

CAPITAL UNIVERSITY OF SCIENCE AND  
TECHNOLOGY, ISLAMABAD



# Encryption Schemes Based on General Linear Groups and Group Rings

by

Saba Inam

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

in the

Faculty of Computing

Department of Mathematics

2019

# Encryption Schemes Based on General Linear Groups and Groupings

By

Saba Inam  
(PA-131002)

Dr. Xingqiang Xiu  
Hainan Normal University, China  
(Foreign Evaluator 1)

Dr. Gerhard Rosenberg  
Hamburg University, Germany  
(Foreign Evaluator 2)

Dr. Rashid Ali  
(Thesis Supervisor)

Dr. Muhammad Sagheer  
(Head, Department of Mathematics)

Dr. Muhammad Abdul Qadir  
(Dean, Faculty of Computing)

DEPARTMENT OF MATHEMATICS  
CAPITAL UNIVERSITY OF SCIENCE AND TECHNOLOGY  
ISLAMABAD

2019

Copyright © 2019 by Saba Inam

All rights reserved. No part of this thesis may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, by any information storage and retrieval system without the prior written permission of the author.

I dedicate this dissertation to my husband

**Saeed Akhtar (Late)**

**My Children**

and

**My Parents**



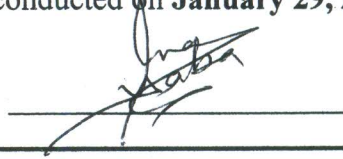
**CAPITAL UNIVERSITY OF SCIENCE & TECHNOLOGY  
ISLAMABAD**

Expressway, Kahuta Road, Zone-V, Islamabad  
Phone: +92-51-111-555-666 Fax: +92-51-4486705  
Email: [info@cust.edu.pk](mailto:info@cust.edu.pk) Website: <https://www.cust.edu.pk>

**CERTIFICATE OF APPROVAL**

This is to certify that the research work presented in the thesis, entitled “**Encryption Schemes Based on General Linear Groups and Groupings**” was conducted under the supervision of **Dr. Rashid Ali**. No part of this thesis has been submitted anywhere else for any other degree. This thesis is submitted to the **Department of Mathematics, Capital University of Science and Technology** in partial fulfillment of the requirements for the degree of Doctor in Philosophy in the field of **Mathematics**. The open defence of the thesis was conducted on **January 29, 2019**.

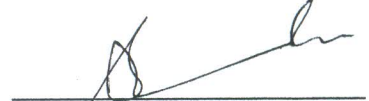
**Student Name :** Ms. Saba Inam (PA131002)



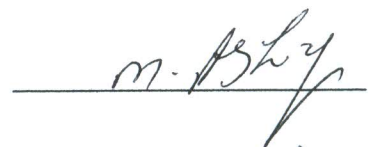
The Examining Committee unanimously agrees to award PhD degree in the mentioned field.

**Examination Committee :**

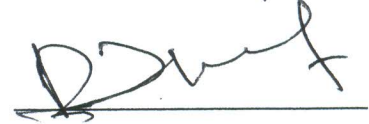
(a) External Examiner 1: Dr. Muhammad Shabir  
Professor  
QAU, Islamabad



(b) External Examiner 2: Dr. Muhammad Ashiq  
Associate Professor  
MCS, NUST, Islamabad




(c) Internal Examiner : Dr. Shafqat Hussain  
Associate Professor  
CUST, Islamabad



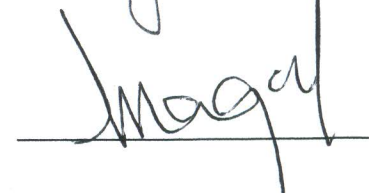
**Supervisor Name :** Dr. Rashid Ali  
Associate Professor  
CUST, Islamabad



**Name of HoD :** Dr. Muhammad Sagheer  
Professor  
CUST, Islamabad



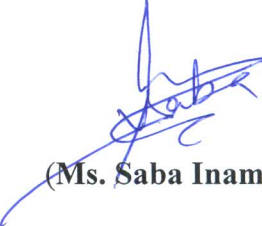
**Name of Dean :** Dr. Muhammad Abdul Qadir  
Professor  
CUST, Islamabad



## **AUTHOR'S DECLARATION**

I, **Ms. Saba Inam (Registration No. PA131002)**, hereby state that my PhD thesis titled, '**New Encryption Schemes Based on General Linear Group Over Finite Fields and Groupings**' 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/ world.

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



(**Ms. Saba Inam**)

Dated: January, 2019

Registration No : PA131002

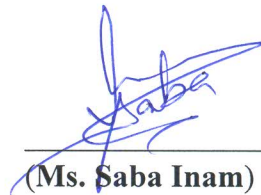
## PLAGIARISM UNDERTAKING

I solemnly declare that research work presented in the thesis titled “**New Encryption Schemes Based on General Linear Group Over Finite Fields and Groupings**” is solely my research work with no significant contribution from any other person. Small contribution/ help wherever taken has been duly 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 PhD Degree, the University reserves the right to withdraw/ revoke my PhD 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 thesis.

Dated: January, 2019



(Ms. Saba Inam)

Registration No. : PA131002

## *List of Publications*

It is certified that following publication has been made out of the research work that has been carried out for this thesis:-

1. S. Inam and R. Ali, "A new ElGamal-like cryptosystem based on matrices over groupring", *Neural Computing and Applications*, vol. 29, 1279-1283, 2018.

**Saba Inam**

(PA-131002)



## *Acknowledgements*

I am thankful to Allah Almighty, the Most Merciful and Compassionate, the Most Gracious and Beneficent, whose bounteous blessings enabled me to perceive and pursue higher ideals of life, Who has given me the abilities to do the sheer hard work and enthusiasm to perform well.

I gratefully acknowledge my supervisor Dr. Rashid Ali, Department of Mathematics, Capital University of Science and Technology, Islamabad, under whose supervision, guidance and illustrative advice, the research work presented in this dissertation became possible. He was always available to offer his guidance and encouragement to me.

I express my deepest gratitude to honorable vice chancellor Prof. Dr. Muhammad Mansoor Ahmed, Capital University of Science and Technology, Islamabad for providing me with the financial help in the form of CUST scholarship, ideal atmosphere of study and research in the department. My sincere thanks are also due to the head, Mathematics department, Dr. Muhammad Sagheer, Capital University of Science and Technology, Islamabad. I also wish to express my appreciation to Higher Education Commission for providing me the latest literature in the form of digital and reference libraries.

This study would have been impossible without the prayers, love, help, encouragement and moral support of my family. I express my appreciation and deep sense of gratitude from the core of my heart to my most of all for my loving, supportive, encouraging, and patient husband Saeed Akhtar, my parents, my brothers and my in laws whose hands always arise in prayers for my success.

Undertaking this PhD has been a truly life-changing experience for me and it would not have been possible to do without the support that I received from my children. I am very much indebted to my children Hajra Saeed and M. Abdur Rehman Saeed, who supported me in every possible way to see the completion of this work. They are the most important people in my world.

Completion of this doctoral dissertation was possible with the support of several people. Words of gratitude and appreciation don't always convey the depth of

one's feelings but I wish to thanks to my class fellow and my friend Shamsa Kanwal and my colleagues of Fatima Jinnah Women University specially Dr. Sadia Hina, Head Department of Mathematical Sciences, Dr. Munazza Naz and Bushra Kanwal, who really helped me and kept my moral high during the dissertation.

**(Saba Inam)**

## *Abstract*

Security of some present day public key cryptosystems is based on general linear groups as it is a good choice for developing such type of cryptosystems. This study presents various public key encryption schemes based on general linear groups. Different techniques including automorphisms in connection with conjugacy search problem and its generalization are used to develop these schemes. Further, the group rings are chosen as platform to enhance the security and efficiency. Numerous aspects related to our new proposals are also elaborated.

# Contents

<b>Author's Declaration</b>	<b>v</b>
<b>Plagiarism Undertaking</b>	<b>vi</b>
<b>List of Publications</b>	<b>vii</b>
<b>Acknowledgements</b>	<b>viii</b>
<b>Abstract</b>	<b>x</b>
<b>List of Figures</b>	<b>xiii</b>
<b>List of Tables</b>	<b>xiv</b>
<b>Abbreviations</b>	<b>xv</b>
<b>Symbols</b>	<b>xvi</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Background . . . . .	3
1.2 Thesis Contribution . . . . .	5
1.3 Outline of the Thesis . . . . .	5
<b>2 Overview of Mathematical Concepts</b>	<b>7</b>
2.1 Number Theory . . . . .	7
2.1.1 Module Arithmetic . . . . .	8
2.2 Abstract Algebra . . . . .	10
2.2.1 Algebra of Matrices . . . . .	20
2.2.2 Polynomial Rings . . . . .	23
2.2.3 Finite Fields . . . . .	24
<b>3 Cryptographic Preliminaries</b>	<b>31</b>
3.1 Primitives of Cryptology . . . . .	31
3.1.1 Characterizations of Cryptosystems . . . . .	32
3.1.2 Cryptographic Applications . . . . .	33

---

3.2	Public Key Cryptography . . . . .	34
3.2.1	General Scheme For Public Key Cryptosystem . . . . .	34
3.3	Cryptanalysis . . . . .	42
3.3.1	Attacks on Encryption Schemes . . . . .	43
3.4	Public Key Cryptography Based on Groups . . . . .	45
<b>4</b>	<b>A Cryptosystem Based on Polynomials over Circulant Matrices</b>	<b>50</b>
4.1	Some Definitions and Group Based Hard Problems . . . . .	51
4.2	Proposed Cryptosystem . . . . .	55
4.3	Security Analysis . . . . .	68
4.4	Efficiency of Cryptosystems . . . . .	69
4.4.1	Efficiency of Proposed Cryptosystem . . . . .	71
4.5	Conclusion . . . . .	72
<b>5</b>	<b>A New ElGamal Like Cryptosystem Based on Matrices over Grouping</b>	<b>73</b>
5.1	Grouping . . . . .	74
5.2	Proposed Cryptosystem . . . . .	78
5.3	Security Aspects of Proposed Cryptosystem . . . . .	85
5.4	Conclusion . . . . .	86
<b>6</b>	<b>A Variant of ElGamal Cryptosystem Based on General Linear Group and Grouping</b>	<b>88</b>
6.1	Proposed Cryptosystem . . . . .	88
6.2	Security Analysis of Proposed Cryptosystem . . . . .	97
6.3	Conclusion . . . . .	98
	<b>Bibliography</b>	<b>100</b>

# List of Figures

2.1	Relationship Between Algebraic Structures . . . . .	19
3.1	Symmetric Cryptosystem . . . . .	32
3.2	General Scheme For Public Key Cryptosystem . . . . .	35
3.3	One-Way Trapdoor Fuction . . . . .	36
3.4	Diffie-Hellman Key Exchange . . . . .	38

# List of Tables

2.1	Multiplicative Inverse Using Extended Euclidean Algorithm . . . . .	10
2.2	Cayley's Table for $S_3$ . . . . .	12
2.3	Cayley's tables for addition . . . . .	18
2.4	Cayley's Table for Multiplication . . . . .	19
2.5	XOR Operation . . . . .	25
3.1	Estimated Time for Successful Brute Force Attack on symmetric Algorithms With Different Key Lengths . . . . .	44
3.2	Bit Lengths of Public-Key Algorithm . . . . .	45
4.1	Complexity of Bit Operation . . . . .	69
5.1	Units of Grouping . . . . .	77
5.2	Augmentation Map . . . . .	77

# Abbreviations

AES	Advance Encryption Standard
CSP	Conjugacy Search Problem
DES	Data Encryption Standard
DH	Diffie Hellman
DLP	Discrete Logarithm Problem
DP	Decomposition Problem
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
GDP	Generalized Decomposition Problem
GF	Galois Field
GR	Grouping
GSDP	Generalized Symmetric Decomposition Problem
IFP	Integer Factorization Problem
PSDP	Polynomial Symmetric Decomposition Problem
PKC	Public Key Cryptography
RC4	Rivest Cipher 4
RSA	Rivest-Shamir-Adleman
SDP	Symmetric Decomposition Problem
WP	Word Problem
XOR	Exclusive OR



# Symbols

$\gcd(a, b)$	Greatest Common Divisor of $a$ and $b$
$\mathbb{Z}$	set of integers
$\mathbb{Z}_{>0}$	set of positive integers
$\mathbb{Z}_+$	set of positive integers
$\mathbb{Z}_n$	set of integers modulo $n$
$\mathbb{Z}_n^*$	set $\mathbb{Z}_n \setminus \{0\}$
$\mathbb{Z}[i]$	set of Gaussian integers
$\mathbb{Q}$	set of Rational numbers
$\mathbb{R}$	set of Real numbers
$\mathbb{R}^*$	set $\mathbb{R} \setminus \{0\}$
$\mathbb{C}$	set of Complex numbers
$\mathbb{F}$	Field
$S_3$	Symmetric group of order 3
$G$	Group
$Z(G)$	Center of group
$R$	Ring
$R[x]$	Polynomial ring in one indeterminate $x$ over the ring $R$
$GL(n, R)$	General linear group of matrices of order $n$ over the ring $R$
$M(n, R)$	set of matrices of order $n$ over the ring $R$

# Chapter 1

## Introduction

Due to rapid development in the area of information technology, a secure commercial and private communication has become a need. Therefore the faster and more efficient methods enable people to protect their valuable information. Adversaries are also there to thwart this secret information. The field of cryptography has played a vital role for the secure transformation of important information between two or more people. The main purpose of cryptography is to send information between participants in such a way that the threats from adversaries can be prevented.

The history of cryptography is very long and fascinating. It is the study of methods of transforming a secret message in such a way that it can be understood only by an authorized recipient who has been provided with a secret key for deciphering it. If the message is intercepted by an unauthorized recipient (enemy or hacker), he/she should not be able to interpret it. Cryptanalysis is the study of techniques for getting the meaning of encrypted information, without having any access to the secret information that is normally required to do so. From this, cryptanalyst comes to know about the working of a cryptosystem and find a secret key. In a simple language we can say that the practice of cracking/breaking the code is called cryptanalysis. The study of cryptography and cryptanalysis is called cryptology.

Cryptography has many uses and in today's world the very important feature of cryptography is in electronic information security. It can easily be seen that there are many perceptions such as data encryption standards, public and private key cryptography, digital signatures, key exchange protocols and others [1, 36]. If we talk about the security aspects, we note that the symmetric or private key encryption schemes are now insecure and inadequate, because one shared secret key is used for encryption and decryption. Handling these shared keys is easy for a few communicating parties but it is very difficult to manage the shared key when there is a large increasing number of communicating parties. In 1976, Diffie and Hellman [16] proposed a new idea in cryptography and this concept was known as public key cryptography and is based on using two keys (private and public). This concept helped to overcome the problems and weaknesses in secret key cryptography, many of public key cryptosystems were specified as RSA [48], Diffie-Hellman key exchange protocol [16], ElGamal public key cryptosystem [17] and discrete logarithm problem (DLP) [53] are considered secure. All the said schemes, systems and methods use some number theoretical and pure algebraic structures. For example, in the field of cryptography, many applications of groups are discussed, see [15, 55]. Especially, we can say that RSA generally depends upon the structure of finite commutative groups and it works on invertible elements (units) of  $\mathbb{Z}_n$  such that  $n = p_1 p_2$ , where  $p_1$  and  $p_2$  are randomly large prime numbers. However, the hard problem is to find these primes  $p_1$  and  $p_2$ , because it depends on the factorization problem known as Integer Factorization Problem (IFP). As said by Hurley and Hurley [25], the most encryption schemes are developed using combinatorial group theory and they tell that conjugacy search problem (CSP) [6] is the generalized form of discrete logarithm problem (DLP) which is defined on groups rather than integers. The (so called) computational difficulty of these problems in specific groups (like in braid groups) has been used in several group based cryptosystems, see Refs. [1, 22]. Using the concepts of group theory, many cryptographic protocols have been developed in the recent years. The investigation for better alternative cryptosystems become very important with the awareness

that quantum computers can efficiently resolve both the IFP and standard variants of the DLP due to Shor [53], Kitaev [29] and Proos-Zalka [46] algorithms. Cryptosystems, comprising group-based [55] examples are not essentially vulnerable to quantum attackers have become identified as post-quantum cryptosystems. McEliece cryptosystem is a very good example which is based on the difficulty of decoding error-correcting codes. Other examples include the cryptosystems which are based on large systems of multivariate polynomial equations and also lattice-based cryptosystems. We investigate the task of matrix groups which is chosen as a platform for group-based cryptosystems. If anyone wants to execute a group-based cryptosystem, then he/she needs a proficient technique of storing, demonstrating, and operating the elements of groups.

## 1.1 Background

For efficient performances and security enhancements, the solid strength is the generation of noncommutative cryptographic schemes. For these schemes many attempts have been made. A brief discussion is given below:

In 1985, Magyarik and Wagner [33] proposed a public key cryptography by using the elements of semigroup with undecidable word problem. A review of group based cryptographic methods is discussed by Myasnikov et al. [41] in the book “Group-based Cryptography”. But Birget et al. [4] told that the PKC proposed by Magyarik and Wagner [33] actually did not depend on word problem and as a result they developed a new scheme which was based on finitely generated groups with hard problem. On braid group based cryptography, Anshel et al. [1] proposed a key exchange protocol in 1999 and the hard problem of this protocol was the difficulty of resolving equations over algebraic structures. In this paper [1] they mentioned that for PKC braid groups as a platform are a good choice. After this in 2000, Ko et al. [30] developed a new key exchange protocol by using braid groups. The conjugacy search problem (CSP) is the underlying hard problem for this protocol. Furthermore, many successful schemes were proposed in this area

by Cha et al. [7] in 2001, Anshel et al [2] in 2003, Dehornoy [15] in 2004 and Anshel et. al [3] in 2006.

Paeng et al. [44] in 2001 also proposed a new scheme which was based on finite noncommutative groups. This method consists of the DLP in inner automorphism group. With further improvement, the system is named as MOR [44]. In this era, Magliveras et al. [32] in 2002 gave a remarkable idea about one way function and trapdoors which were generated on finite fields. In the meantime, on finite groups Magliveras et al. anticipated a new PKC scheme using one way function and trapdoors. Consequently on integer matrices Grigoriev and Ponomarenko [20, 21] extended the difficulty of membership problem [54] for finitely generated group of elements. In 2007, a new proposal was given by Cao et al. [6] on polynomials over noncommutative semi groups or rings. The method is named as  $\mathbb{Z}$  modular method. As an application of this scheme Kubo [31] in 2008 presented a scheme based on noncommutative dihedral group of order 6. Reddy et al. [47] in 2008 developed a signature scheme over noncommutative groups and division ring by using  $\mathbb{Z}$  modular method. The implementation of this scheme was built by Moldovyan and Moldovyan [40]. Another scheme is also formulated by Kanwal and Ali [28] by using noncommutative platform groups.

Now let us talk about some PKC schemes of groupring. A cryptosystem based on the structure of a groupring was proposed by Rososhek [50, 51]. In 2011, Kahrobaei et al. [27] developed a key exchange protocol based on matrices over groupring. After that many PKC schemes based on groupring was proposed. See Refs. [10]. The main idea to apply the grouprings in cryptography depends on the fact that if the cardinality of the finite ring  $R$  is fixed, the cardinality of a groupring  $GR$  for a finite group is an exponent of the cardinality of a group  $G$ . Then cryptographic transformation performed by a legal user separately in the group  $G$  and in the ring  $R$  using polynomial algorithms and an illegal user has to solve computationally difficult problems in groupring  $GR$ .

## 1.2 Thesis Contribution

The main role of the thesis is:

- To develop a cryptosystem based on polynomials over circulant matrices using inner automorphism. We discuss the security aspects of proposed cryptosystem in detail and also discuss the efficiency of the cryptosystem.
- To propose a cryptosystem and it mainly depends on ElGamal scheme. The correctness of the proposed cryptosystem is proved and all the important issues related to proposed scheme and its security are also discussed.
- On the basis of ElGamal cryptosystem, we have developed its variant and the choice of platform is groupring due to its complex structure. All the essential related discussions about the new proposed cryptosystem are present in this thesis.

## 1.3 Outline of the Thesis

The thesis is organized as follows:

- In Chapter 2 and 3, we give the background material related to algebraic number theory and cryptography respectively. These chapters contain basic definitions, concepts and notations and also have explanatory examples which will be helpful for the rest of the thesis. Although there are many books in the literature on abstract algebra and cryptography but for more details on algebra, we refer to [18] and for cryptography, we refer to [43, 57, 58].
- In Chapter 4, we discuss a cryptosystem based on polynomials over circulant matrices and we also prove its correctness. The contents of this chapter is submitted for possible publication.
- Chapter 5 is based on a new ElGamal like cryptosystem based on matrices over groupring. Different aspects of the proposed cryptosystem are also discussed. The contents of this chapter has been published in the journal of Neural Computing and Applications [26].

- In Chapter 6, we present a variant of ElGamal cryptosystem based on general linear group over groupring. The material of this chapter is also submitted for a possible publication.

# Chapter 2

## Overview of Mathematical Concepts

The fundamental concepts of number theory and algebra are very important in modern cryptography. So we need to recall some important tools, before we investigate the subject of cryptography. In the next two sections, we give some fundamental concepts which is the basic necessity to describe and prove the fundamental results from number theory and abstract algebra.

### 2.1 Number Theory

We will discuss some definitions and terminologies from number theory in this section. Modular arithmetic has a major importance in public-key cryptography. We also give the definition and properties of modular arithmetic. Throughout this work,  $\mathbb{Z}$  denotes the set of integers,  $\mathbb{Z}_+$  denotes the set of positive integers,  $\mathbb{Z}_n$  denotes the set of integers modulo  $n$  and  $\mathbb{Z}_n^*$  denotes the set  $\mathbb{Z}_n \setminus \{0\}$ .

We start with a well known result of number theory known as the division algorithm:

#### **Theorem 2.1.1. (Division Algorithm)**

Let  $c$  and  $d$  be two integers and  $d > 0$ , then there exist unique integers  $q, r$  such



that

$$c = qd + r, \text{ where } 0 \leq r < d. \quad (2.1)$$

where quotient is denoted by  $q$  which divides  $c$  by  $d$ , with the remainder  $r$ .

### 2.1.1 Module Arithmetic

The simple method of executing arithmetic in a finite set of integers is known as modular arithmetic. Now we give a complete definition of the modulo operation:

Let us consider the set of integers  $\mathbb{Z}$  and let  $b, r, m \in \mathbb{Z}$  and  $m > 0$ . We write

$$b \equiv r \pmod{m}, \quad (2.2)$$

if  $m$  divides  $b - r$ . Here  $r$  is known as remainder and  $m$  is known as modulus.

The definition gives us few implications which go beyond the casual rule “divide by the modulus and consider the remainder.”

One can use Theorem 2.1.1, to calculate the remainder  $r$  defined in Equation (2.2).

The remainder  $r$  is chosen such that

$$0 \leq r < m - 1.$$

Generally, we select  $r$  as defined in Equation (2.2) where,  $0 \leq r \leq m - 1$ . Consequently, which element of an equivalent class we use does not effect mathematically. By repeated application of the division algorithm Theorem 2.1.1, one can find out the greatest common divisor (gcd) of two positive integers  $c$  and  $d$ . The method is known as Euclidean algorithm and is stated below:

**Algorithm 2.1.2. (The Euclidean Algorithm)**[57]

**Input:** Two positive integers  $c$  and  $d$

**Output:**  $\gcd(c, d)$

1.  $M \leftarrow c; N \leftarrow d$
2. if  $N = 0$  return  $M = \gcd(c, d)$
3.  $T = M \pmod{N}$

4.  $M \leftarrow N$
5.  $N \leftarrow T$
6. Go to Step 2.

