

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Finite Field Computation and Their Applications in Data Security



Dawood Shah

**Department of Mathematics
Quaid-i-Azam University
Islamabad, Pakistan
2021**

Finite Field Computation and Their Applications in Data Security



Dawood Shah

Supervised by

Prof. Dr. Tariq Shah

**Department of Mathematics
Quaid-i-Azam University
Islamabad, Pakistan
2021**

Finite Field Computation and Their Applications in Data Security



A Thesis Submitted to the Department of Mathematics, Quaid-i-Azam University,
Islamabad, in the partial fulfillment of the requirement for the degree of

Doctor of Philosophy

in

Mathematics

By

Dawood Shah

Supervised by

Prof. Dr. Tariq Shah
Department of Mathematics
Quaid-i-Azam University
Islamabad, Pakistan
2021

Author's Declaration

I, **Dawood Shah**, hereby state that my PhD thesis titled **Finite Field Computation and Their Applications in Data Security** is my own work and has not been submitted previously by me for taking any degree from the Quaid-I-Azam University Islamabad, Pakistan or anywhere else in the country/world.

At any time if my statement is found to be incorrect even after my graduate the university has the right to withdraw my PhD degree.



Name of Student: **Dawood Shah**

Date: **30-Aug-2021**

Plagiarism Undertaking

I solemnly declare that research work presented in the thesis titled "Finite Field Computation and Their Applications in Data Security" 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 Quaid-i-Azam University 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 afterward of PhD degree, the University reserves the rights to withdraw/revoke my PhD degree and that HEC and the University has the right to publish my name on the HEC/University Website on which names of students are placed who submitted plagiarized thesis.


Student/Author Signature

Name: Dawood Shah

Finite Field Computation and Their Applications in Data Security

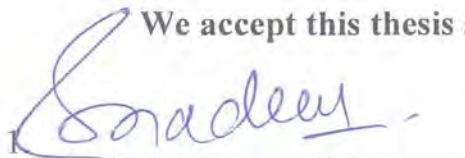
By

Dawood Shah

CERTIFICATE

A THESIS SUBMITTED IN THE PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE OF THE
DOCTOR OF PHILOSOPHY IN MATHEMATICS

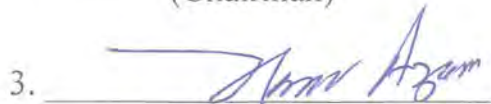
We accept this thesis as conforming to the required standard

1. 

Prof. Dr. Sohail Nadeem
(Chairman)

2. 

Prof. Dr. Tariq Shah
(Supervisor)

3. 

Prof. Dr. Akbar Azam
(External Examiner)

4. 

Dr. Tahir Mehmood
(External Examiner)

Department of Mathematics, COMSATS
University, Park Road Chak Shahzad,
Islamabad.

Department of Mathematics & Statistics
International Islamic University, Sector 11-
10 Islamabad.

Department of Mathematics
Quaid-I-Azam University
Islamabad, Pakistan
2021

Certificate of Approval

This is to certify that the research work presented in this thesis entitled **Finite Field Computation and Their Applications in Data Security** was conducted by **Mr. Dawood Shah** under the kind supervision of **Prof. Dr. Tariq Shah**. No part of this thesis has been submitted anywhere else for any other degree. This thesis is submitted to the Department of Mathematics, Quaid-i-Azam University, Islamabad in partial fulfillment of the requirements for the degree of Doctor of Philosophy in field of Mathematics from Department of Mathematics, Quaid-i-Azam University Islamabad, Pakistan.

Student Name: **Dawood Shah**

Signature: 

External committee:

a) **External Examiner 1:**

Name: **Prof. Dr. Akbar Azam**

Designation: Professor

Office Address: Department of Mathematics, COMSATS University, Park Road Chak Shahzad, Islamabad.

Signature: 

b) **External Examiner 2:**

Name: **Dr. Tahir Mehmood**

Designation: Assistant Professor

Office Address: Department of Mathematics & Statistics, Faculty of Basics Applied Sciences International Islamic University, Islamabad.

Signature: 

c) **Internal Examiner**

Name: **Prof. Dr. Tariq Shah**

Designation: Professor

Office Address: Department of Mathematics, QAU Islamabad.

Signature: 

Supervisor Name:

Prof. Dr. Tariq Shah

Signature: 

Name of Dean/ HOD

Prof. Dr. Sohail Nadeem

Signature: 

Acknowledgment

In the name of Allah, the Most Gracious and the Most Merciful.

All praises to **Allah** and His blessing for the completion of this thesis. I thank God for all the opportunities, trials and strength that have been showered on me to finish writing the thesis. I experienced so much during this process. My humblest gratitude to the holy Prophet **Muhammad** (Peace be upon him) whose way of life has been a continuous guidance for me.

First and foremost, I would like to sincerely thank my supervisor **Prof. Dr. Tariq Shah** for his guidance, understanding, patience and most importantly, he has provided positive encouragement and a warm spirit to finish this thesis. It has been a great pleasure and honour to have him as my supervisor.

I would also like to convey my sincere gratitude to Prof. Dr. Sohail Nadeem, Chairman of the department of mathematics, Quaid-i-Azam University, Islamabad.

My deepest gratitude goes to my beloved parents, brother and sisters for their endless love, prayers and encouragement. It would not be possible to write this thesis without support from them. To those who indirectly contributed in this research, your kindness means a lot to me. Thank you very much.

I also like to thank my colleagues **Tanveer ul Huq**, Ijaz Khalid and Muhammad Imarn Haider, my roommates Adil Sideeq, Muhammad Awais and my friends Fayaz Ali Shah for the necessary cooperation in the accomplishment of my thesis.

Dawood Shah

Preface

In recent decades, due to the speedy development in science and digital technologies, the role of digital data in individual life has been increased. Digital data are nowadays used in every arena of life, such as education, business, banking, engineering and mathematics, art, advertisement, military, medicine, and scientific research. Because of the growing role of digital data in the era of information technologies, the importance of digital data processing tools and digital documentation boosts. Consequently, it has enhanced the distribution of digital data over the internet. Since the internet network is an easily accessible network throughout the world, it has created reasonable prospects that are hazardous for the integrity and secrecy of digital data during distribution over the internet. The study of cryptography is the information security tactics that are used to encounter these threats.

Cryptography has been considered a recognized branch of science for the last 60 years. However, comparatively, it is an entirely new and faster-growing area of the study compared to other science areas, and each moment carries continual developments. Cryptography is broadly divided into two sub-branches; asymmetric-key cryptography and symmetric-key cryptography. This categorization is based on the input key that is secret information used during encryption and decryption. In symmetric-key cryptography, the communicating parties share a private key confidentially. Algorithms such as Lucifer, Data encryption standard (DES), Advanced encryption standard (AES), and the International data encryption algorithm (IDEA) are prominent examples of symmetric key cryptography. The goal of confidential communication can be achieved by using symmetric key cryptography. Since, in symmetric-key cryptography, the communicating entities use the same private key to encrypt and decrypt a message. Thus the distribution of secret keys has enough security issues that enhance the importance of public-key cryptography. In public-key cryptography, a pair of different keys are used for encryption and decryption. The main feature of the asymmetric key cipher is securing the data from the attackers even if they know the key used for encryption. This property resolves two significant problems that are the key distribution problem and authentication with the non-repudiation problem. The RSA algorithm, Elgamal algorithm, Elliptic curve cryptography (ECC), and Pailier cryptosystem are the most commonly practicing examples of public-key cryptography.

Cryptography has been widely used in computer software and hardware in the form of discrete mathematical structures. Accordingly, the binary field $GF(2)$ and its binary Galois

field extensions $GF(2^m)$ are the most useful algebraic structures that have extensive applications in cryptography and computer science. One of the characteristics of $GF(2^m)$ is its soothing implementation in hardware that appeals to researchers to exploit it in cryptography. Reducing the cost and enhancing performance are the primary features of the finite field's applications in cryptology. In this thesis, we have tested the impact of the Galois field on the security feature of symmetric and asymmetric key cryptographic schemes. One of the aims of this study is to improve the arithmetic on the Galois field extension by computations and observe the resultant positive effect on the security of different cryptosystems.

The thesis comprises seven chapters. The first chapter of this thesis briefly discusses the fundamentals of algebraic structures, basic definitions of cryptography, and symmetric and asymmetric cryptography properties. These definitions and properties are then utilized in the other chapters, where various finite field-based cryptographic schemes are discussed. The chapter commences with the basic reports and results of finite extension fields. It has been concluded with complexity theory.

The second chapter of this thesis introduces a fully homomorphic encryption scheme. Homomorphic encryption schemes are the particular kind of encryption schemes that allow computation on the ciphered data. Hence, the data remain confidential during the encryption procedure, enabling practical tasks to be achieved with data residing in the open or untrusted network. The scheme introduced in this chapter is based on finite field isomorphism problems over the matrix field. The finite field isomorphism problems are obtained as; if m is a positive integer and p is a prime number, then there exists a finite field of the order p^m . Finite fields of order p^m are isomorphic. The elements of these fields can be denoted by polynomials or represented by matrices with entries chosen modulo p . The length of an element of the field can be associated with the norm of that element. In general, a non-trivial isomorphic map between any two fields does not preserve the length of the elements. The image of the short element in the other field with entries can uniformly and randomly be distributed over modulo p .

The third chapter of this thesis introduces the modified version of the NTRU scheme. NTRU scheme is the fastest asymmetric key encryption scheme. Its operations take place in the factor ring $\frac{\mathbb{Z}_p[x]}{\langle x^n - 1 \rangle}$ Suitable for both authentication and confidential communication. The security of the NTRU scheme is based on the short vector problem and closest vector

problem in lattices. Its correctness is based on the clustering characteristics of the sums of random values. These hard-mathematical problems are the core of the NTRU techniques against various quantum and classical attacks. However, researchers demonstrate that the scheme is insecure against the lattice-based attack. We have modified the general principle of the NTRU cryptosystem and substitutes the ring $\mathbb{Z}[x]$ with a matrix ring over the Galois field $GF(p^m)$. Since the suggested cryptosystem operates in a high dimensional non-commutative matrix ring. Therefore, the scheme performs more efficiently and can resist lattice-based attacks.

The fourth chapter of this thesis presents a complete review of the Data Encryption Standard (DES) through an improved version. DES is a symmetric key cryptosystem that is widely used in recent times due to its easy implementation in hardware. In the past, the researchers found defects in the assembly of the DES and declared the algorithm insecure against linear and differential cryptanalysis. In this thesis, we have studied the faults in the DES and have made improvements in their internal configuration named the new algorithm Improved DES. The improvement has been made in the substitution step, which is the only nonlinear part of the algorithm. Accordingly, in the substitution phase of the DES, we have introduced a new design of 6×6 S-boxes over the Galois field $GF(2^6)$. On the one hand, the construction method generates robust S-boxes that are secure against linear and differential attacks. Then again, it enhances the keyspace of the Improved DES against brute force attacks.

In chapter five, some efficient algorithms based on binary extension fields $GF(2^m)$ are designed to secure multimedia data. Since multimedia data contain a high amount of data that are significantly correlated, thus, the only dependency on the algorithms like AES, RSA, and DES are not good enough for multimedia data security. Accordingly, in this part of the thesis, some efficient algorithms for multimedia data security are deliberated. The suggested schemes are thoroughly examined against linear and differential attacks. The experimental results demonstrate the efficiency of the systems against various attacks. Furthermore, as a result of a fast and straightforward implementation of the finite binary field in hardware and software, the proposed schemes are more appropriate to implement and applicable for multimedia data security.

Finally, in chapter six, a unique lossless audio data encryption scheme is given. This newly designed scheme is based on arithmetic operations of a Galois field $GF(2^m)$ and an elliptic curve over a finite field \mathbb{Z}_p . As the arithmetic operations of the elliptic curve are performed

efficiently, a decent quality sequence of random numbers is obtained in the initial phase of the encryption procedure. This generated sequence is then used to defuse the matrix of the audio data. The confusion part of the scheme is performed by multiple S-boxes, which have nonlinearity of the optimal level. The experimental results validate the competence of the proposed system against various attacks.

The last chapter is dedicated to the conclusion and a few suggestions for possible future work.

CONTENTS

Algebraic structures and cryptography: A brief review.....	1
1.1 Introduction.....	1
1.2 Algebraic structures.....	1
1.2.1 Ring.....	1
1.2.2 Polynomial Ring.....	3
1.2.3 Field.....	4
1.2.4 Finite Field.....	5
1.2.5 Polynomial ring over a field.....	6
1.2.6 Field Extensions.....	8
1.2.7 Representation of finite field elements.....	10
1.3 Cryptography.....	11
1.3.1 Symmetric Key Cryptography.....	12
1.3.2 Asymmetric Key Cryptography.....	13
1.3.3 Security Analyses of Asymmetric Cryptosystem.....	15
1.4 Algorithm.....	17
1.4.1 Success Probability of an Algorithm.....	18
1.5 On Complexity Theory.....	20
2 Leveled Homomorphic Encryption Scheme Based on Finite Field Isomorphism Problem	22
2.1 Introduction.....	22
2.2 Finite Field Isomorphism.....	23
2.3 Finite Field Isomorphism Problem.....	23
2.4 Basic Definitions and Notations.....	24
2.5 Finding Finite field Isomorphism.....	28
2.6 Homomorphic Encryption.....	28
2.7 Construction of Fully Homomorphic Encryption Scheme.....	29
2.7.1 Symmetric Key Homomorphic Encryption Scheme.....	29
2.7.2 Asymmetric Key Homomorphic Encryption Scheme.....	31
2.8 Performance Analysis.....	35
2.8.1 Lattice Attack.....	36
3 The Study of NTRU Cryptosystem Based on Matrix Ring Over Finite Field Extension	38
3.1 Introduction.....	38
3.2 NTRU Cryptosystem.....	39
3.2.1 Key Generation.....	39

3.2.2	Encryption and decryption	40
3.3	Asymptotic Complexity of NTRU Scheme	42
3.3.1	Mathematical Problem for NTRU Scheme	42
3.3.2	Brute force Attack	43
3.3.3	NTRU key recovery problem as a Lattice Problem	44
3.4	Proposed Cryptosystem	45
3.4.1	Key Generation	46
3.4.2	Encryption	47
3.4.3	Decryption	47
3.5	Mathematical Background	51
3.5.1	Brute Force Attack	51
3.5.2	Asymptotic Complexity	51
4	Security Enhancement of Data Encryption Standard	53
4.1	Introduction	53
4.2	Preliminary ideas	54
4.3	General Outline of DES	55
4.4	Construction of Galois fields $GF(2^6)$ and S-boxes	57
4.4.1	Construction of Galois fields	57
4.4.2	Construction of 6×6 S-boxes	58
4.5	Performance Analyses	60
4.5.1	Nonlinearity	60
4.5.2	Differential Cryptanalysis	60
4.5.3	Strict Avalanche Criterion	61
4.5.4	Linear approximation probability	62
4.6	Modified DES Algorithm	63
4.6.1	Generation of Key dependent 6-bits S-boxes	64
4.6.2	Modified DES Feistel Network	64
4.6.3	Key Complement	65
4.6.4	The Brute force attacks	66
5	A Novel Image Encryption Scheme Based on Finite Algebraic Structures	67
5.1	Introduction	67
5.2	Preliminaries	68
5.3	The algebraic structures-based Encryption algorithm	68
5.3.1	S-boxes Construction	69
5.3.2	Encryption process	69

5.3.3	Decryption process.....	72
5.4	Security and performance analyses	73
5.4.1	Keyspace analysis	73
5.4.2	Histogram analysis.....	74
5.4.3	Information entropy	75
5.4.4	Correlation Analysis	76
5.4.5	Avalanche effect	77
5.4.6	Mean Square Error (MSE).....	79
5.4.7	Peak Signal-to-Noise Ratio (PSNR).....	79
5.4.8	Normalized Cross Correlation (NK).....	80
5.4.9	Average Difference (AD)	80
5.4.10	Structural Content (SC).....	80
5.4.11	Maximum Difference (MD).....	80
5.4.12	Normalized Absolute Error (NAE).....	80
5.4.13	Root Mean Square Error (RMSE).....	81
5.4.14	Universal Quality Index (UQI)	81
5.4.15	Mutual Information (MI)	81
5.4.16	Structural Similarity (SSIM).....	81
5.4.17	Randomness test for cipher.....	82
6	Finite Fields Applications to Digital Audio Security	84
6.1	Introduction	84
6.2	Preliminaries.....	85
6.2.1	Elliptic Curve	85
6.2.2	Elliptic curve arithmetic.....	85
6.2.3	Singular Point.....	86
6.3	Audio Encryption Scheme	87
6.3.1	Proposed Random number generator.....	87
6.3.2	Multiple S-boxes Construction Scheme.....	88
6.3.3	Proposed Algorithm.....	89
6.4	Security analysis.....	91
6.4.1	Spectrogram analysis	92
6.4.2	Histogram Analysis.....	93
6.4.3	Correlation	94
6.4.4	Information entropy	96
6.4.5	Differential attacks.....	97

6.4.6	NIST Statistical Test.....	98
7	Conclusion.....	100
7.1	Summary of Thesis.....	100
7.2	Future Work	101

Chapter 1

Algebraic structures and cryptography

1.1 Introduction

This chapter aims to provide the fundamentals of algebraic structures, cryptography, and complexity theory that are used in the upcoming chapters. Accordingly, this brief review is divided into four sections. The second section consists of basic definitions and properties of the ring and field. The notion of cryptography and the concept of symmetric and asymmetric key cryptography, along with their security analyses, are presented in section three. The fourth section is devoted to the study of algorithms, whereas the notion of asymptotic complexity is given in the last section of this chapter.

1.2 Algebraic structures

Two binary operations, addition and multiplication, are mostly studying in the algebraic system. This section introduces an algebraic structure called ring, which satisfies some basic properties with respect to both of these operations; addition and multiplication. The detail of this section is given in Chapter 2 of Mullen and Panario [1], Chapter 3-6 of Wan [2], Chapter 1 of Mullen and Mummert [3], and Chapter 1-2 of Rudolf and Niederreiter [4].

1.2.1 Ring

A Ring $(\mathcal{R}, +, \cdot)$ is a nonempty set \mathcal{R} together with binary operations, addition $(+)$ and multiplication (\cdot) , such that

1. \mathcal{R} is a commutative group with respect to addition.
2. \mathcal{R} is a semigroup with respect to multiplication.
3. The elements of \mathcal{R} hold left-right distributive law; i.e., for all $x, y, z \in \mathcal{R}$ we have $x \cdot (y + z) = x \cdot y + x \cdot z$ and $(y + z) \cdot x = y \cdot x + z \cdot x$.

Throughout this chapter, we refer symbolically to the ring $(\mathcal{R}, +, \cdot)$ as \mathcal{R} , and emphasize that the binary operations ‘+’ and multiplication ‘ \cdot ’ are not necessarily to be ordinary addition and multiplications of real numbers. Furthermore, element 0 denotes the additive identity of the ring \mathcal{R} . Likewise, the element $-a$ represents the additive inverse of the element $a \in \mathcal{R}$, and ab denotes the multiplication of the elements a and b .

Example 1.1 The most simple and natural example of the ring is a set of integers, which is denoted by \mathbb{Z} . In this way, the set of all integers satisfies all the ring properties with respect to integer addition and multiplication. Besides, if we thoroughly inspect the properties of the

integer ring \mathbb{Z} , we will realize that some of the properties of this ring do not satisfy the ring in general.

Definitions 1.2. The following definitions describe some additional properties of a ring.

- i. \mathcal{R} is said to be a ring with identity if there exists an element e in \mathcal{R} such that

$$ae = a = ea \quad \text{for all } a \in \mathcal{R}.$$

- ii. \mathcal{R} is said to be a commutative ring if for all a and b in \mathcal{R}

$$ab = ba.$$

- iii. \mathcal{R} is said to be a division ring if $\mathcal{R} \setminus \{0\}$ form a group under binary operation multiplication.

- iv. \mathcal{R} is said to be an integral domain if \mathcal{R} is a commutative ring with identity and if for all a and b in \mathcal{R} , whenever

$$ab = 0 \quad \text{implies either } a = 0 \text{ or } b = 0.$$

Example 1.3. The set of integers \mathbb{Z} is a commutative ring with identity. However, ring $2\mathbb{Z}$ is a commutative ring without identity.

Example 1.4. The set $M_n(\mathbb{R})$ of all $n \times n$ matrices with entries from the set of real numbers forms a non-abelian group over binary operations matrix addition and matrix multiplication.

Definition 1.5. A ring \mathcal{R} is said to be a finite ring if \mathcal{R} consists of a limited number of elements and satisfies all the ring's properties.

Example 1.6. The set of residue classes of the integer modulo n forms a finite ring of order n with respect to integer addition and multiplication modulo n . For instance, $n = 4$, then \mathbb{Z}_4 consists of the elements $[0]$, $[1]$, $[2]$ and $[3]$. The addition and multiplication operations of the \mathbb{Z}_4 are defined in the following operation tables that are the same as the Cayley table.

	+	[0]	[1]	[2]	[3]		·		[0]	[1]	[2]	[3]
	[0]	[0]	[1]	[2]	[3]		[0]		[0]	[0]	[0]	[0]
	[1]	[1]	[2]	[3]	[4]		[1]		[0]	[1]	[2]	[3]
	[2]	[2]	[3]	[4]	[0]		[2]		[0]	[2]	[0]	[2]
	[3]	[3]	[4]	[0]	[1]		[3]		[0]	[3]	[2]	[1]

From the operation tables of multiplication, it is clear that \mathbb{Z}_4 is a finite commutative ring with identity, where the identity element is the class [1]. However, it is not an integral domain because $[2][2] = [0]$ and [2] is not equal [0] class.

1.2.2 Polynomial Ring

A polynomial in elementary algebra is an expression of the form $a_0 + a_1x + a_2x^2 + \dots + a_nx^n$, where $a_0 \neq 0$ and a_i (for $0 \leq i \leq n$) are called coefficients. These are mostly from the set of complex or real numbers. The symbol x is the variable that can be substituted by an arbitrary number. The arithmetic operations of polynomials are invented over specific familiar rules. This section discusses the notion of polynomials and their associated arithmetic operations in a generalized algebraic setting.

A polynomial over arbitrary ring \mathcal{R} is an expression that can be written in the form

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^m \quad (1.1)$$

where m is a whole number, the polynomial coefficients a_i (for $0 \leq i \leq m$) are the elements of the ring \mathcal{R} . The symbol x is called indeterminate over the ring \mathcal{R} . In general, it does not belong to \mathcal{R} . Next, we use f for the representation of the polynomial $f(x)$. Let f and g be two polynomials over the ring \mathcal{R} ;

$$f = \sum_{i=0}^n a_i x^i \quad \text{and} \quad g = \sum_{i=0}^m b_i x^i \quad (1.2)$$

Then the polynomials f and g are considered to be equal if and only if $m = n$ and $a_i = b_i$ for all $0 \leq i \leq n$. The addition of the polynomials f and g is defined as;

$$f + g = \sum_{i=1}^{\max(m,n)} (a_i + b_i)x^i \quad (1.3)$$

The polynomial multiplication of the polynomials f and g is defined as

$$fg = \sum_{k=0}^{m+n} d_k x^k, \quad \text{where } d_k = \sum_{i+j=k} a_i b_j \quad (1.4)$$

From these operations, it can be seen that the set of polynomials over polynomial addition and multiplication operations satisfies all the properties of a ring.

Definition 1.7. The ring formed by the set of polynomials over the ring \mathcal{R} with respect to polynomial addition and polynomial multiplication is called polynomial ring, denoted by $\mathcal{R}[x]$.

The additive identity of the polynomial ring $\mathcal{R}[x]$ is the zero polynomial, whose all coefficients are zero that is denoted by 0. The additive inverse of a nonzero polynomial $f \in \mathcal{R}[x]$ is the polynomial $-f$ that belongs to the polynomial ring $\mathcal{R}[x]$. For $a_n \neq 0$, is called the leading coefficient and a_0 is the constant term of the polynomial f . The nonnegative integer n is called the degree of the polynomial f , which is denoted as $deg(f)$. Let \mathcal{R} be a ring with unity, then the polynomial in $\mathcal{R}[x]$ with leading coefficient identity element 1 is called a monic polynomial.

Theorem 1.8. [4, Theorem 1.50] Let \mathcal{R} be an integral domain and let f and g be the elements of the polynomial ring $\mathcal{R}[x]$. Then

$$\begin{aligned} deg(f + g) &= \max\{deg(f), deg(g)\} \\ deg(fg) &= deg(f) + deg(g) \end{aligned}$$

The elements of the ring \mathcal{R} can be view as the constant polynomials. Therefore, the elements of \mathcal{R} contained in the ring $\mathcal{R}[x]$. Thus \mathcal{R} is the subring of $\mathcal{R}[x]$. The properties of \mathcal{R} are inherited by the polynomial ring $\mathcal{R}[x]$. The next theorem shows some of the properties of $\mathcal{R}[x]$, which depend on the subring \mathcal{R} .

Theorem 1.9. [4, Theorem 1.51] Let \mathcal{R} be a ring. Then

- i. $\mathcal{R}[x]$ is a commutative ring if and only if \mathcal{R} is a commutative ring.
- ii. $\mathcal{R}[x]$ is a ring with identity if and only if \mathcal{R} is a ring with identity.
- iii. $\mathcal{R}[x]$ is an integral domain if and only if \mathcal{R} is an integral domain.

From equation (1.4), the polynomial multiplication and addition rely on the coefficients of the polynomials. Accordingly, two polynomials will be commute if their coefficients are commute. The reaming results are apparent. The remaining part of this section is almost deal with the polynomial ring over the field.

1.2.3 Field

The field is an algebraic structure with enormous valuable properties that are substantially studied. These structures are essentials in the applications and theory of cryptology and coding theory. It consists of the elements for which the two binary operations, multiplication and addition satisfy specific properties. The set of Complex numbers, real numbers, and

rational numbers are probably the best examples of the field. Since each of these sets contains an infinite number of distinct elements, therefore these are all infinite fields. Certain finite sets also satisfy the field's properties with appropriate binary operations; such fields are called finite fields. The following subsections focus on the study of finite fields.

Definition 1.10. A field $(\mathbb{F}, +, \cdot)$ is a nonempty set \mathbb{F} together with binary operations, addition denoted by '+' and multiplication denoted by ' \cdot ' such that

- i. \mathbb{F} is an abelian group with respect to addition.
- ii. $\mathbb{F} \setminus \{0\}$ is a commutative group with respect to multiplication.
- iii. The elements of \mathbb{F} hold left-right distributive law; i.e. for all $x, y, z \in \mathbb{F}$, we have

$$x \cdot (y + z) = x \cdot y + x \cdot z \text{ and } (y + z) \cdot x = y \cdot x + z \cdot x.$$

We will use \mathbb{F} as an identification for the field $(\mathbb{F}, +, \cdot)$, and we again emphasize that the binary operations addition '+' and multiplication ' \cdot ' are not necessarily ordinary real numbers addition and multiplications. In addition, we denote the multiplicative identity of the group \mathbb{F}^* by 1 and the multiplicative inverse of an element $a \in \mathbb{F}^*$ by a^{-1} .

Example 1.11. The set of all complex numbers \mathbb{C} , real number \mathbb{R} , rational number \mathbb{Q} are the examples of the field with respect to number addition and multiplication.

1.2.4 Finite Field

A field \mathbb{F} is said to be a finite field if the set \mathbb{F} contains finite numbers of elements and satisfy all the properties of the field with respect to addition and multiplication.

Example 1.12. The set of residue classes of the integer modulo prime integer p satisfies all the properties of the field with respect to integer addition and multiplication mode p . For instance, let $p = 5$ then the set \mathbb{Z}_5 consists of the elements $[0], [1], [2], [3]$ and $[4]$. The addition and multiplication operations in the field \mathbb{Z}_5 are defined in the operations table given as follows;

+	[0]	[1]	[2]	[3]	[4]	\cdot	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[1]	[2]	[3]	[4]	[0]	[1]	[0]	[1]	[2]	[3]	[4]
[2]	[2]	[3]	[4]	[0]	[1]	[2]	[0]	[2]	[4]	[1]	[3]
[3]	[3]	[4]	[0]	[1]	[2]	[3]	[0]	[3]	[1]	[4]	[2]
[4]	[4]	[0]	[1]	[2]	[3]	[4]	[0]	[4]	[3]	[2]	[1]

The set of residue classes \mathbb{Z}_p is the example of a finite field, which containing p elements.

1.2.5 Polynomial ring over a field

This subsection discusses the properties of the polynomial ring over the field. Let \mathbb{F} be a field, then the set $\mathbb{F}[x]$ of all polynomials whose coefficients from the field \mathbb{F} form a polynomial ring over polynomial addition and multiplication. This is a special kind of ring that contributes to the concept of divisibility. Let $f \in \mathbb{F}[x]$; then the polynomial f is said to divide the polynomial g , if there exists a polynomial $h \in \mathbb{F}[x]$ such that $f = gh$. The unit elements of $\mathbb{F}[x]$ are those elements that are divisible by the constant identity polynomial 1. For instance, all nonzero constant polynomials are the unit elements of $\mathbb{F}[x]$. The following result is based on the notion of divisibility.

Theorem 1.13. [5, Part IV Theorem 23.1] *Let f not equal to zero polynomial be an element of $\mathbb{F}[x]$. Then for g such that $\deg(g) < \deg(f)$ in $\mathbb{F}[x]$ there exist polynomials q and r in $\mathbb{F}[x]$ such that*

$$f = gq + r \quad \text{where } \deg(r) < \deg(g).$$

The above results revealed the fact that the polynomial ring over field \mathbb{F} permits the division algorithm, which leads the discussion to a significant result given as follows.

Theorem 1.14. [6, Theorem 16.4] *If \mathbb{F} be a field, then the polynomial ring over field \mathbb{F} is a principal ideal domain. For instance, for every ideal $J \neq \langle 0 \rangle$ in $\mathbb{F}[x]$, there exist unique monic polynomial g in $\mathbb{F}[x]$ such that $J = \langle g \rangle$.*

Proof. The polynomial ring $\mathbb{F}[x]$ is an integral domain by Theorem 1.9, Let $J \neq \langle 0 \rangle$ be an ideal of the ring $\mathbb{F}[x]$. Suppose that h be a nonzero polynomial of least degree in the ideal J . Let a be the leading coefficient of h , then the polynomial $g = a^{-1}h$ is the monic polynomial contain in J . By division algorithm, every element of f can be written as the multiple of g . Thus, J is a principal ideal generated by g . Since J is an arbitrary ideal of $\mathbb{F}[x]$ that is principle ideal; therefore $\mathbb{F}[x]$ is a principal ideal domain.

The prime elements of the polynomial ring $\mathbb{F}[x]$ are called irreducible polynomials. The concept of irreducible polynomial plays an impotent role in the invention of finite fields. The following part of this section presents the definition and properties of irreducible polynomials.

Definition 1.15. A polynomial p of the ring $\mathbb{F}[x]$ is said to be irreducible over the field \mathbb{F} . If it has a positive degree and if $p = fg$ with $f, g \in \mathbb{F}[x]$, implies that the degree of f or the degree of g is zero.

In other words, a polynomial of positive degree is said to be irreducible over the field \mathbb{F} , if it allows only trivial factorizations. The polynomials in $\mathbb{F}[x]$ that are not irreducible are called reducible over the field \mathbb{F} . The irreducibility and reducibility of any polynomial depend on the nature of the field \mathbb{F} . For instance, the polynomial $x^2 - 2 \in \mathbb{R}[x]$ is reducible over the field \mathbb{R} of real numbers. However, $x^2 - 2$ is irreducible over the field \mathbb{Q} of rational numbers. The reducible elements of the polynomial ring can be written as the product of irreducible polynomials in a unique manner. The appearance of this fact is justifying the proof of the result given as follows.

Theorem 1.16. [5, Part IV Theorem 23.20] *Any element f of positive degree in the polynomial ring $\mathbb{F}[x]$ can be written in the form*

$$f = cp_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$$

Where p_1, p_2, \dots, p_k are the different monic irreducible polynomials in a polynomial ring, where n_1, n_2, \dots, n_k are natural numbers, and c is the element of the field \mathbb{F} . Besides, the above representation of factorization is unique.

Since we know that irreducible polynomials over \mathbb{F} in the polynomial ring are prime elements, and the ring $\mathbb{F}[x]$ is the principal ideal domain. Therefore, the following result is ascertained as the consequences of the fact that if \mathcal{R} is a principal ideal domain, then $\frac{\mathcal{R}}{(p)}$ is a field if and only if p is a prime element of \mathcal{R} .

Theorem 1.17. [2. Theorem 5.4] *Let f be a polynomial over \mathbb{F} , then the residue classes of the polynomial ring $\mathbb{F}[x]$ over $\langle f \rangle$ forms a field if and only if f be an irreducible polynomial over the field \mathbb{F} .*

The residue classes of the polynomial ring over $\langle f \rangle$ form a polynomial ring, for an arbitrary nonzero polynomial f in $\mathbb{F}[x]$, which consist of residue classes $g + \langle f \rangle$ for $g \in \mathbb{F}[x]$. Each residue class $g + \langle f \rangle$ can be represented by unique element r in $\mathbb{F}[x]$ with $\deg(f) > \deg(r)$ that is equal to the remainder, whenever f divides g . The process of transforming g into r is called reduction modulo f . Two elements $g_1 + \langle f \rangle$ and $g_2 + \langle f \rangle$ of the ring of residue classes are considered to be identical if g_1 divide f leaves the same remainder as g_2 divides f . Since the ring of residue classes consists of all polynomials of degree less than the degree of f . Accordingly, for a finite field \mathbb{F} of order q , and degree n

irreducible polynomial f , the order of the ring $\frac{\mathbb{F}_q[x]}{\langle f \rangle}$ is q^n , which consists of residue classes modulo f .

1.2.6 Field Extensions

Let K be a subset of the field \mathbb{F} . Then K is said to be a subfield of \mathbb{F} if K itself a field with respect to binary operations of the field \mathbb{F} and the field \mathbb{F} is called the extension of K . If $K \subset \mathbb{F}$, then K is said to be a proper subfield of \mathbb{F} . If K be a subfield of the finite field \mathbb{F}_p of order p . Then K must consist of only one element, which is the additive identity 0. It follows that the finite field \mathbb{F}_p contains no proper field.

Definition 1.18. A field is said to be a prime field if it contains no proper subfield.

From the above definition, the finite field of order p is the prime field. For instance, let p be a prime number, then the set of residue classes \mathbb{Z}_p over module prime number p is the example finite prime field. The set of rational numbers \mathbb{Q} is the example of the infinite prime field.

Definition 1.19. Let \mathbb{F} be the extension field of the field K and superset of a nonempty set M . Then the intersection of all subfields of the field \mathbb{F} , which contain both M and K is called the extension field of K , which is denoted by $K(M)$.

For a finite set, $M = \{\theta_1, \theta_2, \dots, \theta_n\}$ one can write $K(M) = K(\theta_1, \theta_2, \dots, \theta_n)$. If M is a singleton set for instance $M = \{\theta\}$ and $\theta \in \mathbb{F}$, then the extension field $K(\theta)$ is called the simple extension of K , and the element θ is called defining element of $K(\theta)$. The extension field $K(M)$ is the smallest subfield containing the field K and the subset M . The subsection discusses some important types of the extension field.

Definition 1.20. Let \mathbb{F} be the extension field of the subfield K , and θ be the element of \mathbb{F} . Then the element θ is said to be algebraic over K if there exist coefficients $b_i \in K$, such that for all $0 \leq i \leq n$, not all b_i equal to zero, θ satisfy the non-trivial degree n polynomial equation, i.e., $b_n\theta^n + b_{n-1}\theta^{n-1} + \dots + b_1\theta^1 + b_0 = 0$. The extension $K(M)$ is said to be an algebraic extension of K , if every element of $K(M)$ is algebraic over K . The least degree polynomial $f = b_nx^n + b_{n-1}x^{n-1} + \dots + b_1x + b_0$ such that $f(x) \in K[x]$ and $f(\theta) = 0$ is called the minimal polynomial, which is the irreducible polynomial in $K[x]$.

Let K be the subfield of the field \mathbb{F} . Then the extension field \mathbb{F} satisfies all the properties of the vector space over the field K , since the elements of \mathbb{F} form an abelian group with respect

to addition. Besides, for each element $f \in \mathbb{F}$ and $k \in K$, the element kf again belongs to \mathbb{F} . Similarly, the laws for multiplication by scalars satisfies; $k(f + g) = kf + kg$. $(f + g)k = fk + gk$, $(k_1k_2)f = k_1(k_2f)$ and $1f = f$, where 1 is the multiplicative identity of K , for $k_1, k_2 \in K$ and $f, g \in \mathbb{F}$.

Definition 1.21. Let K be the subfield of the finite-dimensional vector space \mathbb{F} over K , then \mathbb{F} is called a finite extension of the field K . The dimension of the vector space \mathbb{F} over the field K is called the degree of the field \mathbb{F} , which is denoted by $[\mathbb{F}; K]$.

The study of a simple algebraic extension $K(\theta)$ is invented by adjoining the algebraic elements. Let K be the subfield of the field \mathbb{F} and $\theta \in \mathbb{F}$, then $K(\theta)$ is a finite extension of K . This property connects the notion of the extension field to the field of residue classes.

Theorem 1.22. [4, Theorem 1.86] Let θ be algebraic over the field K , and let g be the irreducible polynomial in $K[x]$ of degree n . Then:

- i. The extension field $K(\theta)$ is isomorphic $\frac{K[x]}{\langle g \rangle}$.
- ii. The dimension of $K(\theta)$ is equal to n and $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$ is a basis of $K(\theta)$ over K .
- iii. For every ϑ algebraic over K in $K(\theta)$, the degree of θ divides the degree of ϑ .

So far, we have discussed the procedure of constructing finite field extension and their properties. The following lemma shows that for every integer q with specific properties, there exists a finite field of order q , where $q = p^n$.

