\ 6 & 5 & 4 \\ 3 & 2 & 1 \end{bmatrix} \in GL(3; \mathbb{Z}_7)$$

Let us suppose that A's secret non singular power matrix is

$$X = \begin{bmatrix} 2 & 4 & 0 \\ 5 & 1 & 2 \\ 2 & 6 & 3 \end{bmatrix}$$

A choose a secret polynomial $P_U(x) = 2x^2 + x$ and calculates the secret power matrix U as

$$\begin{aligned} U &= P_U(Z_1).P_U(Z_2) \\ &= \begin{bmatrix} 77 & 38 & 65 \\ 86 & 52 & 89 \\ 15 & 4 & 16 \end{bmatrix} \begin{bmatrix} 58 & 39 & 50 \\ 114 & 83 & 124 \\ 45 & 32 & 55 \end{bmatrix} \\ &= \begin{bmatrix} 5 & 5 & 6 \\ 4 & 4 & 5 \\ 2 & 1 & 5 \end{bmatrix} \bmod 7 \end{aligned}$$

She calculates matrix E as

$$\begin{aligned} E &= {}^{X}Q^{U} \\ &= \begin{bmatrix} 2 & 4 & 0 \\ 5 & 1 & 2 \\ 2 & 6 & 3 \end{bmatrix} \begin{bmatrix} x^2+1 & x & 1 \\ x^2+x & x+1 & x^2 \\ x & x^2+x+1 & 1 \end{bmatrix} \begin{bmatrix} 5 & 5 & 6 \\ 4 & 4 & 5 \\ 2 & 1 & 5 \end{bmatrix} \\ &= \begin{bmatrix} x^2 & x & x^2+x+1 \\ x^2+x & x^2 & x \\ x^2 & x^2+x & 1 \end{bmatrix} \bmod (m(x)) \end{aligned}$$

To compute her public matrices, she has to calculate inverse of X by using $X^{-1} = Adj(X)/det(X)$.

Firstly she will find $det(X) = 1 \bmod 7$, calculates its inverse by using extended euclidean algorithm 2.6.1. As $(1)^{-1} \bmod 7 = 1$ and multiply inverse of $det(X)$ with $Adj(X)$ to get the inverse of X as

$$X^{-1} = \begin{bmatrix} 5 & 2 & 1 \\ 3 & 6 & 3 \\ 0 & 3 & 3 \end{bmatrix}$$

A's public matrices A_1 and A_2 are computed as follows.

$$\begin{aligned} A_1 &= XZ_1X^{-1} \\ &= \begin{bmatrix} 2 & 4 & 0 \\ 5 & 1 & 2 \\ 2 & 6 & 3 \end{bmatrix} \begin{bmatrix} 5 & 2 & 3 \\ 4 & 4 & 5 \\ 1 & 0 & 2 \end{bmatrix} \begin{bmatrix} 5 & 2 & 1 \\ 3 & 6 & 3 \\ 0 & 3 & 3 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 5 & 3 \\ 1 & 1 & 5 \\ 3 & 4 & 2 \end{bmatrix} \bmod 7 \\ A_2 &= XZ_2X^{-1} \\ &= \begin{bmatrix} 2 & 4 & 0 \\ 5 & 1 & 2 \\ 2 & 6 & 3 \end{bmatrix} \begin{bmatrix} 2 & 1 & 6 \\ 6 & 5 & 4 \\ 3 & 2 & 1 \end{bmatrix} \begin{bmatrix} 5 & 2 & 1 \\ 3 & 6 & 3 \\ 0 & 3 & 3 \end{bmatrix} \\ &= \begin{bmatrix} 3 & 6 & 3 \\ 5 & 5 & 4 \\ 2 & 2 & 0 \end{bmatrix} \bmod 7 \end{aligned}$$

A's public keys are $PuK_A = (A_1, A_2, E)$ and her private keys are $PrK_A = (X, U)$.

Encryption: Let B wants to send encrypted message to A. Since all the base matrices are taken from $GF(2^3)$ under modulo $m(x) = (x^3 + x + 1)$, therefore the

elements of message matrix M will be coded under 3 bits. So $M = \{m_{ij}\}$, where $m_{ij} \in GL(3, 2^3)$.

$$M = \begin{bmatrix} x+1 & x^2+1 & x \\ x^2+x+1 & x^2+x & x^2 \\ 1 & x & x^2+x+1 \end{bmatrix}$$