**Example 2.1.3.**

By using the Euclidean Algorithm 2.1.2, we calculate  $\gcd(285, 165)$ , which is just the repeated division with remainder.

$$\begin{aligned} 2006 &= 1360 \times 1 + 646 \\ 1360 &= 646 \times 2 + 68 \\ 646 &= 68 \times 9 + 34 \leftarrow \gcd = 34 \\ 68 &= 34 \times 2 + 0 \end{aligned}$$

From the above expression, we see that  $\gcd(285, 155) = 34$ . The main application of Euclidean algorithm is not to find the gcd but the extension of this algorithm permits us to calculate the modular inverses which has a major significance in asymmetric key cryptography and it follows from the following algorithm:

**Algorithm 2.1.4. (Extended Euclidean Algorithm)**

**Input:** Two positive integers  $c$  and  $d$  such that  $c > d$

**Output:** Multiplicative inverse of  $d \pmod{c}$

1.  $(V_1, V_2, V_3) \leftarrow (1, 0, c)$ ;  $(W_1, W_2, W_3) \leftarrow (0, 1, d)$
2. If  $W_3 = 0$ , return  $V_3 = \gcd(c, d)$ ; no inverse
3. If  $W_3 = 1$ , return  $W_3 = \gcd(c, d)$ ;  $W_2 = d^{-1} \pmod{c}$
4.  $Q = \lfloor \frac{V_3}{W_3} \rfloor$  (quotient when  $V_3$  is divided by  $W_3$ )
5.  $(S_1, S_2, S_3) \leftarrow (V_1 - QW_1, V_2 - QW_2, V_3 - QW_3)$
6.  $(V_1, V_2, V_3) \leftarrow (W_1, W_2, W_3)$
7.  $(W_1, W_2, W_3) \leftarrow (S_1, S_2, S_3)$

8. Goto Step 2.

The correctness and termination of the algorithm follows from the above stated procedure for computing modular inverses.

We illustrate Algorithm 2.1.4 by computing the multiplicative inverse of  $17 \pmod{48}$ . The results after each step are summarized in the following TABLE 2.1.

TABLE 2.1: Multiplicative Inverse Using Extended Euclidean Algorithm

$U$	$V_1$	$V_2$	$V_3$	$W_1$	$W_2$	$W_3$
	1	0	48	0	1	17
2	0	1	17	1	-2	14
1	1	-2	14	-1	3	3
4	-1	3	3	5	-14	2
1	5	-14	2	-6	17	1

From the last row, the algorithm returns  $17^{-1} = 17 \pmod{48}$

**Theorem 2.1.5. (Euler’s Theorem)**[38]

Let  $n \geq 2$  be an integer. If  $a \in \mathbb{Z}_n^*$ , such that  $\gcd(a, n) = 1$ , then

$$a^{\varphi(n)} \equiv 1 \pmod{n}, \tag{2.3}$$

where  $\varphi(n)$  = number of integers in  $[1, n]$  that are relative prime to  $n$ . If  $n = p$ , a prime integer, then

$$\varphi(p) = 1 - p,$$

and we get Fermat’s Little Theorem as a special case of Euler’s Theorem.

## 2.2 Abstract Algebra

The basic concepts of algebra and their characteristics are being discussed in this section for the compilation of the thesis. Particularly, we recall the concept of groups, subgroups, finite groups, cyclic groups and some computationally hard problems in algebra.

**Definition 2.2.1. (Group)**[43]

A set  $G$  together with an operation  $*$  is called group, if  $*$  is closed and associative. There exists an identity or neutral element  $e \in G$  and every  $g \in G$  has inverse  $g^{-1}$  such that

$$g * g^{-1} = g^{-1} * g = e.$$

A group  $G$  is called commutative or abelian if,

$$g_1 * g_2 = g_2 * g_1, \quad \forall g_1, g_2 \in G''.$$

A group  $(G, *)$  with finite number of elements is known as finite group. The cardinality of the group  $G$  is denoted by  $|G|$ .

**Definition 2.2.2. (Subgroup)**

Let  $(G, *)$  be a group and  $H \subseteq G$ . Then  $H$  is said to be a subgroup of  $G$ , if  $H$  is a group itself under the same binary operation  $*$ .

**Example 2.2.3.**

1. A permutation is a 1-1 mapping from a non empty set  $Y$  to itself e.g.

if  $Y = \{1, 2, 3\}$ , then  $\delta : Y \rightarrow Y$  defined by

$$\delta(1) = 2, \quad \delta(2) = 3 \text{ and } \delta(3) = 1,$$

is a permutation on  $Y$ . This permutation can also be represented by  $(1 \ 2 \ 3)$ .

Similarly a permutation given by

$$\delta(1) = 2; \quad \delta(2) = 1; \quad \delta(3) = 3,$$

is represented by  $(1 \ 2)$ . Collection of all permutations on this set  $Y$  forms a group called symmetric group of order  $3!$  and is denoted by  $S_3$ . Here

$$S_3 = \{I, \delta_1, \delta_2, \delta_3, \delta_4, \delta_5\}$$

where  $I$  represents the identity permutation and

$$\delta_1 = (1\ 2), \delta_2 = (1\ 3), \delta_3 = (2\ 3), \delta_4 = (1\ 2\ 3), \delta_5 = (1\ 3\ 2).$$

The Cayley table of  $S_3$  is given in TABLE 2.2.

TABLE 2.2: Cayley's Table for  $S_3$

*	$I$	$\delta_1$	$\delta_2$	$\delta_3$	$\delta_4$	$\delta_5$
$I$	$I$	$\delta_1$	$\delta_2$	$\delta_3$	$\delta_4$	$\delta_5$
$\delta_1$	$\delta_1$	$I$	$\delta_4$	$\delta_5$	$\delta_2$	$\delta_3$
$\delta_2$	$\delta_2$	$\delta_5$	$I$	$\delta_4$	$\delta_3$	$\delta_1$
$\delta_3$	$\delta_3$	$\delta_4$	$\delta_5$	$I$	$\delta_1$	$\delta_2$
$\delta_4$	$\delta_4$	$\delta_3$	$\delta_1$	$\delta_2$	$\delta_5$	$I$
$\delta_5$	$\delta_5$	$\delta_2$	$\delta_3$	$\delta_1$	$I$	$\delta_4$

More generally the set of  $n$  elements, we get symmetric group of order  $n$  represented by  $S_n$ .

2. The set  $G = \{\pm 1, \pm i\}$  forms a group under multiplication.
3.  $H_1 = \{\pm 1\}$  is a subgroup of the group  $G$  given above in 2.
4.  $A_3 = \{I, (1\ 2\ 3), (1\ 3\ 2)\}$  is a subgroup of  $S_3$  known as alternating group of order 3. For details see TABLE 2.2.

**Definition 2.2.4. (Cyclic Group)**

A group  $G$  is said to be cyclic if  $G$  has an element  $g$  of maximum order  $|G|$ . That is if there exists  $g \in G$ , such that  $\text{ord}(g) = |G|$ . The element  $g$  is then called the generator because it generates the entire group. Every element  $h \in G$  can be written as a power of  $g$  for some  $n \in \mathbb{N}$ . The generator of a group needs not to be unique i.e. there can be more than one generator of a group.

**Example 2.2.5.**

1.  $G = \langle a : a^n = e \rangle$ , where  $a$  is called the generator of cyclic group of order  $n$ .
2.  $(\mathbb{Z}_n, +)$  is a cyclic group.

3. The set  $G = (\{\pm 1, \pm i\}, \cdot)$  has 4 elements and is a cyclic group generated by  $i$  and  $-i$ .
4. The set  $\mathbb{Z}_p^* = \{1, 2, \dots, p-1\}$  is a cyclic group under multiplication.

**Definition 2.2.6. (Center of a Group)**

The set consisting of those elements which commute with every other element of a group is known as center of that group  $G$ . It is represented by  $Z(G)$ , that is

$$Z(G) = \{x \in G : xh = hx, \quad \forall h \in G\}. \quad (2.4)$$

**Example 2.2.7.**

1. Center of an abelian group is the group itself.
2. Center of  $S_3$  is the identity element can be seen in TABLE 2.2.

**Definition 2.2.8. (Homomorphism)**

A homomorphism from group  $(G_1, *)$  to  $(G_2, \bullet)$  is defined as a function  $\psi : G_1 \rightarrow G_2$  such that

$$\psi(h_1 * h_2) = \psi(h_1) \bullet \psi(h_2), \forall h_1, h_2 \in G_1. \quad (2.5)$$

Hence homomorphism is a function from group  $G_1$  to  $G_2$  that converts the operation in  $G_1$  to the operation in  $G_2$ .

For a homomorphism  $\psi : G_1 \rightarrow G_2$  the kernel of  $\psi$  is defined as:

$$\ker(\psi) = \{g_1 \in G_1 : \psi(g_1) = e_{G_2}\}, \quad (2.6)$$

where  $e_{G_2}$  is the identity element of  $G_2$ .

**Example 2.2.9.**

Define  $\theta : \mathbb{C} \rightarrow \mathbb{C}$  by

$$\theta(x_1 + iy_1) = (x_1 + y_1) + i(x_1 - y_1).$$

Then  $\theta$  is a homomorphism where  $\mathbb{C}$  is the set of complex numbers which is a group under addition.

**Definition 2.2.10. (Isomorphism)**

The homomorphism  $\psi : G_1 \rightarrow G_2$  is called an isomorphism, if  $\psi$  is also onto and one-one. Such groups are said to be isomorphic to each other. It is denoted by

$$G_1 \cong G_2.$$

**Example 2.2.11.**

Let  $G_1 = (\mathbb{R}, +)$  and  $G_2 = (\mathbb{R}^*, \cdot)$ . Then  $\psi : G_1 \mapsto G_2$  is defined as

$$\psi(x) = e^x, \text{ for all } x \in G_1,$$

is an isomorphism.

**Definition 2.2.12. (Automorphism)**

An isomorphism from a group  $G$  to itself is called an automorphism. The set of automorphisms of a group  $G$  forms a group and is denoted  $Aut(G)$ . That is,

$$Aut(G) = \{\beta : G \rightarrow G \mid \beta \text{ is an isomorphism}\}.$$

**Example 2.2.13.**

Let  $G = (\mathbb{R}^*, \cdot)$ . Then an isomorphism  $\beta : G \mapsto G$  is defined as

$$\beta(x) = x^{-1}, \text{ for all } x \in G$$

is an automorphism.

**Definition 2.2.14. (Inner Automorphism)**

Let us consider a group  $G$  and let  $g \in G$ . Then the automorphism  $i_g : G \rightarrow G$  defined by

$$i_g(x) = g^{-1}xg. \tag{2.10}$$

is known as inner automorphism. The set of all the inner automorphisms of a group  $G$  is usually denoted as  $Inn(G)$ .

If  $G$  is abelian, then

$$\begin{aligned} i_g(x) &= g^{-1}xg = g^{-1}gx \\ &= x \\ &= i_D \text{ (identity map)}. \end{aligned}$$

This implies that in an abelian group the inner automorphisms are trivial. More generally,

$$i_g = i_D \Leftrightarrow g \in Z(G).$$

**Example 2.2.15.**

Let  $G = S_3$ . Then  $i_g : G \rightarrow G$  defined by

$$i_{(1\ 2)} = (1\ 2)^{-1} x (1\ 2), \quad \forall x \in G.$$

is an example of an inner automorphism on  $S_3$ . For example if  $x = (2\ 3)$ , then

$$\begin{aligned} i_{(1\ 2)} &= (1\ 2)^{-1} (2\ 3) (1\ 2), \\ &= (1\ 2) (2\ 3) (1\ 2), \\ &= (1\ 3\ 2) (1\ 2), \\ &= (1\ 3). \end{aligned}$$

For more details we refer to TABLE 2.2.

**Definition 2.2.16. (Ring)**

A set  $R$  with two binary operations  $(R, +, \times)$ , where  $+$  denotes addition and  $\times$  denotes multiplication is called a ring if  $(R, +)$  is an abelian group, the operation  $\times$  is associative. There exists multiplicative identity 1, an operation  $\times$  is distributive over  $+$ ,

$$\begin{aligned} a \times (b + c) &= (a \times b) + (a \times c) \\ (b + c) \times a &= (b \times a) + (c \times a), \quad \forall a, b, c \in R. \end{aligned}$$



The ring is a commutative ring if

$$a \times b = b \times a \text{ for all } a, b \in R \text{ .}$$

**Definition 2.2.17. (Units of Ring)**

Let  $R$  be a ring. An element  $a \in R$  is known as an invertible element or unit if there is an element  $a^{-1} \in R$  s.t

$$a \times a^{-1} = 1.$$

**Remark 2.2.18.**

The set of units in a ring  $R$  becomes a group under multiplication. This group is known as the group of units of  $R$ .

**Definition 2.2.19. (Integral Domain)**

Let us consider a commutative ring  $(R, +, \times)$ . A nonzero element  $r_1 \in R$  is known as a zero divisor such that

$$r_1 \times r_2 = 0,$$

for a nonzero element  $r_2 \in R$ . An integral domain is a commutative ring with no zero divisors.

**Definition 2.2.20. (Division Ring)**

If a set  $R$  satisfies the following conditions:

1.  $R$  is an abelian group under addition.
2.  $R \setminus \{0\}$  forms a group under multiplication.
3. Distributivity of addition over multiplication holds.

**Definition 2.2.21. (Groupring)**

Let us consider a ring  $R$  and a group  $G$ . Then we define a groupring [25]  $GR$  as the set of all linear combinations  $\gamma$  of the form

$$\gamma = \sum_{g \in G} b_g g, \tag{2.7}$$

where  $b_g \in R$ . There are finitely many of the  $b_g$ 's  $\neq 0$ . For  $\gamma$  and  $\delta$  in  $GR$ , using Equation (2.7), the sum and product in groupring is defined as

$$\gamma + \delta = \sum_{g \in G} b_g g + \sum_{g \in G} d_g g = \sum_{g \in G} (b_g + d_g) g \quad (2.8)$$

$$\gamma \delta = \left( \sum_{g \in G} b_g g \right) \left( \sum_{h \in G} d_h h \right) = \sum_{g, h \in G} b_g d_h gh \quad (2.9)$$

respectively. Rewrite Equation (2.9), we get

$$\gamma \delta = \sum_{v \in G} E_v v, \quad \text{where} \quad E_v = \sum_{gh=v} b_g d_h.$$

Here we note that groupring  $GR$  is a ring with addition and multiplication defined in Equation (2.8) and Equation (2.9) respectively. We can also define multiplication as if  $\gamma \in GR$  and  $\rho \in R$ , then

$$\rho \gamma = \rho \sum_{g \in G} b_g g = \sum_{g \in G} (\rho b_g) g.$$

If both the ring  $R$  and group  $G$  are finite, then the associated groupring is also finite. The number of elements in a finite groupring can be find out using the following lemma.

**Lemma 2.2.22.** [12]

“Let  $R$  be a ring of order  $m$  and  $G$  a group of order  $n$ . Then  $GR$  is a finite groupring of size  $|R|^{|G|} = m^n$ ”.

For more details on the structure of groupring, we refer to [22, 45].

**Example 2.2.23.**

Consider the following:

$$R = \mathbb{Z}_3 = \{0, 1, 2\} \text{ and } G = C_2 = \{1, y\} = \langle y \rangle = \langle y : y^2 = 1 \rangle.$$

Then we list all the elements of groupring  $\mathbb{Z}_3[C_2]$ .

Here

$$|\mathbb{Z}_3| = 3 \text{ and } |C_2| = 2.$$

By using the Lemma 2.2.22, we have  $3^2 = 9$  elements in  $\mathbb{Z}_3[C_2]$ . By definition

$$\mathbb{Z}_3[C_2] = \left\{ \sum_{g \in C_2} a_g g : a_g \in \mathbb{Z}_3 \right\}$$

$$GR = \mathbb{Z}_3[C_2] = \{0, 1, y, 2y, 1 + y, 1 + 2y, 2, 2 + y, 2 + 2y\}$$

Let us construct the Cayley's tables for  $\mathbb{Z}_3[C_2]$ .

TABLE 2.3: Cayley's tables for addition

+	0	1	y	2y	1 + y	1 + 2y	2	2 + y	2 + 2y
0	0	1	y	2y	1 + y	1 + 2y	2	2 + y	2 + 2y
1	1	2	1 + y	1 + 2y	2 + y	2 + 2y	0	y	2y
y	y	1 + y	2y	0	1 + 2y	1	2 + y	2 + 2y	2
2y	2y	1 + 2y	0	y	1	1 + y	2 + 2y	2	2 + y
1 + y	1 + y	2 + y	1 + 2y	1	2 + 2y	2	y	2y	0
1 + 2y	1 + 2y	2 + 2y	1	1 + y	2	2 + y	2y	0	y
2	2	0	2 + y	2 + 2y	y	2y	1	1 + y	1 + 2y
2 + y	2 + y	y	2 + 2y	2	2y	0	1 + y	1 + 2y	1
2 + 2y	2 + 2y	2y	2	2 + y	0	y	1 + 2y	1	1 + y

From TABLE 2.3, it is clear that  $(\mathbb{Z}_3[C_2], +)$  is a group.

TABLE 2.4 shows that  $(\mathbb{Z}_3[C_2], \cdot)$  is not a group as  $1 + y$  has no multiplicative inverse.

Further details and properties on groupring can be seen in Chapter 5.

**Definition 2.2.24. (Field)**

A division ring which is also commutative is a field.

**Example 2.2.25.**

1. Set of integers  $\mathbb{Z}$ , set of Gaussian integers  $\mathbb{Z}[i] = \{m + in : m, n \in \mathbb{Z}\}$  and set of complex numbers  $\mathbb{C}$  are the well known examples of rings.

TABLE 2.4: Cayley’s Table for Multiplication

$\cdot$	0	1	$y$	$2y$	$1 + y$	$1 + 2y$	2	$2 + y$	$2 + 2y$
0	0	0	0	0	0	0	0	0	0
1	0	1	$y$	$2y$	$1 + y$	$1 + 2y$	2	$2 + y$	$2 + 2y$
$y$	0	$y$	1	2	$1 + y$	$2 + y$	$2y$	$1 + 2y$	$2 + 2y$
$2y$	0	$2y$	2	1	$2 + 2y$	$1 + 2y$	$y$	$2 + y$	$1 + y$
$1 + y$	0	$1 + y$	$1 + y$	$2 + 2y$	$2 + 2y$	0	$2 + 2y$	0	$1 + y$
$1 + 2y$	0	$1 + 2y$	$2 + y$	$1 + 2y$	0	$2 + y$	$2 + y$	$1 + 2y$	0
2	0	2	$2y$	$y$	$2y$	$2 + y$	1	$1 + y$	$1 + y$
$2 + y$	0	$2 + y$	$1 + 2y$	$2 + y$	0	$1 + 2y$	$1 + y$	$2 + y$	0
$2 + 2y$	0	$2 + 2y$	$2 + 2y$	$1 + y$	$1 + y$	0	$1 + y$	0	$2 + 2y$

2.  $\mathbb{Z}$  and  $\mathbb{Z}[i]$  are the examples of integral domain which are not field.
3.  $(\mathbb{Z}_n, +, \cdot)$  is a ring.
4.  $\mathbb{Z}_6$  is a ring which is not an integral domain because 2 and 3 are zero divisors.
5. The set of rational numbers  $\mathbb{Q}$ , the set of complex numbers  $\mathbb{C}$  and set of real numbers  $\mathbb{R}$  are field.

The relationship between the above defined algebraic structures is given in the FIGURE 2.1.

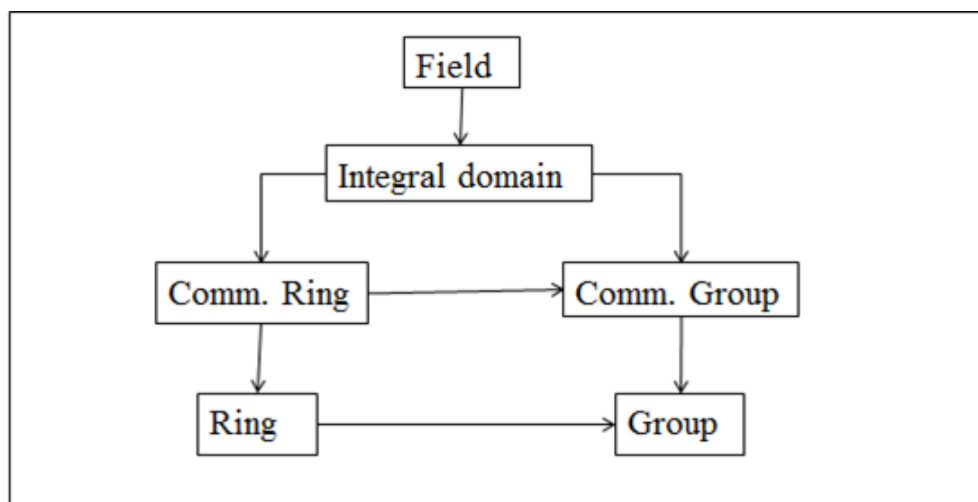


FIGURE 2.1: Relationship Between Algebraic Structures

### 2.2.1 Algebra of Matrices

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

**Definition 2.2.26. (Matrix)**

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

$$\begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1j} & \cdots & r_{1n} \\ r_{21} & r_{22} & \cdots & r_{2j} & \cdots & r_{2n} \\ \vdots & \vdots & \cdots & \vdots & \cdots & \vdots \\ r_{i1} & r_{i2} & \cdots & r_{ij} & \cdots & r_{in} \\ \vdots & \vdots & \cdots & \vdots & \cdots & \vdots \\ r_{m1} & r_{m2} & \cdots & r_{mj} & \cdots & r_{mn} \end{bmatrix}.$$

Matrices are usually identified by capital letters such as  $A, B$  etc. Instead of writing all the elements in rectangular array, it is convenient to write the abbreviated notation as:

$$A = [a_{ij}]_{m \times n},$$

where  $a_{ij}$  denotes the entry in the  $i$ th row and  $j$ th column of the matrix. The matrix which has  $m$  rows and  $n$  columns is called “rectangular matrix ”of order  $m \times n$  and if  $m = n$ , then  $A$  is known as “square matrix ”. If each element of diagonal is an element  $t \in R$  in a square matrix then it is known as “scalar matrix ”of order  $n$  and is written as:

$$\begin{bmatrix} t & 0 & 0 & \cdots & 0 \\ 0 & t & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & t \end{bmatrix}.$$

In scalar matrix if we take  $t = 1$ , then this matrix is called “identity matrix” of order  $n$  and is denoted by  $I_n$ .

### Addition of Matrices:

Let us consider two matrices  $A = [a_{ij}]$  and  $B = [b_{ij}]$  of order  $m \times n$  over a ring  $R$ . Then addition is defined as:

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

of order  $m \times n$ .

### Additive Inverse of a Matrices:

Let us consider an  $m \times n$  matrix  $A = [a_{ij}]$  so we can define  $-A = [-a_{ij}]$  of order  $m \times n$ . Then

$$A + (-A) = (-A) + A = 0.$$

$-A$  is known as additive inverse of  $A$ .

