



Cryptosystems based on Elliptic Curves and Recurrent Sequences



By

Sumaira Azhar

Department of Mathematics

Quaid-i-Azam University

Islamabad, Pakistan

2023

Cryptosystems based on Elliptic Curves and Recurrent Sequences



By

Sumaira Azhar

Supervised By

Dr. Umar Hayat

Department of Mathematics

Quaid-i-Azam University

Islamabad, Pakistan

2023

Cryptosystems based on Elliptic Curves and Recurrent Sequences



By
Sumaira Azhar

Supervised by
Dr. Umar Hayat

*A THESIS SUBMITTED IN THE PARTIAL FULFILLMENT OF THE REQUIREMENT:
FOR THE DEGREE OF THE DOCTOR OF PHILOSOPHY
IN MATHEMATICS*

Department of Mathematics

Quaid-i-Azam University

Islamabad, Pakistan

2023

Author's Declaration

I, Sumaira Azhar, hereby state that my PhD thesis titled "Cryptosystems based on Elliptic Curves and Recurrent Sequences" Method 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: Sumaira Azhar

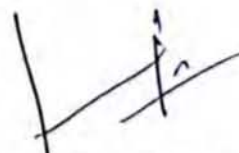
Date: 09-Aug-2023

Plagiarism Undertaking

I solemnly declare that research work presented in the thesis titled "**Cryptosystems based on Elliptic Curves and Recurrent Sequences**" 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: **Sumaira Azhar**

Cryptosystems based on Elliptic Curves and Recurrent Sequences

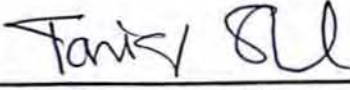
By


Sumaira Azhar

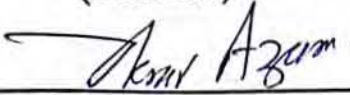
CERTIFICATE

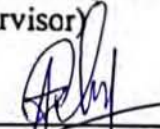
A THESIS SUBMITTED IN THE PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE OF THE
DOCTOR OF PHILOSOPHY IN MATHEMATICS

We accept this thesis as conforming to the required standard

1. 
Prof. Dr. Tariq Shah
(Chairman)

2. 
Dr. Umar Hayat
(Supervisor)

3. 
Prof. Dr. Akbar Azam
(External Examiner)

4. 
Prof. Dr. Mujeeb Ur Rehman
(External Examiner)

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

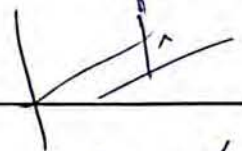
School of Natural Sciences (SNS), National
University of Sciences and Technology
(NUST), Islamabad

**Department of Mathematics
Quaid-I-Azam University
Islamabad, Pakistan
2023**

Certificate of Approval

This is to certify that the research work presented in this thesis entitled Cryptosystems based on Elliptic Curves and Recurrent Sequences was conducted by **Ms. Sumaira Azhar** under the kind supervision of **Dr. Umar Hayat**. 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: Sumaira Azhar

Signature: 

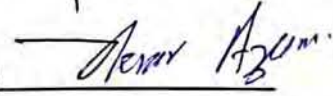
External committee:

a) External Examiner 1:

Name: **Dr. Akbar Azam**

Designation: Professor

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


Signature: 

b) External Examiner 2:

Name: **Dr. Mujeeb Ur Rehman**

Designation: Professor

Office Address: School of Natural Sciences (SNS), National University of Sciences and Technology (NUST), Islamabad

Signature: 

c) Internal Examiner

Name: **Dr. Umar Hayat**

Designation: Associate Professor

Office Address: Department of Mathematics, QAU Islamabad.

Signature: 

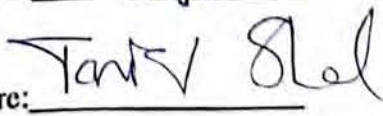
Supervisor Name:

Dr. Umar Hayat

Signature: 

Name of Dean/ HOD

Prof. Dr. Tariq Shah

Signature: 

Acknowledgement

Words are bound and acknowledgement is limited to *praise, thanks* and *glory* of **Allah Almighty**. He, Who is the master and creator of the universe, Owner of the day of judgment, the Responder and self Adequate. I respectfully bow before Him for empowering me to impart a drop, in the sea of knowledge. He has granted me vigor, patience, courage, knowledge, potential and strength, which I felt in each step of my life to accomplish this objective. All the gratitude and respect from bottom of my heart to The **Holy Prophet Muhammad (SAW)** and **Progeny of Muhammad(SAW)** Who is everlastingly source of learning and blessing for all mankind.

I feel great pleasure to express my heartiest appreciation towards my respected supervisor **Dr. Umar Hayat** whose encouragement, motivation and constructive suggestions empowered me to accomplish this thesis in a very efficient manner. I would like to express my heartiest gratitude to all teachers for their guidance and encouragement throughout my studies. I am also thankful to my seniors, particularly **Dr. Naveed Azam** and **Dr. Ikram Ullah** for their encouragement and guidance during my research work and thanks to all lab fellows **Takreem Haidar** and **Ghulam Murtaza** for their worthwhile discussions and suggestions. I owe thanks to my friends Nighat Batool, Wajiha Anwar, Azram Atta Hussain, especially **Dr. Dania Saleem Malik** and **Dr. Saira Jahangir** for their help and persuasion.

This acknowledgement will be incomplete without mentioning my feelings and respect with tearful eyes for my loving parents (**my world**) **Azhar Mehmood** and **Nasreen Azhar**, who taught me to take the first step, to speak the first word and motivated me throughout my life. Thanks to **abu g** and **ami g** for their endless love, encouragement, prayers, unconditional support. It would be impossible for me to acknowledge everything that they have done for me. Without my family, I would not be where I am today. I would like to devote the last line of this acknowledgement to all my well-wishers. May Allah Almighty bless them all.

Preface

People have been using the internet to transmit and store data in recent years. The latest advancements in computing and communication technology have increased the necessity for data security strategies. In this thesis, we generated random numbers and permutations using the points on elliptic curves to build one of the most efficient and unbreakable cryptographic techniques.

The two fundamental categories of data security are cryptography and steganography. Steganography is the study of data security schemes where confidential information is incorporated into host data so that the attackers cannot detect the existence of secret data [1]. Cryptography is the study of data security schemes where secret data is transformed into an unreadable data [2]. Encryption is the key element within cryptography for the provision of security. In encryption, keys of the same or sometimes smaller length are used for encoding messages or data. Mostly ciphering is used for the accomplishment of encryption and decryption at both transmission ends. Cipher is an appropriate way of encrypting or decrypting messages, where ciphering is mostly dependent on the encryption key. A single key is utilized In symmetric cryptography, for both encryption and decryption. Asymmetric cryptography uses two distinct keys, first one encrypts the data and the other for decryption. Recently, elliptic curves (ECs) are used to design strong cryptosystems which creates smaller, quicker, and more effective keys with high security.

In the second and third century A.D. the elliptic curve first appeared in the Diophantuss work. In fact, a polynomial equation with integer or rational solutions is known as a Diophantine equation. An elliptic curve, E over a field K is a set of points that satisfies a plane cubic curve. In the field of cryptography, we use elliptic curve over a finite field. A non-singular

cubic curve E which can be represented as follows

$$Y^2 = X^3 + \alpha X + \beta$$

, is an elliptic curve over field K with a point δ , where the point δ exists on every vertical line and α, β belong to field K . For an elliptic curve, E over a field K , the chord-and-tangent rule exists to add two points of the curve. The set of all points of the elliptic curve along with this addition operation generates an abelian group. The number of points lying on an elliptic curve over the finite field K are also finite, so they construct a finite abelian group. Torsion point is a point of finite order and if it has order n then it is called n -torsion point. Hasse's theorem provides bounds to compute number of points on an EC. In general group law makes it difficult to calculate all curve points [3]. The readers are referred to [2] and [3] for additional information regarding cryptography and elliptic curves, respectively.