Example 1.23. Let $p(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$. Then the order of the ring $\frac{\mathbb{Z}_2[x]}{\langle p(x) \rangle}$ is 2^2 , containing the elements $[0], [1], [x]$, and $[x + 1]$. The binary operations polynomial addition and multiplication modulo $p(x)$ for the residue class ring is defined in the following operation tables.

+	[0]	[1]	[x]	[x + 1]		·	[0]	[1]	[x]	[x + 1]
[0]	[0]	[1]	[x]	[x+1]		[0]	[0]	[0]	[0]	[0]
[1]	[1]	[0]	[x+1]	[x]		[1]	[0]	[1]	[x]	[x + 1]
[x]	[x]	[x+1]	[0]	[1]		[x]	[0]	[x]	[x+1]	[1]
[x+1]	[x+1]	[x]	[1]	[0]		[x+1]	[0]	[x+1]	[1]	[x]

Since $p(x)$ is an irreducible polynomial, thus by Theorem 1.17. it follows that the residue classes in $\frac{\mathbb{Z}_2[x]}{\langle p(x) \rangle}$ form a field. The operation table of multiplication also demonstrate that the elements of $\frac{\mathbb{Z}_2[x]}{\langle p(x) \rangle} \setminus \{[0]\}$ with respect to multiplication modulo f form an abelian group. Thus, $\frac{\mathbb{Z}_2[x]}{\langle p(x) \rangle}$ is a field with respect to modulo polynomial addition and multiplication. It is an example of a finite field that is the extension of the prime field \mathbb{Z}_2 .

Corollary 1.24. [7, Corollary 5.7] *For every prime number and positive integer n there exist a finite field of the order p^n . Any two fields having the same order are isomorphic, which means that between any two finite fields having the same order exists one to one homomorphic map.*

Corollary 1.24 demonstrates that for every positive integer m and prime number p there exist finite fields of order p^m . Any number of finite fields of order p^m are isomorphic. The elements of these can be thought polynomials or matrices. The following subsection discusses all the possible ways to represent the elements of such fields.

1.2.7 Representation of finite field elements

The elements of a finite field \mathbb{F}_q of order $q = p^m$ can be represented in three different arrangements. The first method is relying on the principal exponent. Since it is a well-known fact that the field \mathbb{F}_q is just simply the algebraic extension \mathbb{F}_p . Therefore if g is an irreducible polynomial in the polynomial ring $\mathbb{F}_p[x]$ of degree m , then the root β of g contain in \mathbb{F}_q . So, by Theorem 1.23 (i), the field \mathbb{F}_q is isomorphic to $\mathbb{F}_p(\beta)$ that is also isomorphic to $\frac{\mathbb{F}_p[x]}{\langle g \rangle}$. Then by Theorem 1.17, the elements of the field \mathbb{F}_q are uniquely expressed as polynomials of degree less than m , as shown in Example 1. 23.

The second possibility of expressing the elements of a finite field \mathbb{F}_q is using $q - 1$ cyclotomic polynomials over \mathbb{F}_p . Since we know that the field \mathbb{F}_q is $q - 1$ cyclotomic field over the subfield \mathbb{F}_p . Therefore, one can construct it by finding the decomposition of cyclotomic polynomials $Q_{q-1} \in \mathbb{F}_p[x]$ into the same degree irreducible polynomial, that are the factors of the polynomial ring $\mathbb{F}_p[x]$. The root of any one of these irreducible polynomials is then the primitive $q - 1$ root of unity over \mathbb{F}_p and thus the primitive element of \mathbb{F}_q . Hence, \mathbb{F}_q obtained with the consequences of the appropriate power of a primitive element and 0.

The third possibility of representing the elements of a finite field \mathbb{F}_q in the form of matrices generated by the companion matrix of the irreducible polynomial. Let $f(x) = b_0 + b_1x + \dots + b_{n-1}x^{m-1} + b_nx^m$ be an irreducible polynomial of degree m over the field \mathbb{F}_p . Then the companion matrix of irreducible polynomial $f(x)$ defines by the $m \times m$ matrix that is given as follows;

$$M = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -b_0 \\ 1 & 0 & 0 & \cdots & 0 & -b_1 \\ 0 & 1 & 0 & \cdots & 0 & -b_2 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -b_{m-1} \end{pmatrix}$$

It is a well-known fact in linear algebra that the matrix M satisfies the polynomial equation $f(M) = 0$ that is $b_0I + b_1M + \dots + b_{n-1}M^{m-1} + b_nM^m = 0$, where I denotes $m \times m$ identity matrix. Since the companion matrix of a monic irreducible polynomial over the field \mathbb{F}_p play the role of the root of f . Therefore, the matrix M generates a field of the order q^m with respect to matrix addition and matrix multiplication.

Example 1.25. Let $p(x) = x^2 + 1 \in \mathbb{F}_3[x]$. Then the companion 2×2 matrix of irreducible polynomial p over \mathbb{F}_3 is defined as

$$M = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$$

The elements of the field \mathbb{F}_{3^2} can be represented in the form $\mathbb{F}_{3^2} = \{0, I, 2I, M, I + M, 2I + M, 2M, I + 2M, 2I + 2M\}$.

The second chapter uses the matrix representation of the finite field for the constructions of symmetric and asymmetric cryptographic schemes that are homomorphic.

1.3 Cryptography

Cryptography is the study of protecting information and information systems from unauthorized access and manipulation. Three components of cryptography are Confidentiality, Integrity, and Availability. The term integrity refers to “the property that data has not been altered in an unauthorized manner”. There are two broad categories of integrity protection that are preventive mechanisms and detective mechanisms. The preventive mechanism controls the unauthorized modification of information while the detective mechanism detects the amendment when the preventive mechanism has failed. Availability: the third component is Availability which concerns “The information is

available to authorized users on time”. A disruption of access to or utilization of information or an information system leads to a loss of availability. Attacks against availability are known as denial of service (DoS) attacks. Confidentiality: The term confidentiality refers to the ability to hide information from unauthorized parties. Confidentiality is the highest priority component of information security. And if one fails to achieve that, then there is a chance to access confidential data by any unauthorized person, which can draw unacceptable consequences. The goal of confidential communication can be achieved by using symmetric key cryptography and asymmetric cryptography. The following subsections discuss the subfield of cryptography and analyses of the cryptographic scheme.

1.3.1 Symmetric Key Cryptography

The symmetric key cryptographic algorithms are also called single key or secret key algorithms. A single key is required for both encrypting and decrypting a ciphertext in these approaches. It is a well-known problem that is simple to follow. For instance, two firms are attempting to exchange data over an unprotected and insecure communications channel. The word channel may sound abstract; however, it is a broad word that encompasses the communication data connection. The communication network can be a mobile phone, WIFI network, wireless Lan, or any other communication network nowadays available. The problem creates an eavesdropper, whose intercepting communication. In most cases, the communication party would prefer to communicate confidentially. Symmetric key cryptography offers a solution to the problem of confidential communication. The sender encrypts his/her original message x using a symmetric key scheme and yields an encrypted message y . The receiver decrypts the message y and transforms it into the original message x using the decryption procedure of a symmetric key cryptosystem. If the eavesdropper accesses the communication channel, they will get an unreadable message having no information. The primary method of enciphering the message using the key k is called a cipher. The following definition introduces the simplified concept of the cipher called Shannon cipher. Further detail of this subsection can be found in Chapter 2 of Delfs and Knebl [8], Chapter 2 of Elbirt and Adam [9], Chapter 3 of Kahate [10], and Chapter 1 of Boneh and Shoup [11].

Definition 1.26. (Shannon Cipher) The Shannon cipher is the pair of encryption and decryption functions defined as follows

$$\mathcal{E} = (E, D)$$

where E denotes the encryption function that takes a plain message m and the key k and output the ciphertext c that is $c = E(m, k)$. The ciphertext c is the encrypted version of the plain message m under the key k . The function D is the decryption function that takes the ciphertext c and the key k and outputs the plain message m .

Definition 1.27. (Correctness property). The Shannon cipher $\mathcal{E} = (E, D)$ is said to satisfy the correctness property if for all keys k and all ciphertexts c , the \mathcal{E} hold the following property

$$m = D(E(m, k), k).$$

The above illustrates the basic definition and correctness properties of the Shannon cipher. The following definition discusses the mathematical notion of the security properties of the Shannon cipher

Definition 1.28. The Shannon cipher $\mathcal{E} = (E, D)$ is said to be perfectly secure over \mathcal{K} , \mathcal{M} and \mathcal{C} (\mathcal{K} is the set of keys, \mathcal{M} is the set of all messages and \mathcal{C} is the set of all ciphertext). If for a random key $k \in \mathcal{K}$, for all $c \in \mathcal{C}$ and, for all $m_1, m_2 \in \mathcal{M}$, the following equation hold

$$\Pr[E(m_1, k) = c] = \Pr[E(m_2, k) = c]$$

Then the Shannon cipher \mathcal{E} is said to satisfy the property of perfect security.

Theorem 1.29. [10, Theorem 2.1] Let $\mathcal{E} = (E, D)$ be the Shannon cipher over the sets \mathcal{M}, \mathcal{C} , and \mathcal{K} . Then the following properties are equivalent

- i. The Shannon cipher \mathcal{E} is perfectly secure.
- ii. For all plain images, $m \in \mathcal{M}$ and every ciphertext $c \in \mathcal{C}$ there exist M_c , such that the following equation hold

$$|\{k \in \mathcal{K} : E(k, m) = c\}| = M_c$$

- iii. If the key k is randomly distributed over \mathcal{K} , then for each ciphertext $c = E(m, k)$ has the same distribution for the message $m \in \mathcal{M}$.

The main disadvantage of the symmetric key schemes is that such systems need a secure channel to distribute secret keys between the sender and receiver. To address the problem of secret key distribution, the researcher introduced the notion of asymmetric key cryptography.

1.3.2 Asymmetric Key Cryptography

The Cryptography's most basic purposes are to maintain the secrecy of the information exchange among the communicating entities during communication and to provide

authentication of the sender to the receiver. These goals can be achieved via symmetric key cryptography. However, the symmetric key cryptographic schemes are not convenient in some applications due to specific reasons. For instance, while using symmetric key cryptographic schemes the communication parties should have to share a secret key. So, there must be a secure channel between the communication parties for sharing the secret key. Therefore, the researcher invented the notion of asymmetric key cryptography. In asymmetric key cryptographic schemes, the receiver and sender use different keys for encryption and decryption. Initially, the receiver generates two keys called the public key and private key, whereas these keys are mathematically related. Then keep the private key secret and share his/her public key. The sender uses the public key and encrypts the message and sent the encrypted message to the receiver. Upon receiving the encrypted message, the receiver uses the secret key, decrypts the encrypted message, and gets the original message. This concept was also introduced by Ellis at GCHQ and named it non-secret key cryptography. The earliest and essential example of an asymmetric key cryptographic scheme is RSA, designed by Adlmen, Revist, and Shamir in 1977. The RSA scheme is used for both authentication and digital signature applications. The notion of the asymmetric key cryptographic scheme using a mathematical mechanism required the formal definition of the encryption scheme, which we have discussed in the following subsection. The general references for this subsection are Chapter 1 of Moller [12], Salomaa [13], Chapter 10 of Boneh [11], and Chapter 1 of Galbraith [14].

Definition 1.30. Let a natural number κ be a security parameter. The security parameter κ is not necessarily to be equal to the length of the key. An asymmetric key encryption scheme can be defined as follows;

M_κ denote the set of all possible plaintext.

PK_κ denote the set of all possible public keys.

SK_κ denote the set of all possible secret keys.

C_κ denote the set of all possible ciphertexts.

KeyGen. denote the key generation randomize algorithm, which takes a security parameter κ as an input and perform expected $\mathcal{O}(\kappa^c)$ bit operations for some constant c and output a secret key $sk \in SK_\kappa$ and a public key $pk \in PK_\kappa$.

Encrypt. Then encryption algorithm is denoted by Encrypt , which is a randomized algorithm that takes plain message $m \in M_\kappa$ and public key pk and perform $\mathcal{O}(\kappa^C)$ bit operation for some constant C and output an encrypted message $c \in C_\kappa$.

Decrypt. The decryption algorithm is denoted by Decrypt , which is a randomized algorithm that takes the encrypted text c and perform polynomial times ($\mathcal{O}(\kappa^C)$) bit operation and output the plaintext m or the symbol \perp of invalid encrypted message.

$$\text{Decrypt}(\text{Encrypt}(m, \text{pk}), \text{sk}) = m.$$

Example 1.31. The RSA cryptosystem is an example of the asymmetric key cryptosystem. In this example, we briefly discuss the textbook RSA algorithm. Let A and B be two entities that are willing to communicate using the RSA cryptosystem.

In the first step, A chooses two prime integers $p, q \geq 2^\kappa$ and computes $N = pq$, where $\kappa \in \mathbb{N}$ is the security parameter. Then, A also choose $e \in U(N)$ and compute $d \in U(N)$ such that

$$ed \equiv 1 \pmod{\phi(N)}.$$

Where $U(N)$ is the set of unit elements of the ring \mathbb{Z}_N , and the function $\phi(N)$ is the Euler phi function. A public the pair (e, N) and keep the element d secret.

B convert his/her message to an integer m such $1 < m < N$ and computes the ciphertext text $c = m^e \pmod N$. Then sent the ciphertext c to A .

To obtain the original message m , the user A computes $m = c^d \pmod N$ and get the original message m .

1.3.3 Security Analyses of Asymmetric Cryptosystem

This section briefly discusses the security analyses of asymmetric key encryption schemes. An adversary we consider a polynomial-time algorithm that can intercepts in the cryptosystem in many possible ways. It is requisite to define attack goal and attack model to demonstrate the ways through which the adversary can break the asymmetric key cryptosystem. The following subsection first lists the attack goal for the public key cryptographic scheme. There are four well-studied attacks: the security properties that resist the adversary to attain the attack goal. In the below definition the word oracle has been used that is just the name of an algorithm that outputs the correct answer of any input in constant time.

Definition 1.32. A cryptosystem is said to be a total break if an adversary success to compute the private key of that cryptosystem.

Definition 1.33. A cryptosystem is said to be one-way encryption if the ciphertext c is given to the adversary and they are unable to compute the corresponding plaintext m .

Definition 1.34. An encryption scheme is said to be semantically secure whenever the ciphertext is given to the adversary, and they discover no information at all about the plaintext from the ciphertext apart from its length. A brief discussion of semantic security is given as follows:

Assume that all the plaintext in the set M_κ have the same size. An adversary of semantic security is a randomized polynomial-time algorithm A that initially chooses a map $f: M_\kappa \rightarrow \{0,1\}$, such that for any $m \in M_\kappa$, the probability of $f(m) = 0$ is $\frac{1}{2}$. Then the adversary takes a ciphertext (c, pk) as input and outputs a bit b , where c is the corresponding encrypted version of the message m under the public key pk . The adversary will be successful if the bit b is equal to $f(m)$.

Definition 1.35. An encryption scheme is said to be indistinguishably secure if the adversary is unable to separate the ciphertexts of the two plaintexts m_0 and m_1 of the same length, chosen by the adversary itself. The concept of indistinguishability can be defined as follows;

Let A be a randomized polynomial-time algorithm that is considered to be an indistinguishable adversary, which plays a game with the challenger C . Initially, the challenger computes the public key and sent it to the adversary A . Then the adversary A perform computation and output two messages m_0 and m_1 of the same length and sent the messages to the challenger C . The C computes the ciphertexts using the public key and give one of them c_b to A . In the second phase of the game, A perform some computation and output b' . The adversary A win the game if $b = b'$, otherwise, the challenger wins the game.

One can consider that for a fixed integer κ the adversary successfully outputs all the public keys through KeyGen and outputs all the challenge ciphertext through the algorithm Encrypt. The scheme is considered to not satisfy the security property if the adversary wins the game by the noticeable probability. The scheme is considered to satisfy the security property if the success probability of the adversary for a function κ is negligible. An adversary is said to be perfect if they work on probability 1. In the following definitions, we list the attack model for asymmetric key cryptography.

Definition 1.36. The Adversary has access to the public key of the cryptosystem.

Definition 1.37. The public key of the cryptosystem is given to the Adversary and they can also ask the decryption Oracle for the decryption of its chosen ciphertext, before receiving the challenge ciphertexts of the game.

Definition 1.38. The Adversary has access to the public key of the cryptosystem and they can ask the decryption Oracle for the decryption of the ciphertext of its choosing, before and after receiving the ciphertexts of the game.

The adversary aims to break the above security properties of the scheme over the attack model. In these properties, indistinguishability under adaptive chosen ciphertext attack is the strongest notion. A scheme that resists indistinguishability under an adoptive ciphertext attack is called to have IND-CCA security. In theoretical cryptography, a scheme is considered to be secure if it achieves IND-CCA security; such schemes resist all real-world attacks.

Proposition 1.39. [14, Section 1.3.1] *A scheme is considered to attain semantic security under some attack models if it achieves IND-CCA under some of the same attack models.*

Examples 1.40. The textbook RSA cryptosystem does not have IND-CCA security.

1.4 Algorithm

In general, an algorithm is a well-defined computational process that takes a set of values or some sort of values as input and raises a set of values or some sort of values as output. Therefore, an algorithm is a sequence of computational functions that map the input to the output. The algorithm can be view as a tool for solving problems. The problem sounds like the relationship between input and output. The algorithm depicts a computational mechanism for determining the relationship between the inputs and the outputs.

Examples 1.41. One might need a sorted sequence in non-decreasing order. In practice, this problem often arises and gives a fertile background for introducing many analysis tools and designed techniques. The sorting problem is defined as follows

Input: Sequence of m integer (x_1, x_2, \dots, x_m)

Output: A permutation $(x'_1, x'_2, \dots, x'_m)$ corresponding to the input sequence such that $x'_1 \leq x'_2 \leq \dots \leq x'_m$.

The insertion sort is an efficient algorithm for sorting small sequences. This example presents the pseudocode of the insertion sort to illustrate the notion of the algorithm in more

detail. In the algorithm, the index i denotes the element of the given sequence being inserted in the sorted sequence. At the initial stage of the **for** loop, that is, the index i , the subarray consisting of the elements $S[1 \dots i - 1]$ denotes the sorted array. However, the subarray consisting of elements $S[i + 1 \dots n]$ indicates the unsorted array. The algorithm picks the elements from the unsorted array and puts them on the sorted array, consequently output the sorted array.

Table 1. Algorithm 1. Insertion sort

INSERTION SORT (S)	
1	for $i = 2$ to S.length
2	$K = S[i]$
3	Insert $S[i]$ into the sequence $S[1 \dots i - 1]$
4	$j = i - 1$
5	while $j > 0$ and $S[j] > key$
6	$A[j + 1] = A[j]$
7	$j = j - 1$
8	$A[i + 1] = key$

Definition 1.42. (Randomized Algorithm). An algorithm A is said to be randomized if A have access to a random number generator. The randomized algorithm does not terminate whenever the arbitrary choice of the infinite sequence is made.

Definition 1.43. (Deterministic). An algorithm is said to be deterministic if it solves a problem without making any randomness. For instance, the textbook RSA is the deterministic algorithm.

1.4.1 Success Probability of an Algorithm

Throughout this chapter gives brief definitions of algebraic structures, asymptotic complexity, and algorithms. Therefore, it is more suitable to discuss the success of an algorithm to solve a problem. An algorithm A is considered to be perfect if A always outputs the correct answer. The algorithm A might output the correct answer just for some subset of the instance or for all instances with a certain probability. This section presents the success probability of an algorithm. The success probability of an algorithm is to solve a problem with noticeable probability. It takes $\kappa \in \mathbb{N}$ as an input and runs in polynomial time and output the instance of that problem. The following definition defines the noticeable and negligible functions.

Definition 1.44. A function ϵ from the set of natural number \mathbb{N} to the set positive real number $\mathbb{R}_{>0}$ is said to be noticeable, if there exists an integer N and a polynomial $r(x) \in \mathbb{R}[x]$ such that $r(k) \neq 0$ for all $k > N$ and $\epsilon(k) > \frac{1}{r(k)}$.

Definition 1.45. A function ϵ from the set of natural number \mathbb{N} to the set positive real number $\mathbb{R}_{>0}$ is said to be noticeable, if there exists an integer N and for all polynomial $r(x) \in \mathbb{R}[x]$ such that $r(k) \neq 0$ and $\epsilon(k) < \frac{1}{r(k)}$ for all $k > N$.

Example 1.46. An example of a negligible function is $\epsilon(k) = \frac{1}{r(k)}$.

Definition 1.47. Let A be an algorithm that solves the instance of a problem. Let the function $f: \mathbb{N} \rightarrow [0, 1]$ such that $f(k)$ for $k \in \mathbb{N}$ be the probability of the algorithm A that it outputs the correct answer. Then the function f is said to be the success probability of the algorithm A if f is the noticeable function.

Example 1.48. Let A be an algorithm for the discrete logarithmic problem (DLP). Suppose that the pair (G, g, h) is the input of the algorithm A , where G is the group and $g, h \in G$, such $h = g^x$ for some positive integer x . Let the output of the algorithm A is the integer x chosen uniformly in the range $0 < x \leq r$. Since for the security perimeter κ , the order of the group r is greater than $2^{2\kappa}$. Therefore, the correctness probability of the algorithm A is $\frac{1}{(r-1)} \leq \frac{1}{2^{2\kappa}}$. Thus, for any polynomial $q(x)$ there are $m_1, m_2 \in \mathbb{R}_{>0}$ and natural number n such that $|q(x)| \leq m_2 x^n$ for $m_2 \geq m_1$. Accordingly, there exist some $K \geq m_1$ such that $m_2 K^n \leq 2^{2\kappa}$. Consequently, the success probability of Algorithm A is negligible.

Definition 1.49. A problem that is specified by a certain form of input and output is called a computational problem. The computational problem input and output instance are particular instances. The size of the computational problem input is the number of bits necessitated to symbolize that input.

Definition 1.50. A problem that is specified by a particular form of input and the output is either ‘Yes’ or ‘No’ is called a decisional problem.

Example 1.51. Let G be a cyclic group with respect to multiplication that is generated by an element g . The decision discrete logarithmic problem (DLP) is: Given $(g^a, g^b g^{ab}, g^c)$ for positive integers a, b and c . The problem is that either $g^{ab} = g^c$ or not.

Example 1.52. Let G be a cyclic group with respect to multiplication that is generated by g . The computational discrete logarithmic problem (DLP) is: Given $h, g \in G$, find an element

$a \in \mathbb{Z}^+$ if there exist such that $g^a = h$. The input instance of the computational problem DLP is the group structure G and the elements g, h of the group G . The output instance of computational DLP is the positive integer a , such that $g^a = h$ or the symbol of failure \perp , which indicates that the element h does not belong to the group G . The input size of the DLP depends on the order of the group G and the method used to represent the group. If the order of the group G is n , and assume that $g^a = h$ for $1 \leq a < n$, then at least $\log_2(n)$ bit require to specify h among n possibilities. Thus, the size of the input instance of the DLP is $\log_2(n)$ bits. Since the output instance, a of the DLP is uniformly distributed in the ring \mathbb{Z}_n , thus the size of the output instance is at least $\log_2(n)$ bits.

The upcoming subsection discusses the asymptotic complexity of the algorithm. The complexity of the algorithm is the maximum number of bit operations necessities for the algorithm to solve the computational problem. The upper bound on the complexity is denoted by big oh ‘ \mathcal{O} ’ notation. Whenever the complexity estimate of the algorithm is given in terms of \mathcal{O} then we assume that there are infinite numbers of countable inputs to that algorithm.

1.5 On Complexity Theory

This section aims to discuss the basic definition of complexity theory briefly. The intention of this section is not to describe the implementation guide of the algorithms. However, it sketches some crucial notions and results of complexity that are uses later in this thesis. More detail of this subsection is presented in the handbooks [15], Buhler and Stevenhagen [16], Crandall and Pomerance [17], Bach and Shallit [18], Cormen [19], and Section 2.1 of Galbarith [14].

Definition 1.53. Let f and g be two functions $f, g : \mathbb{N} \rightarrow \mathbb{Z}^+$, then $f = \mathcal{O}(g)$ if there exist $c \in \mathbb{R}_{>0}$ and a natural number N , such that

$$f(m) \leq cg(m). \quad \text{for all } m \geq N$$

Similarly, if $f(m_1, \dots, m_k)$ and $g(m_1, \dots, m_k)$ be two functions from \mathbb{N}^k to $\mathbb{R}_{>0}$, then $f = \mathcal{O}(g)$ if there exist $c \in \mathbb{R}_{>0}$ and $N_1, N_2, \dots, N_k \in \mathbb{N}$ such that $f(m_1, \dots, m_k) \leq cg(m_1, \dots, m_k)$ with $m_i > N_i$. for all $1 \leq i \leq k$.

Example 1.54. $4m^3 + 10n^n + 5n + 10 = \mathcal{O}(m^3)$, $\cos(m) + m = \mathcal{O}(m)$, $2^m + m^{1000} = \mathcal{O}(2^m)$ and $\log_n(m) = \mathcal{O}(\log(m))$.

Definition 1.55. Let f and g be two functions $f, g : \mathbb{N} \rightarrow \mathbb{Z}^+$, then $f = o(g)$ if

$$\lim_{m \rightarrow \infty} \frac{f(m)}{g(m)} = 0.$$

The function can be written as; $f = \tilde{O}(g)$ if there exist $n \in \mathbb{N}$ such that $f(m) = \mathcal{O}(g(m) \log(g(m))^n)$. The function $f = \Omega(g)$ if $g = \mathcal{O}(f)$ and $f = \Theta(g)$ if $f = \mathcal{O}(g)$ and $g = \mathcal{O}(f)$.

Definition 1.56. Let A be an algorithm and $t(m)$ be the upper bound of the running time of the algorithm A to solve any problem of size m bits.

1. An Algorithm A is said to be polynomial-time if there exist a positive a non-negative integer k such that $t(m) = \mathcal{O}(m^k)$.
2. An Algorithm A is said to be super polynomial-time if for all $c \in \mathbb{R}_{>1}$ if the upper bound $t(m) = \Omega(m^c)$.
3. An Algorithm A is said to be exponential-time, if there exists a constant c greater than 1, such that $t(m) = \mathcal{O}(c^m)$.
4. An Algorithm A is said to be super polynomial-time if for all $c \in \mathbb{R}_{>1}$ the upper bound $t(m) = \Omega(m^c)$.

The above definition is for uniform complexity, as all the problems instances are solving through a single algorithm A . In non-uniform complexity, for each positive integer m and input $h(m)$ of polynomial-size, if x is a string of m -bits instance of the computational problem, then the algorithm A solves $A(x, h(m))$ instance.

Chapter 2

Leveled Homomorphic Encryption Scheme Based on Finite Field Isomorphism Problem

2.1 Introduction

The notion of a fully homomorphic encryption scheme was introduced by Rivest, Adlamen, and Dertuozous, after the invention of RSA [20]. The RSA encryption scheme satisfying homomorphic property with respect to multiplication. This property of the RAS scheme was innate. However, it led Rivest et al. to suggest an open problem. In 2009, Gentry proposed a solution to the Rivest et al. problem after thirty years and constructed a fully homomorphic encryption scheme [21]. The structure of the Gentry scheme is based on the ideal lattice, and their security strength hinges on the hard problems in the lattice. The key feature of the Gentry method is bootstrapping, which provides access to boost the noise level in ciphertext without the knowledge of the secret key. Afterward, various construction schemes are followed in order to improve the strength of the fully homomorphic encryption scheme. Vaikuntanathan and Barkerski proposed a fully homomorphic encryption scheme based on learning with error problems [22]. The security capability of the suggested scheme is based on a short vector problem. Subsequently, this scheme was further improved by Vaikuntanathan et al. utilizing the technique of modulo switching, which consequently reduced the noise accumulation [23]. In the improved LWE scheme, modulus switching is applied to the multiplicative level, for the prevention of exponential noise growth. Afterward, Barkerski introduced a novel technique for noise management, which was then applied to the LWE scheme [24]. Then Dijkstra et al. present another fully homomorphic encryption scheme based on the hardness of Integer Approximate-GCD problems [25]. The proposed work was then followed by Coron et al. and reduced the size of their public key [26]. In [27] another fully homomorphic encryption scheme was introduced by Tomer, Lopez-Alt, and Vaikuntanathan, which is based on the NTRU encryption scheme. The NTRU encryption scheme was presented earlier by Steinfeld and Stehle [28]. The presented scheme is for multi-user and is capable of proceeding homomorphically for the different users using different keys. The noise growth is mitigated in the scheme through the re-linearization technique presented in [22]. In 2018, Doröz et al. introduced the finite field isomorphism problems and proposed a symmetric and asymmetric fully homomorphic encryption scheme based on the

finite field isomorphism problem [29]. Their security strength is based on the computational problem over the polynomial field.

This chapter introduces a somewhat homomorphic encryption scheme based on a finite field isomorphism problem over matrix algebra. It is the extension of the homomorphic encryption scheme given in [29]. Initially, the scheme converts a message into a short element of the field $\mathbb{F}_p[M]$, and then add q time an element of the field $\mathbb{F}_p[M]$ as a noise for semantic security. Then transforms it to the field $\mathbb{F}_p[N]$ through isomorphism and get a ciphered text. This procedure builds a symmetric, fully homomorphic encryption scheme. The receiver with knowledge of q and $f(x)$ can easily retrieve the plaintext by using inverse isomorphic map modulo p . The output will be correct if the absolute value of the entries of the plain matrix does not exceed up to p .

2.2 Finite Field Isomorphism

Let p be a prime number and \mathbb{F}_p be a finite field of order p . Let $f(x)$ be a degree n monic irreducible polynomial in a polynomial ring $\mathbb{F}_p[x]$, then the companion matrix M of monic irreducible polynomials $f(x)$ generates a finite field of the order p^n , which is denoted by $\mathbb{F}_p[M]$. Any two finite fields $\mathbb{F}_p[M]$ and $\mathbb{F}_p[N]$ of order p^n generated by the companion matrices M and N of degree n monic irreducible polynomials are isomorphic. It is easy to construct the isomorphism and its inverse isomorphism map between $\mathbb{F}_p[M]$ and $\mathbb{F}_p[N]$, if one knows the monic irreducible polynomials $f(x)$ and $g(x)$.

2.3 Finite Field Isomorphism Problem

The observation given in [29] states that the isomorphism between any two polynomial fields does not preserve Archimedes' property of length. It means, whenever $f(x)$ and $g(x)$ are distinct irreducible polynomials, then the images of the elements having small lengths are uniformly distributed in the other field. This key feature yields finite field isomorphism problems.

Let u be a positive integer. Let $\mathbb{F}_p[M]$ and $\mathbb{F}_p[N]$ be finite fields. Let $\Phi: \mathbb{F}_p[M] \rightarrow \mathbb{F}_p[N]$ be the isomorphic map between them. Let Δ_γ be the subset of $\mathbb{F}_p[M]$, such that $\Delta_\gamma = \{L \in \mathbb{F}_p[M] \mid \|L\| \leq \gamma\}$. Let $L_{x_1}, L_{x_2}, \dots, L_{x_u}$ be the elements of the set Δ_γ , and $L_{y_1} = \Phi(L_{x_1}), L_{y_2} = \Phi(L_{x_2}), \dots, L_{y_u} = \Phi(L_{x_u})$ be the corresponding images in $\mathbb{F}_p[N]$.

- 1) **Computational problem.** The computational problem state that given: $\mathbb{F}_p[N], L_{y_1}, L_{y_2}, \dots, L_{y_u}$ recover $f(x)$ or the preimages $L_{x_1}, L_{x_2}, \dots, L_{x_u}$.

- 2) **Decisional problem.** The decisional problem state that given: $\mathbb{F}_p[N]$, $L_{y_1}, L_{y_2}, \dots, L_{y_u}$, B_{y_1}, B_{y_2}, \dots , such that the pre-image of one of the B_{y_1} or B_{y_2} belong to the subset Δ_γ . Identify the image with preimage sampled from Δ_γ with probability greater than $\frac{1}{2}$.

It can be seen that the decision problem depends on the computational problem; one can easily solve the decision problem if one solves the computational problem. The decision problem is arbitrarily hard for the field having elements in the form of polynomials. In the polynomial isomorphic fields, the representations of the elements are always the same. However, these are generating through different elements. In this case, we observed that the matrix elements in both fields are almost distinct and have different representations. Besides, its length does not depend on the coefficients. Accordingly, finite field isomorphism problems in the case of the finite field generated by the companion matrix are much harder than the case of finite fields having elements in the form of polynomials.

2.4 Basic Definitions and Notations

This section introduces some basic definitions and notations that will be used in the upcoming sections, and some are already used in the previous section.

Definition 2.1. Let $f(x)$ be a monic irreducible polynomial of degree n over the field \mathbb{F}_p . Let M be the companion matrix of the irreducible polynomials $f(x)$. Then the field $\mathbb{F}_p[M]$ generated by M is always isomorphic to \mathbb{F}_{p^n} .

$$\mathbb{F}_p[M] = \{0I, I, M, M^2, \dots, M^{p^n-2}\} \cong \mathbb{F}_{p^n} \quad (2.1)$$

Where M is the $n \times n$ matrix, which satisfies the equation $f(M) = 0$. The following example demonstrates the idea in more detail.

Example 2.2. Let $f(x) = x^2 + 2x + 2$ and $g(x) = x^2 + x + 2$. Since the polynomial f and g are the primitive irreducible polynomials in the principal ideal domain $\mathbb{Z}_3[x]$. Therefore, the companion matrices of f and g generate two isomorphic fields of order 3^2 . The field generated by the companion matrix of the primitive irreducible $f(x) = x^2 + 2x + 2$ is given as follows;

$$\begin{aligned} M_0 &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & M &= \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} & M^2 &= \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \\ M^3 &= \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix} & M^4 &= \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} & M^5 &= \begin{pmatrix} 0 & 2 \\ 2 & 2 \end{pmatrix} \\ M^6 &= \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix} & M^7 &= \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} & M^8 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

Similarly, the companion matrix of the primitive irreducible polynomial $g(x) = x^2 + x + 2$ generate a field of the order 3^2 , that is given as follows;

$$\begin{aligned} N_0 &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & N &= \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} & N^2 &= \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix} \\ N^3 &= \begin{pmatrix} 2 & 2 \\ 2 & 0 \end{pmatrix} & N^4 &= \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} & N^5 &= \begin{pmatrix} 0 & 2 \\ 2 & 1 \end{pmatrix} \\ N^6 &= \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} & N^7 &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} & N^8 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

To construct the isomorphism between the fields $\mathbb{F}_3[M]$ and $\mathbb{F}_3[N]$, find the root of $f(x)$ in the field $\mathbb{F}_3[N]$. Since N^5 satisfies the equation $f(x) = 0$; that is $(N^5)^2 + 2N^5 + 2I \equiv 0 \pmod{p}$, where I is the 2×2 identity matrix. Thus, the map $\phi: \mathbb{F}_3[M] \rightarrow \mathbb{F}_3[N]$ defined as $\phi(M) = N^5$ is an isomorphism.

Proposition 2.3. Let $\mathbb{F}_p[M]$ be the field generated by the companion matrix M of primitive irreducible polynomial $f(x)$ in $\mathbb{F}_p[x]$. Then for all $a \in \mathbb{F}_p$ the element $aI \in \mathbb{F}_p[M]$, where I is the identity matrix.

Proof. Since $\mathbb{F}_p[M]$ is a field. Therefore, the multiplicative identity $I \in \mathbb{F}_p[M]$, which implies $aI = \underbrace{I + I + \dots + I}_{a \text{ time}} \in \mathbb{F}_p[M]$.

Proposition 2.4. Let $\mathbb{F}_p[M]$ and $\mathbb{F}_p[N]$ be the isomorphic matrix fields generated by the companion matrices M and N of the degree n irreducible $f(x)$ and $g(x)$, respectively. Let $\phi: \mathbb{F}_p[M] \rightarrow \mathbb{F}_p[N]$ be the isomorphic map. Then $\phi(aI) = aI$ for all $aI \in \mathbb{F}_p[M]$.

Proof. Given that the map ϕ is an isomorphic map. Thus, $\phi(I) = I$ for $I \in \mathbb{F}_p[M]$, because the map ϕ is one-one. Let $aI \in \mathbb{F}_p[M]$ then

$$\begin{aligned} \phi(aI) &= \phi\left(\underbrace{I + I + \dots + I}_{a \text{ time}}\right) = \underbrace{\phi(I) + \phi(I) + \dots + \phi(I)}_{a \text{ time}} \\ &= \underbrace{I + I + \dots + I}_{a \text{ time}} = aI \end{aligned}$$

Since a is an arbitrary element of the field \mathbb{F}_p , therefore $\phi(aI) = aI$ for all $aI \in \mathbb{F}_p[M]$.

Let M and N be the companion matrices over \mathbb{F}_p of the irreducible polynomials $f(x)$ and $g(x)$, respectively. Let $\mathbb{F}_p[M]$ and $\mathbb{F}_p[N]$ be the two copies of the fields of order p^n , we will denote by \mathbb{X} the field $\mathbb{F}_p[M]$ and by \mathbb{Y} the field $\mathbb{F}_p[N]$ throughout this chapter. Similarly, we will denote the element of \mathbb{X} by capital L letters with index x for instance L_x , and their corresponding image in \mathbb{Y} by the same capital letters with index y , i.e., L_y .

Definition 2.5. Let $L_x \in \mathbb{X}$ be a matrix, then the element L_x is said to be a γ –bounded matrix, if the coordinates of that matrix modulo p reduced to the interval $[-\frac{\gamma}{2}, \frac{\gamma}{2})$.

Definition 2.6. The length of the matrix is defined as follows;

$$\|L\| = \max_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}} |l_{ij}|. \quad (2.3)$$

Definition 2.7. For a positive integer γ . Define a subset \mathcal{X}_γ of \mathbb{X} , such that

$$\mathcal{X}_\gamma = \{L \in \mathbb{X} \mid \|L\| \leq \gamma\} \quad (2.2)$$

Definition 2.8. The class of those matrices whose coordinates belong to the set $\{-1, 0, 1\}$, are called trinary matrices.