### Remark 2.2.27.

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

### Multiplication of Matrix by a Scalar:

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

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

### Multiplication of Matrices:

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

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

then

$$\begin{aligned} C &= AB \\ &= [a_{ij}][b_{ij}], \end{aligned}$$

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

$$\text{where } c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj} = \sum_{k=1}^n a_{ik}b_{kj}.$$

**Remark 2.2.28.** In general, matrices do not commute.

**Example 2.2.29.**

1. Collection of all the  $n \times n$  invertible matrices whose entries are from  $\mathbb{R}$  (real numbers) forms a group under usual operation of multiplication of matrices known as general linear group and is represented by  $GL(n, \mathbb{R})$ .
2. Collection of all square matrices  $M(n, R)$  forms a non-commutative ring.
3. Center of general linear group  $GL(n, R)$  forms a commutative subgroup, where

$$Z(GL(n, R)) = \{gI : g \in R\},$$

and  $I_n$  is an identity matrix of order  $n$ .

4. Let us consider the set  $\mathbb{R}$  and  $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ . Define  $\psi : GL(n, \mathbb{R}) \rightarrow \mathbb{R}^*$  by

$$\psi(B) = \det B, \quad \forall B \in GL(n, \mathbb{R})$$

Then  $\psi$  is a homomorphism.

5. Consider the group  $M(2, \mathbb{R})$  with entries from  $\mathbb{R}$  under addition and the group  $\mathbb{R}^4 = \{(a_1, a_2, a_3, a_4) : a_1, a_2, a_3, a_4 \in \mathbb{R}\}$  is abelian under addition. Define  $\psi : M(2, \mathbb{R}) \rightarrow \mathbb{R}^4$  by

$$\psi \left( \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \right) = (a_1, a_2, a_3, a_4).$$

Then  $\psi$  is an isomorphism.

6. The mapping  $\theta : M(2, \mathbb{R}) \rightarrow M(2, \mathbb{R})$  defined by

$$\theta \left( \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \right) = \begin{bmatrix} a_4 & a_3 \\ a_2 & a_1 \end{bmatrix}$$

is an automorphism.

## 2.2.2 Polynomial Rings

This section is devoted to recall a class of rings called the polynomial rings, describing computation, factorization and divisibility in such rings.

### Definition 2.2.30. (Polynomial)

Let  $R$  be a ring. An expression of the form

$$g(x) = b_n x^n + \cdots + b_2 x^2 + b_1 x + b_0,$$

where every  $b_i \in R$ ,  $b_n \neq 0$  for  $n \geq 0$ , is a polynomial in the indeterminate  $x$  over the ring  $R$ . The integer  $n$  is called the degree of  $g(x)$ . It is denoted by  $\deg g(x)$  and  $b_n$  is called the leading coefficient of  $g(x)$ .

1. If  $g(x) = b_0$  (a constant polynomial) then the degree of  $g(x)$  is 0.
2.  $g(x)$  is said to be a zero polynomial, if all the coefficients of  $g(x)$  are 0 and mathematically its degree is defined to be  $-\infty$ .
3. If the leading coefficient of  $g(x)$  is equal to 1 then the polynomial  $g(x)$  is said to be monic.

### Definition 2.2.31. (Polynomial Ring)

The set of all polynomials in one indeterminate  $x$  with coefficients in  $R$  is known as polynomial ring  $R[x]$ . The polynomial ring is a ring and the operations are simply defined as the ordinary polynomial multiplication and addition, with coefficient arithmetic performed in the ring  $R$ .

### Definition 2.2.32. (Irreducible)

Let us consider any polynomial ring  $\mathbb{F}[x]$  over a field  $\mathbb{F}$ . Let  $G(x)$  be any polynomial from  $\mathbb{F}[x]$ . Then  $G$  is called irreducible if it cannot be expressed as the product of two polynomials.



**Example 2.2.33.**

The polynomial  $x^2 + 1$  is irreducible over  $\mathbb{R}[x]$  but is reducible over  $\mathbb{C}[x]$ .

**Definition 2.2.34. (Division Algorithm for Polynomials)**

For two polynomials  $F(x)$  and non zero  $G(x)$ , the standard polynomial division of  $F(x)$  by  $G(x)$  gives a unique quotient and remainder polynomials  $Q(x)$  and  $R(x)$  respectively. Then  $F(x)$  is expressed as:

$$F(x) = Q(x)G(x) + R(x),$$

with  $\deg R(x)$  is less than  $\deg G(x)$ . The polynomial  $Q(x)$  is known as the quotient and  $R(x)$  is known as the remainder. Sometimes, the remainder of the division is denoted by

$$F(x) \pmod{G(x)},$$

and the quotient is denoted by

$$F(x)/G(x).$$

**Remark 2.2.35.**

If  $F(x), G(x) \in \mathbb{F}[x]$  then  $G(x)$  divides  $F(x)$ , written as

$$G(x)|F(x), \text{ if } F(x) \pmod{G(x)} = 0.$$

**2.2.3 Finite Fields**

In cryptography, we are interested in the fields with a finite number of elements and such fields are called Galois fields or finite fields. The total number of elements in the field is known as the cardinality or order of the field. The theorem given below has a fundamental importance:

**Theorem 2.2.36.** [43]

A field with order  $m$  only exists if  $m$  is a prime power, i.e.,  $m = p^n$ , for some

positive integer  $n$  and prime integer  $p$ . The integer  $p$  is called the characteristic of the finite field. Such finite fields are denoted by  $GF(p^n)$  or  $\mathbb{F}_{p^n}$ .

**Remark 2.2.37.**

There is no finite field with 45 elements because 45 cannot be written as a power of a prime. In fact,

$$45 = 3^2 \cdot 5.$$

Fields of prime order is the best example of a finite field, i.e., fields  $GF(p^n)$  with  $n = 1$ . The elements of the field  $GF(p)$  can be expressed as integers  $0, 1, \dots, p - 1$ . The operations of the field are defined as integer addition modulo  $p$  and integer multiplication modulo  $p$ . Thus  $GF(p) = \mathbb{Z}_p$ . When  $p = 2$ , we get the smallest finite field  $GF(2) = \mathbb{Z}_2 = \{0, 1\}$ . This field is very important from computer point of view as it corresponds to numbers in binary form. The addition operation is referred to as “exclusive Or (XOR)” and is denoted by  $\oplus$ , also called logical addition. Similarly, the multiplication in  $GF(2)$  is called logical multiplication. These arithmetic operations are performed as given in the TABLE 2.5.

TABLE 2.5: XOR Operation

$\oplus$	0	1
0	0	1
1	1	0

.	0	1
0	0	0
1	0	1

**Definition 2.2.38. (Extension Field)**

If  $E$  and  $F$  are fields and  $F \subseteq E$ , we say that  $F$  is an extension of  $E$ , and we write either  $E \leq F$  or  $E/F$ . For example  $\mathbb{C} = \{x + iy, x, y \in \mathbb{R}\}$  is an extension field of  $\mathbb{R}$ .

**Definition 2.2.39. (Extension Fields  $GF(2^m)$ )**

Since each element of this field can be characterized by one byte that’s why we are interested in this field. However, if the order of a finite field is not a prime just like  $2^8$  is clearly not a prime, the multiplication and addition operation cannot be expressed by multiplication and addition of integers modulo  $2^8$ . For  $m > 1$ , such

fields are known as extension fields. To do work in extension fields, we have to define two rules as:

1. Define some different notation for element of field.
2. Define different rules to do arithmetic with the field elements.

The elements of extension fields can be expressed as polynomials, and the calculations in the field  $GF(p^m)$  can be obtained by doing simple polynomial arithmetic and coefficient arithmetic is performed modulo  $p$ . The polynomials can get maximum degree of  $m - 1$ , so that there are total  $m$  coefficients for each element.

1. *Extension field addition and subtraction:*

Let  $F(x), G(x) \in GF(2^m)$ . The sum of the two elements is calculated as:

$$H(x) = F(x) + G(x) = \sum_{i=0}^{m-1} h_i x^i, \quad h_i \equiv (f_i + g_i) \pmod{2}, \quad (2.10)$$

and difference is calculated as:

$$H(x) = F(x) - G(x) = \sum_{i=0}^{m-1} h_i x^i, \quad h_i \equiv (f_i - g_i) \equiv (f_i + g_i) \pmod{2}. \quad (2.11)$$

2. *Extension field multiplication:*

In  $GF(2^8)$ , multiplication is the major operation. Firstly, two elements should be expressed as polynomials of a finite field  $GF(2^m)$  and then multiply them by using the standard polynomial multiplication rule:

$$F(x) \cdot G(x) = (f_{m-1}x^{m-1} + \dots + f_0) \cdot (g_{m-1}x^{m-1} + \dots + g_0)$$

$$H(x) = h_{2m-2}x^{2m-2} + \dots + h_0, \quad (2.12)$$

where

$$h_0 = f_0 g_0 \pmod{2}, \quad (2.13)$$

$$h_1 = (f_0 g_1 + f_1 g_0) \pmod{2}, \quad (2.14)$$

$\vdots$

$$h_{2m-2} = f_{m-1}g_{m-1} \pmod{2}. \tag{2.15}$$

All the coefficients  $f_i, g_i, h_i \in GF(2)$  and the arithmetic of coefficient is also done in  $GF(2)$ . In general, after multiplication as defined in Equation (2.12)  $x$  will obtain a higher degree than  $m - 1$  which has to be reduced. In prime fields  $GF(p)$ , the similar approach has to be done in multiplication i.e., we just multiplied the two integers and then the resultant is divided by a prime, and consider the remainder only. Similarly is the case with the field  $GF(2^m)$ . The product of the multiplication is divided by a certain polynomial, and after the polynomial division we consider the remainder only. For the module reduction, the basic need is irreducible polynomials. We have already defined that irreducible polynomials have the properties of prime numbers, i.e., the factors of polynomial are itself and 1 only.

Let  $F(x), G(x) \in GF(2^m)$  and let

$$Q(x) \equiv \sum_{i=0}^m q_i x^i, \quad q_i \in GF(2^m) \tag{2.16}$$

be any irreducible polynomial. The multiplication of polynomials  $F(x)$  and  $G(x)$  is done as follows:

$$H(x) \equiv F(x) \cdot G(x) \pmod{Q(x)}. \tag{2.17}$$

Thus, an irreducible polynomial  $Q(x)$  is a basic requirement for the field  $GF(2^m)$  of degree  $m$  with coefficients from  $GF(2)$ .

### 3. Inversion in $GF(2^m)$

Let us consider a finite field  $GF(2^m)$  and the corresponding irreducible polynomial  $Q(x)$ . Let  $F \in GF(2^m)$  be a non zero element, then its inverse  $F^{-1}$  is defined as:

$$F^{-1}(x) \cdot F(x) = 1 \pmod{Q(x)}.$$

To find the inverse of polynomial  $F(x)$  modulo  $Q(x)$ , we use the Extended Euclidean Algorithm which is defined as follows:

**Algorithm 2.2.40.**

**Input:** Two Polynomials  $F(x)$  and  $Q(x)$

**Output:** Inverse of  $F(x) \pmod{Q(x)}$

1.  $[F_1(x), F_2(x), F_3(x)] \leftarrow [1, 0, Q(x)]; [H_1(x), H_2(x), H_3(x)] \leftarrow [0, 1, F(x)]$
2. if  $H_3(x) = 0$  return  $F_3(x) = \gcd[Q(x), F(x)];$  There is no inverse
3. if  $H_3(x) = 1$  return  $H_3(x) = \gcd[Q(x), F(x)]; H_2(x) = (F(x))^{-1} \pmod{Q(x)}$
4.  $Q_1(x) = F_3(x) / H_3(x)$
5.  $[G_1(x), G_2(x), G_3(x)] \leftarrow [F_1(x) - Q_1(x)H_1(x), F_2(x) - Q_1(x)H_2(x), F_3(x) - Q_1(x)H_3(x)]$
6.  $[F_1(x), F_2(x), F_3(x)] \leftarrow [H_1(x), H_2(x), H_3(x)]$
7.  $[H_1(x), H_2(x), H_3(x)] \leftarrow [G_1(x), G_2(x), G_3(x)]$
8. return to step 2.

**Example 2.2.41.**

Let us consider the finite field  $GF(2^4)$ . Let  $F(x), G(x) \in GF(2^4)$  such that  $F(x) = x^3 + x + 1$  and  $G(x) = x^2 + x + 1$ . Then addition and multiplication is as follows:

$$F(x) + G(x) = ((1 + 0)x^3 + (0 + 1)x^2 + (1 + 1)x + 1 + 1) \pmod{2}.$$

$\therefore$  By using Equation (2.11), we have

$$H(x) = (x^3 + x^2) \pmod{2}.$$

$$x^0 : f_0g_0 = (1)(1) \pmod{2} = 1 \pmod{2}$$

$$\begin{aligned}
x^1 & : f_0g_1 + f_1g_0 \\
& = (1.1 + 1.1) \pmod{2} \\
& = 0 \pmod{2}
\end{aligned}$$

$$\begin{aligned}
x^2 & : f_0g_2 + f_1g_1 + f_2g_0 \\
& = (1.1 + 1.1 + 0.1) \pmod{2} \\
& = 0 \pmod{2}
\end{aligned}$$

$$\begin{aligned}
x^3 & : f_0g_3 + f_1g_2 + f_2g_1 + f_3g_0 \\
& = (1.0 + 0.1 + 1.1 + 1.1) \pmod{2} \\
& = 0 \pmod{2}
\end{aligned}$$

$$\begin{aligned}
x^4 & : f_0g_4 + f_1g_3 + f_2g_2 + f_3g_1 + f_4g_0 \\
& = (1.0 + 1.0 + 0.1 + 1.1 + 0.1) \pmod{2} \\
& = 1 \pmod{2}
\end{aligned}$$

$$\begin{aligned}
x^5 & : f_0g_5 + f_1g_4 + f_2g_3 + f_3g_2 + f_4g_1 + f_5g_0 \\
& = (1.0 + 1.0 + 0.0 + 1.1 + 0.1 + 0.1) \\
& = (1) \pmod{2}
\end{aligned}$$

Hence by using Equations (2.13-2.15), we get Equation (2.12) as

$$H(x) = x^5 + x^4 + 1.$$

Let  $Q(x) = x^4 + x + 1 \in GF(2^4)$  be an irreducible polynomial, then by using Equation (2.17) we have

$$H(x) = x^2 \pmod{Q(x)}$$

**Remark 2.2.42.** [43]

Note that in an extension field  $GF(p^n)$ , all polynomials are not reducible. For

instance, the polynomials

$$F_1(x) = x^3 + x; \quad F_2(x) = x^3; \quad F_3(x) = x^4 + x^3 + x^2,$$

are not reducible in  $GF(p^5)$ .

# Chapter 3

## Cryptographic Preliminaries

This chapter mainly concerns with the fundamental concepts involved in cryptography. Moreover these basic definitions and concepts are helpful to understand this study. First we discuss with the primitives of cryptography, its applications and characterizations. After that some public key cryptosystems are given in detail.

### 3.1 Primitives of Cryptology

Before going into deep study, we should know about the important ingredients of cryptosystem. Recall that cryptology is the science of secret communications. That is two parties have to share information over a public network in such a way that other than the intended receiver can see that information or message.

Plaintext is the message which has to be encrypted. By using encryption algorithm, the converted form of data is called a ciphertext, which cannot be easily understood by any unauthorized person. In cryptography, a piece of information which concludes the functional output of a cipher or cryptographic algorithm is known as key. Without using key, the algorithm would not create any useful result. In encryption a key identifies the specific conversion of plaintext message into ciphertext, or vice versa during decryption. To understand the message, the



process of converting the ciphertext back into corresponding plaintext is called the decryption algorithm or simply decryption.

### 3.1.1 Characterizations of Cryptosystems

Symmetric/secret key cryptography and asymmetric/public key cryptography are the two main branches of cryptography. In secret key cryptography, the key which is used to encrypt and decrypt the data is shared between two (or more) parties. The security of secret key cryptography relies on keeping the key secret by each communicating party. The secret key cryptography is a typical symmetric key cryptosystem describes in FIGURE 3.1. The well known examples of symmetric key cryptography are Data Encryption Standard (DES) [11] and Advanced Encryption Standard (AES) [13]. On the other hand in public key cryptosystem, a

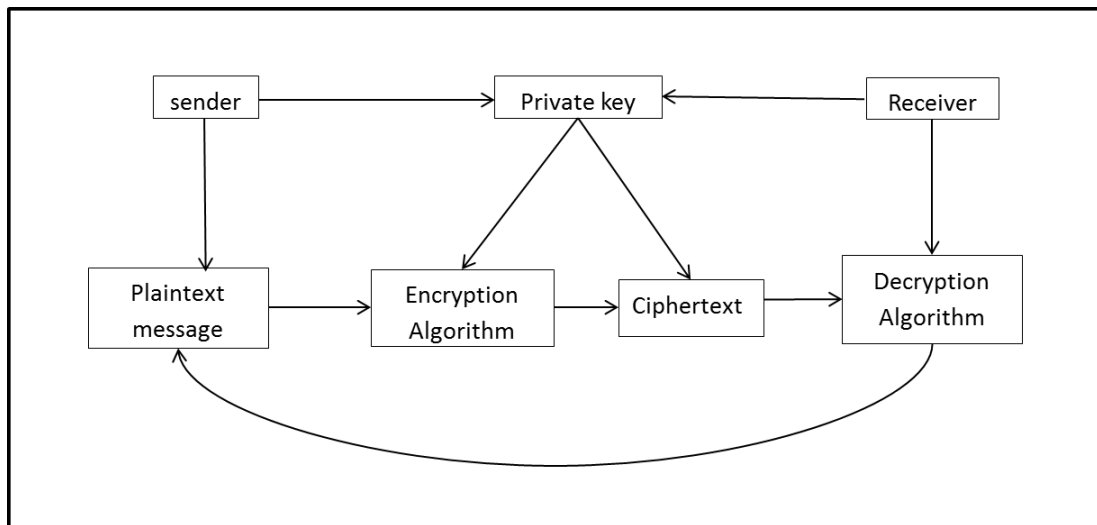


FIGURE 3.1: Symmetric Cryptosystem

pair of keys for each communicating party is being used. In this pair one key is “public” and other is “secret”. In asymmetric cryptography, both parties know the public key whereas the secret key is only known to its owner and must be kept confidential. The most important examples of public key cryptosystems are Rivest-Shamir-Adleman(RSA) [48] and ElGamal [17] and Elliptic curve cryptography [37].

In cryptographic algorithms an important difference is between the way a message is handled.

1. *Stream ciphers* convert one bit of plaintext into a bit of ciphertext directly. Caesar Cipher, Affine Caser Cipher and Vigenere Cipher and RC4 [49] are examples of a stream cipher, which is useful in small or mobile devices.
2. *Block ciphers* encrypt a group of plaintext symbols as one block at a time. Transposition, Hill Cipher, Playfair Cipher, DES and AES are the examples of block ciphers.

### 3.1.2 Cryptographic Applications

The main objective of cryptography is not only providing just confidentiality but it is also used to give the best solutions for the other problems.

#### **Confidentiality:**

Confidentiality means to keep the information secret from unauthorized parties.

#### **Data Integrity:**

Data integrity means to protect the message from being altered during the transmission by unauthorized person. This modification may be accidentally or intentionally. The recipient of a message has the ability to detect the manipulation of a data from unauthorized person.

#### **Authentication:**

This is a service which is related to identification. The parties which are initiating a communication should identify each other.

#### **Non-repudiation:**

This is a service which thwarts the sender from denying the actions or commitments later on.

## 3.2 Public Key Cryptography

Since 1976, as a result of the development of public key cryptography [16], many applications of number theory and algebra have arisen. Recall from the introduction defined earlier that, for encryption or decryption of a message a pair of keys i.e., (public and private key) is used in public key cryptography or asymmetric cryptography so that message arrives securely. Initially, a certificate authority gives public and private key pair to a network user. Any other user who wishes to send a ciphertext can get the intended recipient's public key from a public directory. This key was used to encrypt the message, and after encryption they send it to the recipient. After receiving the message by the recipient, they decrypt it with their own secret/private key.

### 3.2.1 General Scheme For Public Key Cryptosystem

A public key cryptosystem mainly depends upon the following components

$$(P, C, K, E, D),$$

where

1. A possible finite set of plaintexts is denoted by  $P$ , also known as the message space.
2.  $C$  is a possible finite set of ciphertexts, that is, the ciphertext space.
3. The Set  $K$  is called the key space and the elements of that key space are called keys.
4. For every  $k \in K$ , there is a rule  $e \in E$  for encryption and a corresponding rule  $d \in D$  for decryption. So every  $e : P \rightarrow C$  and  $d : C \rightarrow P$  are the functions such that

$$d(e(m)) = m, \tag{3.1}$$

for each plaintext  $m \in P$ .

**Key Generation:**

It is computationally easy to generate a pair  $(P_k, P_R)$ . Further, given a public key  $P_k$ , it is computationally infeasible to find the corresponding secret key  $P_R$ .

**Encryption:**

In encryption, given public key  $P_k$  and the plaintext  $m$ , it is easy to calculate the ciphertext as

$$C = e(P_k, m). \quad (3.2)$$

**Decryption:**

1. In decryption, given private key  $P_R$  and ciphertext  $C = e(P_k(m))$ , it is simple to calculate plaintext  $m$ .
2. To get the original plaintext  $m$  from  $C$  without  $P_R$  is infeasible.
3. Decrypt

$$d(P_R, C) = m. \quad (3.3)$$

The general scheme of public key cryptosystem is describe in the FIGURE (3.2).