B performs encryption with the help of A's public key PuK_A.
He selects his secret non-singular power matrix Y as

$$Y = \begin{bmatrix} 6 & 1 & 4 \\ 2 & 2 & 5 \\ 3 & 4 & 3 \end{bmatrix}$$

B choose a secret polynomial $P_V(x) = 3x^2 + 2x$ and calculates the power matrices V and W as

$$\begin{aligned} V &= P_V(Z_1).P_V(Z_2) \\ &= \begin{bmatrix} 118 & 58 & 99 \\ 131 & 80 & 136 \\ 23 & 6 & 25 \end{bmatrix} \begin{bmatrix} 88 & 59 & 78 \\ 174 & 127 & 188 \\ 69 & 49 & 83 \end{bmatrix} \\ &= \begin{bmatrix} 0 & 6 & 3 \\ 0 & 4 & 6 \\ 5 & 5 & 6 \end{bmatrix} \bmod 7 \\ W &= P_V(A_1).P_V(A_2) \\ &= \begin{bmatrix} 47 & 76 & 108 \\ 53 & 80 & 64 \\ 45 & 89 & 103 \end{bmatrix} \cdot \begin{bmatrix} 141 & 174 & 105 \\ 154 & 199 & 113 \\ 52 & 70 & 42 \end{bmatrix} \end{aligned}$$

$$= \begin{bmatrix} 0 & 6 & 6 \\ 0 & 5 & 3 \\ 4 & 5 & 5 \end{bmatrix} \bmod 7$$

He then calculates key matrix as

$$K = {}^{W}E^{Y} = {}^{XV}Q^{UY}$$

$$K = \begin{bmatrix} 0 & 6 & 6 \\ 0 & 5 & 3 \\ 4 & 5 & 5 \end{bmatrix} \begin{bmatrix} x^2 & x & x^2+x+1 \\ x^2+x & x^2 & x \\ x^2 & x^2+x & 1 \end{bmatrix} \begin{bmatrix} 6 & 1 & 4 \\ 2 & 2 & 5 \\ 3 & 4 & 3 \end{bmatrix}$$

$$= \begin{bmatrix} x^2+x+1 & x^2+1 & x^2+1 \\ x^2+x+1 & x^2+1 & x^2+x+1 \\ 1 & x+1 & x^2+x+1 \end{bmatrix} \bmod (m(x))$$

Message encrypted in ciphertext as the bit-wise sum modulo 2 of all the corresponding entries of K and M.

$$C = K \oplus M$$

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

$$= \begin{bmatrix} 111 & 101 & 101 \\ 111 & 101 & 111 \\ 001 & 011 & 111 \end{bmatrix} \oplus \begin{bmatrix} 011 & 101 & 010 \\ 111 & 110 & 100 \\ 001 & 010 & 111 \end{bmatrix}$$

$$= \begin{bmatrix} 100 & 000 & 111 \\ 000 & 011 & 011 \\ 000 & 001 & 000 \end{bmatrix}$$

$$= \begin{bmatrix} x^2 & 0 & x^2+x+1 \\ 0 & x+1 & x+1 \\ 0 & 1 & 0 \end{bmatrix}$$

To compute her public matrices, he has to calculate inverse of Y by using $Y^{-1} = Adj(Y)/det(Y)$. Firstly he will find $det(Y) = 3 \bmod 7$, calculates its inverse by using extended euclidean algorithm 2.6.1 as $(3)^{-1} \bmod 7 = 5$ and multiply inverse of $det(Y)$ with $Adj(Y)$ to get the inverse of Y as

$$Y^{-1} = \begin{bmatrix} 0 & 2 & 6 \\ 3 & 2 & 2 \\ 3 & 0 & 1 \end{bmatrix}$$

He calculates his public power matrices (B_1, B_2, F) as follows.

$$B_1 = Y^{-1} Z_1 Y$$

$$= \begin{bmatrix} 0 & 2 & 6 \\ 3 & 2 & 2 \\ 3 & 0 & 1 \end{bmatrix} \begin{bmatrix} 5 & 2 & 3 \\ 4 & 4 & 5 \\ 1 & 0 & 2 \end{bmatrix} \begin{bmatrix} 6 & 1 & 4 \\ 2 & 2 & 5 \\ 3 & 4 & 3 \end{bmatrix}$$

$$= \begin{bmatrix} 5 & 6 & 1 \\ 2 & 5 & 1 \\ 1 & 2 & 1 \end{bmatrix} \bmod 7$$

$$B_2 = Y^{-1} Z_2 Y$$

$$= \begin{bmatrix} 0 & 2 & 6 \\ 3 & 2 & 2 \\ 3 & 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 1 & 6 \\ 6 & 5 & 4 \\ 3 & 2 & 1 \end{bmatrix} \begin{bmatrix} 6 & 1 & 4 \\ 2 & 2 & 5 \\ 3 & 4 & 3 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 4 & 6 \\ 3 & 2 & 6 \\ 2 & 4 & 6 \end{bmatrix} \bmod 7$$