Based on various mathematical structures, several data security methods have been presented. Schneier [4] developed a new secret-key block cipher, Blowfish. Rahouma [5] suggested a block cipher data scheme for computer network security. Gupta et al. [6] proposed a data security algorithm depending on logical and shifting operations. Pattanayak et al. [7] used extended Euclidean algorithm and linear congruences to design a text encryption scheme. Abdullah et al. [8] proposed a cryptosystem based on fuzzy logic where triangular fuzzy numbers are used to represent plaintext and ciphertext. In the same way, elliptic curves gained considerable interest in the field of cryptography due to their comparative protection against modern cryptanalysis with low key size. Miller developed an encryption scheme based on elliptic curve cryptography similar but about 20 percent quicker than the Diffie-Hellman key exchange protocol. The concept of a discrete logarithmic problem used in Diffie-public Hellman's key cryptography was applied by Koblitz et al. [9] to the EC group. Amara et al. [10] describe elliptic curve cryptographys network security task with a smaller key size and contrast RSA to elliptic curve cryptography, and conclude that it is a better encryption alternative. An EC

cryptography scheme using the microcontroller with fuzzy modular arithmetic was designed by Ganapathy et al. [11]. Balamurugan et al. [12] used a non-singular matrix to construct a rapid mapping scheme by mapping the plaintext to points of elliptic curve and the ElGamal encryption approach is used to decrypt points using a non-singular matrix. Hayat et al. [13] used elliptic curves to generate pseudo-random numbers as well as S-boxes, then they applied these S-boxes and random numbers in image encryption.

Several authors who have applied text encryption and decryption using elliptic curve cryptography have used an accepted table consisting of mapping characters and elliptic curve coordinates, or the ASCII values of the characters are used to derive affine elliptic curve coordinates by performing point multiplication on the generator "G" and the corresponding character ASCII value. For cryptographic and other applications, researchers are still using ECs. But from literature review, it follows that mathematically structured elliptic curves particularly as ordered elliptic curves, have not yet been deployed for data security as per our knowledge. As a result, this fact drives us to develop new mathematical structures based on elliptic curves to enhance data security. We focus on Mordell elliptic curves, a special elliptic curve, to achieve the following objectives.

- i. To construct the sequences of random numbers by using elliptic curves.
- ii. Use the above structures to create confusion and diffusion in the text encryption algorithm.
- iii. Utilizing the existing elliptic curve structures to construct new structures.
- iv. Next, create new schemes employing the above novel structures to construct non-linear cryptosystem components.
- v. An image encryption algorithm using the aforementioned constructed non-linear cryptosystem components to evaluate their effectiveness.

- vi. To get an encryption algorithm well suited for large size data that can be used for any script with specified ASCII values, not just for English scripts.
- vii. This work also aims at getting efficient encryption algorithm, accuracy, and safety features to maintain the security of data during decryption process.
- viii. Stating and proving theoretical results.

The outline of this thesis is structured as follows:

In chapter 1, basic concepts related to cryptography, pell sequences and elliptic curves over finite fields/rings are briefly discussed.

In chapter 2, We suggest a brand-new, three-step text encryption method that can be shown to be secure against computation-based attacks like key and statistical attack. The first stage of the suggested system, which is based on elliptic curves and the pell sequence, is applying a cyclic shift to the symbol set to transform the plaintext into an abstract plaintext. The second phase involves hiding the elements of the diffused plaintext from the intruders. In the third stage, permutations over elliptic curves are generated in order to confuse the distributed plaintext that has been encoded. We demonstrate the provable security of the suggested approach against some important attacks. The suggested system is also resistant to key spacing attacks, known-plaintext attacks, and ciphertext-only attacks. The suggested scheme is extremely secure against present cryptanalysis than some of the existing text encryption algorithms.

In chapter 3, a novel method of new substitution box construction based on ECs over finite rings is proposed. In addition, the newly developed method is thoroughly evaluated and compared with a few other methods that already exist. Experimental results show that the newly designed substitution box is significantly more resistant to linear attacks and has a higher capacity for confusion than some of the existing substitution boxes.

In chapter 4, we introduced elliptic curves over finite rings based image encryption algorithm. Our scheme consists of three main steps, the first of which is to use points from an EC over

a finite ring to mask the plain image. In the second phase, we generate diffusion by mapping the EC over the finite ring to the EC over the finite field. A substitution box (S-box) is used to permute the pixels of the diffused image to create a cipher image, which will significantly confuse the plaintext. We demonstrated that the suggested scheme is more secure against differential, statical, and linear attacks than existing cryptosystems using computational experiments. Additionally, color image encryption takes less time on average than other existing methods.

In chapter 5, the work provided in this thesis is summarized and some prospective avenues for further research are discussed.

List of Published Articles from the Thesis

A list of published and submitted work from the thesis is included here as it is one of the requirements for the Higher Education Commission of Pakistan.

- i. Hayat, U., Ullah, I., Azam, N. A., and Azhar, S., "A novel image encryption scheme based on elliptic curves over finite rings," *Entropy*, vol. 24, 2022.
- ii. Azhar, S., Azam, N.A., Hayat, U, "Text encryption using pell sequence and elliptic curves with provable security," *Comput. Contin.*, vol. 71, 2022.
- iii. Azam, N.A., Hayat, U, Azhar, S., "A text encryption scheme based on permutations and random number over EC," submitted to "Entropy," 2022.

Contents

1	Introduction	1
1.1	The Elliptic Curves	1
1.1.1	The Elliptic Curve Group Law	3
1.1.2	The Elliptic Curves over Finite Fields	5
1.1.3	Ordering on Elliptic Curves	5
1.1.4	The Elliptic Curves over Finite Rings	7
1.2	Fundamentals of Cryptography	8
1.2.1	Purposes of Cryptography	10
1.2.2	Advanced Cryptographic Tools	10
1.2.3	Substitution Boxes	11
1.2.4	Chosen Plaintext	14
2	Text Encryption Using Pell Sequence and Elliptic Curves with Provable Security	17
2.1	Introduction	17
2.2	Motivation and Related Work	18
2.3	Encryption and Decryption Procedure	19
2.3.1	Ciphertext	21
2.3.2	Secrete Keys	21
2.3.3	Decryption Procedure	22

2.4	Security Analysis and Comparison	27
2.4.1	Key-space Analysis	28
2.4.2	Analysis of Key Sensitivity	28
2.4.3	Statistical Analysis	30
2.4.4	Known-plaintext Attack	31
2.4.5	Ciphertext only Attack	32
2.4.6	Security Comparison	32
2.5	Conclusion	34
3	A Novel Substitution Box Construction Based on an EC Over a Finite Ring of Integers	35
3.1	Introduction	35
3.2	Motivation and Related work	35
3.3	The Proposed S-box	36
3.4	Analysis for Evaluating the Strength of S-box	38
3.5	Conclusion	41
4	A Novel Image Encryption Scheme Based on Elliptic Curves over Finite Rings	42
4.1	Introduction	42
4.2	Related work	43
4.3	The Proposed Encryption Scheme	44
4.3.1	Generation of Keys	45
4.3.2	Masking Phase	45
4.3.3	Diffusion Phase	47
4.3.4	Confusion Phase	48
4.4	Decryption	52
4.5	Security Analysis	52

4.5.1	Differential Attacks Analysis	52
4.5.2	Information Entropy	55
4.5.3	Histogram	56
4.5.4	Correlation	56
4.5.5	Key Space	59
4.5.6	Key Sensitivity	59
4.5.7	Plaintext Attacks	61
4.6	Conclusions	66
5	Summary and Future Directions	67

List of Figures

1.1	Cusp singularity	2
1.2	Isolated point singularity	2
1.3	Node singularity	3
1.4	Addition of Points	4
1.5	Point Doubling	4
1.6	The EC $E_{29,0,1}$ and the effect of the natural, diffusion and modulo ordering on the EC $E_{29,0,1}$: (a) Points of the EC $E_{29,0,1}$ are shown with respect to non-decreasing x -coordinate from left to right; (b) y -coordinates of the points of the ordered EC $E_{29,0,1}$ with natural ordering; (c) y -coordinates of the points of the ordered EC $E_{29,0,1}$ with diffusion ordering; (d) y -coordinates of the points of the ordered EC $E_{29,0,1}$ with modulo ordering.	6
1.7	Symmetric key cryptosystem	9
1.8	Asymmetric key cryptosystem	9
2.1	Flowchart of the proposed encryption and decryption scheme.	23
4.1	Flowchart of the encryption scheme.	49
4.2	Encryption of a 4×4 image by the proposed scheme.	51
4.3	(a,e) Plain images; (b,f) masked images; (c,g) diffused images; (d,h) encrypted images of Lena and Clock, respectively.	53