Proposition 2.9. If M be a $q \times q$ matrix over a field \mathbb{F}_p , then the set $\mathbb{F}_p[M]$ consist of all elements generated by M from a field over \mathbb{F}_p if and only if the characteristic polynomial $f_M(x)$ of M is primitive irreducible, i.e., M is a $p^q - 1$ root of unity.

Proof. Let $Q_q(x)$ be the q_{th} cyclothymic polynomial defined as follows

$$Q_q(x) = \prod_{s=1}^q (x - \zeta^s) \quad (2.4)$$

Where q and s are relatively prime positive integers. Since for a positive divisor m of q , every q_{th} root of unity $x^q - 1 = 0$ is also m_{th} the root of unity. Therefore, it follows from the equation (2.4) that

$$x^q - 1 = \prod_{d|q} Q_d(x) \quad (2.5)$$

and

$$Q_q(x) = \frac{x^q - 1}{\prod_{\substack{d|q \\ d < q}} Q_d(x)} \quad (2.6)$$

From equation (2.6), it follows that $Q_n(x)$ is a monic polynomial of degree $\phi(n)$ with an integer coefficient. (It is important to note that the cyclothymic polynomials are a factor over a finite field, however irreducible over the rational field). If n is prime power, then from the equation (2.6), it follows that

$$Q_q(x) = \frac{x^q - 1}{x^{p-1}} \quad (2.7)$$

Every element of the field \mathbb{F}_q is the root of $x(x^{q-1} - 1)$, and the polynomial $x^q - x$ split in the field \mathbb{F}_q and their elements are $q - 1$ th the root of unity. The root of monic irreducible polynomial $f(x)$ is $q - 1$ th the root of unity if and only if it factors the cyclotomic polynomial $Q_q(x)$, such polynomials are also called a primitive-irreducible polynomial. It follows that if $f(x)$ be a monic irreducible polynomial that factor the cyclotomic polynomial, then the companion matrix of $f(x)$ generates a finite field of the order p^n isomorphic to \mathbb{F}_{p^n} .

Remark. If a monic irreducible polynomial $h(x)$ of degree n does not factor the cyclotomic polynomial $Q_q(x)$, then the cyclic group generated by $B + I$ from a field isomorphic to the \mathbb{F}_{p^n} , where B is the companion matrix.

Lemma 2.10. *For a large natural number n . Given any fixed irreducible polynomial $g(x)$ in the polynomial ring $\mathbb{F}_p[x]$. Let M be companion matrix of $g(x)$, then for any $n \times n$ matrix $C \in \mathbb{F}_p[M]$, there exists a unique companion matrix N of degree n monic irreducible polynomial $f(x)$ with probability approaching 1, such that the map $N \rightarrow C$ induced isomorphism between the fields $\mathbb{F}_p[M]$ and $\mathbb{F}_p[N]$.*

Proof. Let $L \in \mathbb{F}_p[N]$ be a root of the monic irreducible polynomial $g(x)$ over the field \mathbb{F}_p . We have to show that L^{p^i} for $1 \leq i \leq n - 1$ is also a root of the polynomial $g(x)$. Write $g(x) = g_n x^n + g_{n-1} x^{n-1} + \dots + g_1 x + g_0$ with $g_i \in \mathbb{F}_p$, for all i ($0 \leq i \leq n$). Since p is the prime characteristic of the field $\mathbb{F}_p[M]$, therefore it follows that

$$g(L^{p^i}) = g_n (L^{p^i})^n + g_{n-1} (L^{p^i})^{n-1} + \dots + g_1 L^{p^i} + g_0 \quad (2.8)$$

$$= (g_n L^n + g_{n-1} L^{n-1} + \dots + g_1 L + g_0)^{p^i} = 0 \quad (2.9)$$

Therefore, the elements $L, L^p, \dots, L^{p^{n-1}}$ are also the root of $g(x)$ in $\mathbb{F}_p[N]$. Implies that the irreducible $g(x)$ polynomial has n distinct roots. Thus it split entirely in the field $\mathbb{F}_p[M]$. Moreover, the sets of the roots of any number of the same degree irreducible polynomials are disjoint. Since the total number of monic irreducible polynomials are approximately equal to $\frac{q^n}{n}$ see [page 82-84 Corollary 3.21 and Theorem 3.25]. Therefore, $n \times \frac{q^n}{n}$ denote the total amount of isomorphism from $\mathbb{F}_p[M]$ to $\mathbb{F}_p[N]$, where N varies over the companion matrices of all distinct monic irreducible polynomials. Consequently, for any $C \in \mathbb{F}_p[M]$ there exists a unique companion matrix N of degree n monic irreducible polynomial $f(x)$ with

probability approaching 1, such that the map $N \rightarrow C$ induced isomorphism between the fields $\mathbb{F}_p[M]$ and $\mathbb{F}_p[N]$.

Lemma 2.10. *Let M be $n \times n$ companion matrix of degree n monic irreducible polynomial $f(x)$ and $\mathbb{F}_p[M]$ be a field generated by M . Let \mathcal{X}_γ be γ -bounded distribution over the field $\mathbb{F}_p[M]$ and let L_1, L_2, \dots, L_m be the sampled from \mathcal{X}_γ . Then the product $\prod_{i=1}^m L_i$ is $(n\gamma)^m$ -bounded.*

2.5 Finding Finite field Isomorphism

This section illustrates how to find an explicit isomorphism between two isomorphic fields \mathbb{X} and \mathbb{Y} . To find isomorphism, one required a set consist of four tuples (M, N, i, j) . Where M and N are the companion matrices corresponding to monic irreducible polynomial $f(x)$ and $g(x)$. The element i denotes a positive integer which satisfies the equation $f(N^i) = 0$. The algorithm for finding an isomorphic map between two isomorphic fields is shown in Tab.2.

Table 2. Algorithm 2.

Find Finite field Isomorphism
Input: Two degrees n primitive irreducible polynomials $f(x)$ and $g(x)$ over modulo p .
1. Find the companion matrices M and N of $f(x)$ and $g(x)$.
2. Find a positive integer i and j such that $f(N^i) = 0$ and $(M^i)^j = M$.
3. Defined a map $\Phi: \mathbb{X} \rightarrow \mathbb{Y}$ by $\Phi(M) = N^i$.
4. Defined a map $\Phi^{-1}: \mathbb{Y} \rightarrow \mathbb{X}$ by $\Phi^{-1}(N) = M^j$.
Output (M, N, Φ, Φ^{-1})

2.6 Homomorphic Encryption.

Definition 2.11. (\mathcal{C} Homomorphic Encryption Scheme [21]). Let κ be a security parameter, and $\{\mathcal{C}_\kappa\}_{\kappa \in \mathbb{N}}$ be a sequence of functions. An encryption scheme \mathcal{E} is said to be \mathcal{C} -homomorphic encryption scheme if for any function $\zeta \in \mathcal{C}$ and the corresponding inputs $\mu_1, \mu_2, \dots, \mu_j \in \{0,1\}$ (for $j = j(\kappa)$), it follows that

$$PR \left[\mathcal{E}.Dec_{sk} \left(\mathcal{E}.Eval_{evk}(\zeta, c_1, c_2, \dots, c_j,) \right) \neq \zeta(\mu_1, \mu_2, \dots, \mu_j) \right] = \text{negl}(\kappa) \quad (2.10)$$

where

$$c_i \leftarrow \mathcal{E}.Enc_{pk}(\mu_i) \text{ and } (pk, sk, evk) \leftarrow \mathcal{E}.KeyGen(1^\kappa) \quad (2.11)$$

Definition 2.12. (Fully Homomorphic Encryption Scheme) A scheme \mathcal{E} is said to be a somewhat homomorphic encryption scheme if it holds the following axioms:

- i. **Correctness:** The scheme \mathcal{E} is \mathcal{C} homomorphic for all the functions in class \mathcal{C} .
- ii. **Compactness:** The computational complexity of the encryption scheme \mathcal{E} is a polynomial-time over the parameter κ .

Definition. 2.13 (Leveled Homomorphic Encryption Scheme) Let $\mathcal{C}^{\mathcal{D}}$ be a class of the circuits with dept \mathcal{D} . Then the family of the schemes $\{\mathcal{E}^{\mathcal{D}}: \mathcal{D} \in \mathbb{N}\}$ is said to be a fully homomorphic scheme if it holds the following axioms:

- i. **Correctness:** The scheme $\mathcal{E}^{\mathcal{D}}$ is $\mathcal{C}^{\mathcal{D}}$ homomorphic for all the functions in the class \mathcal{C} .
- ii. **Compactness:** The computational complexity of the encryption scheme $\mathcal{E}^{\mathcal{D}}$ is a polynomial-time over the parameter κ .

2.7 Construction of Fully Homomorphic Encryption Scheme

This section presents the proposed somewhat homomorphic encryption scheme based on a finite field isomorphism problem over matrix algebra. Initially, it presents the detailed procedure of the construction scheme and then demonstrates that the proposed scheme is capable of evaluating the dept bounds of the circuit homomorphically.

2.7.1 Symmetric Key Homomorphic Encryption Scheme

The symmetric key version of the homomorphic encryption scheme uses the following four schemes:

I. SK-FHES.KeyGen $\{1^\kappa\}$

Input: κ as a security parameter.

- i. Generate a set $E = \{f(x), g(x), p, \gamma, qI\}$
- ii. Construct finite field isomorphism using Algorithm 1.

Output: $K = \{M, N, \Phi, \Phi^{-1}, \gamma, qI\}$

II. SK-FHES.Enc $\{M, \Phi, \gamma\}$

Input: $\{K, m\}$

- i. Encode a plaintext m in a binary matrix M_x of a field \mathbb{X} by some method.
- ii. Select any matrix R_x sampled from \mathcal{X}_γ .
- iii. Compute $C_x = qIR_x + M_x \text{ mod } p$.
- iv. Then transform the matrix C_x from the field \mathbb{X} into the field \mathbb{Y} through the isomorphic map Φ and get the output C_y .

Output: C_y as a ciphertext.

III. SK-FHES.Dec $\{N, \Phi^{-1}, q\}$

Input: $\{K, C_y\}$

- i. Compute C_x using the inverse isomorphic map Φ^{-1} .
- ii. Then compute the plaintext follows modulo q operation i.e., $M = C_x \bmod q$.

Output: $\{M_x\}$

IV. SK-FHES.Eval $\{ \mathcal{C}, C_{y_1}, C_{y_1}, \dots, C_{y_l} \}$

The circuit \mathcal{C} is consists of two arithmetic operations matrix addition and matrix multiplication modulo p . Since the scheme performs homomorphic multiplication and homomorphic addition. Therefore, the following steps homomorphically evaluate the circuit \mathcal{C} .

- i. **Homomorphic Addition Evaluation:** The homomorphic property of the addition gate + is evaluated for the inputs $C_{y_1}, C_{y_2}, \dots, C_{y_l}$, where $C_{y_i} = qR_{x_i} + M_{x_i} \bmod p$.

$$C_y^{add} = \sum_{i=1}^l C_{y_i} \bmod p \quad (2.11)$$

We have to show that the decryption of C_y^{add} demonstrate the summation of the plaintext M_x^{add} .

$$C_x^{add} = q \sum_{i=1}^l R_{x_i} + \sum_{i=1}^l M_{x_i} \quad (2.12)$$

where M_{x_i} is the plaintext corresponding to the ciphertext C_{y_i} . If $l < q$ and $lq\gamma < p$, then the summation of the ciphertext C_y^{add} will retrieve the $M_x^{add} = \sum_{i=1}^l M_{x_i}$, which is the desired.

- ii. **Homomorphic Multiplication Evaluation:** The homomorphic property of multiplication can be evaluated by multiplying the output ciphertext

$$C_y = C_{y_1} \times C_{y_2} \quad (2.13)$$

The decryption of the product of the message can be written as follows;

$$C_x = q^2 R_{x_1} R_{x_1} + q R_{x_1} M_{x_2} + q R_{x_2} M_{x_1} + M_{x_1} M_{x_2} \bmod p \quad (2.14)$$

$$M_x = M_{x_1} M_{x_2} = C_x \bmod q \quad (2.15)$$

Where M_{x_1} and M_{x_2} are the plaintext corresponding to the ciphertext C_{y_1} and C_{y_2} . If $l < q$ and $3(qn\gamma)^2 < p$, then the multiplication of the ciphertext C_y^{mult} will be decrypted to the plaintext $M_x^{mult} = M_{x_1} M_{x_2}$, which is the desired output.

Example 2.14. This example presents the idea of the above suggested symmetric homomorphic encryption scheme in more detail. Let $p = 251$, $\gamma = 16$, $f(x) = x^2 + x + 19$

and $g(x) = x^2 + 3x + 19$ be the secret keys. The companion matrices M and N of the polynomials $f(x)$ and $g(x)$ is given as follows;

$$M = \begin{pmatrix} 0 & 232 \\ 1 & 250 \end{pmatrix} \text{ and } N = \begin{pmatrix} 0 & 232 \\ 1 & 248 \end{pmatrix}$$

Encryption. Let $M_x = \begin{pmatrix} 14 & 4 \\ 13 & 1 \end{pmatrix}$ be the original message. To make sure the encryption procedure will work. The sender chooses

$$R_x = \begin{pmatrix} 13 & 4 \\ 13 & 0 \end{pmatrix} \in \mathcal{X}_{16} \text{ and } P_x = \begin{pmatrix} 15 & 0 \\ 0 & 15 \end{pmatrix} \in \mathcal{X}_{16}$$

$$M_y = \phi \left(\begin{pmatrix} 14 & 4 \\ 13 & 1 \end{pmatrix} \right) = \begin{pmatrix} 44 & 207 \\ 108 & 222 \end{pmatrix}$$

$$R_y = \phi \left(\begin{pmatrix} 13 & 4 \\ 13 & 0 \end{pmatrix} \right) = \begin{pmatrix} 43 & 207 \\ 108 & 221 \end{pmatrix}$$

$$P_y = \phi \left(\begin{pmatrix} 15 & 0 \\ 0 & 15 \end{pmatrix} \right) = \begin{pmatrix} 15 & 0 \\ 0 & 15 \end{pmatrix}$$

$$C_y = \begin{pmatrix} 43 & 207 \\ 108 & 221 \end{pmatrix} \begin{pmatrix} 15 & 0 \\ 0 & 15 \end{pmatrix} + \begin{pmatrix} 44 & 207 \\ 108 & 222 \end{pmatrix} \text{ mod } 251$$

$$C_y = \begin{pmatrix} 187 & 49 \\ 222 & 23 \end{pmatrix}$$

The required ciphertext is C_y . The sender sent the ciphertext C_y to the receiver.

Decryption. Upon receiving the sender ciphertext, the receiver decrypts the message using the decryption procedure. Initially, they apply the inverse isomorphism map ϕ^{-1} on the ciphertext and then compute mode 15 operations.

$$C_x = \phi^{-1} \left(\begin{pmatrix} 187 & 49 \\ 222 & 23 \end{pmatrix} \right) = \begin{pmatrix} 209 & 64 \\ 208 & 1 \end{pmatrix}$$

$$M_x = \begin{pmatrix} 209 & 64 \\ 208 & 1 \end{pmatrix} \text{ mod } 15 = \begin{pmatrix} 14 & 4 \\ 13 & 1 \end{pmatrix}$$

2.7.2 Asymmetric Key Homomorphic Encryption Scheme

The asymmetric version of the proposed homomorphic encryption scheme is mostly similar to the symmetric homomorphic encryption scheme. However, in this scheme, the subset problem is used to convert the scheme into an asymmetric version. The scheme consists of the following techniques.

I. PK-FHES.KeyGen $\{1^\kappa\}$

Input: κ as a security parameter.

- i. Select two integers J and j such that $\binom{J}{j} > 2^\kappa$.

- ii. Choose random elements $\{L_{x_1}, L_{x_2}, \dots, L_{x_j}\}$ from β -bounded distribution and compute $H_x = \{H_{x_1}, H_{x_2}, \dots, H_{x_j}\}$ where $H_{x_i} = qL_{x_i}$ for some positive integer q greater than γ and $1 \leq i \leq j$. Select a set S_x consist of random elements of γ -bounded distribution. Then transform both the set H_x and S_x into the field \mathbb{Y} using the isomorphic map Φ .

Output: $\text{Pk}=\{H_y, S_y\}$. $\text{Sk}=\{ \Phi^{-1}, qI\}$

II. PK-FHES.Enc

Input: $\{\text{Pk}, m\}$

- i. Encode a plaintext m in a binary matrix M_y and convert it into an element of a field \mathbb{Y} by some method.
- ii. Select random elements from the set H_y and embed the message in a random element of S_y . Then sum the selected elements and add them with the message matrix M_y , and compute the ciphertext.

$$C_y = \sum_{\text{random}(i)} H_{y_i} + M_y \quad (2.16)$$

Output: C_y as a ciphertext.

III. PK-FHES.Dec

Input: $\{\text{Sk}, C_y\}$

- i. Compute C_x using the inverse isomorphic map. $\Phi^{-1}(C_y)$.
- ii. Then compute M_x using modulo q operation i.e., $M_x = q \sum_{\text{random}(i)} L_{x_i} + M_x \text{ mod } q$.
- iii. Compute the plaintext $M_y = \Phi(M_x)$

Output: Plaintext M_y .

Example 2.15. This example elaborates the concept of the above suggested asymmetric homomorphic encryption scheme in detail. Let $p = 251$, $\gamma = 20$, $f(x) = x^2 + x + 19$ and $g(x) = x^2 + 3x + 19$ be the secret keys. The companion matrices M and N of the polynomials $f(x)$ and $g(x)$ is given as follows;

$$M = \begin{pmatrix} 0 & 232 \\ 1 & 250 \end{pmatrix} \text{ and } N = \begin{pmatrix} 0 & 232 \\ 1 & 248 \end{pmatrix}$$

Key generation. Initially, the user A uses the companion matrix M and N and generate the public and the private key. They choose random elements $\{H_{x_1}, H_{x_2}, H_{x_3}, H_{x_4}\}$ from the set \mathcal{X}_{20} . Let

$$L_{x_1} = \begin{pmatrix} 7 & 0 \\ 0 & 7 \end{pmatrix} \quad L_{x_2} = \begin{pmatrix} 14 & 4 \\ 13 & 1 \end{pmatrix} \quad L_{x_3} = \begin{pmatrix} 16 & 4 \\ 13 & 3 \end{pmatrix} \quad L_{x_4} = \begin{pmatrix} 15 & 4 \\ 13 & 2 \end{pmatrix}$$

Compute H_{x_i}

$$H_{x_i} = 2I \times L_{x_i} \text{ for } 1 \leq i \leq 4$$

$$H_{x_1} = \begin{pmatrix} 14 & 0 \\ 0 & 14 \end{pmatrix} \quad H_{x_2} = \begin{pmatrix} 28 & 8 \\ 26 & 2 \end{pmatrix} \quad H_{x_3} = \begin{pmatrix} 32 & 8 \\ 26 & 6 \end{pmatrix} \quad H_{x_4} = \begin{pmatrix} 30 & 8 \\ 26 & 4 \end{pmatrix}$$

$$H_{y_1} = \phi \left(\begin{pmatrix} 14 & 0 \\ 0 & 14 \end{pmatrix} \right) = \begin{pmatrix} 14 & 0 \\ 0 & 14 \end{pmatrix}$$

$$H_{y_2} = \phi \left(\begin{pmatrix} 28 & 8 \\ 26 & 2 \end{pmatrix} \right) = \begin{pmatrix} 88 & 163 \\ 216 & 193 \end{pmatrix}$$

$$H_{y_3} = \phi \left(\begin{pmatrix} 32 & 8 \\ 26 & 6 \end{pmatrix} \right) = \begin{pmatrix} 92 & 163 \\ 216 & 197 \end{pmatrix}$$

$$H_{y_4} = \phi \left(\begin{pmatrix} 30 & 8 \\ 26 & 4 \end{pmatrix} \right) = \begin{pmatrix} 90 & 163 \\ 216 & 195 \end{pmatrix}$$

Then the user A publish the elements $\{H_{y_1}, H_{y_2}, H_{y_3}, H_{y_4}\}$ and the primitive irreducible polynomial $g(x)$, and keep the integer matrix $2I$ and the primitive irreducible polynomial secret as a private key. User B encrypts his/her message using the publish key.

Encryption. Let $M = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ be the plain message, and user B wants to send it to user A securely. So, they encrypt the message while using the proposed public key. The encryption procedure is given as follows;

$$C_y = \sum_{\substack{\text{random}(i) \\ 1 \leq i \leq 4}} H_{y_i} + M_y \quad (2.17)$$

Implies

$$C_y = \begin{pmatrix} 179 & 75 \\ 181 & 138 \end{pmatrix}$$

After the encryption procedure, the user B sent the ciphertext C_y to A. Then the user A follows the proposed decryption procedure and gets the original message.

Decryption. Initially, user A uses his/her private key and applies the inverse isomorphic map on the ciphertext. Such as;

$$C_x = \phi^{-1} \left(\begin{pmatrix} 179 & 75 \\ 181 & 138 \end{pmatrix} \right) = \begin{pmatrix} 59 & 16 \\ 52 & 17 \end{pmatrix}$$

Then they apply the mod operation over the secret integer. In this case, we choose it 2 to obtain the plaintext.

$$M_x = \begin{pmatrix} 59 & 16 \\ 52 & 17 \end{pmatrix} \text{ mod } 2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Lemma 2.16. Let \mathcal{X}_γ be a γ -bounded distribution with $p < 2^{n^\epsilon}$ for $\epsilon \in (0,1)$. Then the scheme \mathcal{E} is homomorphic with circuit depth less than $\mathcal{D} < \log(\log(p-2) - \log(\log(jq\beta + 1)))$.

Proof. Let C_{y_1} and C_{y_2} be the encrypted messages of the original messages M_{y_1} and M_{y_2} respectively. Assume that C_{x_1} and C_{x_2} are decrypted successfully, if their noise growth after multiplication and addition less than $\frac{p}{2}$.

a) **Addition.** Let

$$C_y = C_{y_1} + C_{y_2} \text{ mod } p$$

$$C_x = q \sum_i L_{x_i} + M_{x_1} \text{ mod } p + q \sum_i L_{x_i} + M_{y_1} \text{ mod } p$$

Implies that the norm of the matrix

$$\|C_x\| \leq 2(jq\beta + 1)$$

b) **Multiplication.** As we evaluate the addition, similarly one can evaluate the multiplication.

$$C_y = C_{y_1} \times C_{y_2}$$

$$C_y = \left(\sum_i H_{y_i} + M_{y_1} \right) \left(\sum_i H_{y_i} + M_{y_1} \right) \text{ mod } p$$

$$C_x = \left(\sum_i qL_{x_i} + M_{x_1} \right) \left(\sum_i qL_{x_i} + M_{x_2} \right)$$

$$= \sum_i qL_i \sum_i qL_{x_i} + \sum_i qL_{x_i} M_{x_2} + \sum_i qL_{x_i} M_{x_1} + M_{x_2} M_{x_1}$$

$$= q^2 \sum_i L_{x_i} \sum_i L_{x_i} + q \sum_i L_{x_i} M_{x_2} + q \sum_i L_{x_i} M_{x_1} + M_{x_2} M_{x_1}$$

We compute the norm of the matrix C_x , using Lemma 2.10.

$$\|C_x\| \leq 4n(jq\beta)^2$$

c) In order to compute \mathcal{D} -level homomorphic, one has to calculate the bound of $\left\| (qLL_x + M_{x_1})^{2^{\mathcal{D}}} \right\|$. Since the length of qLL_x are $q\beta$ and the length of the binary matrix M_x

is 1, therefore it must be less or equal to $(q\beta + 1)^{\mathcal{D}}$. In this case, we want to reduce this noise to less than $\frac{p}{2}$ accordingly, it follows that

$$(jq\beta + 1)^{2^{\mathcal{D}}} < \frac{p}{2}$$

$$2^{\mathcal{D}} \log(jq\beta + 1) < \log(p - 2)$$

$$\mathcal{D} + \log(\log(jq\beta + 1)) < \log(\log(p - 2))$$

$$\mathcal{D} < \log(\log(p - 2)) - \log(\log(jq\beta + 1))$$

One can simplify the above inequality by omitting the small-term and consequently obtained

$$\mathcal{D} < \log(\log(p - 2)) < \log(\log(p))$$

By Taking $p < 2^{n^\epsilon}$, the upper bound for the multiplicative depth \mathcal{D} is $\mathcal{O}(\epsilon \log(n))$

2.8 Performance Analysis

The semantic security of the proposed construction scheme hinges on two assumptions. The first assumption is the difficulty of solving the computational finite field isomorphism problem, which assures that the images of small elements in \mathbb{X} are randomly distributed in \mathbb{Y} . Since the isomorphism function Φ between \mathbb{X} and \mathbb{Y} is unknown thus the attackers have to link the key consist of random elements of \mathbb{Y} with the short preimages in \mathbb{X} to break the encryption scheme. The finite field isomorphism problems are even more difficult to solve in the case of matrix fields because the elements in the isomorphic matrix fields are always distinct, and in the case of polynomial fields the polynomial representation of the elements in isomorphic fields are always the same. The second assumption is the hardness of solving subset sum problems. As the scheme is based on the subset sum problem. The sender chooses j elements from the set H_y of order J and an element from the set S_y . Therefore, the pair of the parameter $\binom{J}{j}$ must be proved to have reasonable combination security.

Theorem 2.17. *Let $\{H_y, S_y\}$ be any public key that encrypts a message M_y of either 0 or identity matrix I . If there exists a scheme \mathcal{A} that is capable to break the encryption scheme with parameter $\{n, q, \gamma\}$ and deciphered the message M_y with probability $\frac{1}{2} + \eta$ for a non-negligible function $\eta > 0$, then there will exist an algorithm \mathcal{B} able to solve finite field isomorphism problem with probability $\frac{1}{2} + \eta$.*

Proof. Given that the algorithm \mathcal{A} can compute the output of the input $\{C_y, H_y, S_y\}$ with probability greater than 0.5, so if the input is invalid to the algorithm \mathcal{A} it means that either the ciphered matrix C_y is not the encrypted form of the 0 matrices or identity matrix, or C_y is not equal to the subset-sum of the set H_y . The algorithm \mathcal{A} will be must decipher the ciphered text M_y with probability greater than 0.5, if the inputs are valid to the scheme. Now we can build an algorithm \mathcal{B} utilizing \mathcal{A} . Let $L_{y_1}, L_{y_1}, \dots, L_{y_j}, M_{y_1}$ and M_{y_2} be the input to the decisional finite field isomorphism problem. As obtain the inputs the algorithm \mathcal{A} call on algorithm \mathcal{B} with public ciphertext 0 and public key $pk = L_{y_1}, L_{y_1}, \dots, L_{y_j}, M_{y_1}$. Suppose that the pre-image of M_{y_1} is a sampled from the distribution \mathcal{X} , implies that the public key $L_{y_1}, L_{y_1}, \dots, L_{y_j}, M_{y_1}$ is the legit key, and the algorithm can recover the plaintext with probability greater then $\frac{1}{2}$. Suppose that M_{y_1} is chosen uniformly from the field \mathbb{X} , then the algorithm must output an error to the input $pk=L_{y_1}, L_{y_1}, \dots, L_{y_j}, M_{y_1}$. Accordingly, the algorithm \mathcal{B} solved the decisional problem with probability greater than $\frac{1}{2}$.

2.8.1 Lattice Attack

Let $L_{x_1}, L_{x_2}, \dots, L_{x_u}$ be distinct matrices of \mathbb{X} sampled from the distribution \mathcal{X}_y , and $L_{y_1}, L_{y_2}, \dots, L_{y_u}$ be the corresponding images in \mathbb{Y} under the isomorphism Φ . Since we know that the field \mathbb{X} and \mathbb{Y} can be viewed as finite-dimensional vector spaces over the field \mathbb{F}_p . Let $1, M, M^2, \dots, M^{n-1}$ and $1, N, N^2, \dots, N^{n-1}$ be the bases for the field \mathbb{X} and \mathbb{Y} respectively. Then for each $0 \leq k \leq n - 1$ it follows that

$$M^k \rightarrow (N^k)^s \text{ mod } p = \sum_{j=0}^{n-1} c_{kj} N^j \text{ mod } p \quad (2.18)$$

Let $C = (c_{kj})$ be the associated $n \times n$ matrix. Let

$$L_x = \sum_{i=0}^{n-1} x_i M^i \text{ mod } p \quad (2.19)$$

Implies that

$$L_y = \sum_{k=0}^{n-1} x_k (N^k)^s = \sum_{k=0}^{n-1} x_k \left(\sum_{j=0}^{n-1} c_{kj} N^j \right) \quad (2.20)$$

by comparing the coefficients

$$y = xC \text{ mod } p \quad (2.21)$$

In the above equation, the attacker knows the vector y and she does not have the knowledge of x and C . In the case of the matrix field, she does not have an idea about the length of x , because in this case the length of the matrix L_x does not depend on the coefficients of x_i for $0 \leq i \leq n - 1$. However, in the case of a polynomial field, the length of the polynomial depends upon the coefficients of the polynomial. Therefore, in that case, she knows that the length of x is short. From equation 2.18, one can be observed that there are $n^2 + n$ unknown, which are the entries of the matrix M and the entries of the vector x . So, this is the matrix decomposition problem, which does not reveal the exact information about M or x . Since the attacker knows more than one images $L_{y_1}, L_{y_2}, \dots, L_{y_u}$. Therefore for

$$x_1, x_2, \dots, x_u \quad (2.22)$$

Writing $x_i = (x_{i_1}, x_{i_2}, \dots, x_{i_{n-1}})$ and similarly, write $y_i = (y_{i_1}, y_{i_2}, \dots, y_{i_{n-1}})$ and from a matrix

$$Y = (y_{ij})_{\substack{1 \leq i \leq u \\ 0 \leq j \leq n-1}} \text{ and } X = (x_{ij})_{\substack{1 \leq i \leq u \\ 0 \leq j \leq n-1}} \quad (2.23)$$

that gives the matrix equation

$$Y = XM \text{ mod } p \quad (2.23)$$

In the case of the polynomial field given in [29], the unknown matrix X has small coordinates and thus it becomes a short vector in the space $\mathbb{Z}^{n \times u}$, which yields to setup a lattice problem to find X . Because in the case of computational finite field isomorphism problem over the polynomial field the length of the polynomials depends on the coefficients of the polynomial. However, in the case of the finite field over matrix field the length of the matrix does not depend on the coefficients, therefore it is quite difficult for the attacker to set up a short vector lattice problem to find X .

Chapter 3

The Study of NTRU Cryptosystem Based on Matrix Ring Over Finite Field Extension

3.1 Introduction

In 1996 Hoffstein, Pipher, and Silverman introduced the idea of the NTRU cryptosystem; afterward, it was published in the proceeding conference [30]. The NTRU scheme is one of the quickest public-key cryptosystems and its operations take place in a ring $\frac{\mathbb{Z}_p[y]}{\langle y^n - 1 \rangle}$ and suitable for both confidential communication and authentication. A simple linear transformation over ring elements performs the process of encryption and decryption of the scheme. Since this transformation is used to execute simple polynomial addition and multiplication, thus their implantation cost is $\mathcal{O}(n^2)$. Accordingly, the NTRU cryptosystem is fast and more efficient than other asymmetric key cryptosystems, which are hinges on a discrete logarithm and factorization problem. The efficiency of this scheme is relying on the hardness of the shortest vector problem; therefore, it is conceived to be secured against classical and post-quantum attacks. Besides, researchers have improved the speed of the NTRU cryptosystem by operating the scheme in different rings. In 2002, Gaborit et al. [31] presented a CTRU scheme corresponding to NTRU, while substitute the ring $\frac{\mathbb{Z}_p[y]}{\langle y^n - 1 \rangle}$ by the ring $\mathbb{Z}_2[y]$, and they claimed that the CTRU scheme has no decryption failure. Afterward, Kouzmenko established new kinds of attacks in 2005, which were called polynomial-time attacks, and elaborated that the CTRU scheme can be easily disrupted by polynomial-time attacks [32]. In addition to this, Kouzmenko presents the GNTRU scheme by an example alternate to NTRU by replacing the ring with Gaussian integers $\mathbb{Z}[i]$. In 2005 Coglianesi and Goi introduced MNTRU based on the matrix module n [33].

This chapter further extends the idea of the MNTRU scheme and presents a new scheme based on the non-commutative matrix ring over a Galois field. For the successful implementation of the proposed scheme, the suitability criteria are presented to avoid decryption failure. Since the scheme operates in a non-commutative ring, thus the linear transformations are performing from two side multiplication, which enhances the keyspace of the scheme. Moreover, the lattice attack is hard to affect the scheme due to the high dimension of the lattice matrix and the non-commutativity property of a matrix ring.

3.2 NTRU Cryptosystem

This section discusses the NTRU cryptosystem in brief. The NTRU algorithm is operating in a polynomial ring $\frac{\mathbb{Z}_p[y]}{\langle y^{n-1} \rangle}$, we denote this polynomial ring by R_{p^n} . The cryptosystem depends on the set positive integers given as (n, q, p, d_g, d_f, n_1) . Where the integer q should be considerably greater than the integer p . Besides, these integers are coprime such that $\gcd(p, q) = 1$. The integers d_f, d_g and n_1 are less than $\frac{n}{2}$. Select the bounded subsets $\mathcal{S}_f, \mathcal{S}_g, \mathcal{S}_r$ and \mathcal{S}_m of the ring R associated with the integers d_f, d_g and n_1 . We denote the elements of the ring R_{q^n} by \bar{a} , and the elements of a ring R by a having coefficient in the interval $[\frac{q}{2}, \frac{q}{2})$. Moreover, the notation ab is used to represent the multiplication of the polynomial a and b and similarly $a + b$ for the polynomial addition. One needs to describe one more definition before introducing the NTRU encryption scheme.

Definition 3.1. Let n_1 and n_2 be two positive integers. Then the set of polynomials

$$\mathcal{T}(n_1, n_2) = \left\{ \begin{array}{l} \mathcal{K}(y) \in R: \text{ The } n_1 \text{ number of coefficients of } \mathcal{K}(y) \text{ is equal to } 1 \\ \text{ The } n_2 \text{ number coefficients of } \mathcal{K}(y) \text{ is equal to } -1 \\ \text{ All the other coefficients of } \mathcal{K}(y) \text{ equal to } 0 \end{array} \right.$$

The elements of the set $\mathcal{T}(n_1, n_2)$ is said to be ternary polynomials. If these are analogs to the binary polynomials i.e., all the coefficients of the polynomials are either 0 or 1.

3.2.1 Key Generation

Let Bob and Alice be the two communicating entities, both the parties want to communicate through the NTRU encryption scheme. Bob initially chooses two random polynomials $\mathbf{f}(y)$ and $\mathbf{g}(y)$ such that both the polynomials satisfy the condition given as follows.

$$\mathbf{f}(y) \in \mathcal{T}(n_1 + 1, n_1) \text{ and } \mathbf{g}(y) \in \mathcal{T}(n_1, n_2) \quad (3.1)$$

Subsequently, she calculates the multiplicative inverse of the polynomials $\mathbf{f}(y)$ in both rings R_{q^n} and R_{p^n} respectively.

$$\mathbf{F}_q(y) = \mathbf{f}(y)^{-1} \in R_q \text{ and } \mathbf{F}_p(y) = \mathbf{f}(y)^{-1} \in R_{p^n} \quad (3.2)$$

Afterward, Bob computes the polynomial $\mathbf{h}(y)$ by using the polynomial $\mathbf{F}_q(y)$, the mathematical representation is given as follows.

$$\mathbf{h}(\mathbf{y}) = \mathbf{F}_q(\mathbf{y})\mathbf{g}(\mathbf{y}) \text{ in } \mathbf{R}_{q^n} \quad (3.3)$$

The pair of polynomials $(\mathbf{f}(\mathbf{y}), \mathbf{F}_p(\mathbf{y}))$ is the Bob private key that will be required to decipher the ciphertext, and $\mathbf{h}(\mathbf{y})$ is her public key, which she will public to Alice. Alice will encrypt her message using this public key. The detail of the encryption and decryption procedure is given as follows.

3.2.2 Encryption and decryption

To encrypt a plaintext $m(\mathbf{y})$, Alice initially chose a random element $r(\mathbf{y})$ from the set \mathcal{S}_r and calculate the ciphertext. Mathematically, it can be written as;

$$\overline{c}(\mathbf{y}) = p\overline{h}(\mathbf{y})r(\mathbf{y}) + m(\mathbf{y}) \in R_{q^n}. \quad (3.4)$$

To decrypt the ciphertext \overline{c} , initially compute the following *mod q* operation;

$$\overline{a} = f(\mathbf{y})\overline{c}(\mathbf{y}) = f(\mathbf{y})(p\overline{h}(\mathbf{y})r(\mathbf{y}) + m(\mathbf{y})) \in R_{q^n}. \quad (3.5)$$

Then compare the unique polynomial $a \in R$ having coefficient from the interval $[\frac{q}{2}, \frac{q}{2})$ with the polynomial *mod q* in a ring R_q . If the polynomial $a = f(hpr + m) \in R$ free from *mod q* reduction coincides with the polynomial \overline{a} modulo q , then one can get the plaintext m , by making the following *mod p* calculation.

$$b(\mathbf{y}) = pr(\mathbf{y})\mathbf{g}(\mathbf{y}) + f(\mathbf{y})m(\mathbf{y}) = f(\mathbf{y})m(\mathbf{y}) \in R_{p^n} \quad (3.6)$$

$$F_3(\mathbf{y})b(\mathbf{y}) = F_3(\mathbf{y})f(\mathbf{y})m(\mathbf{y}) = m(\mathbf{y}) \in R_{p^n}. \quad (3.7)$$

Otherwise, the decryption will be considered a failure. The following necessary condition on the element a is essential for the successful decryption.

$$\|a\|_\infty = \max a_i - \min a_i < q. \quad (3.8)$$

Thus, the elements p and q should be selected in a manner that the probability of successful decryption is maximum. The following proposition discusses the conditions on the parameters of the NTRU scheme, which make ensure successful decryption.