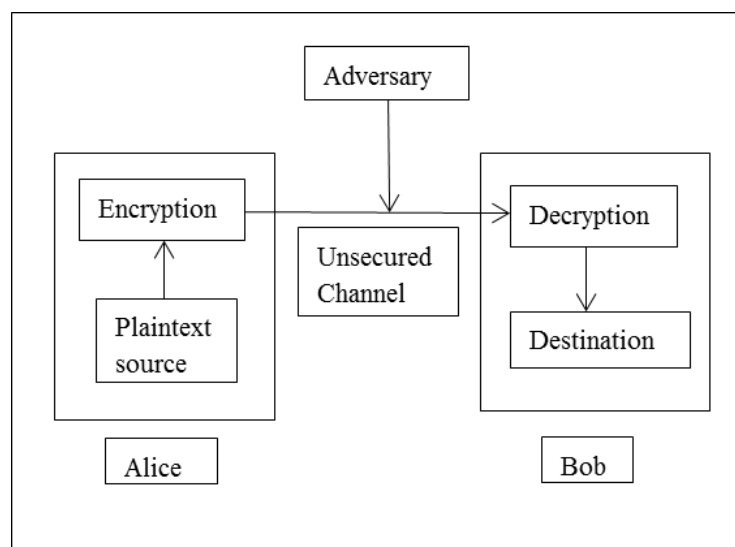


FIGURE 3.2: General Scheme For Public Key Cryptosystem

A one way function and its trapdoor information takes a very important role in public key cryptography. It is defined as follows:

**Definition 3.2.1. (One-Way and Trapdoor Function)**

A function  $f : A \rightarrow B$  is known as one way function, if  $f(a)$  is easy to calculate  $\forall a \in A$  but for “virtually all” elements  $b \in B$  it is “computationally infeasible” to find any  $a \in A$  such that  $f(a) = b$ . A trapdoor one way function is a one way function  $f : A \rightarrow B$  with the property which gives auxiliary information (called the trapdoor information), so that it becomes feasible to find for any given  $b \in B$ , an element  $a \in A$  such that  $f(a) = b$  as shown in FIGURE (3.3)

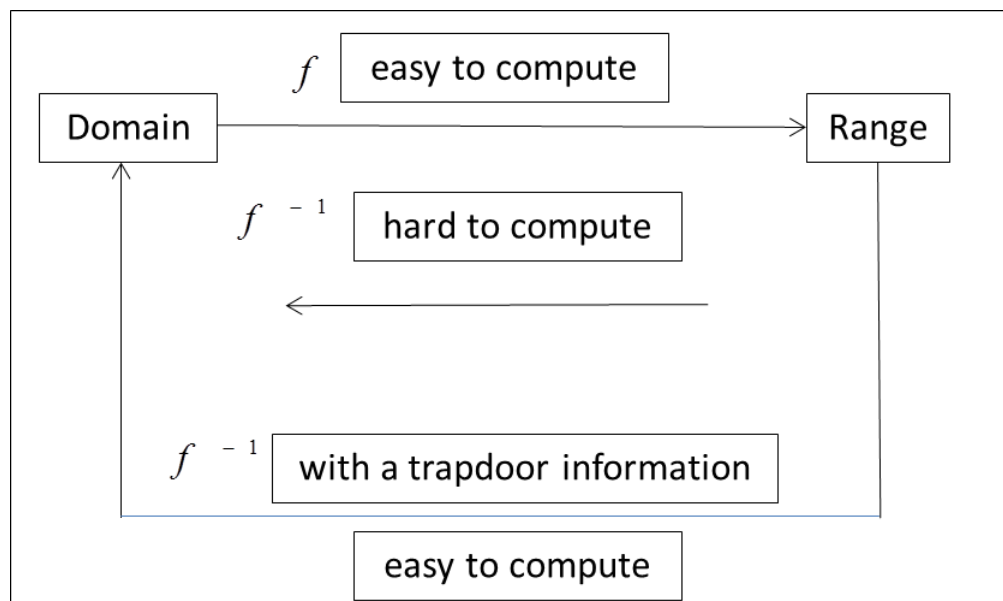


FIGURE 3.3: One-Way Trapdoor Function

The Diffie-Hellman key exchange protocol was the first asymmetric scheme for creating a shared secret information over an unsecured communication channel. It gives a solution to the problem of key distribution, that allows two communicating parties (say Alice and Bob) to develop a common secret key over an open channel. The underlying hard problem is the complexity of discrete logarithm problem in  $\mathbb{Z}_p$ . That is, given a prime  $p$ , a generator  $\beta$  of  $\mathbb{Z}_p$  and an element  $\alpha \in \mathbb{Z}_p$ , finding an integer  $k$ , such that  $\beta^k \equiv \alpha \pmod{p}$  where  $0 \leq k \leq p - 2$  is called the discrete logarithm problem.

**Protocol 3.2.2. (Diffie-Hellman Protocol)****Global Parameters**

A large prime  $p$  (atleast 512 bits) and  $g \pmod p$  (a primitive root).

1. Alice picks randomly  $a > 0$  (secret integer) and presents  $g^a \pmod p$  to Bob. Similarly Bob randomly chooses  $b > 0$  (secret integer) and sends  $g^b \pmod p$  to Alice.
2. After receiving  $g^b \pmod p$  Alice calculates

$$K_A = (g^b)^a \pmod p = g^{ba} \pmod p,$$

and similarly Bob receives  $g^a \pmod p$  and calculates

$$K_B = (g^a)^b \pmod p = g^{ab} \pmod p.$$

Since  $\mathbb{Z}_p$  is abelian, so

$$ab = ba.$$

After step 2, both Bob and Alice have the same secret shared key  $K$  for secure communication

$$K = K_A \pmod p = K_B \pmod p.$$

The illustration of protocol is shown in FIGURE 3.4. Note that to find  $a$  from  $g^a \pmod p$  and  $b$  from  $g^b \pmod p$ , the adversary has to solve the discrete logarithm problem. The lack of authentication is very serious problem of Diffie Hellman protocol. Man in the middle attacks [42] is one of the attacks on Diffie-Hellman. In this type of attack, an attacker shows himself as Bob and takes information from Alice and then he shows himself as Alice and takes information from Bob. So in this way, an cryptanalyst can compromise the communication between Alice and Bob and get the secret key. This protocol is suitable for use in data communication.

In 1978, Rivest, Shamir, and Adleman [48] gave the idea of the first practical public-key encryption and signature scheme and now it is known as RSA. The

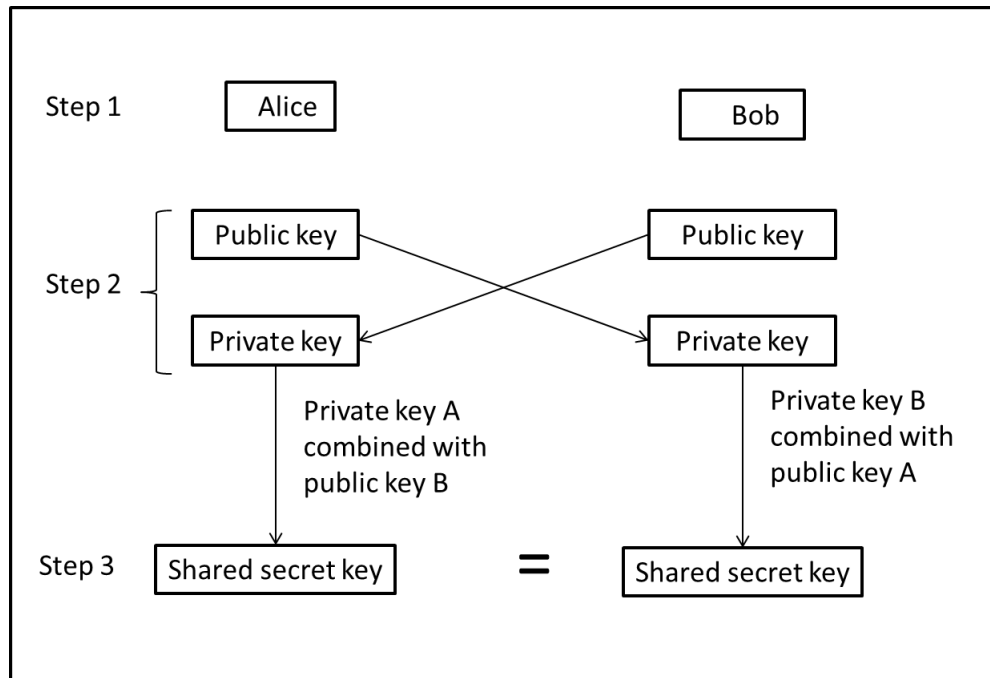


FIGURE 3.4: Diffie-Hellman Key Exchange

mathematical underlying hard problem of RSA scheme is the complexity of factoring large integers and it is called the integer factorization problem (IFP). This application of a said hard problem to cryptography gives fruitful efforts to find out more effective and efficient methods to factor. In this area major advances have been seen in 1980's, but no one can prove that the RSA cryptosystem is insecure.

### Cryptosystem 3.2.3. (RSA Cryptosystem)

The security of RSA depends on difficulty of factoring large integers. It is one of the most famous public key cryptosystem, which is extensively used in hardware and software to secure electronic data transport.

Creating two randomly large primes  $p_1$  and  $q_1$  of approximately same size such that the essential bit length of the product  $N_1 = p_1q_1$  is 1024 bits.

#### Key Generation

1. Alice chooses two randomly large primes  $p_1$  and  $q_1$  of equal size and computes

$$N_1 = p_1q_1 \text{ and}$$

$$\varphi(N_1) = (p_1 - 1)(q_1 - 1), \quad (3.4)$$

2. She picks an integer  $e$ ,  $1 < e < \varphi(N_1)$ , such that

$$\gcd(e, \varphi(N_1)) = 1. \quad (3.5)$$

Equation (3.5) gives us the surety that the inverse of  $e \pmod{N_1}$  exists.

3. She calculates the secret exponent  $d$ ,  $1 < d < \varphi(N_1)$  by using Algorithm 2.1.4, such that

$$ed \equiv 1 \pmod{\varphi(N_1)}$$

4. The public key is

$$K_{pu} = (N_1, e) \quad (3.6)$$

and the private key

$$K_{pr} = (d, p_1, q_1). \quad (3.7)$$

### Encryption

Now Bob chooses the plaintext message  $M$ . He picks the Alice's public key and encrypts the message as

$$C = M^e \pmod{N_1}, \quad (3.8)$$

and present it to Alice.

### Decryption

To get the original plaintext  $M$ , Alice calculates

$$M = C^d \pmod{N_1}, \quad (3.9)$$

by using her own private key  $d$ .

Due to the increasing computing power more efficient factoring algorithms are also discovered and the capability to factor very large numbers has also increased. Encryption strength is directly tied to key size, and doubling key length delivers an exponential increase in strength, although it does impair performance. The



key size of RSA is usually 1024 or 2048 bits long, but experts believe that in the near future, 1024-bit key size could be broken. This is the reason that the industry and government are moving to choose the minimum key size of about 2048-bits. Barring an unforeseen breakthrough in quantum computing, it should be many years before longer keys are required. It can generate smaller, faster, and more efficient cryptographic keys. Finally, a researchers team comprised with Adi Shamir and a co-inventor of RSA, has successfully finds key size of about 4096-bit using acoustic cryptanalysis.

ElGamal found another class of practical public-key schemes and it is also based on the discrete logarithm problem.

#### **Cryptosystem 3.2.4. (The ElGamal Cryptosystem)**

Like RSA, Taher ElGamal [17] presented a public key cryptosystem in 1985. ElGamal utilizes the Diffie-Hellman protocol so that it can be used as an encryption-decryption algorithm. In this cryptosystem, the decryption key is kept private while encryption key is published. The underlying mathematical hard problem of this public key cryptosystem is discrete logarithm problem which is discussed in Section 3.2.2. For sufficiently large prime modulus, ElGamal cryptosystem is thought to be secure.

#### **Global Parameters**

A large prime  $p$  (atleast 512 bits) and generator of multiplicative group  $g$  modulo  $p$ .

Alice generates the public/private key pair as follows:

#### **Key Generation**

1. She chooses any random integer  $b$  such that,  $b \in \{1, 2, \dots, p-2\}$ , and computes

$$A = g^b \pmod{p}.$$

2. The public key of Alice is

$$(p, g, A),$$

and her private key is  $b$ .

### Encryption

Bob encrypts the plaintext  $m$  and sends to Alice

1. Bob gets Alice authentic public key  $(p, g, A)$ .
2. He represents the plaintext as integers  $m$  in the range  $\{0, 1, 2, \dots, p - 1\}$ .
3. Then he selects any random integer  $k$ ,

$$k \in \{1, 2, \dots, p - 2\}.$$

4. He computes

$$c_1 = g^k \pmod{p}, \text{ and}$$

$$c_2 = mA^k \pmod{p}.$$

5. Finally he sends ciphertext

$$C = (c_1, c_2)$$

to Alice.

### Decryption

Alice receives encrypted message  $C$  from Bob and follows the following steps to get the original plaintext/message  $m$ .

- 1 She uses her private key  $b$  to compute

$$y = c_1^b \pmod{p}$$

**2** Finally she finds the plaintext  $m$  by computing

$$m = y^{-1}c_2 \pmod{p}.$$

All the algorithms that is, RSA, Diffie Hellman and ElGamal are based on number theory (commutative groups). There is need to move towards the development of new cryptosystem, that are believed to be as secure on a quantum computer as on a conventional computer (machine). The conjugacy search problem (CSP) is a generalization of DLP. DLP is defined on integers whereas CSP is defined on groups. ElGamal suggested braid groups as platform because CSP is meaningful in such problems[1, 30].

### 3.3 Cryptanalysis

The art of examining cryptographic schemes is called cryptanalysis. This examination includes the understanding of working of these schemes and analyzing them that how these schemes can be broken. In simple words we can say that to find the weakness in the implementation rather than algorithms. To understand the cryptography in a practical way, cryptanalysis is a very important part because it gives the deep knowledge about the encryption functions and also its weaknesses which exists in their implementations. In the past, cryptanalyst only try to get the key which involves in the encryption algorithm rather to decrypt a message. But now the main attention of a cryptanalyst has been shifted from solving ciphers and investigating the technique used in the encryption to rather solving difficulties in mathematics, to determine the best computationally effective method of examining a ciphertext. Over the years on cryptographic protocols and primitives, several types of attacks have been identified . How an adversary mount these attacks are classified as follows:

An attack in which attacker only observe the communication channel is known as the passive attack. In this attack adversary just threatens the data confidentiality.

An attack, where the attacker tries to add, delete or alter the transmission on the channel in some other way is known as active attack. In this attack adversary threatens authentication, confidentiality and data integrity as well. To deduce the plaintext from ciphertext, an active attack is divided into more specialized attacks which are described in the next section.

### 3.3.1 Attacks on Encryption Schemes

Cryptanalytic attacks [60] are generally classified into different categories that distinguish the kind of information a cryptanalyst has available to mount an attack. In all cases without having any additional information, the main aim of the cryptanalyst is to be capable to decrypt new pieces of ciphertext. To extract the secret key is ideal for an attacker.

#### **Ciphertext Only Attack:**

The ciphertext only attack is most common, but due to lack of information it is also the most difficult. In this attack, the cryptanalyst tries to find out the plaintext or decryption key by only observing the ciphertext.

#### **Known Plaintext Attack:**

In this type of attack, a cryptanalyst has a large number of plaintext corresponding ciphertext. A known plaintext attack is usually a little bit hard to mount.

#### **Chosen Plaintext Attack:**

The chosen plaintext attack is completely changed from known plaintext attack because in this attack the cryptanalyst can select which plaintext has to be encrypted. Then he later examines the relationship of the output ciphertext to get the key which is used for encryption. This is the stronger attack because the attacker has more control of the operation.

**Chosen Ciphertext Attack:**

The chosen ciphertext attack is generally related with the decryption process where the adversary has got short term access to the decryption algorithm (but not key). He then chooses a string of ciphertext to construct the corresponding string of plaintext. From these pieces of information, a cryptanalyst tries to recover the secret key.

**Brute Force Attack:**

The method of searching the key from key space until the cryptanalyst gets the original plaintext message is called the brute force attack that is personal identification number or user password. In this type of attack, consecutive guesses are generated by automated software. as to the value of the desired data. For a symmetric ciphers, the rough indication with respect to brute force attack describes in TABLE 3.1 and for public-key algorithms like RSA, ElGamal and ECC is given in the TABLE 3.2 for different security levels [43].

“

TABLE 3.1: Estimated Time for Successful Brute Force Attack on symmetric Algorithms With Different Key Lengths

Key Length	Security Estimation
56 – 64 bits	short term: a few hours or days
112 – 128 bits	Long Term: Several decades in the absence of quantum computers
256 bits	Long Term: Several decades even with quantum computers
	that can run the currently known quantum computing algorithms

There are two two fundamentally different ways by which ciphers may be secure:

*Unconditional security* means no matter how much resources and computer power we have, the cryptosystem cannot be broken.

*Computational security* means if we have limited computing resources (e.g time needed for calculations is greater than age of the universe), the cryptosystem cannot be broken.

TABLE 3.2: Bit Lengths of Public-Key Algorithm

Algorithm Family	Cryptosystem	Security Level (bit)			
		80	128	192	256
Integer factorization	RSA	1024 bit	3072 bit	7680 bit	15360 bit
Discrete logarithm	DH, DSA, ElGamal	1024 bit	3072 bit	7680 bit	15360 bit
Elliptic curves	ECDH, ECDSA	160 bit	256 bit	384 bit	512 bit
Symmetric keys	AES, 3DES	80 bit	128 bit	192 bit	256 bit

”

### 3.4 Public Key Cryptography Based on Groups

In this section, we discuss some particular problems of group theory, which has very importance in cryptography.

#### Definition 3.4.1. (Decision problems)

We are given a property  $Q$  and any item  $I$ . To find whether or not the item  $I$  has the property  $Q$  is called the decision problem.

#### Definition 3.4.2. (Search problems)

Given a property  $Q$  and the information that there are more items which have the property  $Q$ . To find at least one that main item which has the property  $Q$  is known as the search problem.

#### Definition 3.4.3. (The conjugacy search problem (CSP))

Let us consider a group  $G$  and two elements  $g_1$  and  $g_2$  such that  $g_1, g_2 \in G$  and the fact that

$$g_2 = g_1^y = y^{-1}g_1y, \quad (3.10)$$

for some  $y \in G$  to find atleast an element  $y$  is called the conjugacy search problem.

#### Definition 3.4.4. (The word problem (WP))

It is a recursive presentation of a group  $G$  and an element  $g \in G$ , find out whether or not  $g = 1$  in  $G$ . In word problem, the description consists of two parts: “whether” and “not”. We call them the “yes” and “no” parts of the word problem, respectively.

Here we are going to describe two key establishment protocols. We have shown that the solution of CSP is unnecessary for a cryptanalyst to find out the secret key (common) in Ko-Lee and Anshel Anshel Goldfeld protocol.

**Protocol 3.4.5. (Ko-Lee Protocol)**

Let us consider a non commutative group  $G$  and its two subsets  $M, N \subseteq G$  (i.e.,  $mn = nm$  for any  $m \in M; n \in N$ ) are publically announced. An element  $g \in G$  is public too.

1. Alice chooses  $m \in M$  and sends the element  $m^{-1}gm$  to Bob.
2. Similarly Bob chooses  $n \in N$  and element  $n^{-1}gn$  is send to Alice.
3. Alice calculates

$$K_M = m^{-1}n^{-1}wnm, w \in G$$

and Bob calculates

$$K_N = n^{-1}m^{-1}wmn.$$

Since

$$mn = nm$$

therefore,

$$m^{-1}n^{-1} = n^{-1}m^{-1} \text{ in } G,$$

so one has

$$K_M = K_N = K \quad K \in G,$$

which is shared secret key for both communicating parties.

The two communicating parties want the key space as big as possible in a sense that the set  $M$  is maximal with the property such that  $mn = nm$  for any  $m \in M, n \in N$ . Now let us consider if the cryptanalyst finds  $m_1, m_2$  which satisfy

$$m_1gm_2 = m^{-1}gm,$$

and  $n_1, n_2$ , which satisfies

$$n_1 w n_2 = n^{-1} g n.$$

Here also suppose that both  $m_1, m_2$  commute with any  $n \in N$ . Then cryptanalyst simply gets

$$\begin{aligned} m_1 n_1 g n_2 m_2 &= m_1 n^{-1} g n m_2 \\ &= n^{-1} m_1 g m_2 n \\ &= n^{-1} m^{-1} g m n \\ &= K \end{aligned}$$

The emphasize is that these  $m_1, m_2$  and  $n_1, n_2$  do not have to do anything with the private elements originally selected by both communicating parties. The important point is that, the cryptanalyst can easily get the common shared key if he/she just only know one pair  $m_1, m_2 \in M$ , such that

$$\begin{aligned} m_1 (n^{-1} g n) m_2 &= n^{-1} m_1 g m_2 n \\ &= n^{-1} m^{-1} g m n \\ &= K \end{aligned}$$

In simple words, to find out the secret key  $K$ , the cryptanalyst does not have to solve the CSP, but instead, it is sufficient to solve an apparently easier problem which some authors [7, 30] call the decomposition problem. We can also notice that a special case of the decomposition problem is conjugacy search problem. The claim is clear that the decomposition problem is easier than the conjugacy search problem, because it is easy to solve an equation with two unknowns than a special case of the same equation with just one unknown.

The protocol presented in [1] is complexed than the Ko-Lee protocol [30]. For implementing this protocol the only restriction on group is that it is efficiently solvable word problem. This is the main advantage of the protocol.



**Protocol 3.4.6. (Anshel Anshel Goldfeld Protocol)**

A group  $G$  and its elements

$$g_1, \dots, g_k; h_1, \dots, h_m \in G$$

are announced publically.

1. Alice chooses a word  $w \in G$  privately as

$$g_1, \dots, g_k (\text{i.e., } w = w(g_1, \dots, g_k)),$$

and sends  $h_1^w, \dots, h_m^w$  to Bob.

2. Bob selects a word  $x \in G$  privately in  $h_1, \dots, h_m$  and sends back to Alice as:

$$g_1^x, \dots, g_k^x.$$

3. She calculates

$$\begin{aligned} w(g_1^x, \dots, g_k^x) &= w^x \\ &= x^{-1}wx, \end{aligned}$$

and Bob calculates

$$\begin{aligned} x(h_1^w, \dots, h_m^w) &= x^w \\ &= w^{-1}xw. \end{aligned}$$

4. So the private key of Alice and Bob is

$$K = w^{-1}x^{-1}wx$$

“called the commutator of  $w$  and  $x$ ” and calculate in the following manner:

She multiplies on the left side of  $x^{-1}wx$  by  $w^{-1}$ , while Bob multiplies on the left side of  $w^{-1}xw$  by  $x^{-1}$ , and then takes the inverse of complete expression

$$(x^{-1}w^{-1}xw)^{-1} = w^{-1}x^{-1}wx.$$

It can easily be seen that in the group  $G$ , the solution of simultaneous CSP

$$h_1^w, \dots, h_m^w; \quad g_1^x, \dots, g_k^x$$

would allow a cryptanalyst to obtain the private key  $K$  [23, 24]. However, by looking at Step (3) of this protocol, it can be seen that the cryptanalyst would have a knowledge of either  $w$  or  $x$  as a word in  $g_1, \dots, g_k$  (respectively, as a word in  $h_1, \dots, h_m$ ) instead of the generators of the group  $G$ . Otherwise, he has no option to combine,  $w^x$  out of  $g_1^x, \dots, g_k^x$ . This means that cryptanalyst has to solve another problem, known as membership search problem [54].

## Chapter 4

# A Cryptosystem Based on Polynomials over Circulant Matrices

The main focus of this chapter is to develop cryptographic schemes which are based on polynomials over circulant matrices using inner automorphism. The working rule is based on the choice of random polynomials over circulant matrices. It gives us the best safety measures which will be discussed in the last section of this chapter.

Why we use the circulant matrices? This motivational idea came from the research article [35]. In this paper Mahalanobis proposed a new cryptosystem which is based on ElGamal scheme over circulant matrices. In his paper he proves that elliptic curve is not the only one which gives the better security but the group of non singular circulant matrices of size  $n$  over  $\mathbb{F}_q$  gives the same security level as of using the field  $\mathbb{F}_{q^{n-1}}$  [34].

## 4.1 Some Definitions and Group Based Hard Problems

Before going to propose the cryptosystem, there are some basic concepts which will be helpful to understand the proposed scheme.

### Definition 4.1.1. (Circulant Matrix)

In a matrix, if each column (row) is a cyclic shift of the preceding column (row), then this matrix is called the circulant matrix of order  $n \times n$  over a field  $\mathbb{F}$ .

$$K = \begin{bmatrix} k_0 & k_{n-1} & \cdots & k_2 & k_1 \\ k_1 & k_0 & k_{n-1} & & k_2 \\ \vdots & k_1 & k_0 & \ddots & \vdots \\ k_{n-2} & & \ddots & \ddots & k_{n-1} \\ k_{n-1} & k_{n-2} & \cdots & k_1 & k_0 \end{bmatrix},$$

and is denoted by

$$\text{circ}(k_0, k_{n-1}, \dots, k_2, k_1)$$

Here we note that the

1. Circulant matrix is completely determined by a single column (row).
2. Circulant matrices are always square matrices.
3. The inverse of non singular circulant matrix is again circulant. Hence the circulant matrices over a field  $\mathbb{F}$  form a subgroup of  $GL(n, \mathbb{F})$ . By using the Algorithm 2.1.4 one can find the inverse of circulants.
4. The product and sum of two circulant matrices is again circulant.
5. Circulant matrices commute with each other.