4.4	(a) Random values of i, j and $I(i, j)$; (b–d) for the whole image database, entropy, UACI, and NPCR results, respectively.	54
4.5	Histograms of plain and encrypted images: (a,c) histogram of the plain images in Figure 4.3(a,e), respectively; (b,d) histogram of the encrypted images in Figure 4.3(d,h), respectively.	57
4.6	Correlation among the adjacent pixels of each encrypted image in the databases: (a) vertical; (b) horizontal; (c) diagonal; (d) off-diagonal correlation.	58
4.7	Correlation distribution of adjacent pixels of plain image along the (a) horizontal, (b) diagonal, (c) off-diagonal, and (d) vertical directions, respectively; correlation distribution of adjacent pixels of cipher image along the (e) horizontal, (f) diagonal, (g) off-diagonal, and (h) vertical directions, respectively.	59
4.8	Decrypted image with (a) actual keys; (b) $p_1 = p_2 = 257$; (c) $b = 8$; (d) $\ell_1 = \ell_1 + 1$	61
4.9	(a) Two ECs generated for a small change in the key b ; (b) points of ECs for two different primes.	61
4.10	(a,e) Plain images; (b,f) masked images; (c,g) diffused images; (d,h) encrypted images of all-black and all-white images, respectively; (i,k) histograms of (a,e), respectively; (j,l) histograms of (d,h), respectively.	63
4.11	(a–c) Histogram of the plain R, G, and B channels of the color Lena _{512×512} , respectively; (d–f) histogram of the encrypted R, G, and B channels of the color Lena _{512×512} , respectively.	64
4.12	Encryption time for color images according to different encryption schemes.	65

List of Tables

2.1	Entries $S(i)$, $\psi_{k=6}(S(i))$, and q_i of an ordered symbol set S , the permuted symbol set $\psi_{k=6}(S)$, and the restricted Pell sequence $Q_{h=18, h'=22}$, respectively .	25
2.2	Plaintext entries $T(i)$, diffused plaintext entries $T'(i)$, weight function entries $w(i)$, binary sequence entries α_i , and encoded diffused plaintext entries (c_i, d_i) , respectively	26
2.3	Permutations due to the ordered ECs $E_{11,0,9}$ and $E_{11,0,4}$ with natural and diffusion ordering, respectively	26
2.4	Entries of $\sigma(c_i)$ and $\sigma'(d_i)$ of the confused plaintext $\sigma(C)$ and $\sigma'(D)$, respectively	27
2.5	Different ciphertexts generated by the proposed scheme for a fixed plaintext .	30
2.6	A ciphertext generated by the proposed scheme with uniform histogram and optimal entropy	31
2.7	Security comparison between different schemes	33
3.1	The S-box $\sigma(2491, 255)$ generated by the proposed algorithm.	38
3.2	Comparison of the S-boxes generated by the proposed algorithm and some recent algorithms.	40
4.1	Comparison of NPCR results due to the proposed algorithm and some other schemes, where the bold value shows that the corresponding image passed the test.	55

4.2	Comparison of UACI results due to the proposed algorithm and some other schemes, where the bold value shows that the corresponding image passed the test.	55
4.3	Comparison of entropy results due to the proposed algorithm and some other schemes.	56
4.4	Comparison of correlation results along all the three directions for the Lena and Barbara images, due to the proposed algorithm and some other schemes. .	60
4.5	Analysis of the proposed encryption technique against plain-text attacks. . . .	62
4.6	Correlation coefficients of two adjacent pixels in encrypted color images. . . .	64

Chapter 1

Introduction

In this introductory chapter, we provide some basic definitions, and concepts of cryptography and elliptic curves. The outline of this chapter is organized as follows. Firstly, we provide some mathematical background of elliptic curves. Following, numerous cryptographic fundamentals are provided in relevance to this thesis.

1.1 The Elliptic Curves

An algebraic non-singular cubic curve over a field K represented by the general Weierstrass equation;

$$y^2 + axy + by = x^3 + cx^2 + dx + e \quad (1.1.1)$$

is called an elliptic curve, where $a, b, c, d, e \in K$.

Definition 1.1.1. *For the characteristic $K \neq 2, 3$, the short Weierstrass equation is*

$$y^2 = x^3 + ax^2 + b \quad (1.1.2)$$

with discriminant $\Delta = -16(4a^3 + 27b^2) \neq 0$.

This condition ensures that for each point on curve, there is a unique tangent line, i.e. the curve is smooth and hence contains no singular points. Cusps, isolated points, and nodes are three different forms of singular points. As singular point contains a repeated root, thus we can write the EC equation as

$$y^2 = x^3 + ax + b = (x - \alpha)^2(x - \beta)$$

and simplification gives

$$x^3 + ax + b = x^3 - 3\alpha^2x - 2\alpha^3$$

For $a = 0$, we get the curve $y^2 = x^3$ which has a triple root at $(0, 0)$. As shown in Figure 1.1,

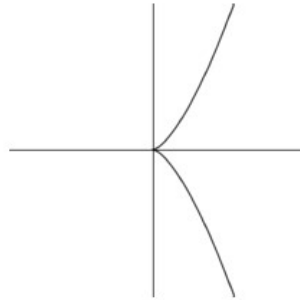


Figure 1.1: Cusp singularity

this forms a cusp at $(0, 0)$.

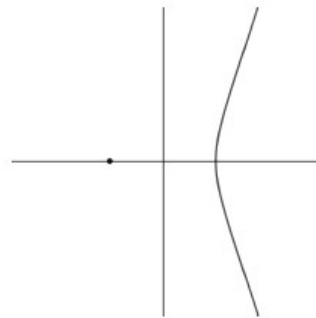


Figure 1.2: Isolated point singularity

Fig. 1.2 illustrates the curve containing an isolated point at $(a, 0)$, for $a < 0$. Furthermore when $a > 0$, the resulting curve (shown in Figure 1.3) has a node at $(a, 0)$.

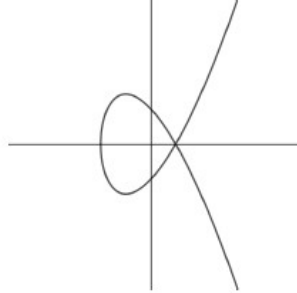


Figure 1.3: Node singularity

Definition 1.1.2. *The set of points $(x, y) \in K \times K$ on an elliptic curve that satisfy the curve, including a point at infinity $\delta \in \{E_k\}$ is defined as*

$$E_k = \{(x, y) \in K \times K : y^2 = x^3 + ax + b\} \cup \{\delta\} \quad (1.1.3)$$

forms an abelian group.

1.1.1 The Elliptic Curve Group Law

According to Bézout Theorem, a line precisely intersects the elliptic curve represented by the Weierstrass equation (1.1.2), at three points. The point addition for any two points Q_1 and Q_2 on (1.1.2) is another point $-Q_3$ on the curve. It is the reflection of the third point Q_3 where the line passing through Q_1 and Q_2 intersects the elliptic curve E as shown in Figure (1.4).

Point doubling is another important operation mainly used in cryptography based on ECs. For identical points Q_1 and Q_2 , we perform a similar method using the tangent line to find $Q_1 + Q_1 = [2].Q_1$ shown in Figure (1.5).

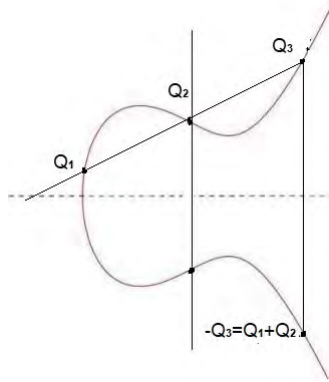


Figure 1.4: Addition of Points

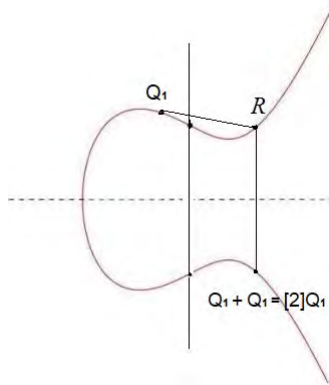


Figure 1.5: Point Doubling

From the above given geometrical description of group law, derived algebraic formulas are given as follows; For any two points Q_1 and Q_2 on ECs $Q_1(x_1, y_1) + Q_2(x_2, y_2) = -Q_3(x_3, y_3)$, where $x_3 = m^2 - x_1 - x_2$ and $y_3 = m_1x_1 - m_1x_3 - y_1$, $y_1 \neq 0$ with slope m of the line $\overline{Q_1Q_2}$ is equal to $\frac{y_2 - y_1}{x_2 - x_1}$ if $Q_1 \neq Q_2$ and $m = \frac{3x_1^2 + a}{2y_1}$ if Q_1 and Q_2 are identical.