Proposition 3.2. [34] *If the parameters (n, q, p, n_1) of the NTRU encryption scheme are chosen, so that it satisfies the following property.*

$$q > (6n_1 + 1)p$$

Then the decipher text obtain after the decryption procedure will equal the original plaintext.

Example 3.3. We present an example of the NTRU encryption scheme to elaborate the idea in more detail. Let the public parameters are

$$(n, q, p, n_1) = (7, 41, 3, 2)$$

implies

$$39 = (6n_1 + 1)p < 41$$

Since the parameters satisfy the equation. Therefore, by Proposition 3.2. the decryption will work successfully. Let Bob choose the following polynomial.

$$f(y) = y^6 - y^4 + y^3 + y^2 + 1 \in \mathcal{T}(3, 2) \text{ and } g(y) = y^6 + y^4 - y^2 - y \in \mathcal{T}(2, 2).$$

Afterward, she computes the inverse of the polynomials $f(y)$ and $g(y)$

$$F_{41}(y) = f(y)^{-1} \text{mod } q = 8y^6 + 26y^5 + 31y^4 + 21y^3 + 40y^2 + 2y + 37 \text{ in } R_{41}$$

$$F_3(y) = f(y)^{-1} \text{mod } p = y^6 + 2y^5 + y^3 + y^2 + y + 1 \text{ in } R_3.$$

She computes and then publishes the key $h(y)$ and keep the pair $(f(y), F_3(y))$ of the polynomials secret as her private key to use for decryption.

$$h(y) = F_{41}(y)g(y) = 20y^6 + 40y^5 + 2y^4 + 38y^3 + 8y^2 + 26y + 38 \text{ in } R_{41}.$$

Suppose Bob willing to send the message polynomial $m(y)$ to Alice, and choose the random polynomial $r(y)$ for semantic security.

$$m(y) = -y^5 + y^3 + y^2 - y + 1 \text{ and } r(y) = y^6 - y^5 + y - 1$$

Then Bob computes the ciphertext $c(y)$ using the public polynomials $h(y)$ and random polynomial $r(y)$. Then she sent it to Alice through insecure channel.

$$c(y) = pr(y)h(y) + m(y) = 31y^6 + 19y^5 + 4y^4 + 2y^3 + 40y^2 + 3y + 25 \text{ mod } 41$$

After receiving the Bob ciphertext, Alice proceeds with the decryption method and deciphers the ciphertext $c(y)$. Initially, she computes

$$f(y)e(y) = y^6 + 10y^5 + 33y^4 + 40y^3 + 40y^2 + y + 40 \text{ mod } q$$

Subsequently, she center-left the obtained $f(y)e(y) \text{mod } q$ into the ring R , and then she again reduces it modulo p .

$$a(y) = y^6 + 10y^5 - 8y^4 - y^3 - y^2 + y - 1$$

$$F_3(y)a(y) = 25y^5 + y^3 + y^2 + 2y + 1 \text{ mod } p$$

Finally, she center-left the polynomial $F_3(y)a(y) \bmod p$, which consequently retrieves the Bob plaintext.

$$m(y) = -y^5 + y^3 + y^2 - x + 1.$$

3.3 Asymptotic Complexity of NTRU Scheme

The main advantage of lattice-based cryptography is its performing speed as compared to the cryptographic scheme based on the prime factorization problem and discrete logarithmic problem. The question arises as that how fast is the NTRU cryptosystem? In the encryption and decryption procedure, the most consuming part is the product of polynomials. Since in polynomial multiplication each coefficient performs the dot product of a vector, therefore, the product of two degree n polynomials usually require n^2 multiplication. The polynomial products required by the encryption-decryption procedure of the NTRU scheme have the form $r(y)h(y)$, $f(y)e(y)$ and $F_p(y)a(y)$. Since the polynomials $r(y)$, $f(y)$ and $F_p(y)$ are the ternary polynomials. Therefore, these convolution polynomials can compute without multiplications and requires $\frac{3}{2}n^2$ subtractions and additions. If n_1 less than $\frac{n}{3}$, then the first two of these require just $\frac{3}{2}nn_1$ subtractions and additions. Therefore, the encryption and decryption procedure of the NTRU scheme requires $O(n^2)$ step, which is polynomial time and extremely fast.

3.3.1 Mathematical Problem for NTRU Scheme

Since we know that the coefficients of the public key polynomial are distributed as random integers modulo q . However, there is a hidden relation between the polynomial $f(y)$ and $h(y)$ that is

$$g(y) \equiv f(y)h(y) \bmod q \quad (3.9)$$

As we know that the coefficients of the polynomial $f(y)$ and $g(y)$ are small. Thus, breaking the NTRU scheme over the problem finding the secrete key is reduce to solving the problem given as follows;

Key Recovery problem. *Given the public key polynomial $h(y)$, find the ternary polynomials $g(y)$ and $f(y)$ that satisfying*

$$g(y) \equiv f(y)h(y) \bmod q \quad (3.10)$$

The solution to the key recovery problem of the NTRU scheme is not unique. Suppose the pair $(f(y), g(y))$ is the one solution of the key recovery problem, then the pairs

$(y^m f(y), y^m g(y))$ is also the solution, for all positive integers m less than n . Since the polynomial $y^m f(y)$ cyclically rotate the coefficients therefore such polynomials are called the rotation of the polynomial $f(y)$. The decryption with such rotated polynomial output rotated plaintext $y^m m(y)$.

3.3.2 Brute force Attack.

This section discusses the hardness of the Eavesdropper task if she tries to search and apply all the possible public keys. The Eavesdropper can ascertain that either she has found or not the private key polynomial through verification; that all the coefficients in the center-left polynomial $f(y)h(y) \bmod q$ is not greater than 1 and less than -1 . So, we have to figure out the order of the set of trinary polynomials. Generally, one has to specify the elements of the set $\mathcal{T}(n_1, n_2)$, initially by choosing n_2 coefficient equal to -1 and then choosing the n_1 coefficient of the remaining $n - n_2$ equal to 1. Thus

$$\#\mathcal{T}(n_1, n_2) = \binom{n}{n_1} \binom{n - n_1}{n_2} = \frac{n!}{n_1! n_2! (n - n_1 - n_2)!} \quad (3.11)$$

Besides, this number can be increased if the number n_1 and n_2 are both approximately equal to $\frac{n}{3}$. In the brute force attack, the Eavesdropper must try all the polynomial in the set $\mathcal{T}(n_1 + 1, n_2)$ until she finds the private key polynomial $h(y)$. Since all the rotation polynomials of the polynomial $h(y)$ are counts as the private key and the order of the rotation polynomials is n . Therefore, in brute force, the Eavesdropper will approximately $\frac{\mathcal{T}(n_1+1, n_2)}{n}$ try to find out some rotation polynomial of the decryption key $f(y)$.

Proposition 3.4. [34] *Let A be an algorithm for solving the key recovery problem of the NTRU encryption scheme. Let $\mathcal{T}(n_1 + 1, n_2), g(y)$ and $h(y)$ be the input of the algorithm A , where $h(y)$ is the public key polynomial and $\mathcal{T}(n_1 + 1, n_2)$ is the set of trinary polynomials, for $n_1 \approx \frac{n}{3}$. Let $f(y)$ be the output of A chosen uniformly and randomly from the set of trinary polynomials, such that $g(y) \equiv f(y)h(y) \bmod q$. Then the algorithm A to output the correct decryption key with negligible probability.*

Proof. Given that, the size is maximized by sitting $n_1 \approx \frac{n}{3}$. Then by using the Stirling formula the estimated order of the trinary polynomial $\mathcal{T}(n_1 + 1, n_1)$ is equal to

$$\#\mathcal{T}(n_1 + 1, n_1) = \frac{n!}{((n/3)!)^3} \approx \left(\frac{n}{e}\right)^n \cdot \left(\left(\frac{n}{3e}\right)^{\frac{n}{3}}\right)^{-3} \approx 3^n$$

Therefore, the probability that the algorithm A to output the exact decryption key is $\frac{1}{3^n}$. Since for any polynomial $q(y)$ there are $m_1, m_2 \in \mathbb{R}_{>0}$ and natural number n such that $|q(y)| \leq m_2 y^m$ for $m_2 \geq m_1$. Accordingly, there exist some $K \geq m_1$ such that $m_2 K^n < 3^n$. Thus, the success probability of the Algorithm A to output the correct decryption key is negligible.

3.3.3 NTRU key recovery problem as a Lattice Problem

In this section, we describe a complete review of the NTRU key recovery problem that are reduced to the short vector problem in some sort of certain lattice. Let $h(y)$ be the public key polynomial for the NTRU encryption. Supposes

$$h(y) = h_0 + h_1 y + h_2 y^2 + \dots + h_{n-1} y^{n-1} \quad (3.12)$$

then the NTRU lattice L_h^{NTRU} is $2n$ dimensional lattice associated with the public key polynomial $h(y)$ generated by the row spanned of the matrix M_h^{NTRU} .

$$M_h^{NTRU} = \left(\begin{array}{cccccc|cccccc} 1 & 0 & 0 & \dots & 0 & 0 & h_0 & h_1 & h_2 & \dots & h_{n-2} & h_{n-1} \\ 0 & 1 & 0 & \dots & 0 & 0 & h_{n-1} & h_0 & h_1 & \dots & h_{n-3} & h_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 1 & h_1 & h_2 & h_3 & \dots & h_{n-1} & h_0 \\ \hline 0 & 0 & 0 & \dots & 0 & 0 & q & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 & q & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & \dots & 0 & q \end{array} \right)$$

It can be seen that four $n \times n$ matrices are merged in the matrix M_h^{NTRU} . The upper left matrix is the $n \times n$ identity matrix, the upper right matrix is the $n \times n$ matrix composed of cyclic permutation of the public key polynomial $h(y)$. The lower left block is the 0 matrix, and the lower right block is the q time $n \times n$ identity matrix. In the following results the NTRU matrix M_h^{NTRU} is abbreviate as;

$$M_h^{NTRU} = \begin{pmatrix} I & h \\ 0 & qI \end{pmatrix} \quad (3.13)$$

where the M_h^{NTRU} visualize as a 2×2 matrix with coefficients in the ring R . The pair of the polynomials f and g can be defined in R as $2n$ dimensional vector. Let $f(y) = f_0 + f_1 y + \dots + f_n y^n$ and $g(y) = g_0 + g_1 y + \dots + g_n y^n$, then the $2n$ dimensional vector (f, g) is defined as follows;

$$(f, g) = (f_0, f_1, \dots, f_n, g_0, g_1, \dots, g_n). \quad (3.14)$$

Suppose the public key $h(y)$ of the NTRU encryption scheme is created through the private polynomial $f(y)$ and $g(y)$. Now the following result illustrates what happening whenever the NTRU matrix is multiplying with the chosen vectors.

Proposition 3.5. [34, Proposition 7.59] *Let $f(y)$ and $g(y)$ be two trinary polynomials and $h(y)$ be the polynomial such that $f(y)h(y) \equiv g(y) \pmod{q}$. Let the polynomial $u(y) \in R$ satisfying the following equation*

$$f(y)h(y) = g(y) + qu(y).$$

Then

$$(g, f) = (f, -u)M_h^{NTRU}$$

Thus, the vector (f, g) is an element of the lattice L_h^{NTRU} .

The proof of Proposition 3.5 becomes straight forward while using the abbreviation of the matrix M_h^{NTRU} , that is

$$(f, g) = (f, fh - qu) = (f, -u) \begin{pmatrix} I & h \\ 0 & qI \end{pmatrix}. \quad (3.15)$$

Proposition 3.6. [34, Proposition 7.61] *Let (n, q, p, n_1) be the parameters of the NTRU scheme, for computational simplicity, assume that*

$$p = 3 \text{ and } n_1 = \frac{n}{3} \text{ and } q \approx 6pn_1 \approx 2pn$$

Suppose that the lattice associated with the private key (f, g) is L_h^{NTRU} . Then the following conditions hold.

- i. $\det(L_h^{NTRU}) = q^n$.
- ii. $\|(f, g)\| \approx \sqrt{4n} \approx \sqrt{\frac{4n}{3}} \approx 1.155\sqrt{n}$.

Proposition 3.5 and Proposition 3.6 demonstrate that the pair private key polynomials (f, g) is short in the lattice L_h^{NTRU} . Thus, solving the NTRU encryption scheme recovery problem reduces to the short vector problem in the lattice L_h^{NTRU} .

3.4 Proposed Cryptosystem

This section begins by introducing some basic definitions and results that are used in the upcoming sections. Recall that, a polynomial f of degree n of the ring $R[x]$ can be written as;

$$f(y) = a_0 + a_1y + \dots + a_{n-1}y^{n-1} \text{ for all } a_i \in R \quad (3.16)$$

The length of the polynomial f or the norm is defined as;

$$\|f\|_\infty = \max_{1 \leq i \leq n} |a_i|. \quad (3.17)$$

The suggested NRTU cryptosystem operates in a non-commutative ring of $k \times k$ matrices over the Galois field \mathbb{F}_{p^n} , we denote it by $\mathcal{M}^k(\mathbb{F}_{p^n})$. The elements of the field \mathbb{F}_{p^n} consist of the polynomial of degree at most $(n - 1)$ having coefficient from the field \mathbb{Z}_p . The scheme began by fixing two irreducible polynomials $f(x)$ and $g(x)$ of degree n with coefficient moduli q and p respectively. Let \mathcal{R} , \mathbb{F}_{p^n} and \mathbb{F}_{q^n} be the corresponding integral domain and convolution quotient fields.

$$\mathcal{R} = \frac{\mathbb{Z}[x]}{\langle x^n - 1 \rangle} \quad \mathbb{F}_{q^n} = \frac{\mathbb{Z}_q[x]}{\langle f(x) \rangle}, \quad \mathbb{F}_{p^n} = \frac{\mathbb{Z}_p[x]}{\langle g(x) \rangle}$$

Where p and q are prime integers, the elements in the \mathcal{R} are also the elements in \mathbb{F}_{p^n} and \mathbb{F}_{q^n} reduced their coefficient moduli p and q in cosets form. Similarly, $q \geq p$, thus the elements of \mathbb{F}_{p^n} are contained in \mathbb{F}_{q^n} moduli q . Moreover, we use the map α defined as follows to move the elements from \mathcal{R} to \mathbb{F}_{p^n} .

$$\begin{aligned} \alpha_p: \mathcal{R} &\rightarrow \mathbb{F}_{q^n} \\ \alpha_p(h(x)) &= \overline{h_p(x)}. \end{aligned} \quad (3.18)$$

Let $\mathcal{B}(\mathcal{R})$ be the subset of the integral domain \mathcal{R} consist of all binary polynomials, which is defined as follows;

$$\mathcal{B}(\mathcal{R}) = \left\{ f(x) = \sum_{i=0}^n a_i x^i \in \mathcal{R} \mid 0 \leq i < \frac{n}{4}, \|f(x)\|_\infty = 1 \right\}. \quad (3.19)$$

The degree of polynomials in $\mathcal{B}(\mathcal{R})$ is less than $\frac{n}{4}$ with coefficients equal to 1 or 0. Let $\mathcal{D}(\mathcal{R})$ be the subset of the matrix ring $\mathcal{M}^k(\mathcal{R})$ defined as;

$$\mathcal{D}(\mathcal{R}) = \{M \in \mathcal{M}^k(\mathcal{R}) \mid m_{i,j} \in \mathcal{B}(\mathcal{R})\}. \quad (3.20)$$

Assume that Bob chooses the public parameters $(N, p, q, f(x), g(x))$ satisfying some necessary conditions. The next subsections describe the key generation step, encryption, and decryption process.

3.4.1 Key Generation

To generate the public and private key, Bob chose an element from the general linear group $GL(k, \mathcal{M}^k(\mathbb{F}_{q^n}))$ and an element N from the subset $\mathcal{D}(\mathbb{F}_{q^n})$. Then Bob computes the public key

$$H = MN \in \mathcal{M}^k(\mathbb{F}_{q^n}). \quad (3.21)$$

The Bob public key is H and her private key is a pair (M^{-1}, M) that is essential to decrypt the message.

3.4.2 Encryption

The Alice plaintext P' is an element of $\mathcal{M}^k(\mathbb{F}_{q^n})$, each entry of P' is a polynomial with the coefficients between 0 and $\frac{p}{2}$. Alice chose random matrix $R \in \mathcal{D}(\mathcal{R})$ and $p \cdot I = I_p$ where p the characteristic of the field is \mathbb{F}_{p^n} and I represents the identity matrix. Compute the ciphertext defined as;

$$C = HI_pR + P' \in \mathcal{M}^k(\mathbb{F}_{q^n}). \quad (3.22)$$

Then Alice sent the ciphertext C to Bob.

3.4.3 Decryption

After receiving the Alice ciphertext, Bob computes the plaintext P' using the private $M^{-1} \in GL(k, \mathcal{M}^k(\mathbb{F}_{q^n}))$, The procedure is defined as follows;

$$A = M^{-1}$$

$$\bar{A} = NI_pR + M^{-1}P' \in \mathcal{M}^k(\mathbb{F}_{q^n}). \quad (3.23)$$

Afterward, verify the answer \bar{A} with a unique matrix $A \in \mathcal{M}^k(\mathcal{R})$, that each entry $a_{i,j}$ of the matrix A has degree less than n with coefficients in the interval $[0, q - 1]$ by using the following map;

$$\alpha_q(m_{i,j}) = \overline{m_{i,j}} \quad (3.24)$$

if

$$m_{i,j} = \overline{m_{i,j}}. \quad \forall m_{i,j} \in A \quad (3.25)$$

If the resultant $\overline{m_{i,j}}$ in the field \mathbb{F}_{q^n} is coinciding with the elements $m_{i,j}$ in the ring \mathcal{R} . Then the Bob will be able to obtain the plaintext P' follows the calculation in the field \mathbb{F}_{p^n} .

$$\alpha_p(A) = M^{-1}P' \in \mathcal{M}^k(\mathbb{F}_{p^n}). \quad (3.26)$$

Since p is the characteristic element in \mathbb{F}_{p^n} , accordingly, NI_pR in \mathbb{F}_{p^n} is a zero matrix in the ring $\mathcal{M}^k(\mathbb{F}_{p^n})$.

$$P' = MM^{-1}P' \in \mathcal{M}^k(\mathbb{F}_{q^n}). \quad (3.27)$$

Otherwise, Bob will be unable to decrypt the message successfully. In the next subsection, we discussed the necessary condition for successful decryption.

Example 3.7. We illustrate the proposed cryptosystem by choosing the primes $p = 3$ and $q = 11$. Let Alice chooses the primitive irreducible polynomial $f(y) = y^6 + y + 2 \in \mathbb{Z}_3[y]$ and $g(y) = y^6 + y^2 + 2y + 8 \in \mathbb{Z}_{11}[y]$ and then she computes the public and private keys.

$$M = \begin{pmatrix} y & 1 \\ 1 + y & y \end{pmatrix} \text{ and } N = \begin{pmatrix} 1 + y & y + y^2 \\ 1 + y & y^2 \end{pmatrix}$$

$$M^{-1} = \begin{pmatrix} 9y + 10y^2 + 3y^3 + 7y^4 + 7y^5 & 2 + y + 8y^2 + 4y^3 + 4y^4 \\ 2 + 3y + 9y^2 + y^3 + 8y^4 + 4y^5 & 9y + 10y^2 + 3y^3 + 7y^4 + 7y^5 \end{pmatrix}$$

$$PK = M^{-1} \times N$$

$$PK = \begin{pmatrix} 1 + 9y + 10y^2 + 3y^3 + 7y^4 + 7y^5 & 10 + 7y + y^2 + 2y^3 + 10y^4 + 3y^5 \\ 2 + 3y + 9y^2 + y^3 + 8y^4 + 4y^5 & 2 + 8y + 8y^2 + 10y^3 + 9y^4 + 1y^5 \end{pmatrix}$$

She computes M^{-1} and $PK = M^{-1}N$ in the ring $\mathcal{M}^2(\frac{\mathbb{Z}_{11}[y]}{\langle g(y) \rangle})$. Then share the key PK with

Bob through an open network as a public key and store the key $SK = (M, M^{-1})$ as a private key.

Let $MS = \begin{pmatrix} y & y \\ 0 & 1 + y^2 \end{pmatrix} \in \mathcal{M}^2(\frac{\mathbb{Z}_{11}[y]}{\langle g(y) \rangle})$ be the Bob plain message and she wants to send it insecurely. So, she computes the ciphertext to follow the proposed encryption procedure. Initially, she multiplies pI with the public key and chooses an element $R \in \mathcal{M}^2(\frac{\mathbb{Z}_{11}[y]}{\langle g(y) \rangle})$ for semantic security.

$$pI = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} \text{ and } R = \begin{pmatrix} y & y \\ 1 & y^2 \end{pmatrix}$$

$$S = \begin{pmatrix} 1 + 9y + 10y^2 + 3y^3 + 7y^4 + 7y^5 & 10 + 7y + y^2 + 2y^3 + 10y^4 + 3y^5 \\ 2 + 3y + 9y^2 + y^3 + 8y^4 + 4y^5 & 2 + 8y + 8y^2 + 10y^3 + 9y^4 + 1y^5 \end{pmatrix} \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}$$

$$S = PK \times 3$$

$$S = \begin{pmatrix} 3 + 5y + 8y^2 + 9y^3 + 10y^4 + 10y^5 & 8 + 10y + 3y^2 + 6y^3 + 8y^4 + 9y^5 \\ 6 + 9y + 5y^2 + 3y^3 + 2y^4 + 1y^5 & 6 + 2y + 2y^2 + 8y^3 + 5y^4 + 3y^5 \end{pmatrix}$$

$$C = S \times R + MS$$

$$C = \begin{pmatrix} 5 + 5y + 9y^2 + 3y^3 + 6y^4 + 8y^5 & 10 + 6y + 10y^2 + 9y^3 + y^4 + y^5 \\ 9 + 6y + 10y^2 + 2y^3 + 8y^4 + 5y^5 & 8 + 3y + 4y^2 + 4y^3 + 5y^4 + 10y^5 \end{pmatrix}$$

Bob then sends the ciphertext C to Alice. Alice receives the ciphertext and then decrypts it by following the decryption procedure of the proposed scheme and get the original message.

Initial she computes

$$A = M \times C$$

$$A = \begin{pmatrix} y & 1 \\ 1+y & y \end{pmatrix} \begin{pmatrix} 5 + 5y + 9y^2 + 3y^3 + 6y^4 + 8y^5 & 10 + 6y + 10y^2 + 9y^3 + y^4 + y^5 \\ 9 + 6y + 10y^2 + 2y^3 + 8y^4 + 5y^5 & 8 + 3y + 4y^2 + 4y^3 + 5y^4 + 10y^5 \end{pmatrix}$$

$$A = \begin{pmatrix} 6y + 7y^2 & 1 + 3y + 5y^2 + 3y^3 + 3y^4 \\ 4y + 7y^2 & 5y + 4y^2 + y^3 + 3y^4 \end{pmatrix}.$$

Afterward, she reduces the obtained matrix A modulo p , which reduces the coefficients of the polynomial.

$$B = A \text{ mod } 3$$

$$B = \begin{pmatrix} y^2 & 1 + 2y^2 \\ y + y^2 & 2y + y^2 + y^3 \end{pmatrix}$$

She computes the inverse of the matrix M in the polynomial ring $\mathcal{M}^2\left(\frac{\mathbb{Z}_3[y]}{\langle f(y) \rangle}\right)$. Then multiply the inverse of the matrix M with the reduced matrix B . Consequently, get the original plaintext matrix.

$$M^{-1} = \begin{pmatrix} y + y^3 + 2y^4 + 2y^5 & 2 + 2y^2 + y^3 + y^4 \\ 2 + 2y + 2y^2 + 2y^4 + y^5 & y + y^3 + 2y^4 + 2y^5 \end{pmatrix} \text{ in } \mathcal{M}^2\left(\frac{\mathbb{Z}_3[y]}{\langle f(y) \rangle}\right).$$

$$MS = \begin{pmatrix} y + y^3 + 2y^4 + 2y^5 & 2 + 2y^2 + y^3 + y^4 \\ 2 + 2y + 2y^2 + 2y^4 + y^5 & y + y^3 + 2y^4 + 2y^5 \end{pmatrix} \begin{pmatrix} y^2 & 1 + 2y^2 \\ y + y^2 & 2y + y^2 + y^3 \end{pmatrix}$$

$$MS = \begin{pmatrix} y & y \\ 0 & 1 + y^2 \end{pmatrix}$$

In the above example, the elements are chosen carefully for the key generation and in the encryption process to avoid decryption failure. The following section discusses the bounds for successful decryption.

Proposition 3.8. *Let g be a degree n primitive irreducible polynomial. Then the product of two polynomials $\overline{h_1}, \overline{h_2} \in \frac{\mathbb{Z}_p[y]}{\langle g(y) \rangle}$ will equal to the product of $h_1 h_2$ in the ring $\mathbb{Z}_p[x]$, if the $\deg(h_1) \leq \deg(h_2) < \frac{n}{2}$.*

Proposition 3.9. *Let f and g be two polynomials of degree n in a polynomial ring $\mathbb{Z}[x]$ such that $\|f\|_\infty = 1$ and $\|g\|_\infty = 1$, then $\|fg\|_\infty \leq n + 1$.*

Proof Let B be the subset of $\mathbb{R}[x]$, which consist of all binary polynomial of degree n , defined as follows

$$B = \{f \in R[y] \mid \deg(f) \leq n \text{ and } \|f\|_\infty = 1\}$$

Let $f = 1 + y + \dots + y^n \in B$, then $\|f\|_1 \geq \|g\|_1 \forall g \in B$. Since $ff = 1(1 + \dots + y^n) + \dots + y^n(1 + \dots + y^n)$. Therefore, it implies that $\|ff\|_\infty = n$. Hence $\|gh\|_\infty \leq \|ff\|_\infty = n$, for all $g, h \in B$.

Proposition 3.10. Let $F, H \in \mathcal{D}(\mathcal{R})$, and defined a norm $\|F\|_\infty = \max \|f_{ij}\|_\infty$ then $\|FH\|_\infty \leq k(n+1)$.

Proof. We know that

$$FH = \begin{pmatrix} f_{11}h_{11} + \dots + f_{1k}h_{1k} & \dots & f_{11}h_{k1} + \dots + f_{1k}h_{kk} \\ \vdots & \ddots & \vdots \\ f_{k1}h_{11} + \dots + f_{kk}h_{k1} & \dots & f_{k1}h_{k1} + \dots + f_{kk}h_{kk} \end{pmatrix}$$

Where f_{ij} and h_{ij} ($1 \leq i \leq k$ and $1 \leq j \leq k$) represents the polynomials of the matrix F and H respectively. Given that $F, H \in \mathcal{D}(\mathcal{R})$, accordingly $\|f_{ij}\|_\infty = 1 = \|h_{ij}\|_\infty$. Implies that $\|f_{ij}h_{ij}\|_\infty \leq n+1$. From Proposition 3.9, we get

$$\|\sum f_{ij}h_{ij}\|_\infty \leq \sum \|f_{ij}h_{ij}\|_\infty \leq k(n+1).$$

Proposition 3.11. If the NRTU $(N, p, q, f(x), g(x))$ is chosen to satisfy the following condition

$$p > 6k(n+1)^2 \text{ and } q > p(n+1)$$

Then the decrypted matrix $M\alpha_p(A)$ computed by Bob equal to the original plain text P' .

Proof. The preliminary calculation of the decryption process is;

$$M^{-1}C = M^{-1}(MNI_pR + P')$$

$$A = NI_pR + M^{-1}P'.$$

Since the matrix, I_p is the center element and $N, R \in \mathcal{D}(\mathcal{R})$. Implies that $\|N\|_\infty = \|R\|_\infty = 1$

So, by Proposition 3.9. $\|NR\|_\infty \leq k(n+1)$. And we know that $\|P\|_\infty < \frac{p}{2}$. Thus, $\|M^{-1}P\|_\infty < k\frac{p}{2}(n+1)$, which implies that

$$\|NR + M^{-1}P\|_\infty < k(n+1) + k\frac{p}{2}(n+1) \leq p.$$

Thus, our assumption assures that the degree of each polynomial (a_{ij}) in A is less n with the magnitude of the largest coefficient less than p . Thus, by Proposition 3.11 whenever Bob computes A in a field \mathbb{F}_{q^n} , then lift it into \mathbb{F}_{p^n} , she will recover the exact matrix P' .

3.5 Mathematical Background

It can be seen, that the coefficients of the polynomial entries of the public key matrix are randomly distributed over modulo q . However, there is also a hidden relation between the polynomials of the matrix M and the public key matrix PK that is

$$N \equiv M \times PK \text{ mod } q \quad (3.28)$$

As we know that the coefficient of the polynomials of the matrix M and the matrix N are small. Thus, breaking the proposed scheme by the problem of finding the secret key is reduced to solve the following problem.

Key Recovery problem. *Given that the public key polynomial PK , find matrices M and N of polynomials having all binary coefficients, which satisfying.*

$$N \equiv M \times PK \text{ in } \mathcal{M}^2\left(\frac{\mathbb{Z}_{11}[y]}{\langle g(y) \rangle}\right)$$

$$n_{ij} \equiv \sum_{x=1}^k m_{xj} pk_{ix} \text{ in } \frac{\mathbb{Z}_{11}[y]}{\langle g(y) \rangle} \text{ for all } n_{ij}$$

The solution to the key recovery problem of the suggested scheme is not unique, same as not unique for NTRU over a polynomial ring. If the pair (M, N) is the one solution of the key recovery problem, then the pairs $(y^u M, y^u N)$ are also the solution, for all positive integer u less than $\frac{n}{4}$. The polynomials $y^u m_{ij}$ of the matrix $y^u M$ cyclically rotate the coefficient of the polynomial m_{ij} . Therefore, the decryption with such matrices rotates the polynomial of the ciphertext.

3.5.1 Brute Force Attack

A first essential requirement for the well-organized cryptosystem is that the decryption process of the scheme is not practically solvable by collision search or Brute force attack. The private key used for the suggested NTRU is the set of all matrices whose polynomials coefficients are either 0 or 1. So the attacker will take the roundabout $\# \mathcal{B}(\mathcal{R}) = 2 \times (2^n)^{k \times k}$ tries to find the pair of the private key (M, N) . For instance, we consider $n = 10$ and $k = 4$ then the attackers expect to check 2×2^{160} .

3.5.2 Asymptotic Complexity

The question arises as that: How fast the suggested NTRU cryptosystem is? In the encryption and decryption procedure, the most consuming part is the product of matrices and the product of polynomials. Since the asymptotic complexity of the $k \times k$ square matrix multiplication is $\mathcal{O}(k^3)$, the entries of the matrix are polynomials and the product of two-degree n

polynomials usually require n^2 multiplication. Therefore, the encryption and decryption procedure of the proposed scheme requires $\mathcal{O}(k^3n^2)$ step. For $k = n$ the complexity is equal to $\mathcal{O}(n^5)$ which is the polynomial-time not better than the complexity of the NTRU scheme over a polynomial ring.

Chapter 4

Security Enhancement of Data Encryption Standard

4.1 Introduction

Data encryption standard (DES) is a symmetric key cryptosystem that is designed by international business Machines (IBM). It was adopted and published by the US National Institute of Standard Technology (NIST) in 1971, as a federal information processing scheme. The aim was to provide a secure cryptosystem for the security of sensitive data and information during transmission. This algorithm became a distinguished and broadly used algorithm [35]. In the same way, a considerable number of cryptanalytic papers on DES were published since its acceptance in 1971. In 1977, Diffe and Hellman suggested a parallel machine for the comprehensive search of the complete keyspace [36]. The author claimed was, that very-large-scale integration (VLSI) chips are constructed, each chip is used to search one key per microsecond. The construction of the search machine contains millions of such chips, all working in parallel and each chip is capable to search 1012 keys per second. There are 7×10^{16} number of keys in the set of keyspace of the DES, that can be approximately searched in 10^5 seconds, which is almost 24 hours. The estimated price of this machine was \$20 million. Therefore, the monetary value per solution was \$5k. In 1980 Hellman demonstrated a time-memory tradeoff technique for the chosen plaintext attack [37]. The time memory tradeoff method takes vu words of memory and u^2 operations. The vu^2 operations are equivalent to the total number of all possible keys of DES. This technique is the same as the Differential Cryptanalysis attack on the cryptosystems that are the same as DES, which carries about 2^{38} operations, required 2^{38} memory and 256 pre-processing times for a special case $m = t$. The author suggested a special machine that produced about a hundred solutions with an average time of 24 hours. The approximate cost of that machine was \$4 million so the monetary value per solution was in the range between \$1 – \$100. The processing time for the same machine was estimated and it was claimed that it required two years or three years. In 1985 Evertse and Chaum depicted that the meet-in-the-middle attack is capable to decrease the computation of key search of DES [38]. The reduction factors are $2^{19}, 2^9, 2^2$ for the reduced number of rounds 4, 5, and 6 respectively. They also claimed that a somewhat altered form of DES, for instance, the algorithm which consists of recursive seven rounds can be cracked through the reduction factor of 2. Besides, they showed that a

meet-in-the-middle attack of the same kind is not appropriate for eight or more round reduced DES. In 1987 Devias presented a new kind of attack on DES called the known-plaintext attack [39]. They assumed that sufficient data might produce sixteen linear relationships amid the key bits. Accordingly, it decreases the computation of the key search up to 2^{40} . The correlation among the outputs of the adjacent S-boxes was the main target of the plaintext attack. Since the correlation can disclose the linear relationship between the four bits of the key that are utilized for these S-boxes as input bits. Moreover, the consequence of the splits 32-bit of DES receives these outputs independently. Thus, each pair of the adjacent S-boxes can be exploited twofold, yielding 16 bits of key information. In 1991 Eli Biham and Adil Shamir designed the differential attacks which can apply to various DES-like substitution permutation cryptosystems [40]. This was a powerful attack, which used just the pairs of ciphertexts and was capable to break the DES in a few minutes. According to [40], any modification in the algorithm, for instance, key scheduling of the algorithm, altering the permutation step by any other permutation, or the change the order of the eight S-boxes cannot make the algorithm less successful against the differential attack. A complete review of these attacks shows that the main targets of these cryptanalyses are the substitution phase, which is the only nonlinear part of the algorithm. Since the S-boxes used in the algorithm were not cryptographically strong and thus the DES proved to be insecure against differential attacks.

Keeping the above facts in view, this chapter proposed a novel 6×6 cryptographically strong S-boxes. The proposed S-boxes are then deployed in the Feistel function F of the DES to achieve the aim of substitution transformation, which is the necessary step for the confusion criterion. The cryptographic characteristics of the new S-box are analyzed over different analyses such as Differential approximation probability (DP), linear approximation probability (LP), Nonlinearity, strict avalanche criterion (SAC), and bit independent criterion (BIC). The results of the new S-boxes show that the proposed S-boxes are bijective, highly nonlinear, and low costly than AES 8-bit S-box to implement and are identical in the term of linear, differential and other algebraic properties. Hence, the essential criterion for a substitution step of the DES algorithm is successfully achieved. The major contribution of this chapter is to fortify the DES algorithm against brute force, linear and differential attacks.

4.2 Preliminaries

We denote by \mathbb{Z}_p^n a direct product of n copies of the field \mathbb{Z}_p , where p is a positive prime integer. The p -ary function of rang in \mathbb{Z}_2 is denoted by f throughout in this chapter namely

Boolean functions, which is defined as $f: \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$. However, the function $F: \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m$ is called the vectorial Boolean function.

Definition 4.1. Let $f: \mathbb{Z}_p^n \rightarrow \mathbb{Z}_2$ be a Boolean function. The nonlinearity of a function f can be defined as the smallest Hamming distance amid the set of all affine Boolean functions and the function f . The nonlinearity of the function f is denoted by N_f and its mathematical form can be written as;

$$N_f = \min \{d(h, a): a \in A \} \quad (4.1)$$

In the above equation $d(h, a)$ refer to the Hamming distance within h and a and A signifies the set of affine Boolean functions. Consequently, the maximum probable N_f value of a function f is equal to $2^{n-1} - 2^{\frac{n}{2}-1}$.

Definition 4.2. Followed by [41], a function $F: \mathbb{Z}_p^m \rightarrow \mathbb{Z}_p^n$ is said to exhibit the avalanche effect if and only if the function F satisfies the following.

$$\sum_{y \in \mathbb{Z}_p^m} wt(F(y) \oplus F(X \oplus C_i^m)) = n \cdot 2^{m-1}. \quad (4.2)$$

For all i ($1 \leq i \leq m$) the equation 4.2, implies that the average of one-half of the output bits must be changed whenever one bit is complemented by the input data.

Definition 4.3. Followed by [41], let $F: \mathbb{Z}_p^m \rightarrow \mathbb{Z}_p^n$ be a function then the set $\partial(x, y)$ that is defined as follows;

$$\partial(x, y) = |\{x | F(z + x) - F(z) = y\}|. \quad (4.3)$$

The positive integer Δ_F is called differential Δ_F -uniform. The mathematical representation of Δ_F is defined as:

$$\Delta_F = \max_{\substack{x \in \mathbb{Z}_p^m, x \neq 0 \\ y \in \mathbb{Z}_p^n}} \partial(x, y). \quad (4.4)$$

4.3 General Outline of DES

DES is a symmetric key encryption scheme, which is designed to encrypt a 64-bits block of data. Thus, the input size of the algorithm is 64-bits and the output size is also 64-bits. The length of the key is 56-bits and the key is mostly expressed as the block of 64-bits. The 56-bits are used as a key and the remaining eight least significant bits are utilized for the parity check purpose. DES is consisting of two modules that are the product cipher and the Feistel

cipher. The product cipher is used to combine two or more transformations because the combinations of the ciphers are more secure than the separated ciphers. A Feistel cipher is the iterated cipher that consists of the sequential repetition of the round function. The formal definition of the Feistel function is given as follows.