$$F = {}^{V}Q^{Y}$$

$$= \begin{bmatrix} 0 & 6 & 3 \\ 0 & 4 & 6 \\ 5 & 5 & 6 \end{bmatrix} \begin{bmatrix} x^2+1 & x & 1 \\ x^2+x & x+1 & x^2 \\ x & x^2+x+1 & 1 \end{bmatrix} \begin{bmatrix} 6 & 1 & 4 \\ 2 & 2 & 5 \\ 3 & 4 & 3 \end{bmatrix}$$

$$= \begin{bmatrix} x^2+x+1 & x & x \\ x^2 & x^2+x+1 & 1 \\ x^2+x & 1 & 1 \end{bmatrix} \bmod (m(x))$$

B sends his public triplet keys (B_1, B_2, F) along with ciphertext C to A.

Decryption: A will now decrypt the message in following steps. A will use her secret polynomial $P_U(x)$ and evaluates the power matrix $Y^{-1}UY$.

$$Y^{-1}UY = P_U(B_1).P_U(B_2)$$

$$= \begin{bmatrix} 81 & 130 & 25 \\ 44 & 83 & 17 \\ 21 & 38 & 9 \end{bmatrix} \begin{bmatrix} 48 & 68 & 126 \\ 39 & 82 & 138 \\ 50 & 84 & 150 \end{bmatrix}$$

$$= \begin{bmatrix} 2 & 5 & 4 \\ 4 & 5 & 5 \\ 0 & 1 & 0 \end{bmatrix} \bmod 7$$

A calculate the key matrix as

$$K = {}^{X}F^{Y^{-1}UY} = {}^{XV}Q^{UY}$$

$${}^{X}F^{Y^{-1}UY} = \begin{bmatrix} 2 & 4 & 0 \\ 5 & 1 & 2 \\ 2 & 6 & 3 \end{bmatrix} \begin{bmatrix} x^2+x+1 & x & x \\ x^2 & x^2+x+1 & 1 \\ x^2+x & 1 & 1 \end{bmatrix} \begin{bmatrix} 2 & 5 & 4 \\ 4 & 5 & 5 \\ 0 & 1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} x^2+x+1 & x^2+1 & x^2+1 \\ x^2+x+1 & x^2+1 & x^2+x+1 \\ 1 & x+1 & x^2+x+1 \end{bmatrix} \bmod (m(x))$$

A will now decrypt the original message M.

$$M = C \oplus K$$

$$= \begin{bmatrix} x^2 & 0 & x^2+x+1 \\ 0 & x+1 & x+1 \\ 0 & 1 & 0 \end{bmatrix} \oplus \begin{bmatrix} x^2+x+1 & x^2+1 & x^2+1 \\ x^2+x+1 & x^2+1 & x^2+x+1 \\ 1 & x+1 & x^2+x+1 \end{bmatrix}$$

$$= \begin{bmatrix} 100 & 000 & 111 \\ 000 & 011 & 011 \\ 000 & 001 & 000 \end{bmatrix} \oplus \begin{bmatrix} 111 & 101 & 101 \\ 111 & 101 & 111 \\ 001 & 011 & 111 \end{bmatrix}$$

$$= \begin{bmatrix} 011 & 101 & 010 \\ 111 & 110 & 100 \\ 001 & 010 & 111 \end{bmatrix}$$

$$= \begin{bmatrix} x+1 & x^2+1 & x \\ x^2+x+1 & x^2+x & x^2 \\ 1 & x & x^2+x+1 \end{bmatrix}$$

4.3 Security Analysis

In this section, we are going to present the security analysis of the our proposed modified work. Our research presents the platform semi-groups with particular Galois fields $GF(p^q)$ in base matrices. Due to high level of security and large

key space, Galois fields are incorporated in this scheme, an attacker must have to search this wide space to attempt for brute force attack. We have used the matrix power function for the construction of our cipher as MPF is a candidate one-way function (OWF), since the effective (polynomial-time) inversion algorithm for it is not yet known.

4.3.1 Algebraic Attack

Algebraic attack is a cryptanalytic technique based on solution of system by reducing the whole system in the form of equations. In the author's proposed scheme [23], if an attacker find the matrices $\widetilde{X}, \widetilde{Y}$ and $\widetilde{U}$ which satisfies the given equations, then the proposed cipher of non-commuting cryptography based on matrix power function can be compromised.

$$\begin{aligned} XAX^{-1} &= B, \\ Y^{-1}AY &= D, \\ {}^{X}Q^{U} &= E, \\ U &= \sum_{i=0}^{n-1} a_i A^i. \end{aligned}$$

So to enhance the security and complexity of discrete log Problem, we present this modified form. As in this work, our basic platform is Galois field $GF(p^q)$ and to search for this big space and solve the decomposition problem, algebraic attack will be in feasible.