The multiplying and squaring algorithms of circulant matrices is much faster than the same size of finite field. The important feature of circulant matrices is that it

is one dimensional item used by its first column or row whereas a matrix is two dimensional item. For example the circulant matrix  $C$  of order 2 is

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{12} & a_{11} \end{bmatrix}$$

can be stored as  $(a_{11} \quad a_{12})$ .

The second row is just the circulant shift of the first row. Note that

$$\begin{aligned} C &= \begin{bmatrix} a_{11} & a_{12} \\ a_{12} & a_{11} \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} \\ a_{12} & a_{11} \end{bmatrix} \\ &= \begin{bmatrix} a_{11}^2 + a_{12}^2 & 2a_{11}a_{12} \\ 2a_{11}a_{12} & a_{11}^2 + a_{12}^2 \end{bmatrix}. \end{aligned}$$

Hence multiplication of  $C$  by itself can be efficiently computed just represent  $C^2$  as  $(a_{11}^2 + a_{12}^2 \quad 2a_{11}a_{12})$ . Therefore computation cost for squaring circulant matrix is much less than that of squaring non circulant matrices. Precisely one has to compute the result of a single row or column and the rest of rows or column are just the circular shift.

Let us define a representer polynomial for the circulant matrix  $K$  as

$$\phi(K) = k_0 + k_1x + k_2x^2 + \dots + k_{n-1}x^{n-1}.$$

Under matrix addition and multiplication circulants become commutative ring which is isomorphic to

$$R = \mathbb{F}[x]/(x^n - 1)$$

as defined in [14]. To make this thesis self-contained, we include the following easily deducible characterizations of operations of addition and multiplication of matrices in corresponding polynomials operations.

**Addition**

Let us consider two representer polynomials of circulant matrices  $C$  and  $D$  over a field  $\mathbb{F}$  as:

$$\phi(C) = c_0 + c_1x + c_2x^2 + \dots + c_{n-1}x^{n-1}, \tag{4.1}$$

$$\phi(D) = d_0 + d_1x + d_2x^2 + \dots + d_{n-1}x^{n-1}. \quad (4.2)$$

Then addition Equation (4.1) and Equation (4.2) is defined as:

$$\phi(C + D) = \phi(C) + \phi(D)$$

where

$$\begin{aligned} \phi(C) + \phi(D) &= (c_0 + c_1x + c_2x^2 + \dots + c_{n-1}x^{n-1}) + (d_0 + d_1x + d_2x^2 + \dots \\ &\quad + d_{n-1}x^{n-1}) \\ &= (c_0 + d_0) + (c_1 + d_1)x + (c_2 + d_2)x^2 + \dots + (c_{n-1} + d_{n-1})x^{n-1}. \end{aligned}$$

### Multiplication

The multiplication of Equations (4.1) and (4.2) is defined as:

$$\phi(C \cdot D) = \phi(C) \cdot \phi(D),$$

where

$$\begin{aligned} \phi(C) \cdot \phi(D) &= (c_0 + c_1x + c_2x^2 + \dots + c_{n-1}x^{n-1}) \cdot (d_0 + d_1x + d_2x^2 + \dots + d_{n-1}x^{n-1}), \\ \phi(E) &= e_0 + e_1x + e_2x^2 + \dots + e_{n-1}x^{n-1}. \end{aligned} \quad (4.3)$$

The main aim of multiplication is to find  $e_k$  for  $k = 0, 1, 2, \dots, n - 1$ . Here we note that if

$$x_i x_j = \sum_{k=0}^{n-1} l_{ij}^k x^k.$$

We can define  $n \times n$  matrix  $L_k$  as  $\{l_{ij}^k\}_{ij}$  and it follows that  $c_k = CL_k D^l$ . For more details on circulant matrices, see [8, 9, 59].

### Definition 4.1.2. (Decomposition Problem (DP))

Let us consider a noncommutative group  $G$  and  $H \subseteq G$ . Let  $g_1, g_2 \in G$ . To find

the elements  $h_1, h_2 \in H$  from the relation

$$g_1 = h_1 g_2 h_2,$$

is called the decomposition problem.

**Definition 4.1.3. (Generalized Decomposition Problem (GDP))**

Let us consider a noncommutative group  $G$  and  $H_1, H_2 \subseteq G$ . Let  $g_1, g_2 \in G$ . To find the elements  $h_1 \in H_1$  and  $h_2 \in H_2$  from the relation

$$g_1 = h_1^n g_2 h_2^m,$$

is called the generalized decomposition problem.

**Definition 4.1.4. (Symmetric Decomposition Problem (SDP))**

Let us consider a noncommutative group  $G$ . Let  $g_1, g_2 \in G$  and  $n, m \in \mathbb{Z}$ . To find the element  $g_3 \in G$  from the relation

$$g_1 = g_3^n g_2 g_3^m,$$

is called the symmetric decomposition problem.

**Definition 4.1.5. (Generalized Symmetric Decomposition Problem (GSDP))**

Let us consider a noncommutative group  $G$  and a subset  $H$  of  $G$ . Let  $g_1, g_2 \in G$  and  $n, m \in \mathbb{Z}$ . To find the element  $g_3 \in H$  from the relation

$$g_1 = g_3^n g_2 g_3^m,$$

is called the generalized symmetric decomposition problem.

**Definition 4.1.6. (Polynomial Symmetric Decomposition Problem)**

Let  $R$  be a noncommutative ring. For any element  $r \in R$ , consider the set  $S_r \subseteq R$  defined as

$$S_r = \{P(r) \mid P(x) \in \mathbb{Z}_{>0}[x]\}$$

and  $m, n \in \mathbb{Z}$ . Given two elements  $g_1, g_2 \in R$ , finding the element  $h \in S_r$ , where

$$g_2 = h^m g_1 h^n ,$$

is known as the polynomial symmetric decomposition problem (PSDP).

## 4.2 Proposed Cryptosystem

Let us consider a matrix ring  $M(n, \mathbb{Z}_p)$  and  $GL(n, \mathbb{Z}_p)$ . The center of  $GL(n, \mathbb{Z}_p)$  be the set

$$Z(GL(n, \mathbb{Z}_p)) = \{kI \mid k \in \mathbb{Z}_p\}, \quad \text{where}$$

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

is the identity matrix. In our proposed cryptosystem, let  $C$  be the set of invertible circulant matrix and  $C[X]$  be the polynomial ring over  $C$ . Consider  $\xi$  and  $\varphi$  be the inner automorphism of the ring  $M(n, \mathbb{Z}_p)$ .

### Cryptosystem 4.2.1.

The proposed cryptosystem is defined as follows:

#### Key Generation

To generate a key, Alice performs the following steps:

1. Alice chooses a matrix  $A \in Z(GL(n, \mathbb{Z}_p))$ .
2. She selects two polynomials

$$f(x), g(x) \in C[X],$$

and computes the two invertible circulant matrices

$$f(A) \text{ and } g(A).$$



3. Here Alice defines two inner automorphisms  $\xi$  and  $\varphi$  of the ring,

$$\xi(N) : N \mapsto [f(A)]^{-1} N f(A), \quad (4.4)$$

$$\varphi(N) : N \mapsto [g(A)]^{-1} N g(A), \quad (4.5)$$

for every matrix  $N \in M(n, \mathbb{Z}_p)$ . Since  $f(x), g(x) \in C[X]$ , therefore automorphisms  $\xi$  and  $\varphi$  commutes.

4. Now Alice calculates the following automorphisms of the ring

$$\alpha = \xi^2 \varphi \text{ and } \beta = \xi \varphi^2,$$

$$\alpha(N) : N \mapsto [(f(A))^2 g(A)]^{-1} N [(f(A))^2 g(A)] \quad (4.6)$$

$$\beta(N) : N \mapsto [f(A)(g(A))^2]^{-1} N [f(A)(g(A))^2]. \quad (4.7)$$

5. She randomly picks a matrix  $B \in GL(n, \mathbb{Z}_p)$  and computes

$$(B^{-1}, \beta(B), \alpha(B)).$$

6. Alice's private key is

$$K_R = (f(A), g(A)),$$

and public key is

$$K_p = (p, B, \beta(B), \alpha(B^{-1})).$$

**Remark 4.2.2.** From now onward,  $(j)$  only denotes the corresponding  $j$ th block.

### Encryption

Suppose Bob wants to communicate, he will do the following steps:

1. He represents the message (plaintext)  $M$  as a sequence of matrices over  $\mathbb{Z}_p$ ,

$$M^{(1)}, M^{(2)}, \dots, M^{(n)}, \text{ such that } M = (M^{(1)} \| M^{(2)} \| \dots \| M^{(n)})$$

for  $(j = 1, 2, \dots, n)$ .

2. Next, he chooses a random polynomial

$$h^{(j)}(x) \in C[x],$$

corresponding to every  $M^{(j)}$  ( $j = 1, 2, \dots, n$ ). Then compute  $h^{(j)}(A)$ .

3. He defines the automorphism for every  $(j = 1, 2, \dots, n)$  as

$$\psi^{(j)} : N \mapsto (h^{(j)}(A))^{-1} N (h^{(j)}(A)), \quad (4.8)$$

for every  $N \in M(n, \mathbb{Z}_p)$ .

4. He calculate the matrices for every  $(j = 1, 2, \dots, n)$

$$\psi^{(j)}(\beta(B)) \text{ and } \psi^{(j)}(\alpha(B^{-1})).$$

5. He chooses a random unit  $\rho_j \in \mathbb{Z}_p^*$  for every  $(j = 1, 2, \dots, n)$  and calculates the ciphertext as

$$C = (C^{(1)} \| C^{(2)} \| \dots \| C^{(n)}),$$

where

$$C^{(j)} = (C_1^{(j)}, C_2^{(j)}), \text{ and} \quad (4.9)$$

$$C_1^{(j)} = \rho_j^{-1} \psi^{(j)}(\alpha(B^{-1})), \quad (4.10)$$

$$C_2^{(j)} = \rho_j^2 \psi^{(j)}(\beta(B)) M^{(j)} \psi^{(j)}(\beta(B)). \quad (4.11)$$

## Decryption

On receiving the ciphertext, Alice will go with the following procedure:

1. First she calculates

$$s^{(j)} = \varphi^{-1} \xi(C_1^{(j)}) \quad (4.12)$$

$$= \varphi^{-1} \xi(\rho_j^{-1} \psi^{(j)} \alpha(B^{-1})).$$

2. Finally she gets original (plaintext) message as

$$M^{(j)} = s^{(j)} C_2^{(j)} s^{(j)},$$

and reinstate the message  $M$  from the sequence of matrix  $M^{(1)}, M^{(2)}, \dots, M^{(n)}$ .

**Remark 4.2.3.** The size of  $GL(n, \mathbb{F}_p)$  can be computed as

$$N_1 = |GL(n, \mathbb{F}_p)| = \prod_{k=0}^{n-1} (p^n - p^k). \quad (4.13)$$

So we can choose the matrices from a space of size  $N_1$ .

**Theorem 4.2.4.**

All the automorphisms defined in proposed cryptosystem 4.2 are commutative.

1.  $\xi\varphi = \varphi\xi$ .
2.  $\alpha = \varphi^{-1}\xi\beta$ , and  $\beta = \xi^{-1}\varphi\alpha$ .
3.  $\psi\alpha = \alpha\psi$ .

*Proof.* The proof is as follows:

Let us consider

$$\begin{aligned} \xi\varphi(D) &= \xi(g^{-1}Dg) && \because \text{using (4.5)} \\ \xi\varphi(D) &= f^{-1}g^{-1}Dgf, && \because \text{using (4.4)} \\ &= g^{-1}f^{-1}Dfg, && \because f \text{ and } g \text{ are circulant matrices} \\ &= g^{-1}(f^{-1}Df)g, \\ &= \varphi\xi(D). \end{aligned}$$

Hence we get  $\xi\varphi = \varphi\xi$ .

In the same manner, we can prove that  $\xi, \varphi, \alpha$  and  $\beta$  commutes, since circulant matrices commute as shown in Section 4.1, Equation (4.3).

To prove part 2, let us consider first

$$\varphi^{-1}\xi\beta(D) = \varphi^{-1}\xi(g^{-2}f^{-1}Dfg^2) \quad \because \text{using (4.7)}$$

$$\begin{aligned}
&= \varphi^{-1}(f^{-1}(g^{-2}f^{-1}Dfg^2)f) \\
&= \varphi^{-1}(f^{-2}g^{-2}Dg^2f^2) \quad \because f \text{ and } g \text{ are circulant matrices} \\
&= g(f^{-2}g^{-2}Dg^2f^2)g^{-1} \\
&= g^{-1}f^{-2}Df^2g \\
&= (f^2g)^{-1}Df^2g \\
&= \alpha(D)
\end{aligned}$$

In the same way we can easily find that  $\beta = \xi^{-1}\varphi\alpha$  by using (4.7).

Let us consider

$$\begin{aligned}
\psi\alpha(D) &= \psi(h^{-1}Dh) \\
&= g^{-1}f^{-2}(h^{-1}Dh)f^2g \\
&= h^{-1}(g^{-1}f^{-2}Df^2g)h \\
&= \alpha\psi(D)
\end{aligned}$$

Similarly automorphism  $\psi$  commutes with automorphisms  $\alpha, \beta, \varphi$  and  $\phi$ .  $\square$

**Theorem 4.2.5.**

Given

$$C_2^{(j)} = \rho_j^2 \psi^{(j)}(\beta(B)) M^{(j)} \psi^{(j)}(\beta(B)),$$

and

$$s^{(j)} = \varphi^{-1} \xi \left( C_1^{(j)} \right).$$

In view of given equations, the correctness of decryption of proposed scheme is guaranteed.

*Proof.* (Correctness)

We can easily justify correctness by using Theorem 4.2.4 and doing the following the procedure as

$$C_2^{(j)} s^{(j)} = \rho_j^2 \psi^{(j)}(\beta(B)) M^j \psi^{(j)}(\beta(B)) \left( \varphi^{-1} \xi \left( C_1^{(j)} \right) \right). \quad (4.14)$$

As

$$\varphi^{-1}\xi\left(C_1^{(j)}\right)=\varphi^{-1}\xi\left(\rho_j^{-1}\psi^{(j)}\alpha\left(B^{-1}\right)\right), \quad (4.15)$$

so from Equations (4.14, 4.15), we have

$$\begin{aligned} s^{(j)}C_2^{(j)}s^{(j)} &= \varphi^{-1}\xi^{(j)}\left(C_1^{(j)}\right)\rho_j^2\psi^{(j)}\left(\beta\left(B\right)\right)M^{(j)}\psi^{(j)}\left(\beta\left(B\right)\right)\varphi^{-1}\xi^{(j)}\left(C_1^{(j)}\right) \\ &= \varphi^{-1}\xi^{(j)}\left(\rho_j^{-1}\psi^{(j)}\left(\alpha\left(B^{-1}\right)\right)\right)\rho_j^2\psi^{(j)}\left(\beta\left(B\right)\right)M^{(j)}\psi^{(j)}\left(\beta\left(B\right)\right)\times \\ &\quad \varphi^{-1}\xi^{(j)}\left(\rho_j^{-1}\psi^{(j)}\left(\alpha\left(B^{-1}\right)\right)\right) \\ &= \rho_j^{-1}\rho_j^{-1}\rho_j^2\varphi^{-1}\xi^{(j)}\left(\psi^{(j)}\left(\alpha\left(B^{-1}\right)\right)\right)\psi^{(j)}\left(\beta\left(B\right)\right)M^{(j)}\psi^{(j)}\left(\beta\left(B\right)\right)\times \\ &\quad \varphi^{-1}\xi^{(j)}\left(\psi^{(j)}\left(\alpha\left(B^{-1}\right)\right)\right) \\ &= \varphi^{-1}\xi^{(j)}\left(\psi^{(j)}\left(\alpha\left(B^{-1}\right)\right)\right)\psi^{(j)}\left(\beta\left(B\right)\right)M^{(j)}\psi^{(j)}\left(\beta\left(B\right)\right)\varphi^{-1}\xi^{(j)}\times \\ &\quad \left(\psi^{(j)}\left(\alpha\left(B^{-1}\right)\right)\right) \\ &= \varphi^{-1}\xi^{(j)}\left(\psi^{(j)}\left(\alpha\left(B^{-1}\right)\right)\right)\beta\left(\psi^{(j)}\left(B\right)\right)M^{(j)}\varphi^{-1}\xi^{(j)}\beta\left(\psi^{(j)}\left(B\right)\right)\times \\ &\quad \left(\psi^{(j)}\left(\alpha\left(B^{-1}\right)\right)\right) \\ &= \varphi^{-1}\xi^{(j)}\beta\left(\psi^{(j)}\left(B\right)\right)\left(\psi^{(j)}\left(\alpha\left(B^{-1}\right)\right)\right)M^{(j)}\varphi^{-1}\xi^{(j)}\beta\left(\psi^{(j)}\left(B\right)\right)\times \\ &\quad \left(\psi^{(j)}\left(\alpha\left(B^{-1}\right)\right)\right) \end{aligned}$$

Using Theorem 4.2.4 part 2.

$$s^{(j)}C_2^{(j)}s^{(j)}=\alpha\left(\psi^{(j)}\left(B\right)\right)\left(\psi^{(j)}\left(\alpha\left(B^{-1}\right)\right)\right)M^{(j)}i\alpha\left(\psi^{(j)}\left(B\right)\right)\left(\psi^{(j)}\left(\alpha\left(B^{-1}\right)\right)\right)$$

Using Theorem 4.2.4 part 3.

$$\begin{aligned} s^{(j)}C_2^{(j)}s^{(j)} &= \alpha\left(\psi^{(j)}\left(B\right)\right)\left(\alpha\left(\psi^{(j)}\left(B^{-1}\right)\right)\right)M^{(j)}\psi^{(j)}\left(\alpha\left(B\right)\right)\left(\psi^{(j)}\left(\alpha\left(B^{-1}\right)\right)\right) \\ &= \alpha\left(\psi^{(j)}\left(BB^{-1}\right)\right)M^{(j)}\psi^{(j)}\left(\alpha\left(BB^{-1}\right)\right) \\ &= \alpha\left(\psi^{(j)}\left(I\right)\right)M^{(j)}\psi^{(j)}\left(\alpha\left(j\right)\right) \\ &= \alpha\left(I\right)M^{(j)}\psi^{(j)}\left(j\right) \\ &= IM^{(j)}I \\ &= M^{(j)} \end{aligned}$$

□

**Example 4.2.6. (Toy Example)**

Let us explain our proposed cryptosystem with the help of toy example. For this let us consider

1. Alice chooses a matrix

$$A = \begin{bmatrix} 5 & 0 \\ 0 & 5 \end{bmatrix} \in Z(GL(2, \mathbb{Z}_{11}))$$

and two polynomials

$$f(x) = \begin{bmatrix} 4 & 3 \\ 3 & 4 \end{bmatrix} x^2 + \begin{bmatrix} 3 & 1 \\ 1 & 3 \end{bmatrix} \in C[X], \text{ and}$$

$$g(x) = \begin{bmatrix} 7 & 1 \\ 1 & 7 \end{bmatrix} x^2 + \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \in C[X].$$

2. She calculates

$$\begin{aligned} f(A) &= \begin{bmatrix} 4 & 3 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 5 & 0 \\ 0 & 5 \end{bmatrix}^2 + \begin{bmatrix} 3 & 1 \\ 1 & 3 \end{bmatrix} \\ &= \begin{bmatrix} 4 & 3 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix} + \begin{bmatrix} 3 & 1 \\ 1 & 3 \end{bmatrix} \\ &= \begin{bmatrix} 4 & 10 \\ 10 & 4 \end{bmatrix} \end{aligned}$$

$$\begin{aligned} g(A) &= \begin{bmatrix} 1 & 7 \\ 7 & 1 \end{bmatrix} \begin{bmatrix} 5 & 0 \\ 0 & 5 \end{bmatrix}^2 + \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 7 \\ 7 & 1 \end{bmatrix} \begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix} + \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix} \end{aligned}$$

3. She selects a random matrix

$$B = \begin{bmatrix} 3 & 2 \\ 4 & 5 \end{bmatrix} \in GL(2, Z_{11})$$

and its inverse is

$$\begin{aligned} B^{-1} &= \frac{1}{B} \text{adj}(B) = \frac{1}{7} \begin{bmatrix} 5 & 9 \\ 7 & 3 \end{bmatrix} \\ &= 8 \begin{bmatrix} 5 & 9 \\ 7 & 3 \end{bmatrix}, \quad \because (7)^{-1} = 8 \pmod{11} \\ &= \begin{bmatrix} 7 & 6 \\ 1 & 2 \end{bmatrix}. \end{aligned}$$

4. She computes

$$\begin{aligned} f(A) [g(A)]^2 &= \begin{bmatrix} 4 & 10 \\ 10 & 4 \end{bmatrix} \begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix}^2 \\ &= \begin{bmatrix} 4 & 10 \\ 10 & 4 \end{bmatrix} \begin{bmatrix} 6 & 8 \\ 8 & 6 \end{bmatrix} \\ &= \begin{bmatrix} 5 & 4 \\ 4 & 5 \end{bmatrix} \quad \text{and} \end{aligned}$$

$$\begin{aligned} [f(A) (g(A))^2]^{-1} &= \frac{1}{|[f(A) (g(A))^2]^{-1}|} \text{adj}([f(A) (g(A))^2]^{-1}) \\ &= \frac{1}{9} \begin{bmatrix} 5 & 7 \\ 7 & 5 \end{bmatrix} \\ &= 5 \begin{bmatrix} 5 & 7 \\ 7 & 5 \end{bmatrix}, \quad \because (9)^{-1} = 5 \pmod{11} \\ &= \begin{bmatrix} 3 & 2 \\ 2 & 3 \end{bmatrix} \end{aligned}$$

$$\beta(B) = [f(A) (g(A))^2]^{-1} B [f(A) (g(A))^2]$$

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

and

$$\begin{aligned}
(f(A))^2 g(A) &= \begin{bmatrix} 4 & 10 \\ 10 & 4 \end{bmatrix}^2 \begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix} \\
&= \begin{bmatrix} 6 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix} \\
&= \begin{bmatrix} 7 & 5 \\ 5 & 7 \end{bmatrix}
\end{aligned}$$

$$\begin{aligned}
[(f(A))^2 g(A)]^{-1} &= \frac{1}{|[(f(A))^2 g(A)]^{-1}|} \text{adj} \left( [(f(A))^2 g(A)]^{-1} \right) \\
&= \frac{1}{2} \begin{bmatrix} 7 & 6 \\ 6 & 7 \end{bmatrix} \\
&= 6 \begin{bmatrix} 7 & 6 \\ 6 & 7 \end{bmatrix}, \quad \because (2)^{-1} = 6 \pmod{11} \\
&= \begin{bmatrix} 9 & 3 \\ 3 & 9 \end{bmatrix},
\end{aligned}$$

then

$$\begin{aligned}
\alpha(B^{-1}) &= [(f(A))^2 g(A)]^{-1} B^{-1} [(f(A))^2 g(A)] \\
&= \begin{bmatrix} 3 & 2 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 7 & 6 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 5 & 4 \\ 4 & 5 \end{bmatrix} \\
&= \begin{bmatrix} 3 & 2 \\ 5 & 6 \end{bmatrix}
\end{aligned}$$