Definition 4.4. (Feistel function). A Feistel function is an iterated cipher that maps plaintext of size $n = 2m$. We denote the left t -bits block and right t -bits block for the plaintext by \mathcal{L}_0 and \mathcal{R}_0 respectively. Assume that the Feistel function consists of r rounds and the output of the r_{th} round is the ciphertext, thus we denote the ciphertext by $(\mathcal{L}_r, \mathcal{R}_r)$. The Feistel function for the i_{th} round (for $1 \leq i \leq r$) is defined as follows;

$$(\mathcal{L}_{i-1}, \mathcal{R}_{i-1}) \mapsto (\mathcal{L}_i, \mathcal{R}_i) \quad (4.5)$$

$$(\mathcal{L}_i, \mathcal{R}_i) = \begin{cases} \mathcal{L}_i = \mathcal{R}_{i-1} \\ \mathcal{R}_i = \mathcal{L}_{i-1} \oplus f(\mathcal{R}_{i-1}, \mathcal{K}_i) \end{cases} \quad (4.6)$$

Where \mathcal{K}_i is the subkey derived through the key schedule algorithm. In DES the number of rounds $r = 16$ and the subkeys \mathcal{K}_i size is 48-bits.

The Feistel function is bijective and thus reversible. So, the same key uses for the encryption and decryption procedure. The Xor is used in the function to combine the output of the round function with the left half using the following equation.

$$\mathcal{L}_{i-1} \oplus f(\mathcal{R}_{i-1}, \mathcal{K}_i) \oplus f(\mathcal{R}_{i-1}, \mathcal{K}_i) = \mathcal{L}_{i-1} \quad (4.7)$$

The equation 4.7 and Fig. 1. demonstrate that the DES algorithm is independent of the design of the function f . The invertibility of f function does not produce an impact on the invertibility of the DES algorithm. Accordingly, if the function f is invertible or not, though the Feistel function is always invertible.

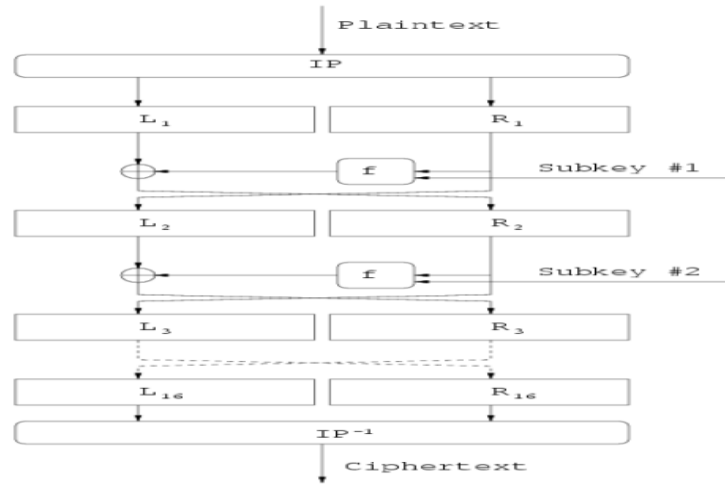


Figure 1. The Feistel function structure of DES

4.4 Construction of Galois fields $GF(2^6)$ and S-boxes

It is already discussed in chapter 1, that \mathbb{Z}_p is a prime field of order p . A polynomial $p(y) \in \mathbb{Z}_p[y]$ that cannot factor in the product of polynomials of the ring $\mathbb{Z}_p[y]$ is called an irreducible polynomial. Let $p(y)$ be an irreducible polynomial in $\mathbb{Z}_p[y]$, and the ring $\mathbb{Z}_p[y]$ is the principal ideal domain by Theorem 1.14. Therefore, the ideal generated by $p(y)$ is a maximal ideal in $\mathbb{Z}_p[y]$, which is denoted by $\langle p(y) \rangle$ and defined as;

$$\langle p(y) \rangle = \{a(y) : a(y) = p(y) \cdot h(y), \text{ for some } h(y) \in \mathbb{Z}_p[y]\}. \quad (4.8)$$

Thus, the quotient ring $\frac{\mathbb{Z}_p[y]}{\langle p(y) \rangle}$ is a finite field of the order p^n , which is known as Galois field $GF(p^n)$, where n is the degree of the polynomial $p(y)$. The field $\frac{\mathbb{Z}_p[y]}{\langle p(y) \rangle}$ consists of all polynomials having a degree strictly less than n . The subtraction and addition operation performs over the field \mathbb{Z}_p , that are the same operations as performed in $\mathbb{Z}_p[y]$. However, the product of the polynomials performs over modulo $p(y)$. A polynomial $f(y) \in \frac{\mathbb{Z}_p[y]}{\langle p(y) \rangle}$ is said to be the multiplicative inverse of the non-zero polynomial $g \in \frac{\mathbb{Z}_p[y]}{\langle p(y) \rangle}$, if and only if $f(y)g(y) \equiv 1 \pmod{p(y)}$.

4.4.1 Construction of Galois fields

The main interest of this study is the Galois fields $GF(2^6)$ of order 2^6 . To construct Galois field $GF(2^6)$, initially choose a degree 6 primitive irreducible polynomial $p(y)$ in $\mathbb{Z}_2[y]$, and then find the root β of the polynomial $p(y)$ i.e., $p(\beta) = 0$. Subsequently, generate the multiplicative cyclic group $GF(2^6) - \{0\}$ from the root β by computing all β^i for $1 \leq i \leq 2^6 - 1$. Hence each nonzero element of the field $GF(2^6)$ can be expressed as a power of the primitive element β . We consider the set $\{p_i(y) \in \mathbb{Z}_2[y] : p_i(y) \text{ is irreducible and } 1 \leq i \leq 6\}$

of six primitive irreducible polynomials of degree 6, to construct corresponding the Galois Fields $\frac{\mathbb{Z}_2[y]}{\langle p_i(y) \rangle}$, $1 \leq i \leq 6$. Next, these Galois fields are utilized to construct 6×6 S-boxes.

The primitive irreducible polynomials of degree 6 and their corresponding Galois fields are listed in Tab. 3.

Table 3. List of degree 6 primitive irreducible polynomials over \mathbb{Z}_2

Primitive Polynomials	$GF(2^6)$	Primitive Polynomials	$GF(2^6)$
$p_1(y) = y^6 + y + 1; \beta_1$	$\frac{\mathbb{Z}_2[y]}{\langle p_1(y) \rangle}$	$p_4(y) = y^6 + y^5 + 1; \beta_4$	$\frac{\mathbb{Z}_2[y]}{\langle p_4(y) \rangle}$
$p_2(x) = y^6 + y^4 + y^3 + y + 1; \beta_2$	$\frac{\mathbb{Z}_2[y]}{\langle p_2(y) \rangle}$	$p_5(x) = y^6 + y^5 + y^3 + y^2 + 1; \beta_5$	$\frac{\mathbb{Z}_2[y]}{\langle p_5(y) \rangle}$
$p_3(x) = y^6 + y^5 + y^2 + y + 1; \beta_3$	$\frac{\mathbb{Z}_2[y]}{\langle p_3(y) \rangle}$	$p_6(x) = y^6 + y^5 + y^4 + y + 1; \beta_6$	$\frac{\mathbb{Z}_2[y]}{\langle p_6(y) \rangle}$

4.4.2 Construction of 6×6 S-boxes

The construction of the S-box required a nonlinear bijective map. In the proposed work, we use the multiplicative inverse function module degree 6 primitive irreducible polynomial $p_i(y)$ as a power permutation for the construction of S-boxes. The mapping is defined as follows:

$$g_i: \frac{\mathbb{Z}_2[y]}{\langle p_i(y) \rangle} \rightarrow \frac{\mathbb{Z}_2[y]}{\langle p_i(y) \rangle}$$

$$g_i(w) = \begin{cases} w^{-1} & \text{if } w \neq 0 \\ 0 & \text{if } w = 0 \end{cases} \quad (4.9)$$

The images $g_i(w)$ for all $0 \leq w \leq 63$ are then converted into an 8×8 lookup table, which is the required S-box. Thus, for each degree 6 primitive irreducible $p_i(w)$ for $1 \leq i \leq 6$ one can obtain a different S-box that is denoted by S_i . Tab. 4 (a-f) depicted the generated S-boxes corresponding to different primitive irreducible polynomials and Galois field $\frac{\mathbb{Z}_2[y]}{\langle p_i(y) \rangle}$. Section 4.5 analyzed the Proposed S-boxes with well-known analyses such as nonlinearity, BIC, SAC, LP, and DP to examine the quality of the S-boxes.

Table 4. Proposed S-boxes

4 (a) Proposed S-box 1 S_1								4 (b) Proposed S-box 2 S_2							
0	1	33	62	49	43	31	44	0	1	45	54	59	18	27	30
61	54	51	39	26	35	14	24	48	10	9	49	32	62	15	14
63	2	27	21	56	9	50	19	24	51	5	58	41	56	53	35
42	4	38	18	10	29	17	60	16	50	31	6	42	38	7	26
57	37	52	28	46	40	22	25	12	63	52	23	47	61	29	43
23	15	20	34	11	53	45	6	57	20	28	39	55	2	60	36
13	47	48	5	7	30	12	41	8	11	25	17	34	22	3	44
36	8	59	58	55	16	3	32	21	40	19	4	46	37	13	33
4 (c) Proposed S-box 3 S_3								4(d) Proposed S-box 4 S_4							
0	1	51	34	42	30	17	56	0	1	48	32	24	63	16	45
21	53	15	29	59	55	28	10	12	27	47	37	8	26	38	21
57	6	41	27	52	8	61	48	6	44	61	28	39	15	34	41
46	33	40	19	14	11	5	43	4	62	13	9	19	60	58	50
47	25	3	50	39	63	62	36	3	49	22	40	46	11	14	20
26	18	4	31	45	44	24	32	35	23	55	53	17	7	36	10
23	60	35	2	20	9	58	13	2	33	31	59	54	43	52	42
7	16	54	12	49	22	38	37	57	56	30	51	29	18	25	5
4 (e) Proposed S-box 5 S_5								4 (f) Proposed S-box 6 S_6							
0	1	54	36	27	28	18	20	0	1	57	46	37	26	23	33
59	12	14	46	9	58	10	47	43	31	13	51	50	10	41	39
43	62	6	21	7	19	23	22	44	29	54	35	63	60	32	6
50	48	29	4	5	26	33	34	25	24	5	36	45	17	42	9
35	30	31	32	3	55	60	45	22	7	55	19	27	4	40	15
53	57	63	16	61	39	11	15	38	14	30	8	16	28	3	56
25	51	24	49	56	40	2	37	53	58	12	11	59	48	18	34

Theorem. 4.5. ([42]) Let l be an affine transformation and g be the power permutation with good cryptographic properties in the Galois field $GF(2^m)$, then the APA composition is defined as follows:

$$S(x) = l \circ g \circ l \quad (4.10)$$

The equation (4.10) preserves the cryptographic properties of g and takes on stronger algebraic complexity.

Remark. 4.6. A composition function of an affine function with a function g from the right-hand side or the left-hand side preserved the properties of linearity and differential uniformity of the function g .

4.5 Performance Analyses

An efficient cryptosystem should be secure against all kinds of attacks. Since the security of the block ciphers depends on the choice of the S-box, therefore this section thoroughly analyzes the performance of the proposed 6×6 S-boxes to figure out the best S-box. The good quality S-box in these S-boxes is then deployed in the proposed modified DES. Besides, we will also compare the obtained results with the super AES 8-bits S-box.

4.5.1 Nonlinearity

In section 4.2, the definition of the nonlinearity for the Boolean function has been already discussed. The general formula to calculate the upper bound of the nonlinearity of the function $f: \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2$ is $2^{m-1} - 2^{\frac{m}{2}-1}$ [43]. Therefore, the maximum possible nonlinearity for $m = 6$ is $N_{max} = 28$. The nonlinearity of all S-boxes is calculated, the obtained results are listed in Tab. 5 (a-f). It can be seen that overall, the average nonlinearity analyses of all S-boxes are quite good and capable to resist linear attacks. Moreover, from the tables, one can observe that the average nonlinearity of the S-box S_1 is equal to S_2 . Similarly, the average nonlinearity value of S_3 is equal to S_4 and the S_5 average nonlinearity value is the same as S_6 . Therefore, the pair of S-boxes that are consist of S_5 and S_6 are the best S-boxes with respect to nonlinearity analysis.

Table 5. The nonlinearity of the proposed S-boxes

5 (a). The nonlinearity of the S-box S_1							5 (b). The nonlinearity of the S-box S_2						
Function	f_0	f_1	f_2	f_3	f_4	f_5	Function	f_0	f_1	f_2	f_3	f_4	f_5
Nonlinearity	24	22	16	24	20	20	Nonlinearity	22	22	22	22	22	20

5 (c). The Nonlinearity of the S-box S_3							5 (d). The Nonlinearity of the S-box S_4						
Function	f_0	f_1	f_2	f_3	f_4	f_5	Function	f_0	f_1	f_2	f_3	f_4	f_5
Nonlinearity	20	24	22	20	22	22	Nonlinearity	22	24	22	22	22	20

5 (e). The Nonlinearity of the S-box S_5							5 (f). The Nonlinearity of the S-box S_6						
Function	f_0	f_1	f_2	f_3	f_4	f_5	Function	f_0	f_1	f_2	f_3	f_4	f_5
Nonlinearity	24	22	22	22	24	20	Nonlinearity	24	20	22	22	24	22

4.5.2 Differential Cryptanalysis

Differential approximation probability (DP) analysis is applied to evaluates the differential uniformness of the S-box. The minimum possible value of differential uniformity for the $m \times n$ S-box is $\delta(S) = 2^{m-n+1}$ [44]. Thus, for the 6-bit S-box in which $m = n = 6$ the $\delta_{min} = 2$. The S-box having minimum differential uniformity is known as almost perfect Nonlinear [43]. We have calculated the differential distribution matrix $\Lambda(S)$ of all the

generated S-boxes, which are shown in Tab. 6 (a-f). As can be seen in the tables that the differential distribution table of all 6-bit S-boxes are consist of 4, 6, and 8 except the element λ_{63} and the distribution table for the S-box S_5 also contain 10. Therefore, the differential approximation probability is 0.1250 for the S-boxes S_1, \dots, S_4 and S_6 , however the differential probability of the S-box S_5 is 0.1563. Overall, the differential approximation values of all S-boxes are approximately equal to the DP value of the AES S-box, nowadays considered as a super S-box. Accordingly, the modified DES S-boxes have enough strength against the differential cryptanalysis attack.

Table 6 DP Analysis of the Proposed S-boxes

6 (a) DP table of S_1	6 (b) DP table of S_2	6 (c) DP table of S_3
6 6 8 4 4 6 6 4	6 4 6 6 6 4 4 4	6 4 6 6 6 4 4 4
4 6 4 6 6 4 6 4	6 6 4 8 8 6 4 6	6 6 8 6 6 4 4 4
4 6 4 6 6 4 6 6	6 6 8 6 6 4 6 6	4 4 6 4 4 4 6 6
6 6 4 6 4 6 6 6	6 6 4 4 6 4 6 8	8 6 4 4 6 4 8 6
6 6 6 8 4 4 6 4	6 4 6 6 4 4 4 6	4 6 4 4 8 6 4 8
4 4 4 4 4 8 4 4	8 4 6 4 6 6 6 4	6 8 4 4 6 6 6 6
8 8 6 6 6 6 8 6	4 6 4 6 6 4 4 8	6 6 4 4 4 4 6 4
6 4 4 8 4 4 6 0	4 6 4 6 8 6 6 0	4 6 6 6 6 6 6 0
6 (d) DP table of S_4	6 (e) DP table of S_5	6 (f) DP table of S_6
4 6 6 8 6 4 6 6	6 6 6 4 4 6 4 6	6 6 6 6 6 6 6 6
4 8 6 6 4 6 6 4	6 4 4 4 8 4 6 6	4 6 8 6 6 6 4 6
6 8 6 4 6 4 6 4	4 6 4 4 4 4 6 6	8 4 4 6 4 4 4 8
8 4 6 4 4 6 6 8	4 4 4 4 6 6 6 6	4 4 6 6 6 4 6 4
6 6 8 6 4 8 4 4	4 4 8 4 6 4 8 6	6 4 6 4 6 6 6 4
8 4 8 4 6 6 8 6	4 6 6 6 6 4 6 4	6 6 6 6 6 4 6 6
6 8 6 6 6 4 6 8	4 4 6 4 4 4 8 4	4 6 4 4 4 4 6 4
6 8 4 8 6 6 6 0	4 1 4 4 4 6 6 0	8 6 6 8 6 6 4 0

4.5.3 Strict Avalanche Criterion

In general, an S-box is considered a lookup table of Boolean functions from \mathbb{Z}_2^m to \mathbb{Z}_2^n for $m \geq n$ (see [45]). Feistel has suggested an important criterion for the designation of cryptographic function. A Boolean function $f: \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^n$ is said to be exhibit the avalanche effect if the following equation hold.

$$\sum_{u \in \mathbb{Z}_2^m} wt(f(u) \oplus f(u \oplus c_i^n)) = n2^{m-1}. \quad (4.11)$$

For all i ($1 \leq i \leq m$), where c_i^n is a vector consist of all zeroes except at the i_{th} position. Accordingly, this definition means, that a Boolean function is said to fulfill the avalanche criterion if and only if the average half of the output bits change, whenever one changes a single bit in the input bits. This implies that if a single input bit changes, then the output bits

will change with 0.5 probability. According to Adams and Tavares, the function of Hamming weight 2^{m-1} for all output, m -bits leads the S-box with the good avalanche. Because every vector f_j complement the input bit x_b according to alteration in the location from the position f_{j_i} and f_{j_k} , for some positive integer j and k . If the vector f_j contains an equal number of ones and zeroes, then for all possible inputs with complementing the bit x_b yields the function y_i to be inverted 50%. Therefore, for all f_1, f_2, \dots, f_n with the property of hamming weight 2^{m-1} inverts average half bits in y_1, y_2, \dots, y_n by inverting a bit x_b of the input bits. Since all the Boolean functions of the proposed S-boxes are complete, therefore the proposed S-boxes successfully satisfy SAC with an average probability approximately equal to 0.5 as can be seen in Tab. 7(a-g).

Table 7. SAC Analysis of proposed S-boxes

7 (a) SAC Analysis of S-box S_1				7 (b) SAC Analysis of S-box S_2			
Result	Minimum	Maximum	Average	Result	Minimum	Maximum	Average
SAC	0.3750	0.6250	0.5069	SAC	0.4063	0.5938	0.5130

7 (c) SAC Analysis of S-box S_3				7 (d) SAC Analysis of S-box S_4			
Result	Minimum	Maximum	Average	Result	Minimum	Maximum	Average
SAC	0.437500	0.4965277	0.49652	SAC	0.37500	0.4904	0.49045

7 (e) SAC Analysis of S-box S_4				7 (f) SAC Analysis of S-box S_5			
Result	Minimum	Maximum	Average	Result	Minimum	Maximum	Average
SAC	0.43750	0.49998	0.49913	SAC	0.40625	0.49499	0.49479

4.5.4 Linear approximation probability

In a linear approximation probability, the study of the greatest imbalance of the system is carried out. The input and output L_i and L_o o, respectively. L_o equal output bits ordered in the same way as the equal input bits with mask L_i define LP. From a mathematical perspective, it may be stated as follows:

$$LP = \max_{L_i, L_o \neq 0} \left| \frac{\#\{i \in Z \mid i.L_i = S(i).L_o\}}{2^n} - \frac{1}{2} \right| \quad (4.12)$$

Where the order of the set of the input value is 2^n . In Table 8 (a-f), the values of maximum linear approximation probability of the S-boxes S_2 , S_3 and S_4 are the same, their value is equal to 0.187500. Similarly, the result of the linear approximation of the S-box S_5 and S_6 are same that is equal to 0.2187500. The result of S_1 is equal to 0.25000 as shown in the tables. Since the

probability results of all S-box are near zero therefore all S-boxes are secure against linear cryptanalysis.

8 (a). LP Analysis of S-box S_1				8 (b). LP Analysis of S-box S_2			
Result	Minimum	Maximum	Average	Result	Minimum	Maximum	Average
SAC	0	0.25000	0.04765	SAC	0	0.187500	0.04908
8 (c). LP Analysis of S-box S_3				8 (d). LP Analysis of S-box S_4			
Result	Minimum	Maximum	Average	Result	Minimum	Maximum	Average
SAC	0	0.187500	0.04960	SAC	0	0.187500	0.04895
8 (e). LP Analysis of S-box S_5				8 (f). LP Analysis of S-box S_6			
Result	Minimum	Maximum	Average	Result	Minimum	Maximum	Average
SAC	0	0.218750	0.04882	SAC	0	0.218750	0.04895

The performance analyses demonstrate that the results of all analyses of the proposed S-boxes are quite better. According to Theorem 4.5, the APA transformations preserve the cryptographic properties of the S-box, so we used the APA transformation to increase the number of good quality S-boxes and robust their algebraic complexity. In the next section, we deployed the APA transformation in the Feistel network to enhance the security of the DES algorithm.

4.6 Modified DES Algorithm

DES is a sixteen-round cryptosystem, each of its rounds is the combination of bits permutation, expansion of bits, substitution step, and XOR operation. The practice of the bit permutation step is to rearrange the order of the data aims to produce diffusion in the ciphered data. The usage of exclusive XOR operation is used to mix the round key with the plain data. The S-box is used to produce confusion in the ciphered data. In these operations the S-box is the only nonlinear component, thus modification in any other operation of the algorithm would not make them less successful. In this study, we modified the DES algorithm by fitting a good quality 6-bits S-box in the F -function and keep the other operation unchanged. The modified DES attains the following obligatory principles.

- i. Large Key Space, against the brute force attack.
- ii. Highly nonlinear output functions; the maximum distance from the linear functions.
- iii. Successfully resist the linear and differential cryptanalysis.

- iv. High nonlinearity is attained; degrees of the output bit functions are increased.
- v. Efficient construction that can be easily implemented in hardware and software.

4.6.1 Generation of Key dependent 6-bits S- boxes

The key size of the modified DES is increased up to $12n+56$ -bits. The first 56-bits of the key are used to derive the sixteen round keys k_i . There is no change in the design procedure of the round keys schedule. The last $12n$ -bits are divided into $2n$ sub-blocks of 6-bits. Afterward, the subblocks are transformed into the decimal forms, which are of course the elements of the Galois field $GF(2^6)$. The obtained elements are then used as parameters of APA transformation. For instance, let a_1, a_2, \dots, a_{2i} be the obtained elements. Then the APA transformation can be written as follows:

$$S(w) = (a_{2i-1}(\dots a_7(a_5(a_3(a_1(w^{-1}) \oplus a_2) \oplus a_4) \oplus a_6) \oplus a_8 \dots)) \oplus a_{2i} \quad (4.13)$$

Where w is the element of the Galois field $GF(2^6)$. Accordingly, for each different combination of $a_i \neq 0$, one can obtain different S-box of the same cryptographic properties and algebraic complexity. The purpose of the APA transformation is: first, it increases the keyspace of the algorithm, increases the algebraic complexity of the S-box, and generates a considerable number of key-dependent S-boxes having the same cryptographic properties. For the decryption, the same key generates the inverse of the S-box using the inverse of the APA transformation S , which is given in the equation (4.13).

4.6.2 Modified DES Feistel Network

The Feistel network was introduced by Horst Feistel. In general, it is a transformation that consists of permutation and substitution, called F function. The F -function is the nonlinear, reversible, and key-dependent mapping, that maps the input string of the data into the output string of the data. The Feistel network has been widely used in many block ciphers such as in DES, GOST [46], FEAL [48], RC5[47], Khufu and Khafre [48], Blowfish [49], and LOKI [50]. In this study, the Feistel network used in the DES is of our specific interest. The Feistel network plays a vital role in the security of DES. The input string of F -function of the round i is the right half output of the round $i - 1$, which is denoted by R_{i-1} . The detailed procedure of the modified F -function as the modified F -function initially uses the E expansion and expands the 32-bit input data into 48-bit blocks. Afterward, the F -function carries out the XORed operation and mixed the 48-bits with the round key K_i . After the xor operation, the scheme divides the 48-bits block into eight 6-bits sub-blocks and substitutes each sub-block by the generated 6×6 S-box. The substitution method is: the first three least significant bits

(LSB) selects the column of the S-box and the most significant bits (LSB) selects the row of the S-box. The output data are then again fed into eight different DES S-boxes. The detailed procedure of the modified Feistel network is demonstrated in Fig. 2.

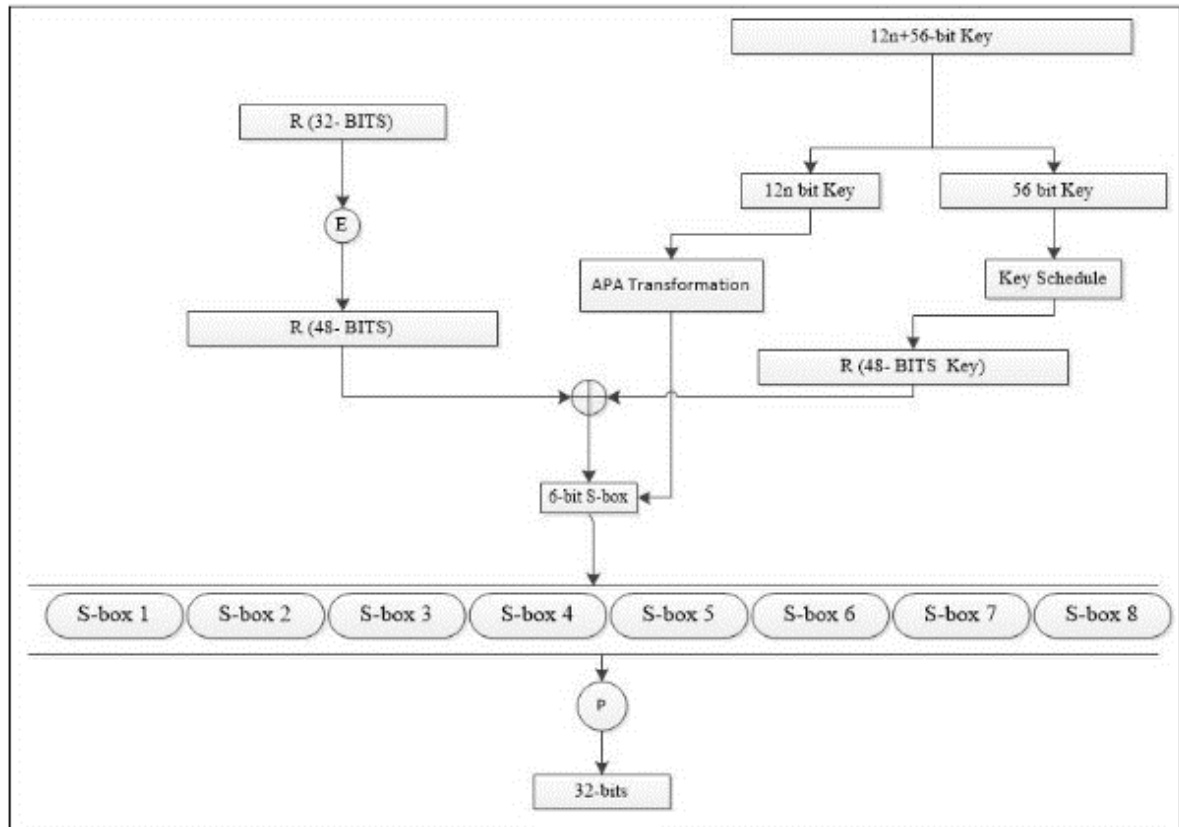


Figure 2. Flow Chart of the Modified F-function

Example 4.6. Let $I = 45$ be the input for the proposed 6×6 S-box. The decimal representation of 45 is 101101_x . From the decimal representation, the MSB of the input I is $101_x = 5$, which indicates the fifth row of the 6×6 S-box, the counts of the rows start from zero 0. Similarly, the decimal representation of the LSB of the input I is again $101_x = 5$ that indicates the fifth column of the S-box S_1 . The counts of the columns also start from zero 0. Thus, if the input I is substitute with the S-box S_1 , which is given in Tab. 1, then the output of the S-box is $S_1(45) = 53$.

4.6.3 Key Compliment

The order of the keyspace of the DES algorithm is equal to 2^{52} . In that key space, half of the keys can be obtained by complimenting bitwise the other half keys. Since the DES cipher holds the following properties.

$$E(P, K) = C \Rightarrow \bar{C} = E(\bar{P}, \bar{K}) \quad (4.14)$$

Therefore, it makes the brute force attack simpler. The attacker has to check half possible keys to break the DES through brute force attack. However, the S-boxes deployed in the modified DES are key-dependent, which does not satisfy the following property.

$$S(P, k) = C \Rightarrow \bar{C} = S(\bar{P}, \bar{k}) \quad (4.14)$$

Implies that

$$ME(P, K) = C \not\Rightarrow \bar{C} = ME(\bar{P}, \bar{K}) \quad (4.15)$$

Where ME denote the modified DES cipher, K denote the Modified DES key, S denote the substitution cipher of the scheme and k signify the subblock of the keys K that is used to generate the S-box S . Since the modified DES scheme does not hold the property given in equation 4.13. Hence, the attackers have to check all the keys in case of a brute force attack. We have examined the claim about the compliment property while using the arbitrary key and the plaintext using both algorithms DES and modified DES ciphers, the outcome is depicted in Tab. 9. From the table, it can be seen that the compliments of the DES cipher are equal to the ciphertext obtained as a result of using the key compliment and the plaintext compliment. However, the compliment of the Modified DES ciphertext is not equal to the ciphertext given in the compliment row. Accordingly, the modified DES algorithm does not satisfy the complement property.

Table 9. Testing Result

Data	Original	Compliment
Key	8, 9, 10, 11, 12, 13, 14, 15	247, 246, 245, 244, 243, 242, 241, 240
Plaintext	50, 54, 12, 43, 23, 54, 53, 55	205, 201, 243, 212, 232, 201, 202, 200
Ciphertext (DES)	126,248,50,203,126,186,50,103	129, 7, 205, 52, 129, 69, 205, 152
Ciphertext (M DES)	133, 34, 22, 27, 234, 98, 194, 62	29, 16, 66, 205, 192, 5, 56, 74

4.6.4 The Brute force attacks

A brute force attack is a classical attack that is used to check all the possible keys until the correct key is found. In this era, symmetric key ciphers with 100-bits key or less are susceptible to brute force attacks. The DES algorithm uses 56-bit keys and therefore, it was proved to be insecure against the brute force attack. The modified DES algorithm uses $12n+56$ -bits. Accordingly, for $n \geq 5$, the algorithm will be able to resist the brute force attack. Since the modified DES algorithm is almost secure against linear and differential attacks, so the algorithm will be secure for $n = 1$, if all the round keys K_i are derived independently or by another complex method.

Chapter 5

A Novel Image Encryption Scheme Based on Finite Algebraic Structure

5.1 Introduction

Nowadays digital image plays an important role in different societal segments. The image data have various applications across the world such as in defense, medical imaging, advertisement, and business, etc. Due to the extensive use of digital images in different fields, the security of digital image data gains considerable attention in the field of cryptography. Therefore, researchers have presented numerous new crypto-algorithms for image encryption in the last few years. Researchers have presented various algorithms based on chaos theory that are specific for the encryption digital images [51 -58]. Subsequently, some of them are proved to be unsecured against different attacks, due to defect in their internal structure [59,60]. Li et al. examined the algorithm presented in [61] and claimed that the encryption schemes based on only pixel position permutations and substitution can be easily broken over the chosen-plaintext attack. Zang et al. explored the security weakness of the image encryption scheme based on the perceptron model given in [59] and concluded that the secret key can be rebuilt easily if just one pair of plaintexts or ciphertext is known. Norouzi et al. [62] devised an image encryption technique utilizing a hyperchaotic system that is used to create diffusion in a single round. Whereas Zong et al. [63] observed error in the Norouzi technique and claimed that this technique is not secure against different attacks such as chosen plaintext. Moreover, the combination of DNA and chaos is used in numerous image encryption algorithms. The scheme that utilized DNA and 3D chaotic system for image encryption schemes are given in [64]. In continuation, they investigated defects in the proposed scheme and found the weakness in the scheme, which manifested the scheme unsecured against the chosen-plaintext attack. Furthermore, Liu et al. examined the internal structure of image cipher based on one round modified permutation-diffusion pattern and confirmed the weakness of the scheme, they reported that the scheme is not capable to resist chosen-plaintext attack. Keeping all these problems in view, this chapter proposed a novel color image encryption technique utilizing permutation network and substitution network based on integer ring module n and 16 Galois fields of 256 elements constituted by 16 distinct degrees 8 primitive irreducible polynomials over the field \mathbb{Z}_2 . For the design of the

cryptosystem first, we picked \mathbb{Z}_n , the ring of integers modulo n , whereas the non-negative integer n depends on the size of an image and carried out row-wise permutation. Along with this, we considered 16 newly constructed Galois fields of 256 elements. After row-wise permutation on the image, we divide it into sixteen blocks and substitute each sub-block with a different S-box. In continuation, we further used the structure of the ring \mathbb{Z}_{256} and multiplicative operation over a 256 elements Galois field \mathbb{F}_{2^8} . Consequently, random sequences are obtained, the substituted image is shuffled using acquired sequences. The strength of the proposed scheme is determined by different renowned cryptographic analyses. The results revealed that the anticipated technique is more secure as equated to the chaotic image encryption presented in literature.

5.2 Preliminaries

Definition 5.2.1. The set of all $n \times n$ invertible matrices having entries from a field \mathbb{F} and satisfy all the group properties under matrix multiplication and is called general linear group, denoted by $GL(n, \mathbb{F})$.

Definition 5.2.2. Let \mathcal{G} be a group and \mathcal{X} be a non-empty set. Then the map $w: \mathcal{G} \times \mathcal{X} \rightarrow \mathcal{X}$ is said to be a group action if for all g, h in \mathcal{G} and x in \mathcal{X} , the following axioms hold;

- i. $w(g, w(h, x)) = w(gh, x)$
- ii. $w(e, x) = x$, where e is the identity element of \mathcal{G}

5.3 The algebraic structures-based Encryption algorithm

This section introduces the proposed algorithm. The proposed scheme is suitable for colour image encryption and is comprised of four rounds. In the first round, the scheme splits the color channels of the RGB plain image. Then permutes row-wise R, G and B channels utilize 2×2 matrix with entries from the unite group $\mathcal{U}(\mathbb{Z}_{\mathcal{M}})$ intersect $\mathcal{U}(\mathbb{Z}_{\mathcal{N}})$, where \mathcal{M} and \mathcal{N} represent the number of rows and columns respectively, in the plain image. This transformation provides three altered channels. For the purpose to attain high nonlinearity in the algorithm, the scheme uses the S-box construction method, which is being discussed in section 3.1, and the set of all degree 8 primitive irreducible polynomials with the coefficient from the field \mathbb{Z}_2 to generate sixteen S-boxes. Furthermore, the scheme splits each shuffled colour component into sixteen subblocks, and substitute each subblock with different S-box and then combine the substituted subblocks. After getting three substituted matrices, the algorithm builds a random matrix of the size $\mathcal{M} \times \mathcal{N}$ utilize the structure of integer ring \mathbb{Z}_{256} and polynomial multiplication module degree 8 irreducible polynomial over a field \mathbb{Z}_2 . Then perform XOR operation bitwise between the randomly generated matrix and each substituted

matrix and one get three twisted matrices. In the final round, we combine the color-modified channels and obtained the ciphered image. The step-by-step procedure of the new encryption scheme is displayed in Fig. 3.

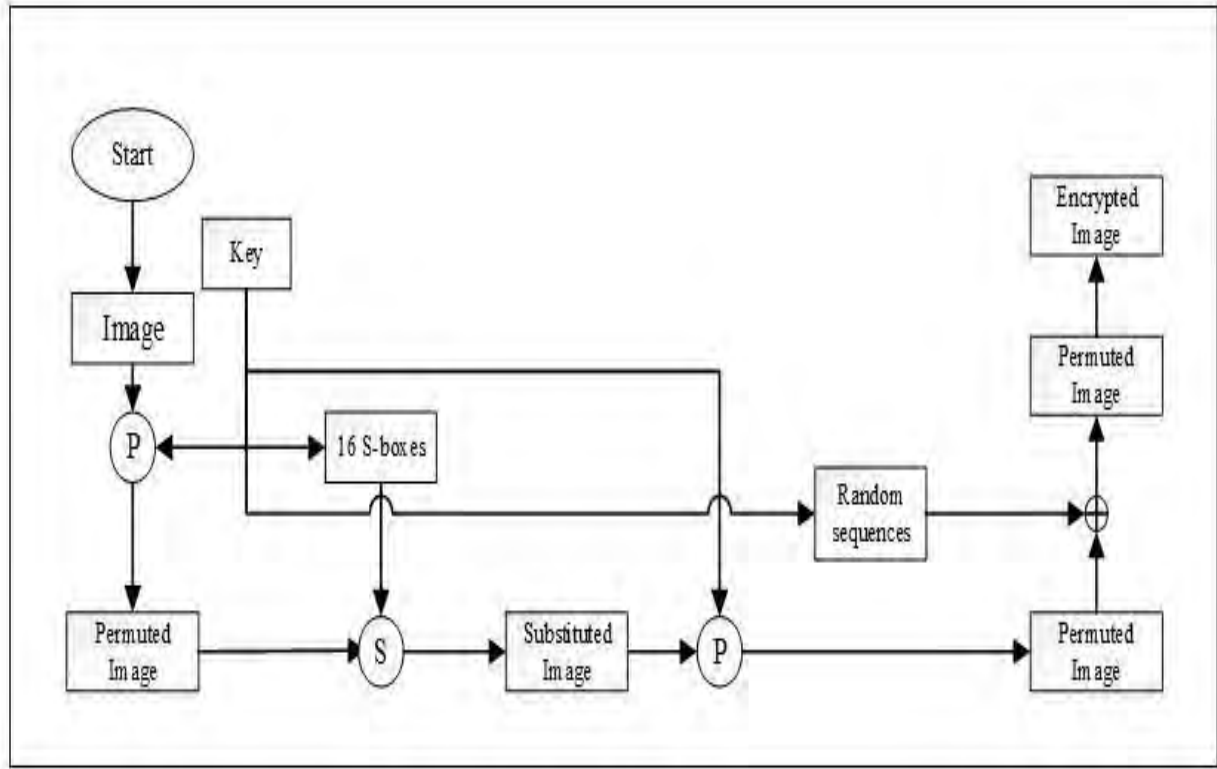


Figure 3. Flow chart of the proposed scheme

5.3.1 S-boxes Construction

The construction of S-box utilized in the proposed approach is based on the action of general linear group $GL(2, \mathbb{F}_{2^8})$ on the finite field \mathbb{F}_{2^8} of order 256.

$$w: GL(2, \mathbb{F}_{2^8}) \times \mathbb{F}_{2^8} \rightarrow \mathbb{F}_{2^8}$$

$$w(\mathcal{M}, \psi) = \mathcal{F}_{\mathcal{M}}(\psi) \quad (5.1)$$

Where $\mathcal{F}_{\mathcal{M}}(\psi) = \frac{\alpha(\psi)+\beta}{\gamma(\psi)+\delta}$ and α, β, γ and δ are the elements of \mathbb{F}_{2^8} . $\mathcal{F}_{\mathcal{M}}$ is a bijective mapping from \mathbb{F}_{2^8} to \mathbb{F}_{2^8} , and the resultant values of $\mathcal{F}_{\mathcal{M}}$ are then converted into a 16×16 lookup table, which is the required S-box.