4.3.2 Brute Force Attack

If we choose 60 decimal digits as order of prime p and polynomial with degree greater than 10 in the Galois field $GF(p^q)$, we can acquire a secure protocol, so that the brute force attack will become in-feasible. The public and private matrices should have $2^n - 1$ form of order, so that it become a Mersenne prime.

4.3.3 Known Plaintext Attack

In this kind of attack, attacker has the apprehension of some of the ciphertext as well as its corresponding plaintext. On this basis, he attempts to recover the key or makes a logical algorithm to decode any further ciphertexts. Let us assume that attacker has the knowledge of some previous communication and has the pair (M_y, C_y) of corresponding plaintext M_y and ciphertext C_y. Using this information he wants to reveal the secret communication key, to further discover the next secret session having the corresponding plaintext M_{y+1} and ciphertext (M_{y+1}, C_{y+1}). In our scheme, Firstly attacker will try to find the unknown matrices XV and UY, when Q is given publicly, to reveal the key $K = {}^{XV}Q^{UY}$. This kind of attack is infeasible on our scheme as it provides the following features.

i. X and Y are randomly generated matrices of both the participants, by changing these key will get effected.

ii. For every communication session key will be different.

iii. Calculation of U and V is based on randomly generated polynomials of both the participants. Every time polynomial change it will effect the key.

So, for every session key keeps on changing, this feature provides the security against known plaintext attack as the adversary cannot get his hands on new key on the basis of previous keys.
Let us consider an example to see how known plaintext attack can be mounted on Example 4.2.1 by an attacker.

Example 4.3.1 Suppose an attacker has the knowledge of some previous set of plaintext and corresponding ciphertext (M_1, C_1) and he wants to find the secret key K to reveal the further secret session. In Example 4.2.1, public matrices of Alice are $PuK_A = (A_1, A_2, E)$ and public matrices of Bob are $PuK_B = (B_1, B_2, F)$, while secret matrices of Alice are $PrK_A = (X, U)$ and secret matrices of Bob are $PrK_B = (Y, V)$. Also there are secret polynomials used by both the parties to generate their secret matrices.

To find key $K = {}^{XV}Q^{UY}$, an attacker needs X, Y, U and V, but as in our scheme X and Y are randomly generated and U and V are are also random because they are generated with the help of random polynomial. So, every session key will change for every randomly generated secret matrices. Hence, attacker will be unable to find the next session key on the basis of prior knowledge of plaintext and ciphertext.

4.3.4 Chosen Ciphertext Attack

Recall that an attacker can choose any ciphertext $C^{'}$ and can have its corresponding plaintext $M^{'}$. In equation, $C^{'} = K \oplus M^{'}$ the attacker substitutes $C^{'}$ and $M^{'}$ and gets the corresponding key K by solving it. Let us assume that attacker mounts this attack on the proposed scheme and he gets successful in his attempt. But in the proposed scheme, this attack is infeasible as key K gets changed whenever the encryption algorithm gets changed while encrypting a specified message M. So if he gets a hold on a specific key K, he will not be able to decrypt further messages.

4.4 Conclusion

In this thesis, we have reviewed an article as well as proposed a new key generation algorithm for asymmetric key encryption by using in particular, extended Galois Field $GF(p^q)$.

Firstly, we proposed a new key exchange protocol that utilize matrices over $\mathbb{Z}_p$ and $GF(p^q)$. We have used enhanced matrix power function to create this scheme by introducing group of matrices over $\mathbb{Z}_p$ with group of matrices over extended Galois field $GF(p^q)$ that ensures large key space. Secondly, we review the research paper "New Asymmetric Cipher of Non-Commuting Cryptography Class Based on Matrix Power Function" [23] that utilize enhanced matrix power function. In non-commuting cryptography, this proposed cipher has an effective recognition in restricted computational environments. On the basis of this review, we have proposed a modifiedand improved version of the asymmetric cipher based on matrix power function accompanied with extended Galois field $GF(p^q)$.

For the implementations, we have generated codes by employing platform of computer algebra system ApCoCoA [28]. We gave illustrative examples of our proposed protocol and aysmmetric cipher by employing extended Galois field. One can extend our proposed work by using some other non-commutative algebraic structure. Also as a further work, one can also try implementations of our schemes using some other platform groups.