5. So her private key is



$$K_R = \left( \begin{array}{l} f(A) = \begin{bmatrix} 4 & 10 \\ 10 & 4 \end{bmatrix} \text{ and} \\ g(A) = \begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix} \end{array} \right),$$

and public key is

$$K_p = \left( \begin{array}{l} P = 11, B = \begin{bmatrix} 3 & 2 \\ 4 & 5 \end{bmatrix}, \\ \beta(B) = \begin{bmatrix} 6 & 5 \\ 1 & 2 \end{bmatrix}, \alpha(B^{-1}) = \begin{bmatrix} 3 & 2 \\ 5 & 6 \end{bmatrix} \end{array} \right).$$

1. Now let Bob want to communicate with Alice, he presents a plaintext

$$M = \begin{bmatrix} 8 & 9 \\ 1 & 2 \end{bmatrix} \in M(2, \mathbb{Z}_{11})$$

and chooses a polynomial as

$$h(x) = \begin{bmatrix} 3 & 5 \\ 5 & 3 \end{bmatrix} x^2 + \begin{bmatrix} 7 & 2 \\ 2 & 7 \end{bmatrix} x + \begin{bmatrix} 4 & 6 \\ 6 & 4 \end{bmatrix} \in C[X]$$

and calculates

$$\begin{aligned} h(A) &= \begin{bmatrix} 3 & 5 \\ 5 & 3 \end{bmatrix} \begin{bmatrix} 5 & 0 \\ 0 & 5 \end{bmatrix}^2 + \begin{bmatrix} 7 & 2 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} 5 & 0 \\ 0 & 5 \end{bmatrix} + \begin{bmatrix} 4 & 6 \\ 6 & 4 \end{bmatrix} \\ &= \begin{bmatrix} 3 & 5 \\ 5 & 3 \end{bmatrix} \begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix} + \begin{bmatrix} 2 & 10 \\ 10 & 2 \end{bmatrix} + \begin{bmatrix} 4 & 6 \\ 6 & 4 \end{bmatrix} \\ &= \begin{bmatrix} 9 & 4 \\ 4 & 9 \end{bmatrix} + \begin{bmatrix} 2 & 10 \\ 10 & 2 \end{bmatrix} + \begin{bmatrix} 4 & 6 \\ 6 & 4 \end{bmatrix} \\ &= \begin{bmatrix} 9 & 4 \\ 4 & 9 \end{bmatrix} \end{aligned}$$

2. He computes its inverse as

$$\begin{aligned}
[h(A)]^{-1} &= \frac{1}{h(A)} \text{adj}(h(A)) \\
&= \frac{1}{1} \begin{bmatrix} 4 & 2 \\ 2 & 4 \end{bmatrix} \\
&= \begin{bmatrix} 4 & 2 \\ 2 & 4 \end{bmatrix}
\end{aligned}$$

3. Finally he calculates

$$\begin{aligned}
\psi(\beta(B)) &= [h(A)]^{-1} \beta(B) [h(A)] \\
&= \begin{bmatrix} 4 & 2 \\ 2 & 4 \end{bmatrix} \begin{bmatrix} 6 & 5 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 9 & 4 \\ 4 & 9 \end{bmatrix} \\
&= \begin{bmatrix} 1 & 0 \\ 6 & 7 \end{bmatrix}, \quad \text{and}
\end{aligned}$$

$$\begin{aligned}
\psi(\alpha(B^{-1})) &= [h(A)]^{-1} \alpha(B^{-1}) [h(A)] \\
&= \begin{bmatrix} 4 & 2 \\ 2 & 4 \end{bmatrix} \begin{bmatrix} 3 & 2 \\ 5 & 6 \end{bmatrix} \begin{bmatrix} 9 & 4 \\ 4 & 9 \end{bmatrix} \\
&= \begin{bmatrix} 4 & 3 \\ 4 & 5 \end{bmatrix}
\end{aligned}$$

4. Let  $\rho = 2 \in \mathbb{Z}_{11}$  be the unit element and  $\rho^{-1} = 2^{-1} \pmod{11} = 6 \pmod{11}$ .

5. Then the ciphertext is

$$\begin{aligned}
C_1 &= \rho^{-1} \psi(\alpha(B^{-1})) \\
&= 6 \begin{bmatrix} 4 & 3 \\ 4 & 5 \end{bmatrix} \\
&= \begin{bmatrix} 2 & 7 \\ 2 & 8 \end{bmatrix}
\end{aligned}$$

$$C_2 = \rho^2 \psi(\beta(B)) M \psi(\beta(B))$$

$$\begin{aligned}
C_2 &= 4 \begin{bmatrix} 1 & 0 \\ 6 & 7 \end{bmatrix} \begin{bmatrix} 8 & 9 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 6 & 7 \end{bmatrix} \\
&= \begin{bmatrix} 4 & 0 \\ 2 & 6 \end{bmatrix} \begin{bmatrix} 7 & 8 \\ 2 & 3 \end{bmatrix} \\
&= \begin{bmatrix} 6 & 10 \\ 4 & 1 \end{bmatrix}.
\end{aligned}$$

6. So the ciphertext pair is

$$C = (C_1, C_2).$$

7. When Alice receives the pair of ciphertext, she will first find

$$\begin{aligned}
s &= \varphi^{-1}\xi(C_1) \\
&= [(f(A))^{-1}g(A)]^{-1}C_1[(f(A))^{-1}g(A)],
\end{aligned}$$

where

$$\begin{aligned}
[f(A)]^{-1} &= \frac{1}{|[f(A)]|} \text{adj}[f(A)] \\
&= \frac{1}{4} \begin{bmatrix} 4 & 1 \\ 1 & 4 \end{bmatrix}, \\
&= 3 \begin{bmatrix} 4 & 1 \\ 1 & 4 \end{bmatrix}, \quad \because (4)^{-1} = 3 \\
&= \begin{bmatrix} 1 & 3 \\ 3 & 1 \end{bmatrix}.
\end{aligned}$$

$$\begin{aligned}
[f(A)]^{-1}g(A) &= \begin{bmatrix} 1 & 3 \\ 3 & 1 \end{bmatrix} \begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix} \\
&= \begin{bmatrix} 2 & 7 \\ 7 & 2 \end{bmatrix},
\end{aligned}$$

and

$$\begin{aligned}
 [(f(A))^{-1}g(A)]^{-1} &= \frac{1}{|[f(A))^{-1}g(A)]|} \text{adj}[(f(A))^{-1}g(A)] \\
 &= \frac{1}{10} \begin{bmatrix} 2 & 4 \\ 4 & 2 \end{bmatrix}, \\
 &= 10 \begin{bmatrix} 2 & 4 \\ 4 & 2 \end{bmatrix}, \quad \because (10)^{-1} = 10 \\
 &= \begin{bmatrix} 9 & 7 \\ 7 & 9 \end{bmatrix}.
 \end{aligned}$$

Hence

$$\begin{aligned}
 s &= \xi\varphi^{-1}(C_1) \\
 &= \begin{bmatrix} 9 & 7 \\ 7 & 9 \end{bmatrix} \begin{bmatrix} 2 & 7 \\ 2 & 8 \end{bmatrix} \begin{bmatrix} 2 & 7 \\ 7 & 2 \end{bmatrix} \\
 &= \begin{bmatrix} 6 & 0 \\ 9 & 4 \end{bmatrix}.
 \end{aligned}$$

8. Finally she gets the original plaintext message after calculating

$$\begin{aligned}
 sC_2s &= \begin{bmatrix} 6 & 0 \\ 9 & 4 \end{bmatrix} \begin{bmatrix} 6 & 10 \\ 4 & 1 \end{bmatrix} \begin{bmatrix} 6 & 0 \\ 9 & 4 \end{bmatrix} \\
 &= \begin{bmatrix} 6 & 0 \\ 9 & 4 \end{bmatrix} \begin{bmatrix} 5 & 7 \\ 0 & 4 \end{bmatrix} \\
 &= \begin{bmatrix} 8 & 9 \\ 1 & 2 \end{bmatrix} \\
 &= M
 \end{aligned}$$

### 4.3 Security Analysis

Now we are going to explain the hardness of computation with its related strength to consider its security and performance. Lets have a look on attacks to proposed cryptosystem.

For the original plaintext message  $M$ , we have a ciphertext as  $C = (C_1, C_2)$ , where

$$\begin{aligned} C_1 &= \rho^{-1} \psi (\alpha (B^{-1})) \\ C_2 &= \rho^2 \psi (\beta (B)) M \psi (\beta (B)). \end{aligned}$$

Hence we have the system of equations with the unknown matrices as a plaintext  $M$ ,  $h(A)$  and also unknown invertible element  $\rho \in \mathbb{Z}_p^*$  such as

$$C_1 = \rho^{-1} (h(A))^{-1} \alpha (B^{-1}) (h(A)), \tag{4.16}$$

$$C_2 = \rho^2 (h(A))^{-1} \beta (B) (h(A)) M (h(A))^{-1} \beta (B) (h(A)). \tag{4.17}$$

For the choice of any random invertible element  $\rho$  the cryptanalyst has to solve the above system of equations by supposing a value  $\rho = \rho_0$  and has to solve the CSP to find the matrix  $h(A)$  using the equation:

$$\rho_0 C_1 = (h(A))^{-1} \alpha (B^{-1}) (h(A)).$$

Here  $\beta (B^{-1})$  is defined in Equation (4.7) and in that expression the polynomials  $f, g$  and  $h$  are unknowns. Rewrite the above equation as a linear system of four equations which has number of unknowns, cryptanalyst has to find the solution set which depends on one or more parameters in  $Z_p^*$ . Then each solution intersects at  $h(A) = h_0(A)$  in the Equation (4.16).

$$C_2 = \rho_0^2 (h_0(A))^{-1} \beta (B) (h_0(A)) M (h_0(A))^{-1} \beta (B) (h_0(A))$$

and it corresponds the solution  $M = M_0$ . First the cryptanalyst has to solve polynomial symmetric decomposition problem and then conjugacy search problem. In this manner cryptanalyst has received atleast  $n$  pairs of  $(h_0(A), M_0)$  for the fixed  $\rho_0$  and for this reason the system becomes infeasible.

Let  $(M^{(1)}, C^{(1)}), \dots, (M^{(j)}, C^{(j)})$  be the plaintext ciphertext pair. Cryptanalyst wants to find the unknown original plaintext message  $M^{(j+1)}$  corresponding the ciphertext  $C^{(j+1)}$ . In the proposed cryptosystem we use a new one time random key for encryption to get a new message. Hence the previous ciphertext plaintext pair donot give any information to find the next unknown plaintext.

## 4.4 Efficiency of Cryptosystems

For the complexity of bit operation with the known estimates for encryption and decryption algorithm in modular exponentiation is summarized in the TABLE (4.1). See Ref. [38]

TABLE 4.1: Complexity of Bit Operation

Operations ( $\forall a_1, a_2 \in \mathbb{Z}_n$ )		Bit Complexity
Modular addition	$(a_1 + a_2) \pmod n$	$O(\lg n)$
Modular subtraction	$(a_1 - a_2) \pmod n$	$O(\lg n)$
Modular inversion	$a_1^{-1} \pmod n$	$O((\lg n)^2)$
Modular multiplication	$(a_1 a_2) \pmod n$	$O((\lg n)^2)$
Modular exponentiation	$a_1^k \pmod n, k < n$	$O((\lg n)^3)$

Now here we discuss the bit complexity of modular arithmetic in matrices of order.

### 1. Matrix Multiplication

In matrix multiplication, the operation consists of only 4 modular addition and 8 modular multiplications. Only considering the multiplication, the bit complexity of matrix multiplication is obtained as  $8(\lg n)^2$  -bit operations and the number of bits is denoted by  $(\lg n)$  in  $n$  binary representation.

For 64-bit  $n$ , we have the following complexity:

$$8(64)^2 = 2^{15} = 32 \times 1024 = 3.2 \times 10 \times 10^3 \approx 3.2 \times 10^4\text{-bit operations.}$$

## 2. Matrix Multiplication by a Scalar

Matrix modular multiplication consists of 4 operations. So the bit complexity of this operations is estimated as  $4(lgn)^2$ -bit operations.

For 64-bit  $n$ , we get

$$4(64)^2 = 2^{14} = 16 \times 2^{10} \approx 1.6 \times 10^4\text{-bit operations.}$$

## 3. Matrix Inversion

The operation in matrix modular inversion involves 1 modular subtraction and 2 matrix multiplications, matrix multiplication by a scalar and modular inversion, then the estimated bit complexity of matrix modular inversion by ignoring modular subtraction is:

$$3(lgn)^2 + 4(lgn)^2 = 7(lgn)^2\text{-bit operations.}$$

For 64-bit  $n$ , we have the following estimate:

$$7(64)^2 = 7 \times 2^{12} = 28 \times 2^{10} \approx 2.8 \times 10^4\text{-bit operations.}$$

## 4. Matrix Exponentiation

Let us consider the size of exponent is  $O(lgn)$ . So the bit complexity of matrix exponentiation is as follows:

$$lgn \cdot 8(lgn)^2 = 8(lgn)^3\text{-bit operations.}$$

For 64-bit  $n$ , we get

$$8(64)^3 = 8 \times 2^{18} = 2 \times 2^{20} = 2 \times (2^{10})^2 \approx 2 \times 10^6\text{-bit operations.}$$

As we know that the encryption and decryption of RSA only involves the modular exponentiation, so the bit complexity of RSA in 1024 bit  $n$  is  $(lgn)^3$ . Hence we have the following estimate:

$$1024^3 = (2^{10})^3 \approx (10^3)^3 = 10^9\text{-bit operations.} \quad (4.18)$$

#### 4.4.1 Efficiency of Proposed Cryptosystem

Our encryption scheme consists only on the matrix modular exponentiation and the bit complexity of our scheme is  $8(\lg n)^3$  bit  $n$  as follows:

For 64-bit  $n$ , we get:

$$8(64)^3 = 8 \cdot 2^{18} = 2 \cdot 2^{20} \approx 2 \times 10^6\text{-bit operations.}$$

Our proposed cryptosystem contains 4 matrix modular multiplications and 2 inversions of matrix modulo. Then for decryption scheme, the bit complexity is:

$$4 \cdot 8(\log n)^2 + 2 \cdot 7(\log n)^2 = 46(\log n)^2\text{-bit operations.}$$

For 64-bit  $n$ , we get :

$$46(64)^2 = 46 \cdot 2^{12} = 184 \cdot 2^{10} \approx 184 \times 10^3 \approx 1.8 \times 10^5\text{-bit operations.}$$

From all the above calculations and in view of Equation (4.18), we see that our proposed scheme is very fast for encryption and decryption.



## **4.5 Conclusion**

In this chapter, the cryptographic scheme on polynomials over circulant matrices using inner automorphism has been discussed. For two reasons, the proposed public key cryptosystems give equal security for a far smaller bit size. The operations are applied as a matrix by matrix multiplication instead of multiplication of two integers is the first reason and on the other hand, as much as the size of matrix is increased the intractability and complexity also increased. Decryption of our proposed scheme is much faster than RSA. Hence from the calculations we can say that the proposed cryptosystem is efficient and faster than the existing.

# Chapter 5

## A New ElGamal Like

## Cryptosystem Based on Matrices over Grouping

In this chapter, we have used matrices over a grouping to develop a new public key cryptosystem. The mixture of conjugacy search problem and discrete log problem is underlying problem for the proposed scheme. The exponentiation of elements is replaced by conjugacy to accelerate the calculations. Due to this reason, the key generation becomes more efficient. Different security aspects related to our scheme are also discussed. It is shown that the proposed scheme is secured against known plaintext attack.

The platform that we are suggesting here is the group of non singular circulant matrices [14, 34] over a grouping, with a usual matrix multiplication operation. Since the circulant matrices use less memory storage, it is well known that this group [36, 56] with half the computational cost has the similar security of about same size finite field. For secure implementation, the size of the field for circulant matrices is another motivating factor.

The material of this chapter is based on the exposition of our paper [26] and is organized as follows:

In Section 5.1, we will discuss some basic definitions of grouping which will be used in the next sections. The ElGamal cryptosystem and circulant matrices have already been discussed in Chapter 3, Cryptosystem 3.2.4 and Chapter 4, Definition 4.1.1 respectively. In Section 5.2, we will present the proposed public key cryptosystem, prove its correctness and explain the scheme with a detailed example. In Section 5.3, we will talk about security aspects of the proposed cryptosystem.

## 5.1 Grouping

Here we give some formal definitions which are the basis for the construction of proposed cryptosystem. The aim of this chapter is to propose a novel cryptosystem using matrices over a grouping. This section is devoted to the introduction to the structure of grouping and its properties. The definition of grouping is already defined in Chapter 2, Definition 2.2.21.

### Definition 5.1.1. (Homomorphisms of Grouping)

Since grouping is a ring as defined above, so we can talk about ring homomorphism of grouping. Let us consider the function

$$\psi : GR \rightarrow R$$

defined by

$$\psi \left( \sum_{g \in G} b_g g \right) = \sum_{g \in G} b_g.$$

The function  $\psi$  is called the augmentation map  $GR$  onto  $R$ .

Let  $b_g \in R$  then

$$\psi (b_g \cdot 1) = b_g \text{ (onto).}$$

Let  $b_g g, b_g h \in GR$ . Then

$$\psi (b_g g) = \psi (b_g h) = b_g. \tag{5.1}$$

Since  $b_g g \neq b_g h$ , therefore  $\psi$  is not one-to-one.  $\psi$  is a ring homomorphism from  $GR$  onto  $R$  (an epimorphism).

Let

$$\gamma = \sum_{g \in G} b_g g, \text{ and } \delta = \sum_{g \in G} d_g g \text{ where } \gamma, \delta \in GR. \quad (5.2)$$

Then

$$\begin{aligned} \psi(\gamma + \delta) &= \psi\left(\sum_{g \in G} (b_g + d_g)g\right) \\ &= \sum_{g \in G} (b_g + d_g) = \sum_{g \in G} b_g + \sum_{g \in G} d_g \\ \psi(\gamma + \delta) &= \psi(\gamma) + \psi(\delta). \end{aligned} \quad (5.3)$$

Let us again consider

$$\gamma = \sum_{g \in G} b_g g \text{ and } \delta = \sum_{h \in G} d_h h.$$

Then

$$\psi(\gamma\delta) = \sum_{g, h \in G} b_g d_h gh = \sum_{g, h \in G} b_g d_h, \quad (5.4)$$

and

$$\begin{aligned} \psi(\gamma)\psi(\delta) &= \psi\left(\sum_{g \in G} b_g g\right)\psi\left(\sum_{h \in G} d_h h\right) \\ &= \left(\sum_{g \in G} b_g\right)\left(\sum_{h \in G} d_h\right) \\ \psi(\gamma)\psi(\delta) &= \sum_{g, h \in G} b_g d_h. \end{aligned} \quad (5.5)$$

Therefore

$$\psi(\gamma\delta) = \psi(\gamma)\psi(\delta) \quad (5.6)$$

and above relationship shows that  $\psi$  is ring homomorphism.

$$Ker(\psi) = \left\{ \gamma = \sum_{g \in G} b_g g : \psi(\gamma) = \sum_{g \in G} b_g = 0 \right\}. \quad (5.7)$$

$Ker(\psi)$  is nontrivial and non empty.

**Definition 5.1.2. (Units of Grouping)**

Let

$$\eta \in U(GR) \text{ and } \eta \cdot \rho = \rho \cdot \eta = 1.$$

Then

$$\psi(\eta \cdot \rho) = \psi(1) = 1 = \psi(\eta) \psi(\rho) = 1 \in R.$$

where  $\psi$  is as defined in the Definition 5.1.1. So  $\psi(\eta)$  is invertible in  $R$ , with inverse  $\psi(\rho)$ . So

$$\psi(U(GR)) = U(R). \quad (5.8)$$

**Remark 5.1.3.**

The set of units under multiplication forms a group, it is denoted by  $U(GR)$ .

**Definition 5.1.4. (Zero Divisor of Grouping)**

Let

$$\eta \in ZD(GR) \text{ and } \eta \cdot \rho = \rho \cdot \eta = 0, \text{ where } \eta, \rho \neq 0,$$

with the augmentation map  $\psi$  (see Definition 5.1.1). Then

$$\psi(\eta \cdot \rho) = \psi(\eta) \psi(\rho) = \psi(0) = 0.$$

Thus

$$\psi(\eta) \psi(\rho) = 0. \text{ So either } \psi(\eta) = 0 \text{ or } \psi(\rho) = 0$$

or  $\psi(\eta)$  and  $\psi(\rho)$  are zero divisors in  $R$ .

**Example 5.1.5.**

By considering Example 2.2.22, then we calculate  $U(\mathbb{Z}_3[C_2])$ ,  $ZD(\mathbb{Z}_3[C_2])$ . From TABLE 2.4, the set of units of grouping  $\mathbb{Z}_3[C_2]$  is

$$U(\mathbb{Z}_3[C_2]) = \{1, y, 2, 2y\}.$$

and the Cayley's table for  $U(\mathbb{Z}_3[C_2])$  with respect to multiplication is given below:

TABLE 5.1: Units of Grouping

$\cdot$	1	$y$	2	$2y$
1	1	$y$	2	$2y$
$y$	$y$	1	$2y$	2
2	2	$2y$	1	$y$
$2y$	$2y$	2	$y$	1

From TABLE 5.1, we note that the set of units under multiplication forms a group.

Again from TABLE 2.4, we see that the set of zero divisors is

$$ZD(\mathbb{Z}_3[C_2]) = \{1 + y, 1 + 2y, 2 + y, 2 + 2y\}.$$

Let the augmentation map be  $\psi : \mathbb{Z}_3[C_2] \rightarrow \mathbb{Z}_3$ , then by Definition 5.1.1, we have

$$\psi(\eta) = 0, \Rightarrow \eta = 0, 1 + 2y, 2 + y.$$

In a similar way, TABLE 5.2 defines the augmentation map

TABLE 5.2: Augmentation Map

$\psi(\eta)$	$\eta \in \mathbb{Z}_3[C_2]$
0	$\{0, 2 + y, 1 + 2y\}$
1	$\{1, y, 2 + 2y\}$
2	$\{2, 2y, 1 + y\}$

From all the above calculations, we note that

$$\mathbb{Z}_3[C_2] = \{U(\mathbb{Z}_3[C_2])\} \cup \{ZD(\mathbb{Z}_3[C_2])\} \cup \{0\}.$$

In general in any grouping  $GR$ , we have

$$GR = \{U(GR)\} \cup \{ZD(GR)\} \cup \{0\}.$$

**Remark 5.1.6.**

Nevertheless  $GR$  is in general not commutative and therefore  $M(n, GR)$  and

$GL(n, GR)$  do not make sense in general that is why we need to be extremely careful while making choices for ground structures of group and ring.

In our case, we have taken cyclic group of order  $n$  which is always abelian and ring is  $\mathbb{Z}_n$ , also a unitary commutative ring. Now in our proposed schemes the matrices are either circulant or coming from the center of  $GL(n, GR)$ . There are many units and group rings available of many different types which can be used. These can be non-commutative as well as commutative. One of the author Shiplrain et al. [27] used the structure of non-commutative grouping. Here in Chapter 5 and Chapter 6, the proposed schema are algebraically sound enough to provide a strong and highly secure cryptosystems.

## 5.2 Proposed Cryptosystem

Here, the general scheme of proposed cryptosystem is discussed in detail. A toy example is given to elaborate our proposal.