5.3.2 Encryption process

Step 1. Input color image $I(\mathcal{M}, \mathcal{N}, 3)$ of size $\mathcal{M} \times \mathcal{N}$. Split the image into three Channels Red, Green, and blue. Convert the color channels of the image into three matrices R_Q, G_Q

and B_Q . Subsequently, use the following transformation and change each pixel's position of the image. After alteration, one can get three matrices in the new arrangement $R_{\mathcal{P}}$, $G_{\mathcal{P}}$ and $B_{\mathcal{P}}$.

$$\begin{pmatrix} i' \\ j' \end{pmatrix} = \begin{pmatrix} p_1 & p_2 \\ p_3 & p_4 \end{pmatrix} \times \begin{pmatrix} i \\ j \end{pmatrix} \quad (5.2)$$

$$\begin{pmatrix} i' \\ j' \end{pmatrix} = \begin{pmatrix} p_1 \times i + p_2 \times j \text{ mod } \mathcal{M} \\ p_3 \times i + p_4 \times j \text{ mod } \mathcal{N} \end{pmatrix} \quad \text{if } \begin{matrix} p_1 \times i + p_2 \times j \text{ mod } \mathcal{M} \neq 0 \\ p_3 \times i + p_4 \times j \text{ mod } \mathcal{N} \neq 0 \end{matrix} \quad (5.3)$$

$$\begin{pmatrix} i' \\ j' \end{pmatrix} = \begin{pmatrix} p_1 \times i + p_2 \times j \text{ mode } \mathcal{M} \\ \mathcal{N} \end{pmatrix} \quad \text{if } \begin{matrix} p_1 \times i + p_2 \times j \text{ mod } \mathcal{M} \neq 0 \\ p_3 \times i + p_4 \times j \text{ mod } \mathcal{N} = 0 \end{matrix} \quad (5.4)$$

$$\begin{pmatrix} i' \\ j' \end{pmatrix} = \begin{pmatrix} \mathcal{M} \\ p_1 \times i + p_2 \times j \text{ mode } \mathcal{N} \end{pmatrix} \quad \text{if } \begin{matrix} p_1 \times i + p_2 \times j \text{ mod } \mathcal{M} = 0 \\ p_3 \times i + p_4 \times j \text{ mod } \mathcal{N} \neq 0 \end{matrix} \quad (5.5)$$

$$\begin{pmatrix} i' \\ j' \end{pmatrix} = \begin{pmatrix} \mathcal{M} \\ \mathcal{N} \end{pmatrix} \quad \text{if } \begin{matrix} p_1 \times i + p_2 \times j \text{ mod } \mathcal{M} = 0 \\ p_3 \times i + p_4 \times j \text{ mod } \mathcal{N} = 0 \end{matrix} \quad (5.6)$$

Where p_1, p_2, p_3 and $p_4 \in \mathbb{Z}_{\mathcal{M}} \cup \mathbb{Z}_{\mathcal{N}}$, satisfies the condition $p_1 p_4 - p_2 p_3 \in \mathcal{U}(\mathbb{Z}_{\mathcal{M}}) \cap \mathcal{U}(\mathbb{Z}_{\mathcal{N}})$. In the above equations, the pairs (i, j) represent the position of the pixels in the corresponding matrices R_Q, G_Q and B_Q , and (i'', j'') pair represent the pixel position of each newly permuted matrices $R_{\mathcal{P}}, G_{\mathcal{P}}$ and $B_{\mathcal{P}}$.

Step 2. This step substitutes the obtained permuted matrices using sixteen S-boxes to enhance the randomness in the proposed scheme. For S-boxes generation, the scheme chose the set of all degree 8 primitive irreducible polynomials over the field \mathbb{Z}_2 ;

$$\{\mathcal{h}_j(y) \in \mathbb{Z}_2[y]: \mathcal{h}_j(y) \text{ is irreducible}, 1 \leq j \leq 16\} \quad (5.7)$$

Thus, for each j the quotient ring $\frac{\mathbb{Z}_2[y]}{\langle \mathcal{h}_j(y) \rangle}$ form a field isomorphic to the Galois field $GF(2^8)$.

Accordingly, the nonzero elements of each of these fields form a group known as the Galois cyclic group generated by the primitive element a_i , corresponding to the irreducible polynomial $\mathcal{h}_j(y)$. The list of Galois fields against their primitive irreducible polynomials is given in Tab. 10. For S-boxes construction, it is used the above degree 8 primitive irreducible polynomials and the action of the general linear group over a newly designed finite field that is defined as;

$$w_j: GL\left(2, \frac{\mathbb{Z}_2[y]}{\langle \mathcal{h}_j(y) \rangle}\right) \times \frac{\mathbb{Z}_2[y]}{\langle \mathcal{h}_j(y) \rangle} \rightarrow \frac{\mathbb{Z}_2[y]}{\langle \mathcal{h}_j(y) \rangle};$$

$$w_j(\mathcal{A}, \mathcal{y}) = \mathcal{F}_{j, \mathcal{A}}(\mathcal{y}) \quad (5.8)$$

$$\mathcal{F}_{j, \mathcal{A}}(\mathcal{y}) = \frac{\alpha(\mathcal{y}) + \beta}{\gamma(\mathcal{y}) + \delta} \quad (5.9)$$

Where $\mathcal{A} = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in GF\left(2, \frac{\mathbb{Z}_2[y]}{\langle \hbar_j(y) \rangle}\right)$. For a particular \mathcal{M} and for each $j, 1 \leq j \leq 16$. The mapping $\mathcal{F}_{j, \mathcal{A}}$ generates sixteen S-boxes having diverse algebraic and statistical properties. Moreover, over the cryptographic properties of these S-boxes are closed to the standard S-box of AES and APA S-box, the justification is given [65]. Furthermore, the scheme divides the permuted color components $R_{\mathcal{P}}, G_{\mathcal{P}}$ and $B_{\mathcal{P}}$ into sixteen sub-blocks, and substitute each subblock with a different S-box. At last, after the use of these newly generated sixteen S-boxes, the algorithm combines the substituted sub-blocks and obtained three substituted blocks R_S, G_S and B_S .

Table 10. Primitive irreducible polynomials and their corresponding Galois fields

Irreducible Polynomial $\hbar_i(y)$; Primitive element	Galois Field	Irreducible Polynomial $\hbar_i(y)$ Primitive element	$\frac{\mathbb{Z}_2[y]}{\langle \hbar_i(y) \rangle}$
$\hbar_1(y) = y^8 + y^4 + y^3 + y^2 + 1$	$\frac{\mathbb{Z}_2[y]}{\langle \hbar_1(y) \rangle}$	$\hbar_9(y) = y^8 + y^7 + y^3 + y^2 + 1; a_9$	$\frac{\mathbb{Z}_2[y]}{\langle \hbar_9(y) \rangle}$
$\hbar_2(y) = y^8 + y^5 + y^3 + 1; a_2$	$\frac{\mathbb{Z}_2[y]}{\langle \hbar_2(y) \rangle}$	$\hbar_{10}(y) = y^8 + y^7 + y^5 + y^3 + 1; a_{10}$	$\frac{\mathbb{Z}_2[y]}{\langle \hbar_{10}(y) \rangle}$
$\hbar_3(y) = y^8 + y^5 + y^3 + y^2 + 1; a_3$	$\frac{\mathbb{Z}_2[y]}{\langle \hbar_3(y) \rangle}$	$\hbar_{11}(y) = y^8 + y^7 + y^2 + y + 1; a_{11}$	$\frac{\mathbb{Z}_2[y]}{\langle \hbar_{11}(y) \rangle}$
$\hbar_4(y) = y^8 + y^6 + y^3 + y^2 + 1; a_4$	$\frac{\mathbb{Z}_2[y]}{\langle \hbar_4(y) \rangle}$	$\hbar_{12}(y) = y^8 + y^7 + y^6 + y + 1; a_{12}$	$\frac{\mathbb{Z}_2[y]}{\langle \hbar_{12}(y) \rangle}$
$\hbar_5(y) = y^8 + y^6 + y^4 + y^3 + y^2 + y + 1; a_5$	$\frac{\mathbb{Z}_2[y]}{\langle \hbar_5(y) \rangle}$	$\hbar_{13}(y) = y^8 + y^7 + y^6 + y^5 + y^2 + x + 1; a_{13}$	$\frac{\mathbb{Z}_2[y]}{\langle \hbar_{13}(y) \rangle}$
$\hbar_6(y) = y^8 + y^6 + y^5 + y + 1; a_6$	$\frac{\mathbb{Z}_2[y]}{\langle \hbar_6(y) \rangle}$	$\hbar(y) = y^8 + y^7 + y^6 + y^3 + y^2 + y + 1; a_{14}$	$\frac{\mathbb{Z}_2[y]}{\langle \hbar_{14}(y) \rangle}$
$\hbar_7(y) = y^8 + y^6 + y^5 + y^2 + 1; a_7$	$\frac{\mathbb{Z}_2[y]}{\langle \hbar_7(y) \rangle}$	$\hbar(y) = y^8 + y^7 + y^6 + y^5 + y^4 + y^2 + 1; a_{15}$	$\frac{\mathbb{Z}_2[y]}{\langle \hbar_{15}(y) \rangle}$
$\hbar_8(y) = y^8 + y^6 + y^5 + y^3 + 1; a_8$	$\frac{\mathbb{Z}_2[y]}{\langle \hbar_8(y) \rangle}$	$\hbar_{16}(y) = y^8 + y^6 + y^5 + y^4 + 1; a_{16}$	$\frac{\mathbb{Z}_2[y]}{\langle \hbar_{16}(y) \rangle}$

Step 3. For the pixels, transposition generate a sequence (x_n) from 1 up to $\mathcal{M} \times \mathcal{N}$. Then convert each element of the sequence into the range of 0 – 255 using the following equation:

$$x_n' = \text{mod}(x_n, 256) \quad (5.10)$$

In the next step, the scheme uses the multiplicative operation of a group $\frac{\mathbb{Z}_2[y]}{\langle \hbar_1(y) \rangle} \setminus \{0\}$ and generate a three random sequence from x' with the help of the following equations;

$$x_R = a \times x_n' \text{mod} \hbar_1(y) \quad (5.11)$$

$$x_G = b \times x_n' \text{mod} \hbar_3(y) \quad (5.12)$$

$$x_B = c \times x_n' \text{mod} \hbar_4(y) \quad (5.13)$$

Where a, b and c are the elements of the set $\frac{\mathbb{Z}_2[y]}{\langle \hbar_1(y) \rangle} \setminus \{0,1\}$. After getting matrices x_R, x_G and x_B , permute each matrix by using the following transformation;

$$\begin{pmatrix} m' \\ n' \end{pmatrix} = \begin{pmatrix} z_1 & z_2 \\ z_3 & z_4 \end{pmatrix} \times \begin{pmatrix} m \\ n \end{pmatrix}$$

$$\begin{pmatrix} m' \\ n' \end{pmatrix} = \begin{pmatrix} z_1 \times m + z_2 \times n \text{ mod } \mathcal{M} \\ z_3 \times m + z_4 \times n \text{ mod } \mathcal{N} \end{pmatrix} \text{ if } \begin{matrix} z_1 \times m + z_2 \times n \text{ mod } \mathcal{M} \neq 0 \\ z_3 \times m + z_4 \times n \text{ mod } \mathcal{N} \neq 0 \end{matrix} \quad (5.14)$$

$$\begin{pmatrix} m' \\ n' \end{pmatrix} = \begin{pmatrix} z_1 \times m + z_2 \times n \text{ mod } \mathcal{M} \\ \mathcal{N} \end{pmatrix} \text{ if } \begin{matrix} z_1 \times m + z_2 \times n \text{ mod } \mathcal{M} \neq 0 \\ z_3 \times m + z_4 \times n \text{ mod } \mathcal{N} = 0 \end{matrix} \quad (5.15)$$

$$\begin{pmatrix} m' \\ n' \end{pmatrix} = \begin{pmatrix} \mathcal{M} \\ z_3 \times m + z_4 \times n \text{ mod } \mathcal{N} \end{pmatrix} \text{ if } \begin{matrix} z_1 \times m + z_2 \times n \text{ mod } \mathcal{M} = 0 \\ z_3 \times m + z_4 \times n \text{ mod } \mathcal{N} \neq 0 \end{matrix} \quad (5.16)$$

$$\begin{pmatrix} m' \\ n' \end{pmatrix} = \begin{pmatrix} \mathcal{M} \\ \mathcal{N} \end{pmatrix} \text{ if } \begin{matrix} z_1 \times m + z_2 \times n \text{ mod } \mathcal{M} = 0 \\ z_3 \times m + z_4 \times n \text{ mod } \mathcal{N} = 0 \end{matrix} \quad (5.17)$$

For any z_1, z_2, z_3 and $z_4 \in \mathbb{Z}_{\mathcal{M}} \cup \mathbb{Z}_{\mathcal{N}}$. Where (m, n) represent the coordinates of the x_R, x_G and x_T , and (m', n') pair represents the coordinates of the new matrices x_R', x_G' and x_T' .

Then transpose the substituted blocks using the following formulas:

$$R_{\mathcal{E}} = \text{bitxor}(x_R', R_S) \quad (5.18)$$

$$G_{\mathcal{E}} = \text{bitxor}(x_G', G_S) \quad (5.19)$$

$$B_{\mathcal{E}} = \text{bitxor}(x_T', B_S) \quad (5.20)$$

Then combine $R_{\mathcal{E}}, G_{\mathcal{E}}$ and $B_{\mathcal{E}}$ matrices and recover the encrypted RGB image. The encrypted images with the proposed scheme along with the original images are depicted in Fig. 4.

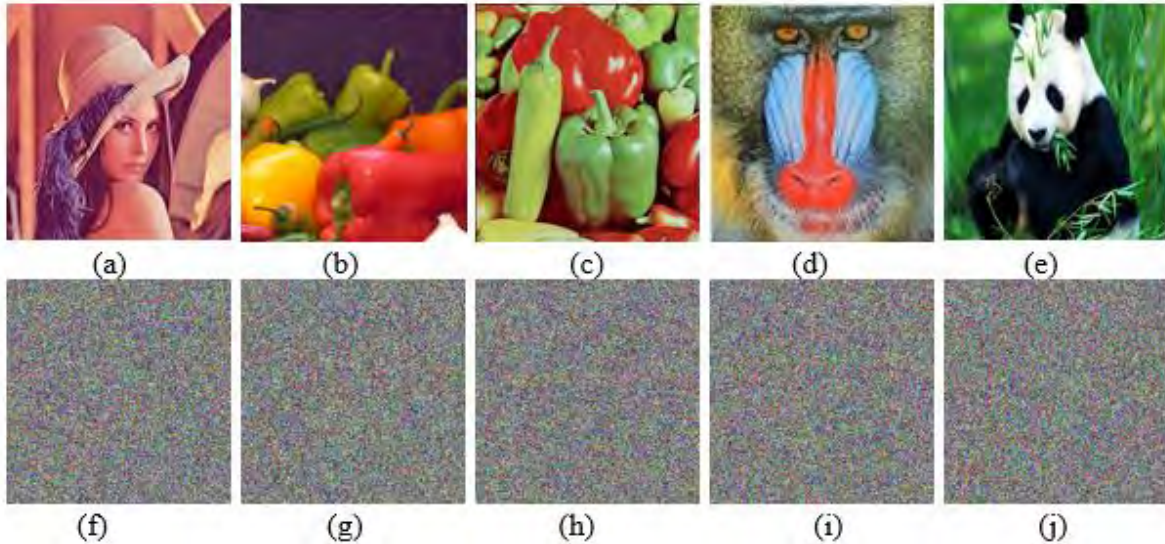


Figure 4. (a-e) shows the original four images; (f-j) represents corresponding encrypted four images

5.3.3 Decryption process

Step 1. The decryption process of the proposed scheme is the same as the encryption process. However, it starts from the last step. For the decryption, first, convert the encrypted image into three matrices $R_{\mathcal{E}}, G_{\mathcal{E}}$ and $B_{\mathcal{E}}$. The first round of the encryption processes is same as the

step 2 of the encryption process which we have already discussed, and get back the matrices R_S , G_S and B_S .

Step 2. In this step, the scheme generates the inverse S-box utilize degree 8 primitive irreducible polynomials given in Tab.10. The inverse sixteen S-boxes are generated using the following inverse map:

$$\mathcal{F}_{j_M}(y) = \delta(y) + \beta/\gamma(y) + \alpha \quad (5.21)$$

Then divide the matrices R_S , G_S and B_S into sixteen sub-blocks, substitute each sub-block with inverse S-box and then combine the sub-blocks and get the matrices R_P , G_P and B_P .

Step 3. The decryption process initially permutes the color components of the encrypted image using the following equations:

$$\begin{aligned} \begin{pmatrix} m' \\ n' \end{pmatrix} &= \begin{pmatrix} d \times p_4 \times m + d \times (-p_2) \times n \text{ mod } \mathcal{M} \\ d \times (-p_3) \times m + d \times p_1 \times n \text{ mod } \mathcal{N} \end{pmatrix} \text{ if } \begin{matrix} d \times p_4 \times m + d \times (-p_2) \times n \text{ mod } \mathcal{M} \neq 0 \\ d \times (-p_3) \times m + d \times p_1 \times n \text{ mod } \mathcal{N} \neq 0 \end{matrix} \\ &= \begin{pmatrix} d \times p_4 \times m + d \times (-p_2) \times n \text{ mod } \mathcal{M} \\ \mathcal{N} \end{pmatrix} \text{ if } \begin{matrix} d \times p_4 \times m + d \times (-p_2) \times n \text{ mod } \mathcal{M} \neq 0 \\ d \times (-p_3) \times m + d \times p_1 \times n \text{ mod } \mathcal{N} = 0 \end{matrix} \end{aligned} \quad (5.22)$$

$$= \begin{pmatrix} \mathcal{M} \\ d \times (-p_3) \times m + d \times p_1 \times n \text{ mod } \mathcal{N} \end{pmatrix} \text{ if } \begin{matrix} d \times p_4 \times m + d \times (-p_2) \times n \text{ mod } \mathcal{M} = 0 \\ d \times (-p_3) \times m + d \times p_1 \times n \text{ mod } \mathcal{N} \neq 0 \end{matrix} \quad (5.23)$$

$$\begin{pmatrix} m' \\ n' \end{pmatrix} = \begin{pmatrix} \mathcal{M} \\ \mathcal{N} \end{pmatrix} \text{ if } \begin{matrix} d \times p_4 \times m + d \times (-p_2) \times n \text{ mod } \mathcal{M} = 0 \\ d \times (-p_3) \times m + d \times p_1 \times n \text{ mod } \mathcal{N} = 0 \end{matrix} \quad (5.24)$$

Where d denote the determinant of a matrix of equation 1, and (m'', n'') pair represent the position of the pixels of matrices R_P , G_P and B_P . After applying the above transformation, the scheme acquires the color components in the original form. In the last step for the recovery of the original image combine the matrices R_Q , G_Q and B_Q and get the original image.

5.4 Security and performance analyses

An efficient cryptosystem should have the capability of resistance against all standard attacks (statistical and differential). In this study, we perform image encryption experiments using JPEG images ‘Lena’, ‘Pepper’ ‘Baboon’, and ‘Deblur’ shown in Fig. 4(a-d). The matrix elements (p_1, p_2, p_3, p_4) were selected (13,3,50,167), the matrix elements for S-boxes generation $(\alpha, \beta, \gamma, \delta)$ were chosen as (121,45,67,145) and the matrix elements for column-wise permutation (q_1, q_2, q_3, q_4) were fixed as (10,7,5,7). The elements a, b, c were chosen to be 128,255 and 100.

5.4.1 Keyspace analysis

The keyspace is the set of all possible keys which are used during the process of encryption and decryption. An efficient cryptosystem should have a large key space to deal with threats like a brute force attack. The keys utilized in the proposed cryptosystem are given below:

- a) The matrix elements are p_1, p_2, p_3 and p_4 .
- b) The elements of the chosen Galois field are α, β, γ and δ .
- c) The elements of a second matrix are considered to be q_1, q_2, q_3 and q_4 .
- d) The integers a, b , and c .

Indeed; (i) each $p_i \in \mathbb{Z}_N, q_i \in \mathbb{Z}_M$ for $1 \leq i \leq 4$, satisfying the extra condition $\text{mod}(p_1 p_4 - p_2 p_3, N) \in \mathcal{U}(\mathbb{Z}_N), (\text{mod}(q_1 q_4 - q_2 q_3, M) \in \mathcal{U}(\mathbb{Z}_M)$, by keeping p_i and q_i fixed. (iii) α, β, γ , and $\delta \in GF(2^8)$ and the parameters a, b , and c denotes the elements of the ring $\mathbb{Z}_{256} \setminus \{0,1\}$. Since, the total number of different α, β, γ and δ which can be used as a part of the secret key is 4.2781×10^{09} , and the total possible numbers of a, b , and c is 16194277, such number of parameters can also be used for the purpose of the secret key. Thus, for a fixed p_i and q_i the keyspace is 6.9281×10^{16} . Therefore, the proposed scheme can resist brute force attacks.

5.4.2 Histogram analysis

Histogram analysis is often used to investigate the cryptosystem's resistance to various forms of attack, including statistical attacks. Since the cryptosystem is expected to manipulate the original data and create unpredictability in the data, it is recommended that it be avoided. For this reason, the well-designed cryptosystem should output data that has values that are highly likely and disparate, since this prevents the encrypted data from providing information that enables the attacker to decipher the data without the secret key. We use histogram analysis to examine the suggested encryption method, and this is shown in Fig. 5. The original Lena image's histogram is initially displayed in the first three figures, while the encrypted image's histogram is shown in the final figures. From the histogram of the original picture, it can be observed that the histogram is entirely random. But although the histogram of the encrypted picture is uniform, it's not correct to say that it is histogram-matched. Under this approach, statistical attack are hard to accomplish, and the evedroppers will be unable to collect information from the encrypted data.

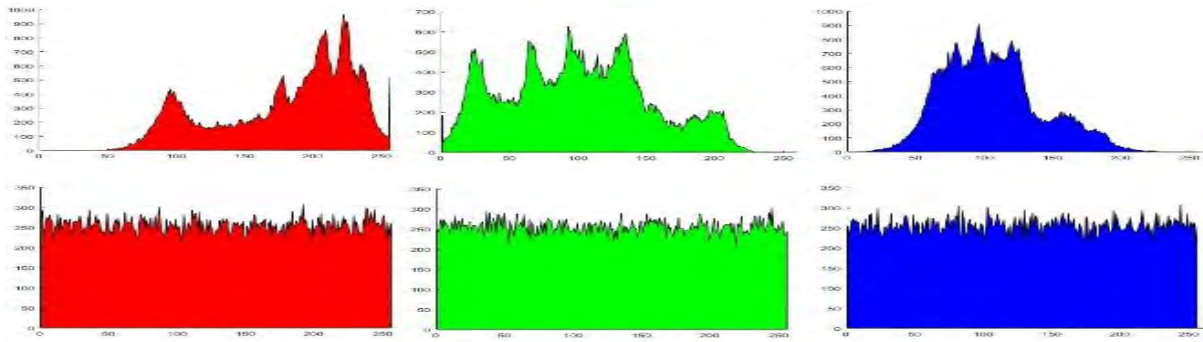


Figure 5 Histogram Analysis of Lena Original and Encrypted Image

5.4.3 Information entropy

In order to determine the uncertainty in the encrypted data, the information entropy analysis is used. When uncertainty increases, so does entropy; when uncertainty reaches its greatest conceivable value, entropy is at its highest point. In layman's terms, the information entropy analysis is shown mathematically as follows.

$$H = - \sum_{k=0}^{\mathcal{L}} \mathcal{P}(k) \log_2 \mathcal{P}(k) \quad (5.25)$$

Where \mathcal{L} indicates the grayscale single component of the image and $\mathcal{P}(k)$ signifies the probability of the appearance of the grey-value k . In this case, the theoretical value H corresponding to the digital image is 8. So, the cryptosystem is considered to be well-secured if the information entropy value of the ciphered image is 8. We inspect the proposed scheme through information entropy analysis; the results are tabulated in Tab.11. From the table, one can noticed, that the information entropy values of the encrypted images that are encrypted via suggested scheme are much closed to 8. The resultant values revealed that the scheme produced optimum uncertainty in the ciphered images, therefore the proposed scheme is capable to defy the entropy attack.

Table 11. Information Entropy Analysis

Images	Original Image			Ciphered Image		
	Red	Green	Blue	Red	Green	Blue
Lena	7.3277	7.6048	7.1326	7.997	7.9972	7.9973
Baboon	7.0359	7.1724	6.4955	7.997	7.9969	7.9972
Peppers	7.3920	7.6150	7.1738	7.997	7.9972	7.9973
Deblur	6.4955	7.1724	6.4955	7.997	7.9969	7.9972
Panda	7.1574	7.6091	7.2604	7.997	7.9973	7.9967

Table 12. Comparing entropy for Lena (256×256) image

Images	Red	Green	Blue	Average	Gray
Proposed	7.9971	7.9972	7.9973	7.9972	7.99722
Ref. [66]	7.9973	7.9969	7.9971	7.9971	-
Ref. [67]	7.9893	7.9896	7.9903	7.9897	-
Ref. [68]	7.9973	7.9972	7.9969	7.99713	-
Ref. [69]	7.9896	7.9893	7.9896	7.98964	-
Ref. [70]	7.9901	7.9912	7.9921	7.91133	-
Ref. [71]	7.9892	7.98987	.9899	7.98963	-
Ref. [72]	-	-	-	-	7.9996
Ref. [73]	-	-	-	-	7.9981
Ref. [74]	-	-	-	-	7.9902
Ref. [75]	-	-	-	-	7.9902
Ref. [76]					7.9904

5.4.4 Correlation Analysis

The correlation coefficient is a statistical test used to examine the strength of the cryptosystem in comparison to various statistical assaults. Data in multimedia is tightly linked. One way to summarise this advice is that well-secured cryptosystems should stop data segment correlation. These studies focus on data segments. The correlation coefficient's mathematical form is:

$$\gamma_{uv} = \frac{cov(p, q)}{\sqrt{\mathcal{D}(p)\mathcal{D}(q)}} \quad (5.26)$$

Where

$$cov(p, q) = \frac{1}{\mathcal{P}} \sum_{i=1}^{\mathcal{P}} p_i - \mathcal{E}(p)(q_i - \mathcal{E}(q)) \quad (5.27)$$

$$\mathcal{D}(p) = \frac{1}{\mathcal{P}} \sum_{i=1}^{\mathcal{P}} (p_i - \mathcal{E}(p))^2 \quad (5.28)$$

And

$$\mathcal{E}(p) = \frac{1}{\mathcal{P}} \sum_{i=1}^{\mathcal{P}} p_i \quad (5.29)$$

In the equation 5.29, p_i denote the selected sample at i_{th} position and q_i denote the corresponding adjacent sample. We use correlation coefficient analysis to evaluate the suggested system. In the majority of cases, several dimensions of data correlation are assessed such as vertical, horizontal, and diagonal. Due to the fact that digital images spread

their data in the form of a matrix, we ran a correlation study in all three dimensions (vertically, horizontally, and diagonally) to identify how our proposal matched with other algorithms. Tab. 13 displays the results. Using the correlation analysis of the original picture, it is determined that the image data pixels are highly linked. Nevertheless, the correlation analysis of the ciphered pictures has a correlation coefficient of nearly zero. Thus, the suggested method interleaves the picture data in a systematic manner. By implementing the suggested system, it is ensured that it is very difficult to launch a statistical assault.

Table 13. Correlation analysis of two adjacent pixels in different directions

Images	Horizontal			Vertical			Diagonal		
	Red	Green	Blue	Red	Green	Blue	Red	Green	Blue
Plain Lena	0.9399	0.938	0.904	0.971	0.974	0.932	0.913	0.914	0.850
Plain Baboon	0.9503	0.919	0.954	0.944	0.901	0.950	0.907	0.850	0.914
Plain Peppers	0.9293	0.966	0.927	0.925	0.963	0.933	0.860	0.942	0.876
Plain Deblur	0.9944	0.991	0.984	0.991	0.987	0.972	0.985	0.980	0.957
Plain Panda	0.9593	0.976	0.912	0.934	0.953	0.976	0.945	0.956	0.845
Cipher Lena	0.0141	0.004	0.002	0.006	0.023	0.006	0.001	0.007	0.009
Cipher Baboon	0.0121	0.007	0.007	0.005	0.001	0.006	0.005	0.002	0.004
Cipher Pepper	0.0054	0.003	0.003	0.005	0.004	0.005	0.003	0.013	0.004
Cipher Deblur	-0.0024	0.007	0.012	0.003	0.009	0.008	0.003	0.001	0.007
Ciphered Panda	-0.015	0.032	0.056	0.037	0.037	0.006	0.006	0.007	0.003

Table 14. Comparing the results of correlation coefficients for Lena (256×256)

Schemes	Horizontal	Vertical	Diagonal	Average
Plain image	0.9603	0.9325	0.9084	0.9337
Proposed	0.0019	-0.0024	0.0012	0.0018
Ref. [66]	-0.0027	0.0033	-0.0035	0.0031
Ref. [77]	0.0072	0.0058	0.0031	0.0054
Ref. [67]	0.0084	0.0004	-0.0015	0.0034
Ref. [78]	0.0373	0.0228	-0.0221	0.0274
Ref. [79]	-0.0001	0.0089	0.0091	0.0060
Ref. [68]	0.0028	0.0018	0.0036	0.0027
Ref. [80]	0.1257	0.0581	0.0504	0.0781

5.4.5 Avalanche effect

There are two criteria's that are commonly used to evaluate the sensitivity of the cryptographic scheme, namely number of pixel change rate (NPCR) and (UACI) unified average changing intensity. Let $J(m, n)$ and $J'(m, n)$ be the pixels of the image J and J' respectively, where (m, n) represent the position of the pixel. Mathematically NPCR and UACI can be calculated using the following formulas.

$$NPCR_{RGB} = \frac{\sum_{m,n} \mathcal{D}(m,n)}{\mathcal{L}} \times 100 \quad (5.30)$$

Where \mathcal{L} denote the total number of pixels and \mathcal{D} is defined as:

$$\mathcal{D}(m, n) = \begin{cases} 1 & \text{if } J(m, n) = J(m, n) \\ 0 & \text{if } J(m, n) \neq J(m, n) \end{cases} \quad (5.31)$$

The UACI analysis can be determined as:

$$UACI_{RGB} = \frac{1}{L} \sum_{m,n} \frac{|J(m,n) - J(m,n)|}{2^{\mathcal{N}-1}} \times 100 \quad (5.32)$$

Where \mathcal{N} represents the total number of bits and $J(m, n)$ denote the pixel values of the image. The values of NPCR and UACI for a well-organized encryption algorithm can be described by the formula given as follows.

$$NPCR = 1 - \frac{1}{2^{m_{R,G,B}}} \times 100 \quad (5.33)$$

and

$$UACI = \frac{1}{2^{m_{R,G,B}}} \left[\frac{\sum_{k=1}^{2^{m_{R,G,B}}-1} k(k+1)}{2^{m_{RGB}-1}} \right] \times 100 \quad (5.34)$$

Where $2^{m_{R,G,B}}$ represent the number of bits in one pixel of the colure component in an RGB image. Since the colure image consists of 24-bit values, therefore the upper predictable values for the NPCR and UACI are 99.72 and 33.4635 respectively. In this study, we have evaluated several images using NPCR and UAC analysis in order to examine the impact of one bit of pixel change in the original image. The average value of NPCR and UACI analyses of the proposed scheme and some of the other schemes presented in the literature is given in Table 15. Results of the Gray image are selected from the literature survey that is based on the chaotic map given in [42]. Table 16 signifies that NPCR and UACI values of the proposed scheme are better as compared to other mentioned schemes. Thus, the suggested technique is sound against differential attack.

Table 15. Differential analyses for the proposed encryption scheme

Images	NPCR			UACI		
	Red	Green	Blue	Red	Green	Blue
Lena	99.6158	99.6531	99.632	33.873	34.165	34.480
Baboon	99.9848	99.6972	99.975	33.944	33.983	34.752
Peppers	99.68931	99.6902	99.545	33.250	34.069	31.356
Deblur	99.68261	99.53613	99.682	35.365	34.775	35.365
Panda	99.675	99.7912	99.663	33.309	32.749	32.149

Table 16. Comparing Differential analyses for 256×256 Lena image

Schemes	NPCR				UACI			
	Red	Green	Blue	Gray	Red	Blue	Green	Gray
Proposed	0.996	0.9965	0.9963	0.9969	33.8734	0.3387	34.165	0.3410
Ref. [66]	0.996	0.9961	0.9961	-	0.3356	0.3345	0.3349	-
Ref. [67]	0.996	0.9960	0.9960	-	0.3346	0.3350	0.3347	-
Ref. [81]	0.996	0.9960	0.9960	-	0.3336	0.3343	0.3337	-
Ref. [82]	0.996	0.9960	0.9960	-	0.3360	0.3330	0.3340	-
Ref. [83]	0.996	0.9959	0.9959	-	0.3344	0.3346	0.3347	-
Ref. [84]	0.996	0.9954	0.9967	-	0.3312	0.3400	0.3390	-
Ref. [72]	-	-	-	0.9962	-	-	-	0.3340
Ref. [73]	-	-	-	0.9962	-	-	-	0.3319
Ref. [74]	-	-	-	0.9961	-	-	-	0.3346
Ref. [75]	-	-	-	0.9963	-	-	-	0.33
Ref. [76]	-	-	-	0.0015	-	-	-	0.0005

5.4.6 Mean Square Error (MSE)

The mean square error analysis evaluates the square error between the ciphered image and the original image in [67]. To estimate the cumulative squared dissimilarity between the plain and encrypted images, the following mathematical formula is used:

$$MSE = \frac{1}{M \times N} \sum_{\zeta_2=1}^M \sum_{\zeta_1=1}^N [I(\zeta_1, \zeta_2) - C(\zeta_1, \zeta_2)]^2. \quad (5.35)$$

Where $I(\zeta_1, \zeta_2)$ denote the pixel values of original the image and $C(\zeta_1, \zeta_2)$ denote the pixel values of the encrypted version. The dimension of the is denoted by M and N. A higher value for MSE can be realized that the scheme produced more error in ciphered and thus suitable for encryption.

5.4.7 Peak Signal-to-Noise Ratio (PSNR)

Corrupting noise can affect the fidelity of a signal representation. Peak signal-to-noise ratio, shortly PSNR is the ratio between the power of a signal and the power of corrupting noise [67]. Symbolically, it is stated in terms of the logarithmic decibel scale due to the wide dynamic range of signals. In this study, the PSNR analysis is used to evaluate the features for the renewal of the encrypted image. In our study, the signal is the plain image and its alteration to the encrypted version is induced through the encryption process. The mathematical representation of the PSNR is given as follows;

$$PSNR = 10 \log_{10} \frac{MAX_I^2}{\sqrt{MSE}} \quad (5.36)$$

In general, the greater value of PSNR designates the high quality of the image. However, in this case, the low value of the PSNR indicates the quality of the encryption scheme.

5.4.8 Normalized Cross Correlation (NK)

The similarity between any two images is determined in terms of correlation function [66]. Normalized Cross-Correlation determines the resemblance between two images. Mathematically, it can be express as:

$$NK = \frac{\sum_{\zeta_2=1}^M \sum_{\zeta_1=1}^N (I(\zeta_1, \zeta_2) \times C(\zeta_1, \zeta_2))}{\sum_{\zeta_2=1}^M \sum_{\zeta_1=1}^N [I(\zeta_1, \zeta_2)]^2} \quad (5.37)$$

Where $I(\zeta_1, \zeta_2)$ denote the pixel value of the original image and $C(\zeta_1, \zeta_2)$ denote the pixel value of the encrypted version and M, N is the dimensions of the image.

5.4.9 Average Difference (AD)

The average difference analysis quantifies the average of the dissimilarity between the mentioned signal and the experiment image. The mathematical form is given as follows:

$$A = \frac{1}{M \times N} \sum_{\zeta_2=1}^M \sum_{\zeta_1=1}^N [I(\zeta_1, \zeta_2) - C(\zeta_1, \zeta_2)] \quad (5.38)$$

Where $I(\zeta_1, \zeta_2)$ denote the pixel value of the original image and $C(\zeta_1, \zeta_2)$ denote the pixel value of the encrypted version and M, N is the dimensions of the images.