The above formula does not apply if Q_1 and Q_2 are distinct but connected with a vertical line. In this case the line $\overline{Q_1Q_2}$ always intersects the EC at infinity point and hence $Q_1 + Q_2 = \delta$, as reflection point of δ is always δ . If $Q_2 = \delta$ then $Q_1 + \delta = Q_1$ because $\overline{Q_1Q_2}$ is the vertical line passing through the point Q_3 and reflection of point Q_3 is the point Q_1 . Hence $Q_2 = \delta$ acts as a identity point on an EC. Also for each point $Q_1 \neq \delta$ on elliptic curve there exists an

inverse point $-Q_1 = (x, -y)$ of Q_1 . Hence, the points on elliptic curve satisfy all the axioms of a group.

1.1.2 The Elliptic Curves over Finite Fields

For a finite prime field \mathbb{F}_p with characteristic other than 2 and 3, prime p and two integers $a, b \in [0, p-1]$ such that $4a^3 + 27b^2 \neq 0$, the short Weierstrass form elliptic curve $E_{p,a,b}$ over the field \mathbb{F}_p is the set

$$\{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p \mid (y^2 = x^3 + ax + b) \pmod{p}\} \cup \{\delta\}, \quad (1.1.4)$$

where δ is the identity element of the EC. We call the integers a, p , and b the *parameters* of the EC $E_{p,a,b}$.

An elliptic curve $E_{p,a,b}$ over \mathbb{F}_p is called Mordell EC when $a = 0$. The following Lemma provides crucial information regarding the number of points on Mordell ECs of a particular class.

Lemma 1.1.3. *when $p \equiv 2 \pmod{3}$ and $a = 0$, the EC $E_{p,0,b}$ has $p + 1$ points that are all unique in their y -coordinates.*

1.1.3 Ordering on Elliptic Curves

On an EC $E_{p,a,b}$, three orderings with good cryptographic properties are defined by Azam et al. [14]. These orderings are diffusion ordering, natural ordering N , D , and modulo diffusion ordering M defined as

$$(s_1, t_1) D (s_2, t_2) \text{ if and only if } "s_1 + t_1 < s_2 + t_2" \text{ or } "s_1 < s_2 \text{ and } s_1 + t_1 = s_2 + t_2"; \quad (1.1.5)$$

$$(s_1, t_1) N (s_2, t_2) \text{ if and only if } "s_1 < s_2" \text{ or } "s_1 = s_2 \text{ and } t_1 < t_2"; \quad (1.1.6)$$

$$(s_1, t_1) M (s_2, t_2) \text{ if and only if } "s_1 + t_1 < s_2 + t_2 \pmod{p}" \text{ or} \quad (1.1.7)$$

$$"s_1 + t_1 = s_2 + t_2 \pmod{p} \text{ and } s_1 < s_2";$$

where (s_1, t_1) and (s_2, t_2) are any two points on an EC $E_{p,a,b}$. The key features of these or-

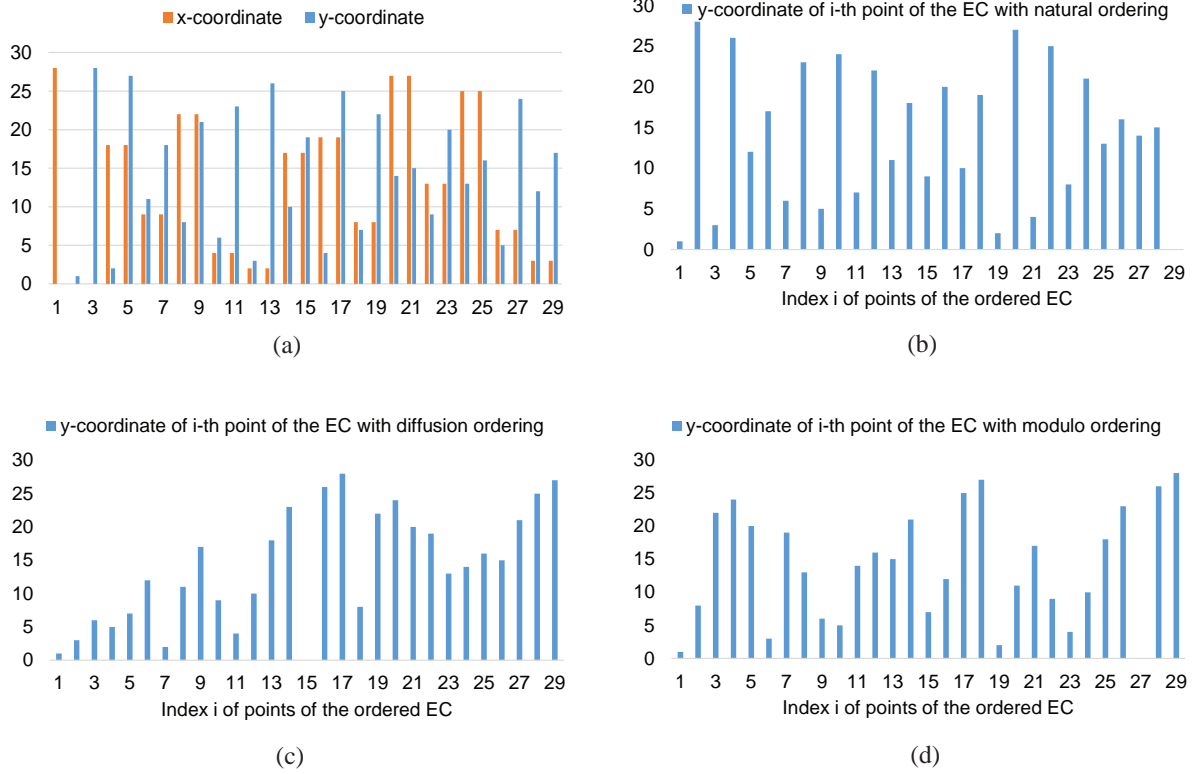


Figure 1.6: The EC $E_{29,0,1}$ and the effect of the natural, diffusion and modulo ordering on the EC $E_{29,0,1}$: (a) Points of the EC $E_{29,0,1}$ are shown with respect to non-decreasing x -coordinate from left to right; (b) y -coordinates of the points of the ordered EC $E_{29,0,1}$ with natural ordering; (c) y -coordinates of the points of the ordered EC $E_{29,0,1}$ with diffusion ordering; (d) y -coordinates of the points of the ordered EC $E_{29,0,1}$ with modulo ordering.

derings are: (i) they diffuse the y -coordinates of the points of the ordered EC; and (ii) these orderings provide highly uncorrelated ordered ECs. Furthermore, it can be observed from Figure 1.6 that the three orderings are non-equivalent and are capable of generating randomness. Due to these properties, Azam et al. [14,15] showed that these orderings are cryptographically suitable for generating a large number of secure permutations over ECs.

1.1.4 The Elliptic Curves over Finite Rings

Let $\{p_i\}_{i \in \Omega}$ be a set of primes for any indexing set Ω . Then, for $k \geq 2$, $n = \prod_{i=1}^k p_i$ is a composite integer and, hence, \mathbb{Z}_n is a ring. As for each prime p , \mathbb{F}_p represents a finite field. Thus, for primes p_i , $1 \leq i \leq k$, we say that \mathbb{F}_{p_i} is a finite field related to the ring \mathbb{Z}_n . For any two integers, $a, b \in \mathbb{Z}_n$, with the condition that $4a^3 + 27b^2 \in \mathbb{Z}_n \setminus \{0\}$, the EC $E_{n,a,b}$ represents the set of points $\{(x, y) \in \mathbb{Z}_n \times \mathbb{Z}_n | y^2 \equiv x^3 + ax + b \pmod{n}\} \cup \{\infty\}$, where ∞ is the neutral point lying at each vertical line passing through the EC, and $4a^3 + 27b^2$ is the discriminant of $E_{n,a,b}$. The condition on the discriminant is imposed so that the EC $E_{n,a,b}$ has no singular point. The integers a, b and n are known as the parameters of $E_{n,a,b}$. For $a = 0$, the ECs are known as Mordell elliptic curves (MECs); we denote them by $E_{n,b}$, and $\#E_{n,b}$ denotes number of points on the this curve. There is a bijection [16] between $E_{n,b}$ and $E_{p_1,b} \times \dots \times E_{p_k,b}$, which maps $(x, y) \in E_{n,b}$ to $(x \pmod{p_1}, y \pmod{p_1}) \times \dots \times (x \pmod{p_k}, y \pmod{p_k}) \in E_{p_1,b} \times \dots \times E_{p_k,b}$. Consequently, an EC $E_{p_i,b}$ may be deduced from $E_{n,b}$ by mapping $(x, y) \in E_{n,b}$ to $(x \pmod{p_i}, y \pmod{p_i})$ and, hence, for each p_i we have a surjective map from $E_{n,b}$ to $E_{p_i,b}$. Let $f : E_{n,b} \rightarrow E_{p_1,b} \times \dots \times E_{p_k,b}$ and $g : E_{n,b} \rightarrow E_{p_i,b}$ represent the former bijective and surjective maps, respectively; then, mathematically, f and g are given by:

$$f(x, y) = (x \pmod{p_1}, y \pmod{p_1}) \times \dots \times (x \pmod{p_k}, y \pmod{p_k}),$$

$$g(x, y) = (x \pmod{p_i}, y \pmod{p_i}).$$

1.2 Fundamentals of Cryptography

The list of basic terminologies and concepts used through the contents of cryptography are given as follows;

Plaintext: The original readable message or data which serves as an input to the algorithm is called plaintext.