### Cryptosystem 5.2.1.

The implementation of the our proposed scheme is elaborated as follows:

Consider the set  $M(n, GR)$ , which contains all matrices with order  $n$  defined over the grouping  $GR$ . Take  $H$ , the collection of all circulant as well as invertible matrices of order  $n$ , with entries from grouping  $GR$ . Then  $H \leq M(n, GR)$  .

### Key Generation

The steps for key generation are as follows:

1. Alice, randomly selects  $A, B \in H$ .
2. She calculates the following matrices:

$$M_1 = A^2 B \tag{5.9}$$

$$M_2 = B^2 A. \tag{5.10}$$

3. Then she chooses a matrix  $N \in GL(n, GR)$  randomly and calculates  $N^{M_1}$ , the conjugate of  $N$  by  $M_1$  and  $(N^{-1})^{M_2}$ .

4. Her private key is

$$(A, B).$$

and the pair

$$(P_1, P_2) = \left( N^{M_1}, (N^{-1})^{M_2} \right) \quad (5.11)$$

is her public key.

### Encryption

Suppose Bob has to send a plaintext

$$m \in M(n, GR)$$

to Alice, he will follow as:

1. He picks randomly  $X \in H$  and calculates  $P_1^X$  and  $P_2^X$ .
2. Then he randomly chooses  $\eta \in GR$ , where  $\eta$  is the unit element and computes

$$C_1 = \eta^{-1} P_2^X \quad \text{and} \quad C_2 = \eta^2 P_1^X m P_1^X. \quad (5.12)$$

Now he sends the ciphertext

$$C = (C_1, C_2) \quad (5.13)$$

to Alice.

### Decryption

Alice decrypts it by first computing:

$$S = (C_1^B)^{A^{-1}} \quad (5.14)$$



and then she finally computes:

$$m = SC_2S \quad (5.15)$$

to find the plaintext  $m$ .

**Theorem 5.2.2.**

In view of specified notation of Cryptosystem 5.2, the correctness of its decryption is guaranteed.

*Proof.* We can easily prove that by noticing that

$$S = (C_1^B)^{A^{-1}} = AC_1^B A^{-1}$$

and

$$C_2 = \eta^2 P_1^X m P_1^X = \eta^2 X^{-1} P_1 X m X^{-1} P_1 X$$

$$\begin{aligned} C_2 S &= \eta^2 P_1^X m P_1^X (C_1^B)^{A^{-1}} \\ &= \eta^2 X^{-1} P_1 X m X^{-1} P_1 X . AC_1^B A^{-1} \\ &= \eta^2 X^{-1} M_1^{-1} N M_1 X m X^{-1} M_1^{-1} N M_1 X . AB^{-1} C_1 B A^{-1} \end{aligned}$$

Since  $C_1 = \eta^{-1} P_2^X = \eta^{-1} X^{-1} P_2 X$ , it follows that

$$\begin{aligned} C_2 S &= \eta^2 m X^{-1} B^{-2} A^{-1} N A B^2 X . AB^{-1} \eta^{-1} P_2^X B A^{-1} \\ &= \eta^2 X^{-1} B^{-2} A^{-1} N A B^2 X m X^{-1} B^{-2} A^{-1} N A B^2 X . AB^{-1} \eta^{-1} X^{-1} P_2 X B A^{-1} \\ &= \eta^2 \eta^{-1} X^{-1} B^{-2} A^{-1} N A B^2 X m X^{-1} B^{-2} A^{-1} N A B^2 X \times \\ &\quad AB^{-1} X^{-1} M_2^{-1} N^{-1} M_2 X B A^{-1} \\ &= \eta X^{-1} B^{-2} A^{-1} N A B^2 X m X^{-1} B^{-2} A^{-1} N A B^2 X \times \\ &\quad AB^{-1} X^{-1} B^{-1} A^{-2} N^{-1} A^2 B X B A^{-1} \\ &= \eta X^{-1} B^{-2} A^{-1} N A B^2 X m X^{-1} B^{-2} A^{-1} N A B^2 X . A^{-1} B^{-2} X^{-1} N^{-1} A B^2 X \\ &= \eta X^{-1} B^{-2} A^{-1} N A B^2 X m X^{-1} B^{-2} A^{-1} N X A B^2 A^{-1} B^{-2} X^{-1} N^{-1} A B^2 X \end{aligned}$$

The choice of matrices  $A, B$  and  $X$  are from invertible circulant matrices and we know that circulant matrices commutes, hence the matrices  $A, B$  and  $X$  commutes.

Only the matrices  $N$  and  $m$  donot commute,

$$\begin{aligned}
 C_2S &= \eta X^{-1}B^{-2}A^{-1}NAB^2XmX^{-1}B^{-2}A^{-1}N(XX^{-1})(AA^{-1})(B^2B^{-2}) \times \\
 &\quad N^{-1}AB^2X \\
 &= \eta X^{-1}B^{-2}A^{-1}NAB^2XmX^{-1}B^{-2}A^{-1}NN^{-1}AB^2X \\
 &= \eta X^{-1}B^{-2}A^{-1}NAB^2XmX^{-1}B^{-2}A^{-1}AB^2X \\
 &= \eta X^{-1}B^{-2}A^{-1}NAB^2Xm(XX^{-1})(B^{-2}B^2)(A^{-1}A) \\
 &= \eta X^{-1}B^{-2}A^{-1}NAB^2Xm
 \end{aligned}$$

Now consider

$$\begin{aligned}
 SC_2S &= \eta^{-1}X^{-1}B^{-2}A^{-1}N^{-1}AB^2X\eta X^{-1}B^{-2}A^{-1}NAB^2Xm \\
 &= \eta^{-1}\eta X^{-1}B^{-2}A^{-1}N^{-1}AB^2XX^{-1}B^{-2}A^{-1}NAB^2Xm \\
 &= X^{-1}B^{-2}A^{-1}N^{-1}(AA^{-1})(B^2B^{-2})(XX^{-1})NAB^2Xm \\
 &= X^{-1}B^{-2}A^{-1}N^{-1}NAB^2Xm \\
 &= X^{-1}B^{-2}A^{-1}AB^2Xm \\
 &= X^{-1}XB^{-2}B^2A^{-1}Am \\
 &= m.
 \end{aligned}$$

Hence proved.

□

**Example 5.2.3. (A Toy Example)**

The proposed scheme is elaborated by the following example:

Take  $G = C_2 = \{1, y\} = \langle y \rangle = \langle y : y^2 = 1 \rangle$  and  $R = \mathbb{Z}_2 = \{0, 1\}$ . Consider the ring

$$\mathbb{Z}_2[C_2] = \left\{ \sum_{g \in C_2} a_g g : a_g \in \mathbb{Z}_2 \right\} = \{0, 1, y, 1 + y\}$$

Consider the set  $M(2, \mathbb{Z}_2C_2)$ .

Let  $(A, B)$  be the private keys of Alice, where

$$A = \begin{bmatrix} y & 1+y \\ 1+y & y \end{bmatrix} \in H, \text{ and}$$

$$B = \begin{bmatrix} 1 & 1+y \\ 1+y & 1 \end{bmatrix} \in H.$$

Alice selects random matrix

$$N = \begin{bmatrix} 1 & 0 \\ 1+y & y \end{bmatrix},$$

from  $GL(2, \mathbb{Z}_2[C_2])$ . Also she calculates the following matrices:

$$\begin{aligned} M_1 &= AB^2 = \begin{bmatrix} y & 1+y \\ 1+y & y \end{bmatrix} \begin{bmatrix} 1 & 1+y \\ 1+y & 1 \end{bmatrix}^2, \\ &= \begin{bmatrix} y & 1+y \\ 1+y & y \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \\ &= \begin{bmatrix} y & 1+y \\ 1+y & y \end{bmatrix}, \text{ and} \end{aligned}$$

$$\begin{aligned} M_2 &= A^2B = \begin{bmatrix} y & 1+y \\ 1+y & y \end{bmatrix}^2 \begin{bmatrix} 1 & 1+y \\ 1+y & 1 \end{bmatrix}, \\ M_2 &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1+y \\ 1+y & 1 \end{bmatrix}, \\ &= \begin{bmatrix} 1 & 1+y \\ 1+y & 1 \end{bmatrix}. \end{aligned}$$

$$\begin{aligned} P_1 &= N^{M_1} = M_1^{-1}NM_1, \\ &= \begin{bmatrix} y & 1+y \\ 1+y & y \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1+y & y \end{bmatrix} \begin{bmatrix} y & 1+y \\ 1+y & y \end{bmatrix}, \\ &= \begin{bmatrix} 1 & 0 \\ 1+y & y \end{bmatrix}, \text{ and} \end{aligned}$$

$$\begin{aligned}
P_2 &= (N^{-1})^{M_2} = M_2^{-1}N^{-1}M_2, \\
&= \begin{bmatrix} 1 & 1+y \\ 1+y & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1+y & y \end{bmatrix} \begin{bmatrix} 1 & 1+y \\ 1+y & 1 \end{bmatrix}, \\
&= \begin{bmatrix} 1 & 0 \\ 1+y & y \end{bmatrix},
\end{aligned}$$

so Alice public key is

$$(P_1, P_2).$$

Now Bob will do the following:

To send a message  $m$

$$m = \begin{bmatrix} y & 1 \\ 1 & y \end{bmatrix} \in M(2, GR),$$

he selects random matrix

$$X = \begin{bmatrix} y & 0 \\ 0 & y \end{bmatrix} \in H$$

and calculate its inverse

$$\begin{aligned}
X^{-1} &= (|X|)^{-1}adj(X), \\
&= \frac{1}{1} \begin{bmatrix} y & 0 \\ 0 & y \end{bmatrix}, \\
&= \begin{bmatrix} y & 0 \\ 0 & y \end{bmatrix}.
\end{aligned}$$

He computes the matrices

$$\begin{aligned}
P_1^X &= X^{-1}P_1X, \\
&= \begin{bmatrix} y & 0 \\ 0 & y \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1+y & y \end{bmatrix} \begin{bmatrix} y & 0 \\ 0 & y \end{bmatrix}, \\
P_1^X &= \begin{bmatrix} 1 & 0 \\ 1+y & y \end{bmatrix}.
\end{aligned}$$

And

$$\begin{aligned}
 P_2^X &= X^{-1}P_2X, \\
 &= \begin{bmatrix} y & 0 \\ 0 & y \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1+y & y \end{bmatrix} \begin{bmatrix} y & 0 \\ 0 & y \end{bmatrix}, \\
 P_2^X &= \begin{bmatrix} 1 & 0 \\ 1+y & y \end{bmatrix}.
 \end{aligned}$$

Take  $\eta = y \in \mathbb{Z}_2C_2$  which is a unit element. Then

$$\begin{aligned}
 C_1 &= \eta^{-1}P_2^X = yX^{-1}P_2X, \\
 &= y \begin{bmatrix} 1 & 0 \\ 1+y & y \end{bmatrix}, \\
 &= \begin{bmatrix} y & 0 \\ 1+y & 1 \end{bmatrix} \text{ and}
 \end{aligned}$$

$$\begin{aligned}
 C_2 &= \eta^2P_1^XmP_1^X \\
 &= y^2 \begin{bmatrix} 1 & 0 \\ 1+y & y \end{bmatrix} \begin{bmatrix} y & 1 \\ 1 & y \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1+y & y \end{bmatrix} \\
 &= \begin{bmatrix} 1 & 0 \\ 1+y & y \end{bmatrix} \begin{bmatrix} 1 & y \\ y & 1 \end{bmatrix} \\
 &= \begin{bmatrix} 1 & y \\ y & 1 \end{bmatrix}
 \end{aligned}$$

and the ciphertext pair is  $C = (C_1, C_2)$ .

For decryption, Alice will first compute the following matrices:

$$\begin{aligned}
 (C_1)^B &= B^{-1}C_1B \\
 &= \begin{bmatrix} y & 1+y \\ 1+y & y \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1+y & y \end{bmatrix} \begin{bmatrix} 1 & 1+y \\ 1+y & 1 \end{bmatrix}
 \end{aligned}$$

$$= \begin{bmatrix} y & 0 \\ 1+y & 1 \end{bmatrix} \text{ and}$$

$$\begin{aligned} S &= (C_1^B)^{A^{-1}} = AC_1^B A^{-1} \\ &= \begin{bmatrix} y & 1+y \\ 1+y & y \end{bmatrix} \begin{bmatrix} y & 0 \\ 1+y & 1 \end{bmatrix} \begin{bmatrix} y & 1+y \\ 1+y & y \end{bmatrix} \\ &= \begin{bmatrix} y & 0 \\ 1+y & 1 \end{bmatrix}. \end{aligned}$$

Finally she gets original plaintext as

$$\begin{aligned} m &= SC_2S \\ &= \begin{bmatrix} y & 0 \\ 1+y & 1 \end{bmatrix} \begin{bmatrix} 1 & y \\ y & 1 \end{bmatrix} \begin{bmatrix} y & 0 \\ 1+y & 1 \end{bmatrix} \\ &= \begin{bmatrix} y & 0 \\ 1+y & 1 \end{bmatrix} \begin{bmatrix} 1 & y \\ y & 1 \end{bmatrix} \\ &= \begin{bmatrix} y & 1 \\ 1 & y \end{bmatrix} \end{aligned}$$

### 5.3 Security Aspects of Proposed Cryptosystem

This section deals with some aspects of security against known attacks related to our proposed cryptosystem.

#### Ciphertext Only Attack

Consider the following ciphertext  $C = (C_1, C_2)$  and plaintext  $m$ . The system of equations are of the following form

$$\begin{aligned} C_1 &= \eta^{-1} P_2^X \\ C_2 &= \eta^2 P_1^X m P_1^X. \end{aligned}$$

The random matrix  $X$ , the plaintext  $m$  and the unit element  $\eta$  are unknown to cryptanalyst. For finding these matrices a cryptanalyst has to find the solution of the system of equations. Further if he guesses the value  $\eta_0 = \eta$  and get

$$\eta_0 C_1 = P_2^X.$$

Powers of units can be handled as easily as units itself but these powers are very difficult to attack as a difficulty to play with a DLP. As knowing the powers of unit is not enough to find the unit itself. This new system has both the difficulty of trying to find the inverse of a unit and the difficulty of the DLP. The obtained system becomes very large with large number of unknowns as compared with the system of non linear equations. In this manner, a solution becomes infeasible.

### Known Plaintext Attack

Now we discuss the known plaintext attack. Let the plaintext ciphertext pair be  $(m^{(i)}, C^{(i)})$ ,  $(i = 2, 3, 4, \dots, n)$ . From the pair  $(m^{(i)}, C^{(i)})$ , an attacker wants to find the plaintext  $m^{(n+1)}$  corresponding the ciphertext  $C^{(n+1)}$ . In our proposed cryptosystem we have used different keys  $X$  to get new plaintext, which does not give enough knowledge to find the next unknown plaintext ciphertext pair. Because of this association of every plaintext with a different  $X$ , the requirement of standard model of known plaintext does not fulfill. So our proposed scheme is clearly secure against known plaintext attack.

## 5.4 Conclusion

This chapter is mainly concerned with the development of a new ElGamal like public key cryptosystem. It was shown that the proposed scheme is secured. We gave some concepts about the structure of grouping as well as units of grouping. The use of invertible circulant matrices is one of the main feature of our proposal since multiplication of such matrices is very efficient. As, we have used the matrices over grouping and no quantum algorithm is known for these structures, the

proposed cryptosystem is secure. Further, for a very small values of  $n$  and  $m$ , the size of a grouping  $\mathbb{Z}_n[C_m]$  grows rapidly very fast. This is the main reason to choose the structure of grouping. For example  $M_n(\mathbb{Z}_n[C_m])$  of  $n \times n$  matrices has an order  $(n^m)^{n \times n}$ . As a resultant, this scheme seems to be more reliable.



# Chapter 6

## A Variant of ElGamal Cryptosystem Based on General Linear Group and Grouping

In this chapter, our main aim is to construct a variant of public key cryptosystem presented in Chapter 5. Here we proposed a cryptosystem based on  $GL(n, GR)$ . Due to choice of our platform it gives good level of security. The hard problem for our proposal is the mixture of DLP and CSP. Some security aspects have also been addressed. This chapter is summarized as follows:

First section presents the proposed public key cryptosystem and a toy example which will help to explain the proposed cryptosystem in detail. Without security, cryptosystems have no value so in the Section 6.2, a detailed discussion will take place on security aspects of proposed cryptosystem .

### 6.1 Proposed Cryptosystem

In Cryptosystem 5.2, we proposed a scheme based on invertible circulant matrices whereas in Cryptosystem 6.1, we proposed a scheme based on general linear group. Subgroup of invertible circulant matrices are special case of general linear group. The cryptosystem based on invertible circulant matrices is easy to handle since

only one row (column) is required to be preserved but it restricts the choices of matrix entries. In general linear group we have lot of choices for the matrix entries. Therefore we have discussed the general case of invertible circulant matrices that is general linear group. The encryption scheme of Cryptosystem 6.1 is different from Cryptosystem 5.2 due to addition of Equation (6.4) and in this way our cryptosystem becomes more secure.

The key generation, encryption and decryption algorithm will help us to define all the characteristics of proposed scheme. To understand this scheme, a toy example will also be given in this section.

### Cryptosystem 6.1.1.

The general scheme of proposed cryptosystem is described as follows:

#### Key Generation

For key generation, Alice will follow these steps:

1. She selects any matrix  $A \in GL(n, GR)$ .
2. Next, she calculates the matrices as:

$$B = A^2 \quad \text{and} \quad D = A^3, \quad (6.1)$$

and

$$M = B^2D \quad \text{and} \quad N = BD^2. \quad (6.2)$$

3. She randomly chooses a matrix  $R \in GL(n, GR)$  to calculate the conjugates of  $R$  by  $M$  and  $N$

$$R^M = P_1, \quad (R^{-1})^N = P_2 \quad \text{and} \quad BD \quad (6.3)$$

4. The public key of Alice is the triplets

$$(P_1, P_2, BD).$$

and the private/secret key is the pair

$$(B, D).$$

### Encryption

If Bob wants to communicate with Alice, then he send the message/plaintext

$$m \in M(n, GR)$$

to Alice and follows these steps:

1. Bob selects an integer  $n_0 \in N$  and computes a matrix

$$Y = (BD)^{n_0} \tag{6.4}$$

and also calculates conjugates

$$P_1^Y, P_2^Y.$$

2. He picks any randomly invertible element  $\rho$  of grouping and sends the ciphertext

$$C = (c_1, c_2), \tag{6.5}$$

where

$$c_1 = \rho^{-1} P_2^Y \quad \text{and} \quad c_2 = \rho^2 P_1^Y m P_1^Y. \tag{6.6}$$

### Decryption

When Alice receives the ciphertext  $C = (c_1, c_2)$ , she first computes

$$t = ((c_1)^B)^{D^{-1}}. \tag{6.7}$$

Then she finally decrypts the ciphertext as

$$tc_2t = m, \tag{6.8}$$

to find the plaintext  $m$ .

**Theorem 6.1.2.**

Decryption in the Cryptosystem 6.1 is correct.

*Proof.* The justification of the scheme is guaranteed as follows:

$$t = (c_1^B)^{D^{-1}} = Dc_1^B D^{-1}$$

and

$$c_2 = \rho^2 P_1^Y m P_1^Y = \rho^2 Y^{-1} P_1 Y m Y^{-1} P_1 Y$$

$$\begin{aligned} c_2 t &= \rho^2 P_1^Y m P_1^Y (c_1^B)^{D^{-1}} \\ &= \rho^2 Y^{-1} P_1 Y . D c_1^B D^{-1} m Y^{-1} P_1 Y . D c_1^B D^{-1} \\ &= \rho^2 P_1 Y . D B^{-1} c_1 B D^{-1} m Y^{-1} P_1 Y . D B^{-1} c_1 B D^{-1}, \end{aligned}$$

since  $c_1 = \rho^{-1} (P_2)^Y = \rho^{-1} Y^{-1} P_2 Y$ , it follows that

$$\begin{aligned} t c_2 t &= \rho m Y^{-1} M^{-1} R M Y . D B^{-1} \rho^{-1} Y^{-1} P_2 Y B D^{-1} \\ &= \rho m Y^{-1} D^{-1} B^{-2} R B^2 D Y . D B^{-1} \rho^{-1} Y^{-1} N^{-1} R^{-1} N Y B D^{-1} \\ &= \rho m Y^{-1} D^{-1} B^{-2} R B^2 D Y \rho^{-1} D^{-1} B^{-2} Y^{-1} R^{-1} B^2 D Y. \end{aligned}$$

Since  $B, D, B^2 D$  and  $B D^2$  are the integral multiples of  $A$ , all the defined matrices commutes.

$$\begin{aligned} t c_2 t &= \rho \rho^{-1} m Y^{-1} D^{-1} B^{-2} R Y B^2 D D^{-1} B^{-2} Y^{-1} R^{-1} B^2 D Y \\ &= m Y^{-1} D^{-1} B^{-2} R Y B^2 B^{-2} Y^{-1} R^{-1} B^2 D Y \\ &= m Y^{-1} D^{-1} B^{-2} R Y Y^{-1} R^{-1} B^2 D Y \\ &= m Y^{-1} D^{-1} B^{-2} R R^{-1} B^2 D Y \\ &= m Y^{-1} D^{-1} B^{-2} B^2 D Y \\ &= m Y^{-1} D^{-1} D Y \\ &= m Y^{-1} Y \\ t c_2 t &= m. \end{aligned}$$

□

**Example 6.1.3. (Toy Example)**

This section concludes with a toy example which illustrates our proposed cryptosystem. For this purpose, let us consider cyclic group  $G = C_3$  the ring  $R = \mathbb{Z}_2$  where  $G = C_3 = \{1, w, w^2\} = \langle w \rangle = \langle w : w^3 = 1 \rangle$  and  $R = \mathbb{Z}_2 = \{0, 1\}$  Then one can define

$$\mathbb{Z}_2 C_3 = \left\{ \sum_{g \in C_3} a_g g : a_g \in R \right\}$$

$$GR = \mathbb{Z}_2 C_3 = \{0, 1, w, 1 + w, w^2, 1 + w^2, w + w^2, 1 + w + w^2\}$$

Let  $GL(2, GR)$  be the general linear group of matrices of order 2 over grouping.