Appendix A

ApCoCoA Codes for Cryptographic Primitive Construction Based on Enhanced Matrix Power Function

This Appendix contains ApCoCoA Codes for Cryptographic primitive construction based on enhanced matrix power function.
The calculation of **LMPF(A,B)**, **RMPF(A,B)**, **GFP(P,Q)**, **ModInv**, **PolyMod**, **PolyInvM**, **MatGF** is performed in computer algebra system ApCoCoA.

A.1 Left Sided Matrix Power Function

Following program computes left matrix power function ${}^{B}A$. where input matrices are always square matrices.

```
Define LMPF(A,B)
Prod:=1;
Rows:=NumRows(A);Cols:=NumCols(A);
C:=NewMat(Rows,Cols,1);
```

```
For K:=1 To Rows Do
For J:=1 To Rows Do
For I:=1 To Rows Do
Prod:=Prod*A[I][J]^B[K][I];
EndFor;
C[K][J]:=Prod;
Prod:=1;
EndFor;
EndFor;

Return C;
EndDefine;
```

A.2 Right Sided Matrix Power Function

Following program computes right matrix power function A^B. where input matrices are always square matrices.

```
Define RMPF(A,B)
Prod:=1;
Rows:=NumRows(A);Cols:=NumCols(A);
C:=NewMat(Rows,Cols,1);

For K:=1 To Rows Do
For J:=1 To Rows Do
For I:=1 To Rows Do
Prod:=Prod*A[K][I]^B[I][J];
EndFor;
C[K][J]:=Prod;
Prod:=1;
EndFor;
```

```
EndFor;


Return C;
EndDefine;
```

A.3 Elements of Extended Galois Field

GFP(P,Q) calculate the elements of galois field. The inputs are P, Q where P is the prime number and Q is any positive integer.

```
Define GFP(P,Q);
Re:=[];
For A:= 0 To P-1 Do
GF:=Poly(A);
Append(Re,GF);
EndFor;
GF1:=Re;
GF2:=Re;
For A:= 1 To Q-1 Do
For J:=1 To P-1 Do
Foreach P In GF1 Do
F:=J*x^A+P;
Append(GF2,F);
EndForeach;
EndFor;
GF1:=GF2;
EndFor;
Return GF2;
EndDefine;
```

A.4 Modular Inverses

ModInv calculate the inverse of a number under the mod . It require the input Q, M where Q is number and M is mod . This function uses the extended euclidean inverse algorithm.

```
Define ModInv(Q,M);
A1:=1;A2:=0;A3:=M;
B1:=0;B2:=1;B3:=Q;
While B3<0 Do
B3:=B3+M;
EndWhile;
While B3<>1 Do
Q:=Div(A3,B3);
--If Q=0 Then Error(" Q is 0");EndIf;
T1:=A1-Q*B1;T2:=A2-Q*B2;T3:=A3-Q*B3;
A1:=B1;A2:=B2;A3:=B3;
B1:=T1;B2:=T2;B3:=T3;
If B2<0 Then B2:=B2+M; EndIf;
If B3=1  Then Return B2;EndIf;
If B3=0 Then Return("Not Invertible!"); EndIf;
EndWhile;
--If B2<0 Then B2:=B2+M; EndIf;
Return B2;
EndDefine;
```

A.5 Polynomial Modulo

PolyMod gives the polynomial F that is reduced on some polynomial mod M.

```
Define PolyMod(F,M)
If Type(F)=RATFUN Then
If Mod(Den(LC(F.Num)),M)=0 Then
```

```
D:=Den(LC(F.Num));
D2:=D*F.Den-D*LPP(F.Den);
If D2= 0 Then Error("Zero Denominator . . .");EndIf;
F:=D*F.Num/(D2);
Return PolyMod(F,M);
EndIf;
CoefNum:=Coefficients(F.Num);CoefDen:=Coefficients(F.Den);
For I:= 1 To Len(CoefNum) Do
If Type(CoefNum[I])=RAT Then
CoefNum[I]:=Mod(CoefNum[I].Num*ModInv(CoefNum[I].Den,M),M);
Else
CoefNum[I]:=Mod(CoefNum[I],M);
EndIf;
EndFor;
For I:= 1 To Len(CoefDen) Do
If Type(CoefDen[I])=RAT Then
CoefDen[I]:=Mod(CoefDen[I].Num*ModInv(CoefDen[I].Den,M),M);
Else
CoefDen[I]:=Mod(CoefDen[I],M);
EndIf;
EndFor;
NewNum:=ScalarProduct(CoefNum,Support(F.Num));
NewDen:=ScalarProduct(CoefDen,Support(F.Den));
If NewDen= 0 Then Error("Zero Denominator . . .");EndIf;
Return NewNum/NewDen;
EndIf;
Coef:=Coefficients(F);
For I:= 1 To Len(Coef) Do
If Type(Coef[I])=RAT Then
Coef[I]:=Mod(Coef[I].Num*ModInv(Coef[I].Den,M),M);
Else
Coef[I]:=Mod(Coef[I],M);
EndIf;
```

```
EndFor;
Return ScalarProduct(Coef,Support(F));
EndDefine;
```