Ciphertext: A ciphertext represents a hidden or unreadable text. When any suitable scheme is applied to plaintext in order to codify it, the resulting codified message is known as ciphertext.

Encryption: Encryption or enciphering is a technique of changing plaintext into ciphertext. Its objective is to protect sensitive data from an adversary.

Key: The plaintext is encrypted using a key, which is a word, number, or phrase. A key or keys control both encryption and decryption.

Decryption: Decryption is an inversion method used to convert ciphertext into plaintext with the help of key.

Cryptosystem: Cryptosystem is a design or plan developed for encryption. A cryptographic system mainly relies on the key. Encryption and decryption are both methods that can be handled by a single key if the sender and recipient of the data can secretly exchange private keys. On the other hand, for encryption and decryption techniques, distinct public and private keys can be used. On this basis, two categories of cryptography are

- i. Symmetric(Private) Cryptosystem
- ii. Asymmetric(Public) Cryptosystem

Symmetric Cryptosystem: A symmetric cryptosystem uses an identical key for both encryption and decryption. This cryptosystem has two requirements

- It is not necessary to keep the algorithm secret; just the key must be kept secret.
- Both the sender and the recipient of the data must have stored backup copies of the secret

key in a secure place and ensured the key's security. If an individual familiar with the algorithm finds a hint to the key, all communications based on this key are vulnerable.

This is further subdivided into two main types. The first is known as a block stream, while the second is known as a block cipher.

Stream Cipher: A stream cipher encrypts data by encrypting it one bit at a time. RC4 and ChaCha20 are examples of stream cipher.



Figure 1.7: Symmetric key cryptosystem

Block Cipher: In private key-based cryptosystems, block ciphers play a significant role. It is a technique of message encryption that works with a symmetric key and acts on a collection of bits known as a "block" rather than encrypting a single bit. Advanced Encryption Standard (AES) [17], Data Encryption Standard (DES) [18], Double Data Encryption Standard (2DES) are well-known block ciphers.

Asymmetric Cryptosystem: The asymmetric cryptosystem depends on two keys. One is known as a "public key," because it is made available to the public, and the second is a "private key," since only the recipient is aware of it. The sender encrypts the text by using a public key. Only a receiver with a private key can decrypt it. RSA(Rivest Shamir Adleman) and Elliptic Curve Cryptography(ECC) are well known Asymmetric Cryptosystems.



Figure 1.8: Asymmetric key cryptosystem

1.2.1 Purposes of Cryptography

Cryptography is used to not just encrypt and decrypt messages, but also to solve real-world problems that need information or data security. The four main purposes that arise in the field of cryptography are as follows:

Confidentially: It assures that private or personal information is only available to the sender and receiver.

Integrity: It ensures that data sent over an insecure channel does not change. In other words, no one can change the information except the transmitter and recipient.

Authentication: This process verifies the identity of the transmitter and recipient. It also ensures that their communications are not being intercepted by an unauthorized party.

Certification: The term "certification" refers to the transmission of information by a trusted source or individual.

1.2.2 Advanced Cryptographic Tools

Before the year 1950, cryptography was considered an art form. However, modern cryptography is a discipline that requires input from a wide variety of other fields, such as computer science, electronics, and mathematics. After World War II, the intelligence agencies of various armed forces started placing a high priority on cryptographic research. As a result, the first symmetric cryptosystems were developed after a delay of two years. These include the Data Encryption Standard (DES) and public key ciphers. During that time period, the algorithms were developed with the assistance of computers. Then, scientists realized that small tools could be combined to produce effective ciphers. The following is a list of these tools:

Permutation: A permutation is a way to arbitrarily change the order of two members of a set.

Substitution: Substitution is the process of changing one symbol with another in cryptogra-

phy. The Caesar Shift Cipher is an example of a substitution cipher in standard cryptography. In this case, every letter in the plaintext should be changed to a letter three spots further down the alphabet.

Diffusion and Confusion: In order to increase the security of a cryptosystem, Shannon proposed two concepts, confusion and diffusion as follows

Confusion: Confusion is the process of linking the ciphertext and the key as complicated as possible so that no one can figure out the key even if they know the ciphertext.

Diffusion: The process of spreading out the effect of single plaintext bit across a number of ciphertext bits so that the statistical redundancies of the plaintext cannot be detected is called diffusion.

1.2.3 Substitution Boxes

Boolean functions and substitution boxes (S-boxes) are essential aspects of modern cryptosystems. The function quantity is used to link both S-boxes and Boolean functions. In contrast to the Boolean function, which produces a single output bit from a single input bit, an S-box consists of Boolean functions with various outputs. If a cryptosystem can create sufficient confusion and diffusion in the data, it is considered secure [1]. Many well-known and widely used cryptosystems use S-box for the data scrambling, including AES, DES, Blowfish cryptosystem [4] and Twofish security system [19].

The $n \times m$ S-box is a boolean function $\sigma : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m$ from n input binary bits to m output binary bits. S-boxes are lookup tables that translate n binary bits to m binary bits. The individuality of the input and output affects the S-box dimension, which could be distressing to S-box properties. For example, if the number of binary input bits is greater than the number of binary output bits in an $n \times m$ S-box, there should be a repetition in the S-box entries. However, if $n = m$, there is a bijection in S-box, meaning that the entries of the S-box are distinct, and the input values are mapped onto distinct output values. Bijective

S-boxes that are reversible are typically referred to as S-boxes that have both surjection and injection properties, demonstrating the existence of the inverse S-box for these S-boxes. However, the cryptosystems that use single S-box cannot create sufficient confusion and diffusion in the data. To secure data, many cryptographers proposed various techniques using multiple S-boxes. A cryptosystem needs S-boxes with high non-linearity and low linear and differential probabilities.

The security strength of S-boxes is evaluated using a variety of standard methods. Some are described individually as follows::

Linear Attacks

For an S-box, linear approximation probability $LAP(S)$ and the non-linearity $NL(S)$ are calculated as follows:

$$LAP(S) = \frac{1}{2^n} \left\{ \max_{\alpha, \beta \neq 0} \left\{ \left| \#\{x \in \mathbb{F}_2^n \mid x \cdot \alpha = S(x) \cdot \beta\} - 2^{n-1} \right| \right\} \right\}, \quad (1.2.1)$$

$$NL(S) = \min_{\alpha \neq 0, \beta, \lambda} \#\{x \in \mathbb{F}_2^n : \alpha \cdot S(x) \neq \beta \cdot x \oplus \lambda\}, \quad (1.2.2)$$

where $\alpha, \beta \in \mathbb{F}_2^n$, and “ \cdot ” denotes the dot product.

Differential Attacks

These attacks are used to study the differences of outputs for the corresponding differences of inputs to obtain useful information. The mathematical representation of the differential approximation probability $DAP(S)$ for $\Delta x, \Delta y \in \mathbb{F}_2^n$, is given by:

$$DAP(S) = \frac{1}{2^n} \left\{ \max_{\Delta x, \Delta y} \left\{ \#\{x \in \mathbb{F}_2^n \mid S(x \oplus \Delta x) = S(x) \oplus \Delta y\} \right\} \right\}, \quad (1.2.3)$$

where the bit-wise addition is denoted by “ \oplus ” in \mathbb{F}_2 . Thus, the S-box S possesses higher security if the $DAP(S)$ is close to $1/2^n$.