5.4.10 Structural Content (SC)

The structural content analysis is used to ascertain the resemblance between two images following [67]. The mathematical form of SC is given in the following equation.

$$SC = \frac{\sum_{\zeta_2=1}^M \sum_{\zeta_1=1}^N [I(\xi_1, \xi_2)]^2}{\sum_{\zeta_2=1}^M \sum_{\zeta_1=1}^N [C(\xi_1, \xi_2)]^2} \quad (5.39)$$

Where $I(\xi_1, \xi_2)$ and $C(\xi_1, \xi_2)$ denotes the pixel value of the original and encrypted image respectively and M, N is the dimensions of the images.

5.4.11 Maximum Difference (MD)

The Maximum Difference demonstrates the maximum value of the error signal and the dissimilarity between the processed and the reference image. Mathematically representation of MD is given as follows:

$$MD = \text{Max } |I(i, j) - C(i, j)| \quad (5.40)$$

The higher the value of the maximum difference indicates the poorer the quality of the image.

5.4.12 Normalized Absolute Error (NAE)

The Normalized absolute error valuates the error between the plain and ciphered image is signal and test image. Mathematically it can be written as;

$$NAE = \frac{\sum_{\zeta_2=1}^M \sum_{\zeta_1=1}^N |I(\zeta_1, \zeta_2) - C(\zeta_1, \zeta_2)|}{\sum_{\zeta_2=1}^M \sum_{\zeta_1=1}^N |I(\zeta_1, \zeta_2)|} \quad (5.39)$$

Where $I(\zeta_1, \zeta_2)$ indicate the pixel of the original image $C(\zeta_1, \zeta_2)$ denote the values of the pixel of encrypted version and M, N is the dimensions of the images.

5.4.13 Root Mean Square Error (RMSE)

It is the square root of the average of the square of all the errors [24]. The mathematical formula for RMSE is:

$$RMSE = \sqrt{\frac{1}{M \times N} \sum_{\zeta_2=1}^M \sum_{\zeta_1=1}^N [I(\zeta_1, \zeta_2) - C(\zeta_1, \zeta_2)]^2} \quad (5.40)$$

Where $I(\zeta_1, \zeta_2)$ represent the pixel value of the original image, $C(\zeta_1, \zeta_2)$ represent the pixel encrypted version and M, N is the dimensions of the images.

5.4.14 Universal Quality Index (UQI)

The Universal quality index disrupts the association between plain and inaccurate images into three contrasts: luminance, contrast, and structural comparisons. UQI for the two images such as X and Y can be defined as:

$$UQI(I, C) = \frac{4\mu_I \mu_C \mu_{IC}}{(\mu_I^2 - \mu_C^2)(\sigma_I^2 - \sigma_C^2)} \quad (5.41)$$

Here μ_I and μ_C represents the mean values of the original and the distorted image, and σ_I, σ_C denote the standard deviation of original and distorted images.

5.4.15 Mutual Information (MI)

The possible information that can attain from the encrypted image and the plain image is known as mutual information. The mutual information of two images I and C can be defined as:

$$MI(I, C) = \sum_{y \in C} \sum_{y \in I} p(\zeta_1, \zeta_2) \log_2 \frac{p(\zeta_1, \zeta_2)}{p(\zeta_1)p(\zeta_2)} \quad (5.42)$$

Where $p(\zeta_1, \zeta_2)$ is the joint probability function of I and C, and $p(\zeta_1)$ and $p(\zeta_2)$ are the marginal probability distribution functions of the plain image I and ciphered image C respectively.

5.4.16 Structural Similarity (SSIM)

This SSIM method is used for evaluating the resemblance between the plain and the ciphered image. The SSIM index estimates on several windows of the image. The measure between two windows X and Y of communal size $M \times N$ is given as follows;

$$SSIM(X, Y) = \frac{(2\mu_X\mu_Y + c_1)(2\sigma_X\sigma_Y + c_2)}{(\mu_X^2 + \mu_Y^2 + c_1)(\sigma_X^2 + \sigma_Y^2 + c_2)}, \quad (4.43)$$

Where μ_X the average of X is, μ_Y is the average of Y , σ_X^2 is the variance of X , σ_Y^2 is the variance of Y , σ_{XY} is the covariance of X and Y , $c_1 = (k_1L)^2$ and $c_2 = (k_2L)^2$ are the variables to stabilize the division with the weak denominator, L is the dynamic range of the pixel values, $k_1 = 0.01$ and $k_2 = 0.03$ by default.

Table 17. Image Quality Measures for proposed Encryption scheme for 256×256 Lena image

No.	Quality Measures	Encrypted image			Optimal		
		Red	Green	Blue	Red	Green	Blue
1	MSE	10703.9	8986.7	7088.35	10057.2	9898.89	6948.19
2	PSNR	7.8354	8.5948	9.62535	8.1060	8.1749	9.7120
3	NCC	0.656818	1.00524	1.09181	0.6725	1.0031	1.0923
4	AD	53.2098	-28.2829	-21.7086	50.0448	-31.4276	-19.7989
5	SC	1.61449	0.578004	0.569411	1.5787	0.5582	0.5711
6	MD	255	222	223	236	210	210
7	NAE	0.467477	0.785734	0.664011	0.4537	0.8310	0.6628
8	RMSE	103.459	94.7982	84.1923	100.286	99.4932	83.3558
9	UQI	0.0004362	0.001013	0.002474	-0.0050	-0.0077	0.0107
10	MI	0.475304	0.613626	0.411744	5.6534	7.2283	6.0723
11	SSIM	0.0106053	0.01004	0.024049	0.0078	0.0053	0.0187

5.4.17 Randomness test for cipher

The security of a cryptosystem has a few properties such as a uniform distribution, high intricacy, and productivity [85,86]. To test that either the proposed scheme achieves these properties, we used NIST SP 800-22 randomness test. A portion of these tests comprises various analyses. The twisted Lena 24-bit digital image is used to complete all NIST tests. The ciphered data is a color image of Lena of size 256×256 . The upshots of the tests can seem in Tab. 18. By breaking down these outcomes, it can be derived from our anticipated digital image encryption tool efficiently passes the NIST tests. Thus, in light of the accomplished outcomes, the produced random ciphers in our encryption algorithm can be declared that are very asymmetrical in their output.

Table 18. NIST test results for 256×256 Lena encrypted image

<i>Test</i>		<i>P – values for color encryptions of encrypted images</i>		
		Red	Green	Blue
Frequency		1	0.062077	0.24198
Rank		0.29191	0.29191	0.29191
Block frequency		0.98143	0.30734	0.37514
Runs (M=10,000)		0.65797	0.23228	0.048694
Long runs of ones		0.7127	0.7127	0.7127
Overlapping templates		0.81567	0.85988	0.85988
No overlapping templates		0.14679	1	0.11048
Spectral DFT		0.14679	0.56166	0.88464
Approximate entropy		0.27672	0.33157	0.49669
Universal		0.98969	0.99097	0.99944
Serial	<i>p values 1</i>	0.10865	0.064743	0.0043523
Serial	<i>p values 2</i>	0.016347	0.99345	0.40361
Cumulative sums forward		0.2424	0.049371	0.19173
Cumulative sums reverse		1.0152	0.096214	1.8054
Random excursions	$X = -4$	0.027889	0.34124	0.30154
	$X = -3$	0.0059538	0.22504	0.72093
	$X = -2$	0.068559	0.78272	0.50225
	$X = -1$	0.33621	0.97465	0.58878
	$X = 1$	0.54926	0.88097	0.45178
	$X = 2$	0.036168	0.83031	0.69603
	$X = 3$	0.084829	0.96993	0.25125
	$X = 4$	0.083847	0.41986	0.64007
	$X = -9$	0.58165	0.56949	0.39647
Random variants	$X = -8$	0.38837	0.54483	0.36668
	$X = -7$	0.57825	0.55431	0.31931
	$X = -6$	0.90379	0.65273	0.19001
	$X = -5$	0.91133	0.66982	0.19657
	$X = -4$	1	0.51915	0.28438
	$X = -3$	0.654	0.70292	0.42371
	$X = -2$	0.72845	0.80554	0.43203
	$X = -1$	0.94673	0.52243	0.13057
	$X = 1$	0.31623	0.39377	0.39509
	$X = 2$	0.17697	0.084838	0.82726
	$X = 3$	0.10662	0.18193	0.83266
	$X = 4$	0.13623	0.51915	0.74789
	$X = 5$	0.16733	0.28642	0.85011
	$X = 6$	0.10272	0.36814	0.88672
	$X = 7$	0.08152	0.72275	0.93733
	$X = 8$	0.09769	0.50888	0.92226
$X = 9$	0.10865	0.50145	0.92696	

Finite Fields Applications v Digital Audio Security

6.1 Introduction

In literature, numerous encryption methods for the security of multimedia data have been introduced. For instance, the encryption algorithm for a digital image hinges on chaotic systems, and the finite algebra of Galois fields is given in [87-92]. Since the audio files contain massive data capacity and somehow different from the other multimedia data. So, for the protection of digital audio data, one should design a cryptosystem that can be easily adapted to deal with all types of audio formats. In this connection, various encryption algorithms are found in the literature for audio data. De Martin and Servetti [93] proposed an encryption algorithm for the encryption of telephonic speech relying on the perceptron method. The author recommended two different techniques that are used to encrypt partial speech. The first scheme was envisioned to have a high bit rate and low-security capability. But the cryptanalysis could easily recover the original data from the ciphered speech. However, the second scheme can encrypt more bitstream with enough security to ciphered audio. Thorwirth et al. presented an algorithm in [94] that consists of a selective encryption technique of perceptual audio coding with standard compression. In the suggested scheme the main focus of the author is on the examination of the encryption process of the encoded MP3 files. Subsequently, Servetti et al. [95] proposed MP3 audio, which is the selective partial encryption algorithm. The presented algorithm has low time complexity. Besides, the scheme misinforms the quality of the original audio sequences, however, it preserves the contents of the audio information and perceptual information. Next, in 2004, Bhargava et al. [96] proposed four fast encryption algorithms for MPEG video, where a single key is used, which randomly changes the sign bits of the Discrete Cosine Transform (DCT) coefficients or the sign bits of motion vectors. Grange et al. [97] introduced a new framework that relies on randomized arithmetic coding for the security of multimedia data. In the recommended framework the security purpose of multimedia data is achieved by producing some randomness in the arithmetic coding process. In 2008, Yan et al. [98] introduced a progressive multimedia data security scheme by scrambling the audio data in a compressed domain. In the proposed scheme the secrete MP3 audio was twisted via a shared secrete key before transmission. However, Au and Zhou in [99], showed that the Yan scheme is conquerable against key search attacks. In [100], Neto and Lima presented an encryption

scheme for digital audio rely on cosine number transform. The suggested encryption procedure recursively applies to a block of uncompressed audio data and uses simple overlapping to select the block and produce diffusion in the encrypted data.

This chapter presents a novel lossless audio data encryption scheme based on arithmetic operations of an elliptic curve over a finite field \mathbb{Z}_p and binary Galois field $GF(2^n)$. Since the arithmetic operations of the elliptic curve are performed efficiently, therefor in the first stage of the encryption process the proposed scheme uses a special type of curve based on the elliptic curve operations and generates a good quality sequence of random numbers. The generated sequences are subsequently used to defuse the matrix of the audio data. The confusion module of the scheme executes through multiple substitution boxes, which have higher nonlinearity. The experimental results demonstrate the efficiency of the proposed scheme against various attacks.

6.2 Preliminaries

6.2.1 Elliptic Curve

An elliptic curve over a finite field \mathbb{F}_p is a plot, which is obtained from the solution of the equation $E: y^2 = x^3 + ax + b \pmod{p}$, where $a, b \in \mathbb{F}_p$ that satisfy the equation $(4a^3 + 27b^2) \not\equiv 0 \pmod{p}$. All these points (solutions) with point of infinity (neutral element) O form an abelian group, which is denoted by $E(\mathbb{F}_p)$ over elliptic curve arithmetic operation that is defined in the following subsection.

6.2.2 Elliptic curve arithmetic

Let $P_1 = (u_1, v_1)$ and $P_2 = (u_2, v_2)$ be any two points lie on the graph of the elliptic curve. The operation defines as $P_1 + P_2 = (u_3, v_3)$.

- i. If $P_1 \neq P_2$ with $u_1 \neq u_2$, then

$$(u_3, v_3) = (\lambda^2 - u_1 - u_2 \pmod{p}, \lambda(u_1 - u_2) - v_1 \pmod{p}) \quad (6.1)$$

and

$$\lambda = \frac{v_2 - v_1}{u_2 - u_1} \pmod{p}. \quad (6.2)$$

- ii. If $P_1 \neq P_2$ with $u_1 = u_2$ but $v_1 \neq v_2$, then $P_1 + P_2 = O$.
 iii. If $P_1 = P_2$ with $v_1 \neq 0$, then

$$(u_3, v_3) = (\lambda^2 - u_1 - u_2 \pmod{p}, \lambda(u_1 - u_3) - v_1 \pmod{p}) \quad (6.3)$$

and

$$\lambda = \frac{3u_1^2 + a}{2v_1} \pmod{p}. \quad (6.4)$$

iv. If $P_1 = P_2$ with $v_1 = 0$, then $P_1 + P_2 = O$.

v. Furthermore, define

$$P + O = P. \text{ for all } P \text{ on } E \quad (6.5)$$

On the above footprints, one can easily show that $E(\mathbb{F}_p)$ is an abelian group with an identity element O .

6.2.3 Singular Point

Let (u, v) be a point on affine curve $f(x, y) = 0$ over the field K . Then the point (u, v) is said to be a singular point of the curve $f(x, y) = 0$ if both partial derivatives $\frac{\partial f}{\partial u}$ and $\frac{\partial f}{\partial v}$ vanish at (u, v) .

The following theorem is from [101].

Theorem 6.1. Let $E^{ns}(\mathbb{F}_p)$ be the set of non-singular points on $E_{\gamma, a}^p$ with $\gamma^2 = a$ for some $\gamma \in \mathbb{F}_p$ against a curve $E_a^p: y^2 = x^3 + ax$ over a finite field \mathbb{F}_p , with $0 \neq a \in \mathbb{F}_p$. Then the homomorphism

$$\varphi_\gamma: E^{ns}(\mathbb{F}_p) \rightarrow \mathbb{F}_p^*$$

Defined as

$$\varphi_\gamma(u, v) = \frac{v+\gamma u}{v-\gamma u}; \text{ and } \varphi_\gamma(O) = 1 \quad (6.6)$$

is an isomorphism.

Proposition. 6.2. Let p be a prime and $GF(p^n), GF(p^m)$ and $GF(p^y)$ be the Galois fields for positive integers m, n , and y . If $y = n + m$ then there exist a bijective from $GF(p^y)$ to $GF(p^m) \times GF(p^n)$.

Proof. Given that $GF(p^n), GF(p^m)$ and $GF(p^y)$ are Galois field and p is a prime number. Given that m, n and y positive integers such that $y = m + n$. Let α be the map from the field $GF(p^y)$ to $GF(p^n) \times GF(p^m)$ given as follows;

$$\alpha: GF(p^y) \rightarrow GF(p^n) \times GF(p^m)$$

Defined by

$$\alpha\left(\sum_{i=0}^{y-1} a_i y^i\right) = \left(\sum_{i=0}^{n-1} a_i y^i, \sum_{i=n}^{y-1} a_i y^{i-n}\right). \quad (6.7)$$

To show that α is well defined, let $f(y) = g(y)$ implies that $g_i = f_i$ for all $1 \leq i \leq m - 1$.

Thus

$$\left(\sum_{i=0}^{n-1} f_i y^i, \sum_{i=n}^{y-1} f_i y^{i-n}\right) = \left(\sum_{i=0}^{n-1} g_i y^i, \sum_{i=n}^{y-1} g_i y^{i-n}\right) \quad (6.8)$$

Since $f(y)$ and $g(y)$ are the elements of the Galois field $GF(p^y)$. Therefore, for all $f(y), g(y) \in GF(p^y)$ if $f(y) = g(y)$ implies $\alpha(f(y)) = \alpha(g(y))$, so the function α is well defined. To show that the function α is one-one, let

$$\alpha(f(y)) = \alpha(g(y)) \quad (6.9)$$

$$\left(\sum_{i=0}^{y-1} f_i y^i, \sum_{i=n}^{y-1} f_i y^{i-n} \right) = \left(\sum_{i=0}^{y-1} g_i y^i, \sum_{i=n}^{y-1} g_i y^{i-n} \right) \quad (6.10)$$

Implies that that $g_i = f_i$ for all $1 \leq i \leq m - 1$. Thus $\sum_{i=0}^{y-1} f_i y^i = \sum_{i=0}^{y-1} g_i y^i$, so the function α is a one-one function. To show that the function α is onto, let $\left(\sum_{i=0}^{n-1} f_i y^i, \sum_{i=n}^{y-1} f_i y^{i-n} \right) \in GF(p^n) \times GF(p^m)$ their exist $\sum_{i=0}^{y-1} f_i y^i \in GF(p^n)$ such that $\alpha\left(\sum_{i=0}^{y-1} f_i y^i\right) = \left(\sum_{i=0}^{n-1} f_i y^i, \sum_{i=n}^{y-1} f_i y^{i-n} \right)$. Hence the α function is onto. Since the function α is well-defined one and onto function thus α is a bijective map from $GF(p^y)$ to $GF(p^n) \times GF(p^m)$.

6.3 Audio Encryption Scheme

The audio technology is used to store, manipulate, reproduce and generate the sound using the arrays of the audio signals encoded in digital format. Digital audio can be referred to as the sample of discrete sequences, which are completely dependent on audio wave format. The digital audio data virtually consists of discrete sockets, which indicate the amplitude of the wave of the digital data. This study manipulates the discrete sockets of the digital audio, aims to encrypt the original content of the audio. The proposed encryption scheme is designed to protect the uncompressed digital audio integer 16 (int16) format. We denote the matrix set of the original audio by A of dimension $M \times N$ for $N \in \{1, 2\}$. The next subsection discusses the step-by-step procedure of the encryption scheme in detail.

6.3.1 Proposed Random number generator

The generation of random numbers plays a significant role in various multimedia data security applications. The elliptic curve is also widely used for the generation of random numbers. In general, the elliptic curve-based random number generation procedure utilizes group law and the arithmetic operation of the elliptic curve. This section presents an efficient scheme for the generation of random numbers based on the elliptic curve operation. The proposed scheme generates distinct random numbers with enough long periods. Initially, the encryption procedure generates a sequence of distinct pseudo-random numbers with a long period greater than the length of the audio data. To generate a random sequence, select a large prime p . Then generate the curve $E_a^p: y^2 = x^3 + ax \pmod p$ through brute force technique. Then use the following map to transmute points of the curve $E_a^p(u, v)$ into the field F_p .

$$\varphi_\gamma: E_a^p \rightarrow \mathbb{F}_p$$

Defined by

$$\varphi_\gamma(u, v) = \frac{v+\gamma u}{v-\gamma u} \quad (6.11)$$

Where $\gamma \in \mathbb{F}_p^*$ is the squared element such that $\gamma^2 = a$ and (u, v) is the element of the curve E_a^p . The map φ_γ is the isomorphism between E_a^p and \mathbb{F}_p by Theorem 2.2.1. The range of the map φ_γ generate a sequence of random numbers in the field \mathbb{F}_p . Afterward, use the obtained sequence of random numbers to shuffle the matrix A and get a new data set A_s . In this study, we fixed the elements $a = 2$ and $p = 99991$ to generate a sequence of random numbers by using the above procedure. Then we analyzed the generated sequence by the NIST test, the results are tabulated in Tab. 22.

6.3.2 Multiple S-boxes Construction Scheme

The S-box plays a significant role in symmetric key cryptography. In general, S-box is used in the substitution module of the cryptosystem and produces confusion in the cipher data. Therefore, the confusion-creating capability of the cryptosystem depends on the quality of the S-box. Since audio contains a large amount of data. So, the proposed cryptosystem is managed to use multiple S-boxes for better random enhancement in the encrypted data. To construct multiple S-boxes, this subsection introduces a novel S-box construction scheme based on Galois field $GF(2^n)$. The traditional S-box construction schemes are based on the finite field of order 256. However, the proposed construction scheme for multiple S-boxes generations is based on the Galois field of order greater than 256. Here, the general idea of the construction scheme is discussed. Initially, define a bijective map from the Galois field $GF(2^n)$ onto $GF(2^n)$. The mapping is defined as follows.

$$\begin{aligned} S: GF(2^n) &\rightarrow GF(2^n) \\ \dot{h} &\mapsto \dot{v} \left((\dot{x}(\dot{h}) + \dot{y})^{-1} \right) + \dot{u} \end{aligned} \quad (6.12)$$

In equation (6.12), the parameters $\dot{x}, \dot{v}, \dot{y}$ and \dot{u} denote the elements of the Galois field $GF(2^n)$. After the above define an inclusion map from the Galois field $GF(2^n)$ onto $GF(2^m)$, follow the following mathematical procedure.

$$I_k: GF(2^n) \rightarrow GF(2^m)$$

Define as

$$I_1(\sum_{i=1}^n a_i x^i) = \begin{cases} \sum_{i=1}^m a_i x^i & \text{if } i \leq m-1 \\ 0 & \text{if } i > m-1 \end{cases} \quad (6.13)$$

$$I_2 \left(\sum_{i=1}^n a_i x^i \right) = \begin{cases} \left(\sum_{i=1}^n a_i x^i - \sum_{i=1}^{m-1} a_i x^i \right) x^{-m-1} & \text{if } m-1 < i \leq 2m-1 \\ 0 & \text{if } i < m-1 \text{ or } i > 2m-1 \end{cases} \quad (6.14)$$

$$I_k \left(\sum_{i=1}^n a_i x^i \right) = \begin{cases} \left(\sum_{i=1}^n a_i x^i - \sum_{i=1}^{(k-1)m-1} a_i x^i \right) x^{-m-1} & \text{if } m-1 < i \leq km-1 \\ 0 & \text{if } i < m-1 \text{ or } i > km-1 \end{cases} \quad (6.15)$$

Where $k \geq 2$ and the integer n is strictly greater than m . The composition map $I_i \circ S$ generates $m \times m$ S-box. Using the above process, one can generate $n - m$ number of S-boxes.

6.3.3 Proposed Algorithm

Step 1. Generate a binary matrix M of dimension $M \times N$ to identify the position of the negative integers in the matrix of the original audio.

$$M_{i,j} = \begin{cases} -1 & \text{if } A_{i,j} < 0 \\ 1 & \text{if } A_{i,j} \geq 0 \end{cases} \quad (6.16)$$

Where $A_{i,j}$ indicates the sample of the audio data at (i,j) position. The aim of generating binary matrix M is to specify the position of the negative samples.

Step 2. Select a prime number $p > M \times N$ and generate a sequence σ of random number via the proposed random number generator discussed in section 6.16. Then reduce the length of the sequence and shuffle the matrix of the original audio using the obtained new sequence.

$$\delta_i = \begin{cases} \sigma_i & \text{if } \sigma_i \leq MN \\ 1 & \text{if } \sigma_i > MN \end{cases} \quad (6.17)$$

$$A_{i,j} = A_{\delta_i, \delta_j} \quad (6.18)$$

Where δ_i, δ_j denote the position of the integer value of A_{δ_i, δ_j} in the newly shuffled matrix A_S . The waveform and the spectrogram graph of the shuffled audio are shown in Fig 6(b) and Fig 7(b) respectively. From the figures, one can observe that the permutation step caused optimum disruption in the plain audio data.

Step 3. Next, use the absolute function to transform the entries of the matrix A_S from the set in the rang $\{-2^{15}, 2^{15-1}\}$ to the elements of the Galois field $GF(2^{15})$. Consequently, get a new matrix A_G .

Step 4. Subsequently, convert the elements of the Galois field $GF(2^{15})$ into the elements of the Galois field $GF(2^8)$ and Galois field $GF(2^7)$ by using the following map.

$$\psi: GF(2^{15}) \rightarrow GF(2^8) \times GF(2^7)$$

Defined by

$$\psi \left(\sum_{i=0}^{14} a_i x^i \right) = \left(\sum_{i=0}^7 a_i x^i, \sum_{i=8}^{14} a_{i-8} x^{i-8} \right) \quad (6.19)$$

Where $x_i \in \{0, 1\}$. By proposition 6.2 the map ψ is bijective. Therefore, by using ψ the data in the matrix A_G splits into two matrices A_p^1 and A_p^2 containing elements of the Galois fields $GF(2^8)$ and $GF(2^7)$ respectively.

Step 5. Divide the blocks A_p^1 into four subblocks. Then generate four 8×8 S-boxes using the proposed S-box construction method, which we have discussed in subsection 6.3.2. Afterwar substitute each subblock with a different S-box and then combine all the subblocks. Similarly, divide the block A_p^2 into four subblocks and generate four 7×7 S-boxes using the proposed S-box construction method. Then substitute each subblock with a different S-box and combine all the substituted subblocks. Consequently, get new blocks A_s^2 and A_s^2 .

Step 6. Combine the resultant matrices A_s^2 and A_s^2 using the inverse map of the map ψ , which we have discussed in step 4. The inverse map is given as follows.

$$\psi^{-1}: GF(2^8) \times GF(2^7) \rightarrow GF(2^{15})$$

Defined by

$$\psi^{-1} \left(\sum_{i=0}^7 a_i x^i, \sum_{i=0}^6 a_i x^i \right) = \sum_{i=0}^7 a_i x^i + \sum_{i=1}^6 a_{i+8} x^{i+8} \quad (6.20)$$

In the result of the above map, we get a new matrix A_{s1} containing elements of the Galois filed $GF(2^{15})$.

Step 7. Then mask each element of the matrix A_{s1} to produce more diffusion in encrypted audio. Firstly, generate a sequence ρ of the nonrandom number of lengths $M \times N$. Subsequently, use mode operation and convert the elements of the sequence into the elements of the Galois field $GF(2^{15})$.

$$A_{s2}(i, j) = (A_{s1}(i, j) + (\rho(i, j))^{-1}) \quad (6.21)$$

Where $A_{s1}(i, j)$ and $\rho(i, j)$ are the elements of the Galois field $GF(2^{15})$ and (i, j) signify integer position in the corresponding matrix. As a consequence of the equation (6.21) get a new matrix A_{s2} .

Step 8. Eventually, use the binary matrix M and convert the entries of the matrix A_{s2} from the Galois field $GF(2^{15})$ into the set of integers sixteen $\{-2^{15}, 2^{15} - 1\}$. The mathematical representation is given as follows.

$$A_E(i, j) = \begin{cases} A_{s2}(i, j) & \text{if } M(i, j) = 1 \\ -A_{s2}(i, j) & \text{if } M(i, j) = -1 \end{cases} \quad (6.20)$$

The resultant matrix then converts into the Audio file which is required for the ciphered audio. The proposed encryption scheme is applied to various audio files of different sizes and different characters. The waveform of the encrypted audio is shown in Fig. 6. From the figure, it is evident that the waveform of the encrypted audio is uniform. Accordingly, the proposed scheme is capable to secure the actual content of the original audio. The decryption process of the scheme is the same as encryption.

6.4 Security analysis

A well-organized multimedia data encryption scheme can resist all kinds of attacks such as statistical, brute force, and other cryptanalytics attacks. This section analyzes the robustness of the proposed encryption scheme against multiple attacks. The test simulations are carried out by Matlab 2019(b) on a portable personal computer. To investigate the proposed encryption scheme, we have chosen multiple audio samples with different characters such as speech, music and we encrypt these samples via the proposed scheme using different keys. Fig. 6. shows the waveforms of the original, encrypted, and decrypted audio files. It can be seen in the Figure, that the amplitude plotted in the waveform of the encrypted audios is uniform and have no similarity with the amplitude of the original audio, thus the audio is successfully encrypted. Moreover, the waveforms of the decrypted audio file shown in Fig. 6(d) are similar to the waveform of the original audio file. Accordingly, the original audio data are successfully recovered from the ciphered data. In the next subsection, we examine the scheme over different analyses such as histogram analysis, keyspace analysis, key sensitive analysis, and Correlation Analysis.

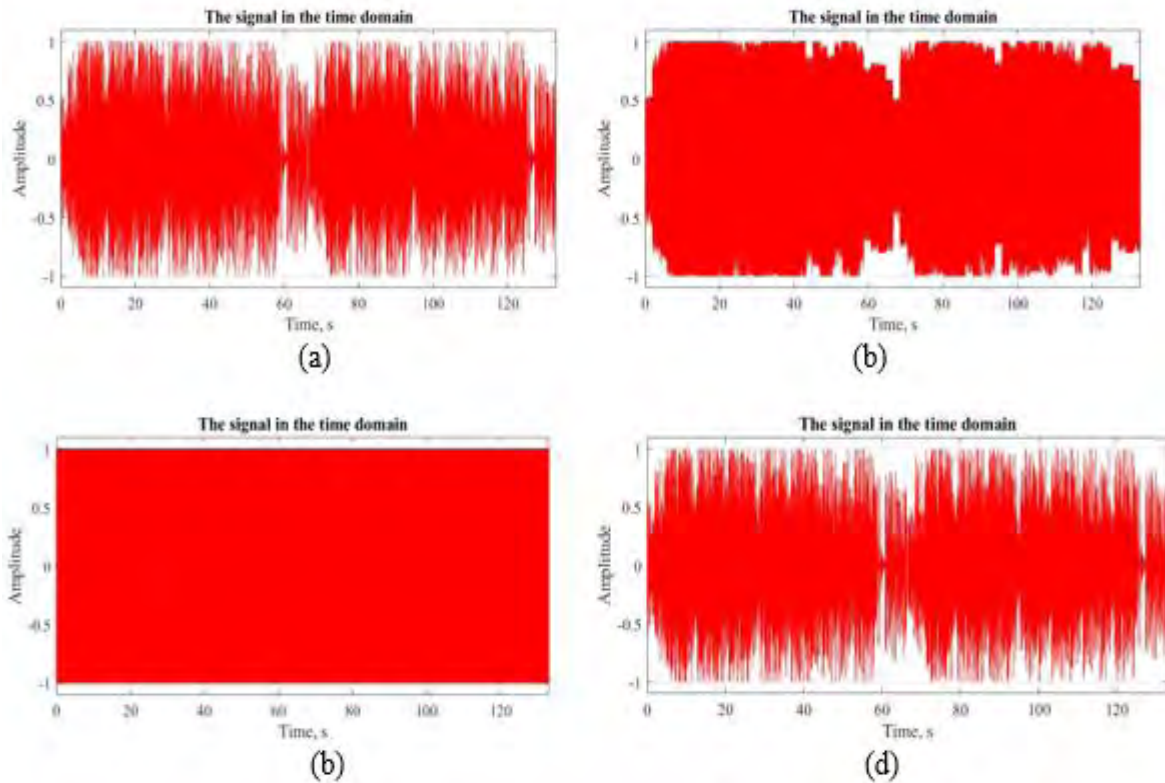


Figure 6. The waveform of the (a) original Audio (b) Permuted Audio. (3) Encrypted Audio (d) Decrypted Audio

6.4.1 Spectrogram analysis

To perform the spectral analysis of sound, it is recommended to use spectrogram analysis. This analysis is demarcated as two-dimensional graph and different colors represent its third dimension. It is considered as the pictorial illustration of the frequency of the spectrum that fluctuates with respect to time. The third-dimension color identifies the amplitude or loudness of the sound at a precise time. The low amplitude is specified by using red and blue colors whereas the bright color indicates the stronger amplitude. The results of the spectrogram analysis of our encryption scheme are given in Fig. 7. The spectrogram graphs of original and encrypted audio files are represented in Fig. 7(a) and Fig. 7(c) respectively. The audio file is effectively encrypted which is evident from the uniformity of the spectrogram graph of the encrypted audio file. This encrypted audio file has a strong amplitude and altogether different spectrogram from the original audio.

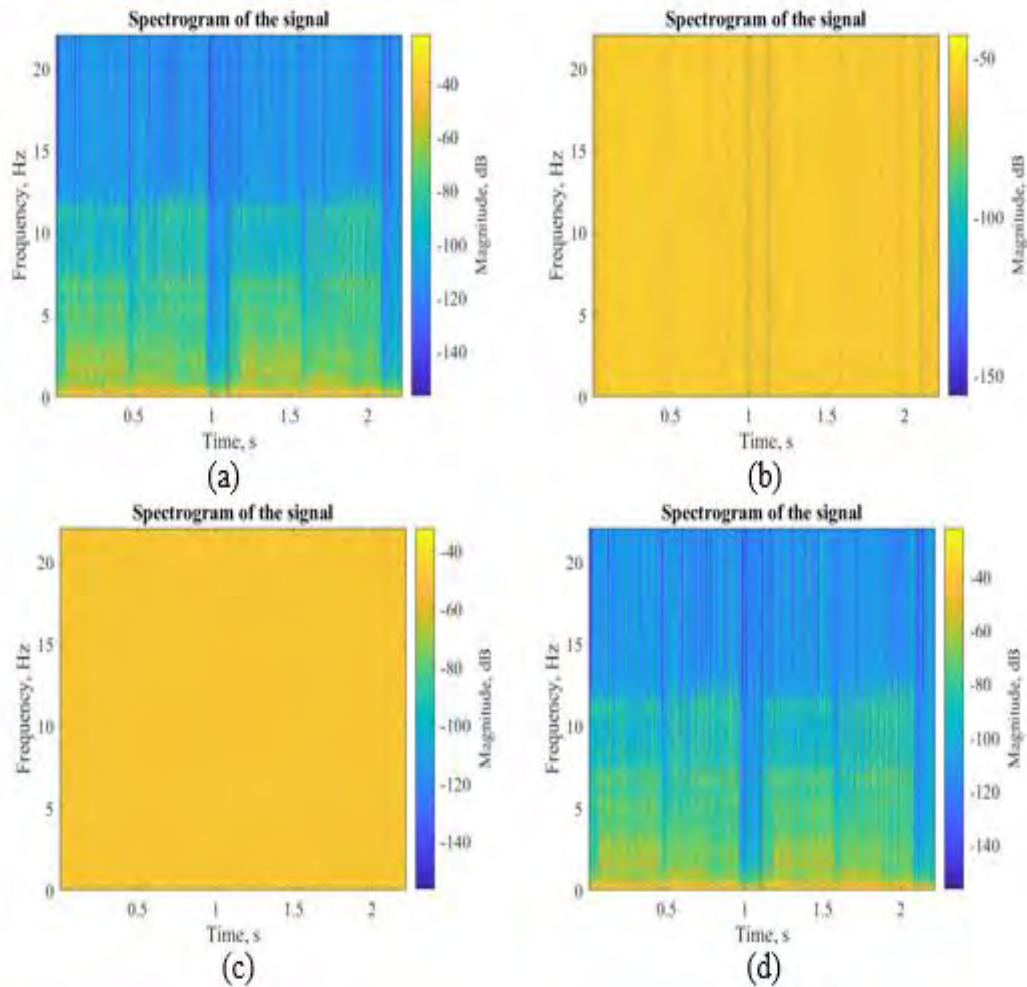


Figure 7. Spectrogram Graph of (a) Original Audio (b) Permuted Audio (c) Encrypted Audio (d) Decrypted Audio

6.4.2 Histogram Analysis

To assess the quality of any encryption scheme against statistical attacks, it is recommended to perform histogram analysis. It is most likely that cryptosystems change the original information into noise and generate randomness in the data. It is observed that in an efficient cryptosystem most likely the encrypted data does not offer any information which helps to decipher the encrypted data free from the requirement of the confidential key. In such cryptosystems, the original data is encrypted with similar possible values. Figure 8 represents the outcomes of histogram analysis of our encryption scheme. The histogram of the original audio is graphically represented in Fig. 8(a) and Fig .8(c) and the histogram of the cryptographed audio is made known in Fig 8(b) and Fig 8(d). One can see that the original audio signal histogram is haphazard and heading towards a single point, but the histogram of the encrypted audio file is absolutely uniform. It concludes that our technique is shown the

strength to counter any statistical outbreak and it's extremely hard to extract info from the encrypted information.