A.6 Polynomial Inverse Modulo

PolyInvM Input F polynomial M mod polynomial and Md is Mod in number. This function calculates inverse of polynomial F on polynomial M under mod Md using Extended Euclidean Inverse algorithm.

```
Define PolyInvM(F,M,Md)
F:=NR(F,[M]);
If MakeSet(Log(F))=[0] Then Return ModInv(LC(F),Md); EndIf;
A1:=1;A2:=0;A3:=PolyMod(M,Md);
B1:=0;B2:=1;B3:=PolyMod(F,Md);
While MakeSet(Log(B3))<>[0] Do
D:=DivAlg(A3,[B3]);
Q:=D.Quotients[1];
Coef:=Coefficients(Q);
For I:= 1 To Len(Coef) Do
C:=Coef[I];
Coef[I]:=Mod(C.Num*ModInv(C.Den,Md),Md);
EndFor;
Q:= ScalarProduct(Coef,Support(Q));
If Q=0 Then Error(" Q is 0");EndIf;
T1:=PolyMod(A1-Q*B1,Md);
T2:=PolyMod(A2-Q*B2,Md);
T3:=PolyMod(A3-Q*B3,Md);
A1:=B1;A2:=B2;A3:=B3;
B1:=T1;B2:=T2;B3:=T3;
If B3=1  Then
Return PolyMod(B2,Md);
```

```
EndIf;
EndWhile;
If B3<>1 Then
Return PolyMod(NR(ModInv(LC(B3),Md)*B2,[M]),Md);
Else
Return PolyMod(B2,Md);
EndIf;
EndDefine;
```

A.7 Matrix Reduction Under Modulo in Galois Field

MatGF is used to reduce elements of matrix A in extented galois field under certain irreducible polynomial mod M.

```
Define MatGF(A,M)
Rows:=NumRows(A);Cols:=NumCols(A);
For I:=1 To Rows Do
For J:=1 To Cols Do
A[I][J]:=PolyMod(NR(A[I][J],[M]),2);
EndFor;
EndFor;
Return A;
EndDefine;
```

A.8 Matrix Reduction Under Modulo

ListModMat is used to reduce the Matrix into Mod Input J which is matrix and M is mod.

```
Define ListModMat(J,M)
Result:=[];
For I:=1 To NumRows(J) Do
K:=ListMod(J[I],M);
Append(Result,K);
EndFor;
Return Cast(Result,MAT);
EndDefine;
```

Bibliography

[1] R. M. Abobeah, M. M. Ezz, and H. M. Harb, "Public-key cryptography techniques evaluation," *International Journal of Computer Networks and Applications*, vol. 2, no. 2, pp. 1–12, 2015.

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

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

[4] Y. Desmedt and J.-J. Quisquater, "Public-key systems based on the difficulty of tampering (Is there a difference between DES and RSA?)," in *Advances in CryptologyCRYPTO86*, vol. 263. Springer, 1987, pp. 111–117.

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

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

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

[8] M. M. Rahman, T. K. Saha, and M. A.-A. Bhuiyan, "Implementation of rsa algorithm for speech data encryption and decryption," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 12, no. 3, pp. 1–74, 2012.

[9] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to elliptic curve cryptography*. Springer Science & Business Media, 2006, vol. 1.

[10] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future generation computer systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[11] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. OBrien, "Quantum computers," *Nature*, vol. 464, no. 7285, pp. 1–45, 2010.

[12] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM review*, vol. 41, no. 2, pp. 303–332, 1999.

[13] J. Patarin and L. Goubin, "Trapdoor one-way permutations and multivariate polynomials," in *International Conference on Information and Communications Security*, vol. 1334. Springer, 1997, pp. 356–368.

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

[15] T. Yasuda, X. Dahan, Y.-J. Huang, T. Takagi, and K. Sakurai, "Mq challenge: Hardness evaluation of solving multivariate quadratic problems." *IACR Cryptology ePrint Archive*, vol. 2015, pp. 1–14, 2015.

[16] K. G. Murty and S. N. Kabadi, "Some np-complete problems in quadratic and nonlinear programming," *Mathematical programming*, vol. 39, no. 2, pp. 117–129, 1987.