Let us consider the random matrix

$$A = \begin{bmatrix} 1 & 1 + w^2 \\ w^2 & w \end{bmatrix} \in GL(2, \mathbb{Z}_2 C_3).$$

Next, Alice will compute the following matrices as

$$B = A^2 = \begin{bmatrix} 1 & 1 + w^2 \\ w^2 & w \end{bmatrix} \begin{bmatrix} 1 & 1 + w^2 \\ w^2 & w \end{bmatrix}$$

$$B = \begin{bmatrix} 1 + w + w^2 & w + w^2 \\ 1 + w^2 & w \end{bmatrix},$$

$$D = A^3 = AA^2$$

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

$$D = \begin{bmatrix} w^2 & 1 + w^2 \\ w^2 & 1 + w + w^2 \end{bmatrix},$$

$$M = B^2 D = \begin{bmatrix} 1 + w + w^2 & w + w^2 \\ 1 + w^2 & w \end{bmatrix}^2 \begin{bmatrix} w^2 & 1 + w^2 \\ w^2 & 1 + w + w^2 \end{bmatrix}$$

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

$$M = \begin{bmatrix} 1 + w + w^2 & 1 + w \\ 1 & 1 \end{bmatrix} \quad \text{and}$$

$$N = BD^2 = \begin{bmatrix} 1 + w + w^2 & w + w^2 \\ 1 + w^2 & w \end{bmatrix} \begin{bmatrix} w^2 & 1 + w^2 \\ w^2 & 1 + w + w^2 \end{bmatrix}^2$$

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

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

Alice again chooses a random matrix

$$R = \begin{bmatrix} 1 & w \\ 1 + w + w^2 & 1 + w \end{bmatrix} \in GL(2, \mathbb{Z}_2C_3)$$

and computes

$$\begin{aligned} R^{-1} &= \frac{1}{|R|} \text{adj}(R) = \frac{1}{w^2} \begin{bmatrix} 1 & w \\ 1 + w + w^2 & 1 + w \end{bmatrix} \\ &= w \begin{bmatrix} 1 + w & w \\ 1 + w + w^2 & 1 \end{bmatrix}, \quad (w^2)^{-1} = w \pmod{\mathbb{Z}_2C_3} \\ &= \begin{bmatrix} w + w^2 & w^2 \\ 1 + w + w^2 & w \end{bmatrix}. \end{aligned}$$

$$M^{-1} = \frac{1}{|M|} \text{adj}(M) = \frac{1}{w^2} \begin{bmatrix} 1 + w + w^2 & 1 + w \\ 1 & 1 \end{bmatrix}$$

$$M^{-1} = w \begin{bmatrix} 1 & 1 + w \\ 1 & 1 + w + w^2 \end{bmatrix}, \quad (w^2)^{-1} = w \pmod{\mathbb{Z}_2C_3}$$

$$M^{-1} = \begin{bmatrix} w & w + w^2 \\ w & 1 + w + w^2 \end{bmatrix}.$$

$$\begin{aligned}
N^{-1} &= \frac{1}{|N|} \text{adj}(N) = \frac{1}{w} \begin{bmatrix} w & w + w^2 \\ 1 + w^2 & 1 + w + w^2 \end{bmatrix} \\
N^{-1} &= w^2 \begin{bmatrix} 1 + w + w^2 & w + w^2 \\ 1 + w^2 & w \end{bmatrix}, \quad (w)^{-1} = w^2 \pmod{\mathbb{Z}_2C_3} \\
N^{-1} &= \begin{bmatrix} 1 + w + w^2 & 1 + w \\ w + w^2 & 1 \end{bmatrix}.
\end{aligned}$$

$$\begin{aligned}
P_1 &= R^M = M^{-1}RM \\
P_1 &= \begin{bmatrix} w & w + w^2 \\ w & 1 + w + w^2 \end{bmatrix} \begin{bmatrix} 1 & w \\ 1 + w + w^2 & 1 + w \end{bmatrix} \begin{bmatrix} 1 + w + w^2 & 1 + w \\ 1 & 1 \end{bmatrix} \\
P_1 &= \begin{bmatrix} 1 & 1 \\ w^2 & w \end{bmatrix}
\end{aligned}$$

$$\begin{aligned}
P_2 &= (R^{-1})^N = N^{-1}R^{-1}N \\
&= \begin{bmatrix} 1 + w + w^2 & 1 + w \\ w + w^2 & 1 \end{bmatrix} \begin{bmatrix} w + w^2 & w^2 \\ 1 + w + w^2 & w \end{bmatrix} \begin{bmatrix} w & w + w^2 \\ 1 + w^2 & 1 + w + w^2 \end{bmatrix} \\
&= \begin{bmatrix} 1 + w^2 & 1 + w + w^2 \\ 1 + w + w^2 & 1 \end{bmatrix} \quad \text{and}
\end{aligned}$$

$$\begin{aligned}
BD &= \begin{bmatrix} 1 + w + w^2 & w + w^2 \\ 1 + w^2 & w \end{bmatrix} \begin{bmatrix} w^2 & 1 + w^2 \\ w^2 & 1 + w + w^2 \end{bmatrix} \\
&= \begin{bmatrix} w^2 & 0 \\ 1 + w + w^2 & w^2 \end{bmatrix}
\end{aligned}$$

So the triplets  $(P_1, P_2, BD)$  is Alice's public key. If Bob wants to send the message  $m$  as:

$$m = \begin{bmatrix} 0 & 1 \\ w^2 & w \end{bmatrix} \in M(2, \mathbb{Z}_2C_3),$$

then he choose a natural number  $n_0 = 3$  and computes the matrix

$$Y = (BD)^{n_0} = \begin{bmatrix} w^2 & 0 \\ 1 + w + w^2 & w^2 \end{bmatrix}^3$$

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

and its inverse is

$$Y^{-1} = \frac{1}{|Y|} \text{adj}(Y) = \frac{1}{1} \begin{bmatrix} 1 & 0 \\ 1 + w + w^2 & 1 \end{bmatrix}$$

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

He calculates the conjugates

$$P_1^Y = Y^{-1}P_1Y$$

$$P_1^Y = \begin{bmatrix} 1 & 0 \\ 1 + w + w^2 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ w^2 & w \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 + w + w^2 & 1 \end{bmatrix}$$

$$P_1^Y = \begin{bmatrix} 1 + w + w^2 & 1 \\ w^2 & 1 + w^2 \end{bmatrix}$$

$$P_2^Y = Y^{-1}P_2Y$$

$$P_2^Y = \begin{bmatrix} 1 & 0 \\ 1 + w + w^2 & 1 \end{bmatrix} \begin{bmatrix} 1 + w^2 & 1 + w + w^2 \\ 1 + w + w^2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 + w + w^2 & 1 \end{bmatrix}$$

$$P_2^Y = \begin{bmatrix} w & 1 + w + w^2 \\ 1 + w + w^2 & w + w^2 \end{bmatrix}$$

Let  $\rho = w^2 \in \mathbb{Z}_2C_3$  be the invertible element of groupring. The inverse is

$$(w^2)^{-1} = w \pmod{\mathbb{Z}_2C_3}$$

Finally he computes



$$c_1 = \rho^{-1}P_2^Y = w \begin{bmatrix} w & 1 + w + w^2 \\ 1 + w + w^2 & w + w^2 \end{bmatrix}$$

$$c_1 = \begin{bmatrix} w^2 & 1 + w + w^2 \\ 1 + w + w^2 & 1 + w^2 \end{bmatrix} \quad \text{and}$$

$$\begin{aligned} c_2 &= \rho^2 P_1^Y m P_1^Y \\ &= (w^2)^2 \begin{bmatrix} 1 + w + w^2 & 1 \\ w^2 & 1 + w^2 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ w^2 & w \end{bmatrix} \begin{bmatrix} 1 + w + w^2 & 1 \\ w^2 & 1 + w^2 \end{bmatrix} \\ &= (w^2)^2 \begin{bmatrix} 1 + w + w^2 & 1 \\ w^2 & 1 + w^2 \end{bmatrix} \begin{bmatrix} w^2 & 1 + w^2 \\ w + w^2 & 1 + w + w^2 \end{bmatrix} \\ &= \begin{bmatrix} 1 + w + w^2 & w \\ 1 & 1 + w \end{bmatrix} \begin{bmatrix} w^2 & 1 + w^2 \\ w + w^2 & 1 + w + w^2 \end{bmatrix} \\ &= \begin{bmatrix} w & 1 + w + w^2 \\ 1 + w + w^2 & 1 + w^2 \end{bmatrix} \end{aligned}$$

to get the ciphertext  $C = (c_1, c_2)$ . To obtain the original plaintext, Alice will perform the following steps:

First she calculates the matrices

$$\begin{aligned} (c_1)^B &= B^{-1}c_1B \\ (c_1)^B &= \begin{bmatrix} 1 & 1 + w \\ w + w^2 & 1 + w + w^2 \end{bmatrix} \begin{bmatrix} w^2 & 1 + w + w^2 \\ 1 + w + w^2 & 1 + w^2 \end{bmatrix} \times \\ &\begin{bmatrix} 1 + w + w^2 & w + w^2 \\ 1 + w^2 & w \end{bmatrix} \\ (c_1)^B &= \begin{bmatrix} w & 1 \\ 1 + w + w^2 & 1 + w \end{bmatrix}. \end{aligned}$$

$$\begin{aligned} t &= \left( (c_1)^B \right)^{D^{-1}} = D (c_1)^B D^{-1} \\ t &= \begin{bmatrix} w^2 & 1 + w^2 \\ w^2 & 1 + w + w^2 \end{bmatrix} \begin{bmatrix} w & 1 \\ 1 + w + w^2 & 1 + w \end{bmatrix} \begin{bmatrix} 1 + w + w^2 & 1 + w^2 \\ w^2 & w^2 \end{bmatrix} \end{aligned}$$

$$t = \begin{bmatrix} w + w^2 & w^2 \\ w & 1 + w + w^2 \end{bmatrix}.$$

She finally obtains original plaintext/message as

$$\begin{aligned} c_2 t &= \begin{bmatrix} w & 1 + w + w^2 \\ 1 + w + w^2 & 1 + w^2 \end{bmatrix} \begin{bmatrix} w + w^2 & w^2 \\ w & 1 + w + w^2 \end{bmatrix}, \\ &= \begin{bmatrix} w & w + w^2 \\ 1 + w & 1 + w + w^2 \end{bmatrix}, \\ t c_2 t &= \begin{bmatrix} w + w^2 & w^2 \\ w & 1 + w + w^2 \end{bmatrix} \begin{bmatrix} w & w + w^2 \\ 1 + w & 1 + w + w^2 \end{bmatrix}, \\ &= \begin{bmatrix} 0 & 1 \\ w^2 & w \end{bmatrix}, \\ &= m. \end{aligned}$$

## 6.2 Security Analysis of Proposed Cryptosystem

In the above section, we have proposed the public key cryptosystem. It is not enough to propose the new cryptosystems but the security aspects are very important. The security of proposed public key cryptosystem against different attacks, is discussed in this section.

Let us consider an attacker only knows the ciphertext  $C = (c_1, c_2)$  where  $c_1$  and  $c_2$  are given in expression (6.6). An adversary knows only the matrices  $P_1$ ,  $P_2$  and  $BD$  which is publicly announced. He wants to know the unknown matrices  $m'$ ,  $Y$  and invertible element  $\rho$  of grouping. Here he has system of equations for the ciphertext  $C = (c_1, c_2)$  corresponding to plaintext  $m$

$$\begin{aligned} c_1 &= \rho^{-1}(P_2)_i^Y, \\ c_2 &= \rho^2 P_1^Y m' P_1^Y. \end{aligned}$$

To find the value of  $Y$  an adversary has to find the solution of the system of equations by letting the invertible element  $\rho_0 = \rho$ , and he gets

$$\rho_0 c_1 = P_2^Y.$$

Then in the second equation of system, he put each solution by letting  $X = X_0$  and get

$$c_2 = \rho_0^2 P_1^{Y_0} m' P_1^{Y_0}.$$

He finds the corresponding solution  $m' = m_0$ . Thus for each fixed  $\rho_0 = \rho$ , an attacker receives number of forms  $(Y_0, m_0)$ .

Here we have a large system of equations with large number of unknowns as adversary has to solve first the DLP then he has to find the conjugators and in the end he will solve the system of non linear equations. No matter how an adversary rearranges these equations, the problem of having a product of two unknown matrices can not be avoided which leads to a large system of nonlinear equations in the large number of unknown entries. This solution becomes infeasible.

Now we will talk about the known plaintext attack. Let us consider an attacker knows the ciphertext  $C = (c_1, c_2)$  corresponding to plaintext  $m'$ . Let the plaintext ciphertext be the pair  $(m', C)$ . From this plaintext ciphertext pair he wants to find the next plaintext  $m'$  corresponding to the ciphertext  $C$ . In the above proposed public key cryptosystem, these type of attacks are impossible because the ciphertext of every block of message is  $m$  calculated with the choice of different session keys. Hence it do not provide enough information to find the next unknown plaintext ciphertext pair. As a consequence, we have shown that our proposed cryptosystem is secured against known plaintext attack.

### 6.3 Conclusion

The successful quantum algorithm radiate doubts on many public key cryptosystems based on discrete logarithm and integer factorization problem. We have shown in Section 6.2 that the proposed scheme is secure against known plaintext

attack. In the Example 6.1.3, we considered the fix grouping and fix unit for encryption and decryption and observes that to find the units and their inverses is such a big problem itself. Our main aim is to construct a variant of ElGamal public key cryptosystem based on general linear group over grouping. As we have already said in the beginning of the Section 6.1, for general linear group we have more options for the matrix entries for example  $GL_n(\mathbb{Z}_n[C_m]) = (n.m)^n(n^m)^n$ . In view of Example 6.1.3, it will be valuable to say that the complex parametric structure of units provide indeterministic peculiarities. As a result, this scheme is more secured.

# Bibliography

- [1] I. Anshel, M. Anshel, and D. Goldfeld, “An algebraic method for public-key cryptography”, *Mathematical Research Letters* 6, 287-291, 1999.
- [2] I. Anshel, M. Anshel, and D. Goldfeld, “Non-abelian key agreement protocols”, *Discrete Applied Mathematics- Special issue on the 2000 com2MaC* , vol. 130, 3-12, 2003.
- [3] I. Anshel, M. Anshel, and D. Goldfeld, “A linear time matrix key agreement protocol over small finite fields”, *Applicable Algebra in Engineering, Communication and Computing*, vol. 17, 195-203, 2006.
- [4] J. C. Birget, S. S. Magliveras, and M. Sramka, “On public key cryptosystems based on combinatorial group theory”, *Tatra Mountains Mathematical Publications*, vol. 33, 137-148, 2006.
- [5] J. Buchmann, “Braid-based cryptography”, Springer-Verlag, New York(2001).
- [6] Z. Cao, X. Dong, and L. Wang, “New public key cryptosystems using polynomials over noncommutative rings ”, *Journal of Cryptology-IACR*, vol. 9, 1-35, 2007.
- [7] J. C. Cha, K. H. Ko, S. J. Lee, J. W. Han, and J. H. Cheon, “An efficient implementation of braid groups” in *Advances in Cryptology-ASIACRYPT 2001*, C. Boyd, vol. 2248 of *Lecture Notes in Computer Science*, 144-156, Springer, Berlin, Germany, 2001.

- 
- [8] C. Y. Chao, "On a type of circulants", *Linear Algebra and its Applications*, vol. 6, 241-248, 1973.
- [9] C. Y. Chao, "A remark on symmetric circulant matrices", *Linear Algebra and its Applications*, vol. 103, 133-148, 1988.
- [10] M. Charalambos, C. Koupparis, "Non-commutative cryptography: Diffie Hellman and CCA secure cryptosystems using matrices over group rings and digital signatures", Pro Quest LLC, Ann Arbor, Thesis (Ph.D), City University of New York, 2012.
- [11] D. Coppersmith, "The Data Encryption Standard (DES) and its strength against attacks", *IBM Journal of Research and Development*, vol. 38, 243-250, 1994.
- [12] L. Creedon, "A Course in Grouping", 2004.
- [13] J. Daemen and V. Rijmen, "AES Proposal: Rijndael, AES algorithm submission", 1999.
- [14] P. J. Davis, "Circulant Matrices", Chelsea, 1994.
- [15] P. Dehornoy, "Braid-based cryptography", *Contemporary Mathematics*, vol. 360, 2004.
- [16] W. Diffie and M. Hellman, "New directions in cryptography", *IEEE Transactions on Information Theory*, vol. 22, 644-654, 1976.
- [17] T. ElGamal, "A public key cryptosystem and a signature scheme based on Discrete Logarithms", *IEEE Transactions on Information Theory*, vol. 31, 469-472, 1985.
- [18] J. B Fraleigh, "A First Course in Abstract Algebra", Addison Wesley Publishers, 1982.
- [19] D. Garber, "Braid group cryptography", arXiv:0711.3941v2, 2008.
- [20] D. Grigoriev and I. Ponomarenko, "On non-Abelian homomorphic public-key cryptosystems", *Journal of Mathematical Sciences*, vol. 126, 1158-1166, 2002.

- [21] D. Grigoriev and I. Ponomarenko, “Homomorphic public-key cryptosystems over groups and rings” <https://arxiv.org/abs/cs/0309010v1>.
- [22] T. Hanoyamak and O. Kusmus, “On construction of cryptographic systems over units of groupings”, *International Electronic Journal of Pure and Applied Mathematics*, vol. 9, 37-43, 2015.
- [23] D. Hofheinz and R. Steinwandt, “A practical attack on some braid group based cryptographic primitives in public key cryptography”, 6th International Workshop on Practice and Theory in Public Key Cryptography, PKC 2003 Proceedings, Y.G. Desmedt, ed., *Lecture Notes in Computer Science* 2567, 187-198, 2002.
- [24] J. Hughes and A. Tannenbaum, “Length-based attacks for certain group based encryption rewriting systems”, Workshop SECI02 Securite de la Communication sur Internet, September 2002, Tunis, Tunisia. <http://www.storagetek.com/hughes/>.
- [25] B. Hurley, and T. Hurley, “Group Ring Cryptography”, *International Journal of Pure and Applied Mathematics*, vol. 69, 67-86, 2010.
- [26] S. Inam and R. Ali, “A new ElGamal-like cryptosystem based on matrices over grouping”, *Neural Computing and Applications*, vol. 29, 1279-1283, 2018.
- [27] D. Kahrobaei, C. Koupparis, V. Shpilrain, “A CCA secure cryptosystem using matrices over grouping”, arXiv:1403.3660, 2014.
- [28] S. Kanwal and R. Ali, “A cryptosystem with noncommutative platform groups”, *Neural Computing and Applications*, vol. 29, 1273-1278, 2018.
- [29] A. Kitaev, “Quantum measurements and the Abelian Stabilizer Problem”, Preprint arXiv: cs.CR/quant-ph/9511026, 1995.
- [30] K. H. Ko, S. J. Lee, J. H. Cheon, J. H. Han, J. S. Kang and C. Park, “New public-key cryptosystems using Braid groups”, *CRYPTO '00 Proceedings of the 20th Annual International Cryptology Conference on Advances in Cryptology*, 166-183, 2000.

- 
- [31] J. Kubo, “The dihedral group as a family group” *Quantum Field Theory and Beyond*, World Science Publication, 46-63, 2008.
- [32] S. S. Magliveras, D. R. Stinson, and T. V. Trung, “New approaches to designing public key cryptosystems using one way functions and trapdoors in finite groups,” *Journal of Cryptology*, vol. 15, 285-297, 2002.
- [33] R. Magyarik and N. R. Wagner, “A public key cryptosystem based on the word problem”, *Workshop on the Theory and Application of Cryptographic Techniques CRYPTO 1984: Advances in Cryptology*, vol. 196, 19-36, 1985.
- [34] A. Mahalanobis, “The Discrete Logarithm Problem in the group of non-singular circulant matrices”, *Groups Complexity Cryptology*, vol. 2, 83-39, 2010.
- [35] A. Mahalanobis, “The ElGamal cryptosystem over circulant matrices”, [arXiv:1109.6416\[cs.CR\]](https://arxiv.org/abs/1109.6416), 2012.
- [36] A. Mahalanobis, “Are matrices useful in public-key cryptography”, *International Mathematical Forum*, vol. 8, 1939-1953, 2013.
- [37] A. Menezes, “*Elliptic Curve Public Key Cryptosystems*”, Kluwer Academic Publications, 1993.
- [38] A. J. Menezes, P. C. V. Oorschot and S. A. Vanstone, “*Handbook of Applied Cryptography*”, CRC Press; 1 edition (October 16, 1996).
- [39] C. P. Milies and S. K. Sehgal, “*An Introduction to Groupings*”, Kluwer Academic Publishers, Dordrecht(2002).
- [40] D. N. Moldovyan and N. A. Moldovyan, “A new hard problem over non-commutative finite groups for cryptographic protocols”, *Computer Network Security: 5th International Conference on Mathematical Methods, Models and Architectures for Computer Network Security, MMM-ACNS 2010*, St. Petersburg, Russia, September 8–10, 2010. Proceedings, vol. 6258 of *Lecture Notes in Computer Science*, 183-194, Springer, Berlin, Germany, 2010.



- 
- [41] A. G. Myasnikov, V. Shpilrain and A. Ushakov, “Group-Based Cryptography”, Advanced Courses in Mathematics, CRM Barcelona, 2007.
- [42] P. C. V. Oorschot and M. J. Wiener, “On Diffie-Hellman key agreement with short exponents”, International Conference on the Theory and Applications of Cryptographic Techniques EUROCRYPT 1996: Advances in Cryptology EUROCRYPT 96, vol. 1070, 332-343, 1996.
- [43] C. Paar and J. Pelzl, “Understanding Cryptography”, Springer-Verlag, 2010.
- [44] S. H. Paeng, K. C. Ha, J. H. Kim, S. Chee, and C. Park, “New public key cryptosystem using finite non abelian groups” Advances in Cryptology-CRYPTO 2001, J. Kilian, vol. 2139 of Lecture Notes in Computer Science, 470-485, Springer, Berlin, Germany 2001.
- [45] D. S. Passman, “The Algebraic Structure of Group Rings”, Wiley (1977).
- [46] J. Proos and C. Zalka, “Shor’s discrete logarithm quantum algorithm for elliptic curves”, Quantum Information and Computation, vol. 3, 317-344, 2003.
- [47] P. V. Reddy, G. S. G. N. Anjaneyulu, D. V. Ramakoti Reddy, and M. Padmavathamma, “New digital signature scheme using polynomials over noncommutative groups”, International Journal of Computer Science and Network Security, vol.8, 245-250, 2008.
- [48] R. L. Rivest, A. Shamir and L. Adleman, “A method for obtaining digital signatures and public key cryptosystems”, Communications of the ACM 21, 120-126, 1978.
- [49] M. Robshaw, “Stream Ciphers. RSA Laboratories Technical Report TR-701”, July 1995. <http://www.rsasecurity.com/rsalabs>.
- [50] S. K. Rososhek, “Cryptosystems in automorphism groups of groupings of abelian groups,” Fundamentalnaya i Prikladnaya Matematika, vol. 13, 157-164, 2007.

- 
- [51] S. K. Rososhek, “Cryptosystems in automorphism groups of groupings of abelian groups”, *Journal of Mathematical Sciences*, Vol. 154, 386-391, 2008. doi:10.1007/s10958-008-9168-2.
- [52] S. K. Rososhek, “Modified Matrix Modular Cryptosystem”, *British Journal of Mathematics and Computer Science*, vol. 5, 613-636, 2015.
- [53] P. W. Shor, “Polynomial-Time algorithms for prime factorization and discrete logarithms on a quantum computer”, *SIAM Journal on Computing*, vol. 26, 1484-1509, 1997.
- [54] V. Shpilrain and A. Ushakov, “Thompsons group and public key cryptography”, *ACNS'05 Proceedings of the Third international conference on Applied Cryptography and Network Security*, 151-163, 2005.
- [55] V. Shpilrain and G. Zapata, “Combinatorial group theory and public key cryptography”, *Applicable Algebra in Engineering, Communication and Computing*, vol. 17, 291302, 2006.
- [56] J. H. Silverman, “Fast multiplication in finite fields  $GF(2^n)$ ”, *International Workshop on Cryptographic Hardware and Embedded Systems CHES 1999: Cryptographic Hardware and Embedded Systems*, vol. 1717, 122-134, 1999.
- [57] W. Stallings, “*Cryptography and Network Security: Principles and Practices*”, Sixth Edition, Prentice Hall, 2013.
- [58] D. R. Stinson, “*Cryptography: Theory and Practice*”, Third Edition, Chapman & Hall, Boca Raton, 2005.
- [59] P. Zellini, “On some properties of circulant matrices”, *Linear Algebra and its Applications*, vol. 26, 31-43, 1979.
- [60] M. Z. W. M. Zulkifli, “*Attacks on Cryptography*”, 2008.