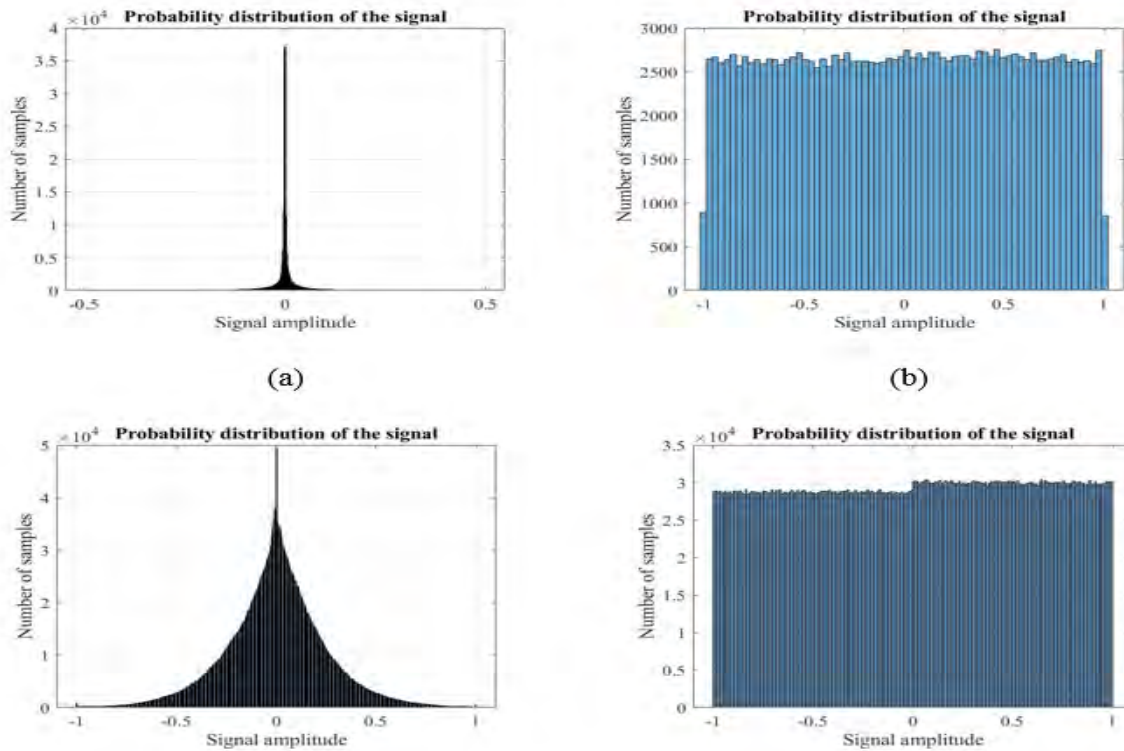


Figure 8. Histogram Analysis (a) Histogram of the Original audio. (b) Histogram of the corresponding encrypted audio (c) Histogram of the original music sound (d) Histogram of the encrypted audio sound

6.4.3 Correlation

The correlation coefficient is one of the analyses which are performed to evaluate the ability of any cryptosystem to fight against various statistical attacks. As data is strongly correlated in multimedia applications so, a robust cryptosystem must intrude on the correlation among the segment of the data. In this analysis, the focus is to observe the correlation between identical sections of the data. The correlation coefficient is given by:

$$\gamma_{uv} = \frac{cov(p, q)}{\sqrt{D(p)D(q)}} \quad (6.21)$$

Where

$$cov(p, q) = \frac{1}{P} \sum_{i=1}^P p_i - \varepsilon(p)(q_i - \varepsilon(q)) \quad (6.22)$$

$$\mathcal{D}(p) = \frac{1}{\mathcal{P}} \sum_{i=1}^{\mathcal{P}} (p_i - \mathcal{E}(p))^2 \quad (6.23)$$

$$\mathcal{E}(p) = \frac{1}{\mathcal{P}} \sum_{i=1}^{\mathcal{P}} p_i \quad (6.24)$$

Where sample at i_{th} position is signified by p_i and q_i indicates the equivalent adjacent sample. Commonly, correlation analyses of the data are performed for horizontal, vertical, and diagonal directions but as our scheme is dealing in audio data so for the single string data only the horizontal direction is taken for correlation analysis. The outcomes of the correlation analysis are shown in Table 19. Table 19 indicates that the original audio correlation is equivalent to 1, which depicts the sections in the audio data have a strong correlation. On the other hand, the correlation analysis for the ciphered audio is nearly a value of 0, i.e., the proposed technique analytically intrudes the correlation of the audio segment. Correlation analysis of the original and the encrypted audio is represented in Figure 9. It establishes that our scheme gradually minimizes the intercorrelation of the audio file. For this reason, our proposed technique is robust against malicious statistical attacks.

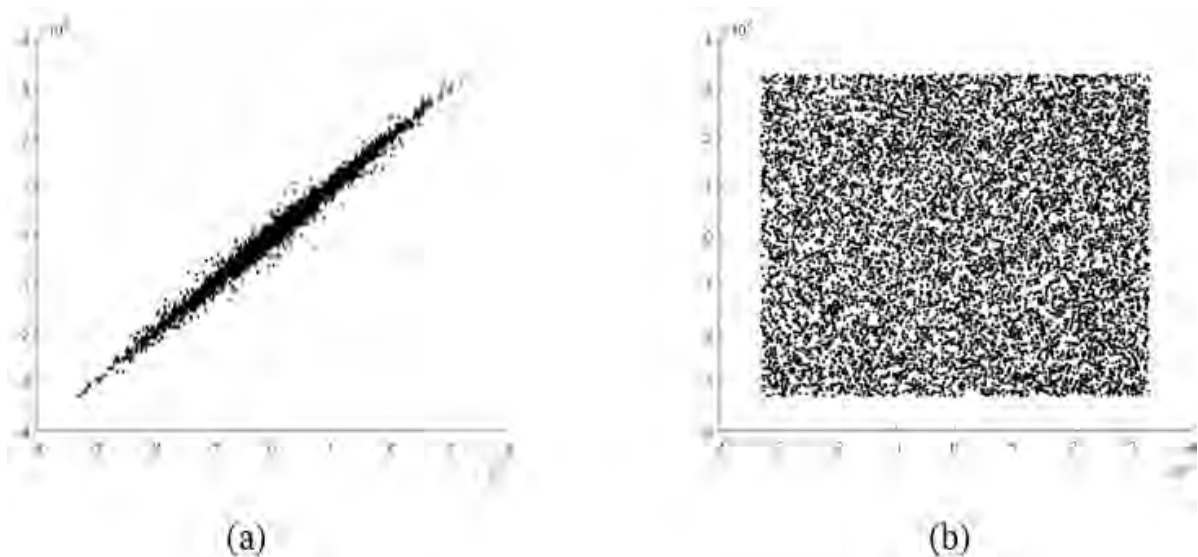


Figure 9. Correlation Analysis (a) Correlation analysis of original image (b) Correlation analysis of encrypted image

Table 19. Correlation Analysis of different Audio

No	Audio	Plain Audio	Ciphered Audio	Size
1	Animal sound.wav	0.9945	-0.0081	530/Kilobyte
2	Alarm sound.wav	0.7317	-0.0033	24000 / Kilobyte
3	Applause sound. Wav	0.8368	-0.0039	783/ Kilobyte
4	Bells sound. Wav	0.9962	0.0011	32000/ Kilobyte
5	Birds sound.wav	0.9924	-0.0031	307/ Kilobyte
6	Female sound.wav	0.9933	-0.0029	32/ Kilobyte
7	44100 Hz tone.wav	0.9886	-0.0010	434/Kilobytes
8	Male sound.wav	0.9464	0.0017	345/Kilobytes
9	Machine sound.wav	0.9523	0.0030	26000 /Kilobyte
10	Music sound.wav	0.9935	-0.0040	11000/Kilobyte
11	New intro sound.wav	0.9847	0.0046	900/Kilobyte
12	Ref .[102]		0.001699	98.6/Kilobyte
13	Ref .[103]		0.0119	138 /Kilobyte
14	Ref .[104]		0.0263	138/Kilobyte

6.4.4 Information entropy

For coded information, the amount of uncertainty is measured by using information entropy analysis. The entropy is directly proportional to the rate of uncertainty i.e.; higher uncertainty in encrypted audio files depicts that it has the higher entropy. We can represent entropy as

$$H = - \sum_{k=0}^{\mathcal{L}} \mathcal{P}(k) \log_2 \mathcal{P}(k) \quad (6.25)$$

Where \mathcal{L} directs the grayscale value of the audio file and $\mathcal{P}(k)$ implies the probability of the presence of the grey-value k . For our case, the audio file has a value of 16 in correspondence to the theoretical value of H . So, the cryptosystem is considered to be well-secured, if the information entropy of the ciphered file is exactly 16. We examine our new proposed scheme by using information entropy analysis and the outcomes are organized in Table 20. It is obvious from the Table that the information value of our proposed technique is almost equal to 16 for all ciphered audio and hence formed ideal vagueness in the audio file. So, our scheme has the ability to resist entropy attacks.

Table 20. Entropy Analysis

No	Audio	Plain Audio	Ciphered Audio	Size
1	Animal sound.wav	8.0065	15.4316	530/Kilobyte
2	Alarm sound.wav	9.8183	15.5592	24000 / Kilobyte
3	Applause sound. Wav	13.4401	15.8693	783/ Kilobyte
4	Bells sound. Wav	13.4216	15.9388	32000/ Kilobyte
5	Birds sound.wav	4.5625	12.2128	307/ Kilobyte
6	Female sound.wav	8.5125	14.9905	32/ Kilobyte
7	44100 Hz tone.wav	9.8134	15.6663	434/Kilobytes
8	Male sound.wav	10.6914	15.6024	345/Kilobytes
9	Machine sound.wav	14.1688	15.9271	26000 /Kilobyte
10	Music sound.wav	14.8475	15.9888	11000/Kilobyte
11	New intro sound.wav	14.8549	15.8779	900/Kilobyte

6.4.5 Differential attacks

For differential attacks mostly, we consider two analyses i.e.; the number of pixel change rates (NPCR) and Unified Average Changing Intensity (UACI). They calculate the sensitivity regarding the cryptosystem. A quality cryptographic algorithm must have sensitivity so a minor alteration in the original data produces a massive variation in the cipher data. Both NPCR and UACI analysis have the tendency to assess the sensitivity of the cryptosystem. NPCR and UACI can be given as.

$$NPCR = \frac{\sum_{u,v} B(u, v)}{K} \times 100 \quad (6.26)$$

In the above equation K represent the cardinality of the audio data set and $B(u, v)$ is given by

$$B(u, v) = \begin{cases} 1 & \text{if } \mathcal{A}_1(u, v) = \mathcal{A}_2(u, v) \\ 0 & \text{if } \mathcal{A}_1(u, v) \neq \mathcal{A}_2(u, v) \end{cases} \quad (6.27)$$

UACI can be represented as

$$UACI = \frac{1}{K} \sum_{u,v} \frac{|\mathcal{A}_1(u, v) - \mathcal{A}_2(u, v)|}{2^K - 1} \times 100 \quad (6.28)$$

where 2^K designates the order of bit in the audio data set. The satisfactory values of NPCR and UACI rate of the algorithm is nearly equal to 100 and 33.3333 respectively. We gauge the proposed audio encryption technique by using NPCR and UACI analysis and the outcomes are shown in Table 21. Table 21 predicts that the proposed technique has tendency to negate differential attacks.

Table 21. Differential Analysis

No	Audio	Plain Audio	Ciphered Audio	Size
1	Animal sound.wav	99.99724	33.1233	530/Kilobyte
2	Alarm sound.wav	99.99974	33.456	24000 / Kilobyte
3	Applause sound. Wav	99.99951	33.2203	783/ Kilobyte
4	Bell's sound. Wav	99.94041	33.1202	32000/ Kilobyte
5	Birds sound.wav	99.9884	33.1344	307/ Kilobyte
6	Female sound.wav	99.99794	33.9205	32/ Kilobyte
7	44100 Hz tone.wav	99.9940	31.6479	434/Kilobytes
8	Male sound.wav	99.99728	33.74039	345/Kilobytes
9	Machine sound.wav	99.9972	33.0987	26000 /Kilobyte
10	Music sound.wav	99.9996	33.67.8	11000/Kilobyte
11	New intro sound.wav	99.9992	33.1233	900/Kilobyte
12	Ref. [102]	99.9972	-	98.6/Kilobyte
13	Ref. [103]	99.9996	-	138 /Kilobyte
14	Ref. [104]	99.9992	-	138/Kilobyte

6.4.6 NIST Statistical Test

For cryptographic applications, we studied the sequence created by the proposed random number generator to assess the random number generator. To examine the randomness of this generated sequence, we first change the random sequence into binary as the NIST test is valid for binary data. The NIST statistical test involves sixteen different tests as presented in Table 22. The generated sequence conceded all the randomness tests, which shows that our proposed technique engenders quality random sequences that have compatibility with different audio encryption applications.

Table 22. NIST Randomness Test for cryptographic applications

No	Type of Test	P-Value	Conclusion	
1	Frequency Test	0.9253077508893466	R	
2	Frequency Test Within Block	0.347578425321557	R	
3	RunTest	0.45321310856174435	R	
4	Longeste Runs of One in a Block	0.43428142438827533	R	
5	Binary Matrices Rank Test	0.7454887332471692	R	
6	Discret Fourier Transform (Spectral) Test	0.12497609962873209	R	
7	Non-Overlapping Template Matching Test	0.622298646456104	R	
8	Overlapping Template Matching Test	0.1716767122905817	R	
9	Maurer Universal Statisticale test	-1.0	NR	
10	Linear Complxity Test	0.4812517437344084	R	
		0.10591374411110245	R	
11	Serial test:	0.013298006380999879	R	
12	Approximate Entropy Test	0.05546464072097093	R	
13	Cummulative Sums (Forward) Test	0.9649804508015285	R	
14	Cummulative Sums (Reverse) Test	0.9921805530466228	R	
15	Random Excursions Test:			
	State	Chi Squared	P-Value	Conclusion
	-4	4.231459930911139	0.5165952795839326	R
	-3	1.7332705882352937	0.8846818589822677	R
	-2	4.758896151053014	0.4460076827348852	R
	-1	5.110294117647058	0.4025686933278576	R
	1	3.360294117647059	0.6446240816842567	R
	2	4.065904139433551	0.5399669541380107	R
	3	5.608141176470588	0.34623345685245316	R
	4	3.5139157703897883	0.6212830486499479	R
16	Random Excursions Variant Test:			
	State	Count	P- Value	Conclusion
	-9.0	197	0.4354513954635062	R
	-8.0	187	0.3467223774673953	R
	-7.0	193	0.34751940774812573	R
	-6.0	195	0.3195447712837526	R
	-5.0	227	0.5201464362953949	R
	-4.0	251	0.7336253801663413	R
	-3.0	248	0.645387747869369	R
	-2.0	259	0.5772743837452569	R
	-1.0	291	0.41529084384812753	R
	+1.0	334	0.12485048506719687	R
	+2.0	353	0.12039826619568533	R
	+3.0	337	0.29218929257880555	R
	+4.0	326	0.4402662823371424	R
	+5.0	303	0.6886093783541819	R
	+6.0	285	0.8771471277417655	R

Chapter. 7

Conclusion

This thesis depicts the critical role of the Galois field in both symmetric and asymmetric key cryptography. This chapter summarizes the significant outcome presented in this thesis. Further, future directions are also discussed.

7.1 Summary of Thesis

This thesis presents the significance of the applications and theory of finite field mathematics and computation in cryptography. A homomorphic encryption scheme has been built that is based on a finite isomorphism problem over matrix Algebra. Furthermore, Galois fields $GF(p^n)$ for general prime p have been used for asymmetric key cryptography and binary Galois field for symmetric key cryptography and multimedia data security.

The second chapter has reviewed the finite field isomorphism problem over the finite field generated by the companion matrix of a primitive irreducible polynomial. Based on the hardness of the finite field isomorphism problem, we have introduced somewhat homomorphic encryption schemes. Initially, an asymmetric key encryption scheme has been introduced, which is homomorphic over matrix addition and matrix multiplication. Subsequently, it is extended to the asymmetric key encryption scheme using the subset sum problem. Afterwards, the scheme has been analyzed against the noise performance and security analysis.

The third chapter has presented the M-NTRU scheme based on a matrix ring over a finite extension field. In addition, some theoretical results are constructed, with the help, one can discuss the essential conditions necessary to avoid the decryption failure. The impact of the Galois field deployment and the commutative property of the matrix ring on the security feature has been discussed.

The improved version of the DES algorithm has been introduced in Chapter 4. The DES is a block cipher that was proved to be unsecured against brute force attack, differential, and linear cryptanalysis. To improve the security of the DES algorithm, we have proposed an algorithm for the construction of 6×6 S-boxes based on Galois field $GF(2^6)$. The S-boxes are then analyzed with different analyses and we have found it secure against linear and differential attacks. Thus, we have improved the DES algorithm by adding the construction

method in the substitution part of the algorithm and strengthened the algorithm against brute force, linear and differential attacks.

In chapter 5, we have presented a novel image encryption algorithm based on \mathbb{Z}_n , the ring of integers modulo n and elements 16 distinctly constructed Galois fields $GF(2^8)$. Substitution-permutation configuration is used in designing a new cryptosystem. Accordingly, confusion among the key streams and the cipher image is increased. In addition, the inclusion of the diffusion layer has improved the security level of the proposed scheme. The strength of the encryption algorithm is examined by different statistical analyses. Image Quality Measures for the proposed encryption scheme for Lena image are also applied and have obtained the results that are found up to the standard. Consequently, after comparison, it is established that the proposed algebraic structures-based image encryption algorithm is much better than other existing chaos-based image encryption methods.

In chapter 6, we have presented a lossless audio encryption scheme based on the arithmetic operations of the elliptic curve and the Galois field. Initially, we have introduced a novel random number generator scheme that is used to generate a quality random number and passed all the NIST tests successfully. The generated random sequence is then used to shuffle the original audio data set. In the diffusion phase of the scheme, a new S-box construction scheme is deployed, which generates multiple S-boxes without much computational effort. The S-boxes are then used to substitute the shuffled audio. The substitution with multiple S-boxes has produced optimum confusion in the encrypted and capable scheme robust against differential attacks. The scheme has been thoroughly securitized over various simulation analyses. The results of the simulation experiment have evidenced that the proposed scheme is secure against various cryptanalysis methods. Accordingly, the proposed scheme is securely suitable for audio encryption applications.

7.2 Future Work

The homomorphic encryption scheme introduced in this thesis is levelled. The levelled homomorphic encryption scheme evaluates the circuit of fixed depth. As we have evaluated and discussed the depth of the proposed scheme in section 2.7. Therefore, levelled homomorphic encryption schemes are not suitable for some applications. In the future, we can convert the proposed scheme into a fully homomorphic encryption scheme using bootstrapping technique.

Furthermore, the performance analyses of the modified NTRU scheme are heuristic. Because there is the possibility of stronger attacks than the attacks on the existing NTRU scheme.

Further research is required on the lattice attack on the modified NTRU, which may yield novel effective techniques.

The DES algorithm is not secure against brute force, linear and differential attacks. In the improved DES algorithm, cryptographically strong S-boxes are deployed, which makes the scheme secured against linear and differential attacks. Since the input block size of the modified DES is greater than the size of the block of its key. Therefore, it has made the brute force attack much complicated, as the brute force attack produces false keys. But the brute force attack is still possible using several pairs of keys. So, in the future, we are intended to improve the security level of the modified DES against the brute force attack up to the standard level.

Multimedia data security schemes presented in this thesis are based on the binary Galois field extensions. The arithmetic operations of the Galois field are the most time-consuming and resourceful operation that can easily be implemented in hardware software. Therefore, these schemes are further extendable for the protection of communication architectures of the future, such as for the internet of things (IoT).

References

1. Mullen, Gary L., and Daniel Panario. *Handbook of finite fields*. CRC Press, 2013.
2. Wan, Zhe-Xian. *Lectures on finite fields and Galois rings*. World Scientific Publishing Company, 2003.
3. Shallit, Jeffrey. "Review of finite fields and applications by Gary L. Mullen and Carl Mummert." *ACM SIGACT News* 43.1 (2012): 30-31.
4. Lidl, Rudolf, and Harald Niederreiter. *Introduction to finite fields and their applications*. Cambridge university press, 1994.
5. Fraleigh, John B. *A first course in abstract algebra*. Pearson Education India, 2003.
6. Isaacs, I. Martin. *Algebra: a graduate course*. Vol. 100. American Mathematical Soc., 2009.
7. Hungerford, Thomas W. *Abstract algebra: an introduction*. Nelson Education, 2012.
8. Delf, Hans, and Helmut Knebl. "Introduction to cryptography: principles and applications [online]." (2007).
9. Elbirt, Adam J. *Understanding and applying cryptography and data security*. CRC press, 2009.
10. Forouzan, Behrouz A. *Cryptography & network security*. McGraw-Hill, Inc., 2007.
11. Boneh, Dan, and Victor Shoup. "A graduate course in applied cryptography." *Draft 0.2* (2015).
12. Möller, Bodo. *Public Key Cryptography: Theory and Practice*. Diss. Darmstadt University of Technology, Germany, 2003.
13. Salomaa, Arto. *Public-key cryptography*. Springer Science & Business Media, 2013.
14. Galbraith, Steven D. *Mathematics of public key cryptography*. Cambridge University Press, 2012.
15. Niederreiter, Harald. "A new efficient factorization algorithm for polynomials over small finite fields." *Applicable Algebra in Engineering, Communication and Computing* 4.2 (1993): 81-87.
16. Mordell, L. J. "JWS Cassels, An introduction to the geometry of numbers." *Bulletin of the American Mathematical Society* 67.1 (1961): 89-94.
17. Diem, Claus. "An index calculus algorithm for non-singular plane curves of high genus." *Talk given at the ECC conference*. 2006.
18. Bach, Eric, and Jonathan Sorenson. "Sieve algorithms for perfect power testing." *Algorithmica* 9.4 (1993): 313-328.

19. Cormen, Thomas H., et al. *Introduction to algorithms*. MIT press, 2009.
20. Rivest, Ronald L., Adi Shamir, and Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems." *Communications of the ACM* 21.2 (1978): 120-126.
21. Gentry, Craig, and Dan Boneh. *A fully homomorphic encryption scheme*. Vol. 20. No. 9. Stanford: Stanford university, 2009.
22. Brakerski, Zvika, and Vinod Vaikuntanathan. "Fully homomorphic encryption from ring-LWE and security for key dependent messages." *Annual cryptology conference*. Springer, Berlin, Heidelberg, 2011.
23. Brakerski, Zvika, Craig Gentry, and Vinod Vaikuntanathan. "(Leveled) fully homomorphic encryption without bootstrapping." *ACM Transactions on Computation Theory (TOCT)* 6.3 (2014): 1-36.
24. Brakerski, Zvika. "Fully homomorphic encryption without modulus switching from classical GapSVP." *Annual Cryptology Conference*. Springer, Berlin, Heidelberg, 2012.
25. Van Dijk, Marten, et al. "Fully homomorphic encryption over the integers." *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, Berlin, Heidelberg, 2010.
26. Coron, Jean-Sébastien, et al. "Fully homomorphic encryption over the integers with shorter public keys." *Annual Cryptology Conference*. Springer, Berlin, Heidelberg, 2011.
27. López-Alt, Adriana, Eran Tromer, and Vinod Vaikuntanathan. "On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption." *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*. 2012.
28. Hoffstein, Jeffrey, Jill Pipher, and Joseph H. Silverman. "NTRU: A ring-based public key cryptosystem." *International Algorithmic Number Theory Symposium*. Springer, Berlin, Heidelberg, 1998.
29. Doröz, Yarkın, et al. "Fully homomorphic encryption from the finite field isomorphism problem." *IACR International Workshop on Public Key Cryptography*. Springer, Cham, 2018.
30. Hoffstein, J., Lieman, D., Pipher, J. and Silverman, J.H., 1999. NTRU: A public key cryptosystem. *Submissions and Contributions to IEEE P, 1363*.
31. Gaborit, P., Ohler, J. and Solé, P., 2002. CTRU, a polynomial analogue of NTRU.
32. Kouzmenko, R., 2006. Generalizations of the NTRU Cryptosystem. *Diploma Project, École Polytechnique Fédérale de Lausanne, (2005–2006)*.

33. Coglianesi, M. and Goi, B.M., 2005, December. MaTRU: A new NTRU-based cryptosystem. In *International Conference on Cryptology in India* (pp. 232-243). Springer, Berlin, Heidelberg.
34. Hoffstein, Jeffrey, et al. *An introduction to mathematical cryptography*. Vol. 1. New York: Springer, 2008.
35. National Bureau of Standards, *Data Encryption Standard*, FIPS publication, No. 46, U.S. Department of Commerce, January 1977.
36. Diffie, Whitfield, and Martin E. Hellman. "Special feature exhaustive cryptanalysis of the NBS data encryption standard." *Computer* 10.6 (1977): 74-84.
37. Hellman, Martin. "A cryptanalytic time-memory trade-off." *IEEE transactions on Information Theory* 26.4 (1980): 401-406.
38. Chaum, David, and Jan-Hendrik Evertse. "Cryptanalysis of DES with a reduced number of rounds." *Conference on the Theory and Application of Cryptographic Techniques*. Springer, Berlin, Heidelberg, 1985.
39. D. W. Davies, Private communications.
40. Biham, Eli, and Adi Shamir. "Differential cryptanalysis of DES-like cryptosystems." *Journal of CRYPTOLOGY* 4.1 (1991): 3-72.
41. Nyberg, Kaisa. "Differentially uniform mappings for cryptography." *Workshop on the Theory and Application of Cryptographic Techniques*. Springer, Berlin, Heidelberg, 1993.
42. Cui, Lingguo, and Yuanda Cao. "A new S-box structure named Affine-Power-Affine." *International Journal of Innovative Computing, Information and Control* 3.3 (2007): 751-759.
43. Feng, D. and W. Wu, *Design and Analysis of Block Ciphers*, Beijing, Tsinghua University Press, 2000.
44. Merkle, Ralph C. "A fast software one-way hash function." *Journal of Cryptology* 3.1 (1990): 43-58.
45. Mar, Phyu Phyu, and Khin Maung Latt. "New analysis methods on strict avalanche criterion of S-boxes." *World Academy of Science, Engineering and Technology* 48.150-154 (2008): 25.
46. COST, Gosudarstvermyi Standard 28147-89, "Cryptographic Protection for Data Processing Systems," *Government Committee of the USSR for Standards*, 1989.
47. Shimizu, Akihiro, and Shoji Miyaguchi. "Fast data encipherment algorithm FEAL." *Workshop on the Theory and Application of Cryptographic Techniques*. Springer, Berlin, Heidelberg, 1987.

48. Rivest, Ronald L. "The RC5 encryption algorithm." *International Workshop on Fast Software Encryption*. Springer, Berlin, Heidelberg, 1994.
49. B. Schneier, *Applied Cryptography*, Second Edition, John Wiley & Sons, 1996.
50. Brown, Lawrence, et al. "Improving resistance to differential cryptanalysis and the redesign of LOKI." *International Conference on the Theory and Application of Cryptology*. Springer, Berlin, Heidelberg, 1991.
51. Yu, Sha-Sha, et al. "Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system." *Optics and Lasers in Engineering* 124 (2020): 105816.
52. Liao, Xin, Kaide Li, and Jiaojiao Yin. "Separable data hiding in encrypted image based on compressive sensing and discrete fourier transform." *Multimedia Tools and Applications* 76.20 (2017): 20739-20753.
53. Shah, Dawood, Tanveer ul Haq, and Tariq Shah. "Image Encryption Based on Action of Projective General Linear Group on a Galois Field $GF(2^8)$." *2018 International Conference on Applied and Engineering Mathematics (ICAEM)*. IEEE, 2018.
54. Huang, Zhi-Jing, et al. "Nonlinear optical multi-image encryption scheme with two-dimensional linear canonical transform." *Optics and Lasers in Engineering* 124 (2020): 105821.
55. Liao, Xin, Zheng Qin, and Liping Ding. "Data embedding in digital images using critical functions." *Signal Processing: Image Communication* 58 (2017): 146-156.
56. Naseer, Yasir, Dawood Shah, and Tariq Shah. "A Novel Approach to improve multimedia security utilizing 3D Mixed Chaotic map." *Microprocessors and Microsystems* 65 (2019): 1-6.
57. Liao, Xin, et al. "A new payload partition strategy in color image steganography." *IEEE Transactions on Circuits and Systems for Video Technology* (2019).
58. Wang, Xingyuan, Lintao Liu, and Yingqian Zhang. "A novel chaotic block image encryption algorithm based on dynamic random growth technique." *Optics and Lasers in Engineering* 66 (2015): 10-18.
59. Zhang, Yu, et al. "Breaking a chaotic image encryption algorithm based on perceptron model." *Nonlinear Dynamics* 69.3 (2012): 1091-1096.
60. Zhang, Yushu, et al. "Breaking an image encryption algorithm based on hyper-chaotic system with only one round diffusion process." *Nonlinear Dynamics* 76.3 (2014): 1645-1650.

61. Liao, Xin, Zheng Qin, and Liping Ding. "Data embedding in digital images using critical functions." *Signal Processing: Image Communication* 58 (2017): 146-156.
62. Norouzi, Benyamin, et al. "A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process." *Multimedia tools and applications* 71.3 (2014): 1469-1497.
63. Zhang, Yushu, et al. "Breaking an image encryption algorithm based on hyper-chaotic system with only one round diffusion process." *Nonlinear Dynamics* 76.3 (2014): 1645-1650.
64. SaberiKamarposhti, Morteza, et al. "Using 3-cell chaotic map for image encryption based on biological operations." *Nonlinear Dynamics* 75.3 (2014): 407-416.
65. Shah, Tariq, and Dawood Shah. "Construction of highly nonlinear S-boxes for degree 8 primitive irreducible polynomials over \mathbb{Z}_2 ." *Multimedia Tools and Applications* 78.2 (2019): 1219-1234.
66. Chai, Xiuli, et al. "A color image cryptosystem based on dynamic DNA encryption and chaos." *Signal Processing* 155 (2019): 44-62.
67. Wu, Xiangjun, Haibin Kan, and Jürgen Kurths. "A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps." *Applied Soft Computing* 37 (2015): 24-39.
68. Wu, Jiahui, Xiaofeng Liao, and Bo Yang. "Color image encryption based on chaotic systems and elliptic curve ElGamal scheme." *Signal Processing* 141 (2017): 109-124.
69. Liu, Hongjun, and Abdurahman Kadir. "Asymmetric color image encryption scheme using 2D discrete-time map." *signal processing* 113 (2015): 104-112.
70. Dong, Chang'E. "Color image encryption using one-time keys and coupled chaotic systems." *Signal Processing: Image Communication* 29.5 (2014): 628-640.
71. Wu, Xiangjun, et al. "Color image DNA encryption using NCA map-based CML and one-time keys." *Signal Processing* 148 (2018): 272-287.
72. Al-Najjar, Hazem Mohammad, Asem Mohammad AL-Najjar, and K. S. A. Arar. "Image encryption algorithm based on logistic map and pixel mapping table." *Proceedings of International Arab Conference on Information Technology,(ACIT 2011)*. 2011.
73. Gupta, Kamlesh, and Sanjay Silakari. "New approach for fast color image encryption using chaotic map." *Journal of Information Security* 2.04 (2011): 139.
74. Fu, Chong, et al. "A chaos-based digital image encryption scheme with an improved diffusion strategy." *Optics express* 20.3 (2012): 2363-2378.

75. Chattopadhyay, D., M. K. Mandal, and D. Nandi. "Symmetric key chaotic image encryption using circle map." *Indian Journal of Science and Technology* 4.5 (2011): 593-599.
76. Al-Maadeed, Somaya, Afnan Al-Ali, and Turki Abdalla. "A new chaos-based image-encryption and compression algorithm." *Journal of Electrical and computer Engineering* 2012 (2012): 15.
77. Enayatifar, Rasul, Abdul Hanan Abdullah, and Ismail Fauzi Isnin. "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence." *Optics and Lasers in Engineering* 56 (2014): 83-93.
78. Chai, Xiu-Li, et al. "A novel color image encryption algorithm based on genetic recombination and the four-dimensional memristive hyperchaotic system." *Chinese Physics B* 25.10 (2016): 100503.
79. Yao, Lili, et al. "An asymmetric color image encryption method by using deduced gyration transform." *Optics and Lasers in Engineering* 89 (2017): 72-79.
80. Huang, Chuan-Kuei, and Hsiau-Hsian Nien. "Multi chaotic systems based pixel shuffle for image encryption." *Optics communications* 282.11 (2009): 2123-2127.
81. ur Rehman, Aqeel, et al. "A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2." *Optik* 159 (2018): 348-367.
82. Wang, Xing-yuan, Hui-li Zhang, and Xue-mei Bao. "Color image encryption scheme using CML and DNA sequence operations." *Biosystems* 144 (2016): 18-26.
83. Kadir, Abdurahman, Mireguli Aili, and Mutallip Sattar. "Color image encryption scheme using coupled hyper chaotic system with multiple impulse injections." *Optik-International Journal for Light and Electron Optics* 129 (2017): 231-238.
84. Kalpana, J., and P. Murali. "An improved color image encryption based on multiple DNA sequence operations with DNA synthetic image and chaos." *Optik* 126.24 (2015): 5703-5709.
85. Pareschi, Fabio, Riccardo Rovatti, and Gianluca Setti. "On statistical tests for randomness included in the NIST SP800-22 test suite and based on the binomial distribution." *IEEE Transactions on Information Forensics and Security* 7.2 (2012): 491-505.
86. Doğanaksoy, Ali, et al. "New statistical randomness tests based on length of runs." *Mathematical Problems in Engineering* 2015 (2015).

87. Alghafis, Abdullah, Hafiz Muhammad Waseem, and Majid Khan. "A hybrid cryptosystem for digital contents confidentiality based on rotation of quantum spin states." *Physica A: Statistical Mechanics and its Applications* (2019): 123908.
88. Arshad, Usman, et al. "An efficient image privacy scheme based on nonlinear chaotic system and linear canonical transformation." *Physica A: Statistical Mechanics and its Applications* (2019).
89. Shah, Dawood, Tariq Shah, and Sajjad Shaukat Jamal. "A novel efficient image encryption algorithm based on affine transformation combine with linear fractional transformation." *Multidimensional Systems and Signal Processing* (2019): 1-21.
90. Khan, Majid, and Hafiz Muhammad Waseem. "A novel image encryption scheme based on quantum dynamical spinning and rotations." *PloS one* 13.11 (2018).
91. Waseem, Hafiz Muhammad, and Majid Khan. "Information confidentiality using quantum spinning, rotation and finite state machine." *International Journal of Theoretical Physics* 57.11 (2018): 3584-3594.
92. Waseem, Hafiz Muhammad, Majid Khan, and Tariq Shah. "Image privacy scheme using quantum spinning and rotation." *Journal of Electronic Imaging* 27.6 (2018): 063022.
93. Servetti, Antonio, and Juan Carlos De Martin. "Perception-based partial encryption of compressed speech." *IEEE Transactions on Speech and Audio Processing* 10.8 (2002): 637-643.
94. Thorwirth, N. J., et al. "Security methods for MP3 music delivery." *Conference Record of the Thirty-Fourth Asilomar Conference on Signals, Systems and Computers (Cat. No. 00CH37154)*. Vol. 2. IEEE, 2000.
95. Servetti, Antonio, Cristiano Testa, and Juan Carlos De Martin. "Frequency-selective partial encryption of compressed audio." *2003 IEEE International Conference on Acoustics, Speech, and Signal Processing, 2003. Proceedings.(ICASSP'03)*.. Vol. 5. IEEE, 2003.
96. Bhargava, Bharat, Changgui Shi, and Sheng-Yih Wang. "MPEG video encryption algorithms." *Multimedia Tools and Applications* 24.1 (2004): 57-79.
97. Grangetto, Marco, Enrico Magli, and Gabriella Olmo. "Multimedia selective encryption by means of randomized arithmetic coding." *IEEE Transactions on Multimedia* 8.5 (2006): 905-917.
98. Yan, Wei-Qi, Wei-Gang Fu, and Mohan S. Kankanhalli. "Progressive audio scrambling in compressed domain." *IEEE Transactions on Multimedia* 10.6 (2008): 960-968.

99. Zhou, Jiantao, and Oscar C. Au. "Security and efficiency analysis of progressive audio scrambling in compressed domain." *2010 IEEE International Conference on Acoustics, Speech and Signal Processing*. IEEE, 2010.
100. Lima, Juliano B., and Eronides F. da Silva Neto. "Audio encryption based on the cosine number transform." *Multimedia Tools and Applications* 75.14 (2016): 8403-8418.
101. Basu, Sandipan. "International data encryption algorithm (IDEA)—a typical illustration." *Journal of global research in Computer Science* 2.7 (2011): 116-118
102. Kordov, Krasimir. "A Novel Audio Encryption Algorithm with Permutation-Substitution Architecture." *Electronics* 8.5 (2019): 530.
103. Sathiyamurthi, P., and S. Ramakrishnan. "Speech encryption using chaotic shift keying for secured speech communication." *EURASIP Journal on Audio, Speech, and Music Processing* 2017.1 (2017): 20.
104. Lima, Juliano B., and Eronides F. da Silva Neto. "Audio encryption based on the cosine number transform." *Multimedia Tools and Applications* 75.14 (2016): 8403-8418.

Turnitin Originality Report

Finite Field Computation and Their Applications in Data Security

by Dawood Shah .



From DRSM (DRSM L)

- Processed on 08-Sep-2021 10:00 PKT
- ID: 1643556715
- Word Count: 36842

Similarity Index
16%

Similarity by Source

Internet Sources:

8%

Publications:

13%

Student Papers:

3%

Dawood Shah
Focal Person (Turnitin)
Quaid-i-Azam University
Islamabad

Tariq Shah
08/11/2021
PROFESSOR
Department of Mathematics
Quaid-i-Azam University
Islamabad

sources:

- 1 1% match (Internet from 30-Jul-2021)
<https://techscience.com/cmc/v67n1/41192/pdf>
- 2 1% match (publications)
[Basic Modern Algebra with Applications, 2014.](#)
- 3 1% match (publications)
[Taryeer ul Haq, Tariq Shah, "12×12 S-box Design and its Application to RGB Image Encryption", Optik, 2020](#)
- 4 1% match (publications)
[Tariq Shah, Asif Ali, Mailed Khan, Ghazanfar Farooq, Antonio Aparecido de Andrade, "Galois Ring \$\mathbb{Z}_8\[x\]\$ Dependent \$24 \times 24\$ S-Box Design: An RGB Image Encryption Application", Wireless Personal Communications, 2020](#)
- 5 < 1% match (Internet from 05-Feb-2020)
<https://link.springer.com/article/10.1007%2Fs00530-019-00640-w>
- 6 < 1% match (Internet from 21-Nov-2019)
<https://link.springer.com/article/10.1007%2Fs11045-019-00689-w>
- 7 < 1% match (Internet from 19-Mar-2019)
<https://link.springer.com/content/pdf/10.1007%2F978-3-642-35261-4.pdf>
- 8 < 1% match (Internet from 30-Jan-2020)
<https://link.springer.com/article/10.1023/B:MTAP.0000033983.62130.00>
- 9 < 1% match (student papers from 14-Feb-2018)
[Submitted to Higher Education Commission Pakistan on 2018-02-14](#)
- 10 < 1% match (student papers from 27-Aug-2018)
[Submitted to Higher Education Commission Pakistan on 2018-08-27](#)
- 11 < 1% match (student papers from 05-Apr-2017)
[Submitted to Higher Education Commission Pakistan on 2017-04-05](#)
- 12 < 1% match (student papers from 20-Jan-2018)
[Submitted to Higher Education Commission Pakistan on 2018-01-20](#)
- 13 < 1% match (student papers from 17-Apr-2012)
[Submitted to Higher Education Commission Pakistan on 2012-04-17](#)
- 14 < 1% match (student papers from 21-Feb-2017)
[Submitted to Higher Education Commission Pakistan on 2017-02-21](#)
- 15 < 1% match (student papers from 08-Oct-2011)