[17] S. Arora, D. Karger, and M. Karpinski, "Polynomial time approximation schemes for dense instances of np-hard problems," *Journal of computer and system sciences*, vol. 58, no. 1, pp. 193–210, 1999.

[18] N. R. Wagner and M. R. Magyarik, "A public-key cryptosystem based on the word problem," in *Workshop on the Theory and Application of Cryptographic Techniques*, vol. 196. Springer, 1984, pp. 19–36.

[19] A. G. Myasnikov, V. Shpilrain, and A. Ushakov, *Non-commutative cryptography and complexity of group-theoretic problems*. American Mathematical Soc., 2011, vol. 177, no. 177.

[20] Q. Cheng, J. Zhang, and J. Zhuang, "Lwe from non-commutative group rings," *arXiv preprint arXiv:1612.06670*, vol. 3, pp. 1–21, 2016.

[21] E. Sakalauskas and K. Luksys, "Matrix power s-box construction." *IACR Cryptology ePrint Archive*, vol. 2007, pp. 1–214, 2007.

[22] E. Sakalauskas, "Enhanced matrix power function for cryptographic primitive construction," *Symmetry*, vol. 10, no. 2, pp. 1–23, 2018.

[23] 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.

[24] E. Sakalauskas, A. Mihalkovich, and A. Venčkauskas, "Improved asymmetric cipher based on matrix power function with provable security," *Symmetry*, vol. 9, no. 1, pp. 1–9, 2017.

[25] A. Mihalkovich, E. Sakalauskas, and A. Venckauskas, "New asymmetric cipher based on matrix power function and its implementation in microprocessors efficiency investigation," *Elektronika ir Elektrotechnika*, vol. 19, no. 10, pp. 119–122, 2013.

[26] E. Sakalauskas and A. Mihalkovich, "Candidate one-way function based on matrix power function with conjugation constraints," *Proceedings of the Bulgarian Cryptography Days*, vol. 15, pp. 29–37, 2012.

[27] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," *Physical review letters*, vol. 92, no. 5, pp. 579–582, 2004.

[28] A. Team, "Apcocoa: Applied computations in commutative algebra."

[29] M. S. Iqbal, S. Singh, and A. Jaiswal, "Symmetric key cryptography: Technological developments in the field," *International Journal of Computer Applications*, vol. 117, no. 15, pp. 1–4, 2015.

[30] B. Schneier, "Description of a new variable-length key, 64-bit block cipher (blowfish)," in *International Workshop on Fast Software Encryption*, vol. 809. Springer, 1993, pp. 191–204.

[31] L. M. Kohnfelder, "Towards a practical public-key cryptosystem." Ph.D. dissertation, Massachusetts Institute of Technology, 1978.

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

[33] J.-C. Faugere and A. Joux, "Algebraic cryptanalysis of hidden field equation (hfe) cryptosystems using gröbner bases," in *Annual International Cryptology Conference*, vol. 2729. Springer, 2003, pp. 44–60.

[34] A. Joux, *Algorithmic cryptanalysis*. Chapman and Hall/CRC, 2009, vol. 2.

[35] F. Grieu, "A chosen messages attack on the iso/iec 9796-1 signature scheme," in *International Conference on the Theory and Applications of Cryptographic Techniques*, vol. 1807. Springer, 2000, pp. 70–80.

[36] M. Joye and M. Tunstall, *Fault analysis in cryptography*. Springer, 2012, vol. 147.

[37] T. Siegenthaler, "Decrypting a class of stream ciphers using ciphertext only," *IEEE Transactions on computers*, vol. 34, no. 1, pp. 81–85, 1985.

[38] M. Matsui, "Linear cryptanalysis method for des cipher," in *Workshop on the Theory and Application of of Cryptographic Techniques*, vol. 765. Springer, 1993, pp. 386–397.

[39] C. Rackoff and D. R. Simon, "Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack," in *Annual International Cryptology Conference*, vol. 576. Springer, 1991, pp. 433–444.

[40] M. Naor and M. Yung, "Public-key cryptosystems provably secure against chosen ciphertext attacks," in *Proceedings of the twenty-second annual ACM symposium on Theory of computing*, vol. 3860. ACM, 1990, pp. 427–437.

[41] G. N. Nayak and S. G. Samaddar, "Different flavours of man-in-the-middle attack, consequences and feasible solutions," in *Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on*, vol. 5. IEEE, 2010, pp. 491–495.

[42] A. Akhunzada, M. Sookhak, N. B. Anuar, A. Gani, E. Ahmed, M. Shiraz, S. Furnell, A. Hayat, and M. K. Khan, "Man-at-the-end attacks: Analysis, taxonomy, human aspects, motivation and future directions," *Journal of Network and Computer Applications*, vol. 48, pp. 44–57, 2015.