Analysis of Boolean Functions

The boolean function strict avalanche criterion (SAC) calculates the change that occur in the output bits due to the inversion of one bit in a set of input bits. The boolean function bit independence criterion (BIC) determines the dependence level of a pair of output bits on inverting an input bit. For an $n \times n$ S-box S , two matrices, $B(S) = [b_{ij}]$, and $M(S) = [m_{ij}]$, compute the $BIC(S)$ and the $SAC(S)$, respectively:

$$b_{ij} = \frac{1}{2^n} \left(\sum_{\substack{x \in \mathbb{F}_2^n \\ 1 \leq r \neq i \leq n}} w \left(S_i(x \oplus \eta_j) \oplus S_i(x) \oplus S_r(x + \eta_j) \oplus S_r(x) \right) \right), \quad (1.2.4)$$

$$m_{ij} = \frac{1}{2^n} \left(\sum_{x \in \mathbb{F}_2^n} w \left(S_i(x \oplus \eta_j) \oplus S_i(x) \right) \right), \quad (1.2.5)$$

where $w(y)$ represents the number of non-zero symbols in y , $\eta_j \in \mathbb{F}_2^n$ with $w(\eta_j) = 1$, and S_i denotes the i -th Boolean function of the S-box S .

Key-Space Analysis

Brute-force attack is commonly used by cryptanalysts to decrypt ciphertext. Key spacing analysis is used to analyze the security of an encryption scheme against brute-force attack. For an encryption scheme, key spacing is defined to be the number of distinct secret keys that it can generate.

Sensitivity Analysis

This is an important feature of a cryptographically strong cryptosystem. Key sensitivity is also necessary to resist brute-force attacks. If a small change in a key leads to a significant change in the cipher, then the cryptosystem is said to be sensitive to the keys.

Ciphertext only Attack

In this attack, the cryptanalyst has access to some ciphertexts and try to get secret keys and hence the plaintext. In the absence of the proposed scheme's secret keys, the cryptanalyst is unable to decrypt the plaintext.

Plaintext Attacks

There are two types of plaintext attacks, i.e., chosen plaintext attacks and known plain-text attacks.

1.2.4 Chosen Plaintext

In this attack, the adversary has a partial access to the encryption scheme. That is, the adversary can obtain the ciphered string for a chosen plaintext string.

Known-Plaintext Attack

In this attack, the attacker knows a pair of plaintext and ciphertext and tries to generate secret keys.

Statistical Analysis

An encryption scheme is highly secure against statistical attacks if it can generate a highly random ciphertext. Histogram analysis and entropy analysis are the two frequently used techniques to assess the scheme' security against statistical attacks.

Histogram

A histogram of an image represents the frequency distribution of the gray values. If each pixel value occurs with almost equal frequency in an image, then the histogram of that image is said to be uniform. The histogram of an ordinary image is always highly nonuniform, while a properly encrypted image has a uniform histogram.

Information Entropy

Information entropy is used to measure randomness in an image. Equation (1.2.6) is used to determine the randomness of an image I :

$$H(I) = - \sum_{i=1}^k p(x_i) \log_2(p(x_i)), \quad (1.2.6)$$

where $p(x_i)$ represents the probability of a pixel value x_i , and k is the total number of gray values in an image I . For an 8-bit encrypted image, the ideal value of entropy is 8, which corresponds to the highest level of uncertainty. Thus, for a cryptographically strong encryption scheme, the value of $H(I)$ should be close to 8.

Correlation

A pixel of an ordinary image has high correlation with adjacent pixels. A good encryption scheme breaks the correlation among the pixels of an encrypted image. For the datasets x and x' of the same size M , the correlation coefficient between them is determined by:

$$C_{xx'} = \frac{\sum_{i=1}^M (x_i - E[x])(x'_i - E[x'])}{\sqrt{\sum_{i=1}^M (x_i - E[x])^2 \sum_{i=1}^M (x'_i - E[x'])^2}}, \quad (1.2.7)$$

where $x_i \in x$ and $y_i \in y$ and $E[x] = \frac{1}{M} \sum_{i=1}^M x_i$.

UACI and NPCR

The UACI criterion computes the average difference in intensity among two images. A criterion for determining the impact of a modification in a plain image on the ciphers is NPCR. If I and I' are any two plain images of the same dimension $u \times v$, and C_I and $C_{I'}$ are the

respective cipher images of I and I' , then NPCR and UACI are calculated as:

$$\text{UACI} = \sum_{i=1}^u \sum_{j=1}^v \frac{|C_I(i, j) - C_{I'}(i, j)|}{255 \times u \times v}, \quad (1.2.8)$$

$$\text{NPCR} = \sum_{i=1}^u \sum_{j=1}^v \frac{\tau(i, j)}{u \times v}, \quad (1.2.9)$$

where $\tau(i, j) = 0$ if $C_I(i, j) = C_{I'}(i, j)$, and $\tau(i, j) = 1$, otherwise.

Pell sequence For initial values $P_0 = 0$ and $P_1 = 1$, the n -th term P_n of the Pell sequence is defined with the recurrence relation

$$P_n = 2P_{n-1} + P_{n-2}. \quad (1.2.10)$$

The first six terms of the Pell sequence are 0, 1, 2, 5, 12, and 29. By [20] it is known that for

$$i \rightarrow \infty \text{ it holds that } \frac{P_i}{P_{i-1}} \rightarrow 1 + \sqrt{2}.$$

Chapter 2

Text Encryption Using Pell Sequence and Elliptic Curves with Provable Security

2.1 Introduction

This chapter introduces a 3-step encryption scheme over a recurrent sequence and elliptic curves. To achieve this, we divided our scheme in three steps, first we diffuse the plaintext. Then an encoding procedure is applied to the diffused plaintext based on the Pell sequence in step 2. Finally, the encoded diffused plaintext is confused in step 3 based on ECs.

The organization of this chapter is as follows. The motivation and related work is present in Section 2.2. We discuss encryption algorithm in Section 2.3. Security analysis and the presented scheme's comparison is discussed in Section 2.4. A conclusion is drawn in Section 2.5.

2.2 Motivation and Related Work

On the basis of various mathematical structures like algebraic structures [21–26], elliptic curves [13–15, 27–30], chaotic maps [31–36] and fuzzy set theory [8, 37], several data security techniques have been developed. While communicating on popular messaging systems like WhatsApp, consumers are concerned about the privacy and security of their information. So, the security of the text messages gained great attention now a days. We briefly review some of the recent text encryption schemes. Abdullah et al. [8] presented a fuzzy logic based cryptosystem where triangular fuzzy numbers are used to represent plaintext and ciphertext. Gupta et al. [6] developed a data security algorithm utilizing shifting and logical operations. Pattanayak and Dey [7] used extended Euclidean algorithm and linear congruences to design a text encryption scheme. 8-bit code values of alphabets are utilized by Agrawal and Pal [38] to employ an efficient algorithm. A hidden encrypted symmetric key algorithm developed by Ghrare et al. [22] by hiding the secret key in the ciphertext. Numerous applications exist in the fields of mathematics and computer science for linear recurrences like modified Fibonacci numbers, Pell numbers, and Pell-Lucas numbers [20, 49, 50]. For the sake of cryptography, the systems in [23, 51, 52] utilize linear recurrences. Luma and Ruafi [39] explored a relationship between Fibonacci and Lucas sequence and used it to generate cryptosystems. Overmars and Venkatraman [40] proposed an efficient method to compute the golden ratio to avoid cryptographic breaches. Agarwal et al. [41] generated a data encryption scheme built upon Fibonacci numbers. Recently, DNA sequences are also used to generate secret keys for data security [42–44]. Clelland et al. [42] combined a DNA based technique and the microdot to send messages secretly. Abbasy et al. [44] employed useful features of DNA sequences for data hiding. Chaotic maps are used to develop new security schemes due to their high sensitivity to the initial condition [45–50]. A model encryption method built upon logistic map was proposed by Murillo-Escobar [45]. Similarly, because of its comparable security against modern cryptanalysis with small key sizes, elliptic curves (ECs) have drawn a lot of attention for image encryption [51–55], text encryption [56–61] and signcryption [62–64]. To

transfer messages securely, Sunneetha et al. [56] suggested utilizing algebraic operations with elliptic curves. Agrawal and Gera [58] created a more complicated and secure text encryption method employing the Hill cipher and ECC. In their new text encryption approach, Keerthi and Surendiran [59] translated the plaintext's ASCII values in the hexadecimal form to the affine points of an EC. Naji et al. [57] suggested a unique text encryption technique based on encoding plaintext characters with affine points on an EC. As an input for the elliptic curve, Kumar et al. [60] utilized paired ASCII values that correspond to the plaintext. Singh and Singh [61] developed an algorithm that can be used for encryption and decryption of any size of text message with given ASCII values. S. Ullah et al. [62] provided a critical review of hyper elliptic curves based signcryption algorithms. A hyper elliptic curve based signcryption scheme more suitable for emerging resource constraints environment is proposed by S. Ullah and N. Din [64]. Most text encryption techniques found in the literature, including [6–8, 38, 41, 42, 44, 45, 56–59, 61, 65], are vulnerable to well-known attacks, including key sensitivity, spacing, ciphertext-only attacks, statistical attacks, and known-plaintext attack.

2.3 Encryption and Decryption Procedure

Step 1. Diffuse plaintext: We select an integer $k \in [0, m - 1]$ and permute the entries of S by using the permutation $\psi_k : S \rightarrow S$ defined as

$$\psi_k(S(i)) = S((i + k) \pmod{m}), \quad (2.3.1)$$

i.e., ψ_k maps the i -th entry of S on its $(i + k) \pmod{m}$ -th entry. Now generate a *diffused plaintext* $T' = T'(1) \dots T'(i) \dots T'(n)$ by using the permutation ψ_k such that the i -th element $T'(i) = \psi_k(T(i))$, $i \in [1, n]$. The diffusion step is similar to the Caesar cipher [66].

Step 2. Encode diffused plaintext: To encode the elements of the diffused plaintext T' , we first generate a restricted Pell sequence as follows.

Select two positive integers h and h' such that $h < h'$ and $h' - h + 1 \leq \beta$, and generate the *restricted Pell sequence* $Q_{h,h'} = q_1 \dots q_i \dots q_m$, if it exists, such that for each integer $i \in [1, m]$ the following hold:

- $q_i = \log(P_i/P_{i-1})$ and q_i has exactly $h' - h + 1$ digits from h -th digit to h' -th digit after the decimal, where P_i is the i -th entry of the Pell sequence, and
- all entries of $Q_{h,h'}$ are distinct, i.e., for any two distinct $i, j \in [1, m]$, it holds that $q_i \neq q_j$. We apply this condition so that each symbol in the diffused plaintext can be encoded uniquely.

Observe that the entries of the restricted Pell sequence $Q_{h,h'}$ are in the closed interval $[0, 1]$ since $P_i/P_{i-1} \rightarrow 1 + (2)^{1/2}$ as $i \rightarrow \infty$ by [20]. We added the constraint $h' - h + 1 \leq \beta$ to generate a restricted Pell sequence to control the length of the ciphertext and increase the key size, since for a fixed integer τ , there exists different pairs h, h' such that $h' - h + 1 = \tau$, and hence different restricted Pell sequences.

Next, generate a *weight function* $w : \{1, 2, \dots, n\} \rightarrow [-1, 1]$ which is an injection, i.e., for any two $i, j \in \{1, 2, \dots, n\}$ such that $i \neq j$, it holds that $w(i) \neq w(j)$. The aim of this weight function is to uniquely encode the position of each element of T' .

Now, generate a *binary sequence* $\alpha = \alpha_1 \dots \alpha_i \dots \alpha_n$. Based on the i -th entry α_i of α , decide if we use weight $w(i)$ with q_j or $q_j - 1$, $j \in [1, n]$ during the encoding procedure.

Now, generate an encoded diffused plaintext $(C, D) = (c_1, d_1) \dots (c_i, d_i) \dots (c_n, d_n)$ such that the i -th element $T'(i)$ of T' is encoded as (c_i, d_i) with

$$(c_i, d_i) = (q_{(j+k) \pmod m} + \alpha_i w(i), 1 - q_{(j+k) \pmod m} + (1 - \alpha_i)w(i)), \quad (2.3.2)$$

where $T(i) = S(j)$, for some $j \in [1, m]$ and $T'(i) = \psi_k(S(j)) = S((j+k) \pmod m)$.

Step 3. Confuse encoded plaintext: In this step, we create confusion in the encoded plain text (C, D) . For this purpose, we generate two bijections $\sigma : C \rightarrow C$ and $\sigma' : D \rightarrow D$ by using ordered subsets of two ECs. These ordered subsets are such that each integer in $[1, n]$ appears exactly once as y -coordinates of the points. The existence of such subsets is ensured by considering the ECs with $a = 0$ and $p \equiv 2 \pmod{3}$. Finally, the i -th entries of C and D are mapped on some entries of C and D whose indices are determined by the y -coordinates of the i -th points in the ordered sets. More precisely, select two primes $p, p' \geq n$ with $p, p' \equiv 2 \pmod{3}$, two integers $b, b' \in [1, p-1]$ and two orderings \prec and \prec' . Compute the ordered subsets $\{(a_i, b_i) \mid b_i \in [1, n] \text{ and } (a_i, b_i) \in E_{p,0,b}\}$ and $\{(a'_i, b'_i) \mid b'_i \in [1, n] \text{ and } (a'_i, b'_i) \in E_{p',0,b'}\}$ ordered w.r.t. the orderings \prec and \prec' , where for each $i \in [1, n]$ it holds that $(a_i, b_i) \prec (a_{i+1}, b_{i+1})$ and $(a'_i, b'_i) \prec' (a'_{i+1}, b'_{i+1})$, respectively. From these ordered subsets, get the sequences $H = b_1 b_2 \dots b_n$ and $H' = b'_1 b'_2 \dots b'_n$. $(\sigma(C), \sigma'(D))(\sigma(c_1), \sigma'(d_1)) \dots (\sigma(c_i), \sigma'(d_i)) \dots (\sigma(c_n), \sigma'(d_n))$ is a resulting confused encoded plaintext generated by using the permutations $\sigma : C \rightarrow C$ and $\sigma' : D \rightarrow D$ such that $\sigma(c_i) = c_{b_i}$ and $\sigma'(d_i) = d_{b'_i}$.

2.3.1 Ciphertext

Transmit the confused sequence $\sigma(C)$ as a ciphertext of the plaintext T .

2.3.2 Secret Keys

The integers h, h' and k , the weight function w and the encoded sequence $\sigma'(D)$ are the secret keys of our encryption scheme. The integers h, h' and k are used to get the representation of symbols in S , the weight function w is used to get the index of the symbols in the plaintext, and the sequence $\sigma'(D)$ is used to get w .

Note that for a given β , the proposed scheme can encrypt a plaintext across a symbol set S of size at most $|Q_{h=1, h'=\beta}|$, i.e., for the proposed scheme it holds that $m \leq |Q_{h=1, h'=\beta}|$. Furthermore, the proposed scheme can encrypt a plaintext T of any arbitrary size, since it encodes each symbol of T individually.

2.3.3 Decryption Procedure

Assume the sender and receiver are connected by a noise-free channel, allowing the receiver to receive the ciphertext. $G = \sigma(c_1)\sigma(c_2)\dots\sigma(c_n)$. Let g be the ℓ -th element of G . We find the position of g in the plaintext by using the keys $\sigma'(D) = \sigma'(d_1)\sigma'(d_2)\dots\sigma'(d_n)$ and weight function as follows. Compute a real $d \in \sigma'(D)$ such that

$$g + d = r + 1, \tag{2.3.3}$$

for some $r = w(i) \in [-1, 1]$ with $i \in [1, n]$. Observe that for each g such a real d always exists by Eq. (2.3.2). The position of the element of the plaintext is integer i , corresponding to the element g of the ciphertext. By using the secret key h , compute the restricted Pell sequence $Q_{h, h'}$ and compute the inverse $\psi_k^{-1} : S \rightarrow S$ defined as

$$\psi_k^{-1}(S(i)) = S((i - k) \pmod{m}), \tag{2.3.4}$$

of the permutation by using the secret key k .

Figure 2.1 provides a flowchart of the proposed scheme.