[43] N. Kumar, "Investigations in brute force attack on cellular security based on des and aes," *IJCEM International Journal of Computational Engineering & Management*, vol. 14, pp. 50–52, 2011.

[44] J. B. Fraleigh, *A first course in abstract algebra*. Pearson Education India, 2003, vol. 7.

[45] J. J. Rotman, *A first course in abstract algebra*. Prentice Hall, 2000, vol. 3.

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

[47] Y. S. Han, "Introduction to finite fields," vol. 1, pp. 1–41, 1999.

[48] C. J. Benvenuto, "Galois field in cryptography," *University of Washington*, vol. 56, pp. 1–11, 2012.

[49] S. D. Cohen, "On irreducible polynomials of certain types in finite fields," in *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 66, no. 2. Cambridge University Press, 1969, pp. 335–344.

[50] L. Carlitz *et al.*, "On certain functions connected with polynomials in a galois field," *Duke Mathematical Journal*, vol. 1, no. 2, pp. 137–168, 1935.

[51] G. Rose, "A stream cipher based on linear feedback over gf (2 8)," in *Australasian Conference on Information Security and Privacy*, vol. 1438. Springer, 1998, pp. 135–146.

[52] K. H. Rosen, B. Goddard, and K. O'Bryant, *Elementary number theory and its applications*. Pearson/Addison Wesley, 2005, vol. 1.

[53] S. Tsujii and T. Itoh, "An ID-based cryptosystem based on the discrete logarithm problem," *IEEE Journal on Selected Areas in Communications*, vol. 7, no. 4, pp. 467–473, 1989.

[54] Y. Ge, "A note on the carmichael function," *Mathematical Reflections*, vol. 15, pp. 232–238, 2007.

[55] D. E. Robling Denning, *Cryptography and data security*. Addison-Wesley Longman Publishing Co., Inc., 1982, vol. 2.

[56] G. Strang, "A proposal for toeplitz matrix calculations," *Studies in Applied Mathematics*, vol. 74, no. 2, pp. 171–176, 1986.

[57] R. M. Gray *et al.*, "Toeplitz and circulant matrices: A review," *Foundations and Trends® in Communications and Information Theory*, vol. 2, no. 3, pp. 155–239, 2006.

[58] C. Van Loan, *Computational frameworks for the fast Fourier transform*. Siam, 1992, vol. 10.

[59] P. J. Davis, *Circulant matrices*. American Mathematical Soc., 2012, vol. 147.

[60] R. P. Feynman, "Simulating physics with computers," *International journal of theoretical physics*, vol. 21, no. 6-7, pp. 467–488, 1982.

[61] R. G. Lyons, *Understanding Digital Signal Processing, 3/E*. Pearson Education India, 2011, vol. 3.

[62] E. Sakalauskas, N. Listopadskis, and P. Tvarijonas, "Key agreement protocol (kap) based on matrix power function," vol. 47, pp. 92–96, 2008.

[63] A. Mihalkovič and E. Sakalauskas, "Asymmetric cipher based on mpf and its security parameters evaluation," vol. 53, pp. 72–77, 2012.

[64] J. Liu, H. Zhang, J. Jia, H. WANG, S. MAO, and W. WU, "Cryptoanalysis of hkks key exchange protocols," *Chinese Journal of Computers*, vol. 39, no. 3, pp. 516–528, 2016.

[65] Z. Cao, X. Dong, and L. Wang, "New public key cryptosystems using polynomials over non-commutative rings." *IACR Cryptology ePrint Archive*, vol. 2007, pp. 1–9, 2007.

[66] M. Zia and R. Ali, "Cryptanalysis and improvement of an elliptic curve based signcryption scheme for firewalls," *PloS one*, vol. 13, no. 12, pp. 1–11, 2018.

[67] P. Falcarin, C. Collberg, M. Atallah, and M. Jakubowski, "Guest editors' introduction: Software protection," *IEEE Software*, vol. 28, no. 2, pp. 24–27, 2011.

[68] M. Tang, Z. Qiu, W. Li, W. Sun, X. Hu, and H. Zhang, "Power analysis based reverse engineering on the secret round function of block ciphers," *Concurrency and Computation: Practice and Experience*, vol. 26, no. 8, pp. 1531–1545, 2014.

[69] Z. Shan, H. Cao, J. Lv, C. Yan, and A. Liu, "Enhancing and identifying cloning attacks in online social networks," in *Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication*, vol. 71. ACM, 2013, pp. 1–59.

[70] G. Svensson, "Auditing the human factor as a part of setting up an information security management system," pp. 1–25, 2013.