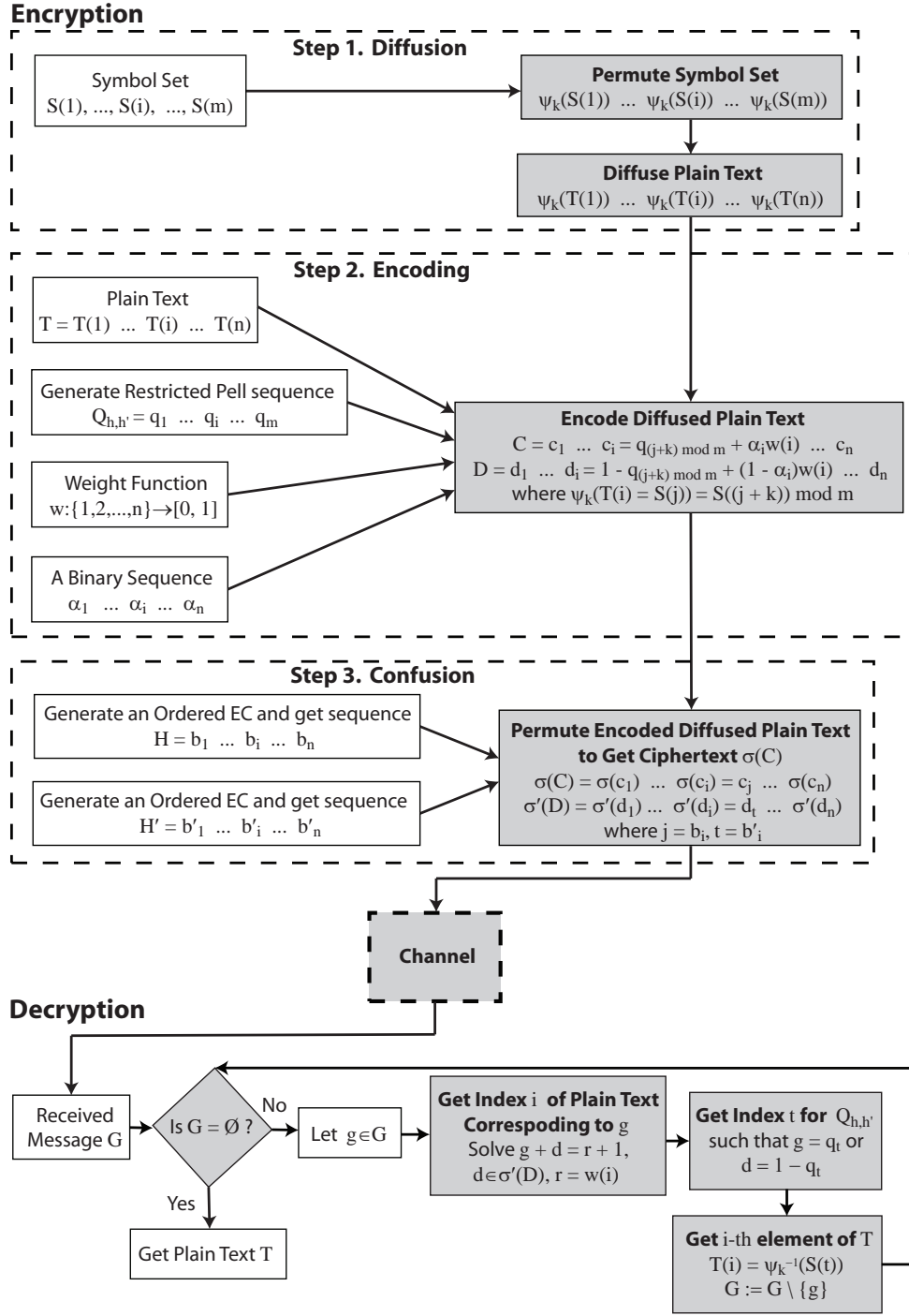


Figure 2.1: Flowchart of the proposed encryption and decryption scheme.

To get the plaintext $T(i)$ at the i -th position of the plaintext T , find the real $q_t \in Q_{h,h'}$

such that $g = q_t$ or $d = 1 - q_t$ for some index t . Find the index t by using Table 2.1 and finally get the i -th plaintext $T(i)$ as $T(i) = \psi_k^{-1}(S(t))$ corresponding to the ℓ -th element g of G . We obtain T by repeating the above procedure for each $g \in G$.

In Example 2.3.1, we provide a complete demonstration of the proposed procedures.

Example 2.3.1. Encryption *Let the ordered symbol set S be the set of the capital English alphabet including blank-space and full-stop. This set is listed in the fourth column of Table 2.1. Let $\beta = 14$, and for $h = 18$ and $h' = 22$, the entries q_i of the restricted Pell sequence $Q_{h,h'}$ are listed in the second column of Table 2.1, while the third column of Table 2.1 contains $1 - q_i$. Select integer $k = 6$ to generate a permutation $\psi_{k=6}$ on the symbol set S . The entries of $\psi_{k=6}$ are listed in the fifth column of Table 2.1.*

Suppose the sender wants to send the plaintext $T = \text{STAY SAFE}$ with nine elements.

For each integer $i \in [1, 9]$, Table 2.2 enlists the original, diffused and encoded plaintexts, T , $T'(i)$ and (c_i, d_i) . Table 2.3 contains the sequences H' and H generated by ordered ECs $E_{11,0,4}$ and $E_{11,0,9}$ using diffusion and natural orderings. Moreover, Table 2.4 presents confused encoded plaintext $\sigma'(D)$ and $\sigma(C)$.

Table 2.1: Entries $S(i)$, $\psi_{k=6}(S(i))$, and q_i of an ordered symbol set S , the permuted symbol set $\psi_{k=6}(S)$, and the restricted Pell sequence $Q_{h=18, h'=22}$, respectively

Index i	q_i	$1 - q_i$	$S(i)$	$\psi_{k=6}(S(i))$
1	0.52137	0.47863	A	W
2	0.95725	0.04275	B	X
3	0.29362	0.70638	C	Y
4	0.96103	0.03896	D	Z
5	0.33794	0.66206	E	Space
6	0.77007	0.22993	F	Full-stop
7	0.30634	0.69366	G	A
8	0.06816	0.93184	H	B
9	0.48980	0.51020	I	C
10	0.73249	0.26751	J	D
11	0.68854	0.31146	K	E
12	0.91754	0.08246	L	F
13	0.81868	0.18132	M	G
14	0.83642	0.16358	N	H
15	0.81864	0.18136	O	I
16	0.79073	0.20927	P	J
17	0.39322	0.60678	Q	K
18	0.38890	0.61110	R	L
19	0.92887	0.07113	S	M
20	0.69338	0.30662	T	N
21	0.56639	0.43361	U	O
22	0.56379	0.43621	V	P
23	0.70637	0.29363	W	Q
24	0.85348	0.14652	X	R
25	0.82824	0.17176	Y	S
26	0.83257	0.16743	Z	T
27	0.83183	0.16817	Space	U
28	0.83196	0.16804	Full-stop	V

Table 2.2: Plaintext entries $T(i)$, diffused plaintext entries $T'(i)$, weight function entries $w(i)$, binary sequence entries α_i , and encoded diffused plaintext entries (c_i, d_i) , respectively

Index i	$T(i)$	$T'(i)$	$w(i)$	α_i	Encoded diffused plaintext (C, D)	
					c_i	d_i
1	S	Y	-0.007	1	0.28662	0.70638
2	T	Z	-0.321	0	0.96103	-0.28204
3	A	G	0.4	1	1.21868	0.18132
4	Y	C	-0.49751	0	0.48980	0.01269
5	Space	F	0.8812	1	1.79874	0.08246
6	S	Y	0.163	1	0.45662	0.70638
7	A	G	0.97350	1	1.79218	0.18132
8	F	L	0.65	0	0.38890	1.26110
9	E	K	0.2817	0	0.39322	0.88848

Table 2.3: Permutations due to the ordered ECs $E_{11,0,9}$ and $E_{11,0,4}$ with natural and diffusion ordering, respectively

Index i	1	2	3	4	5	6	7	8	9
Entries b_i of H due to $E_{11,0,9}$	3	8	1	5	6	9	2	4	7
Entries b'_i of H' due to $E_{11,0,4}$	2	1	4	3	7	9	8	5	6

Table 2.4: Entries of $\sigma(c_i)$ and $\sigma'(d_i)$ of the confused plaintext $\sigma(C)$ and $\sigma'(D)$, respectively

Index i	Ciphertext $\sigma(c_i)$	Key $\sigma(d_i)$
1	1.21868	-0.28204
2	0.38890	0.70638
3	0.28662	0.01269
4	1.79874	0.18132
5	0.45662	0.18132
6	0.39322	0.88848
7	0.96103	1.26110
8	0.48980	0.08246
9	1.79218	0.70638

Decryption We demonstrate the decryption procedure for the 5-th element $g = \sigma(c_5) = 0.45662$ of the ciphertext G .

Note that $g + d = r + 1$ holds for $d = \sigma(d_2) = 0.70638$, $r = w(i) = 0.163$ with $i = 6$. This implies that g is the $(i = 6)$ -th element of the plaintext. The real q_t for which it holds that $g = 1 - q_t$ has index $t = 3$ in the third column $Q_{h=18, h'=22}$ of Table 2.1. We get the $(i = 6)$ -th element $T(6) = \psi_k^{-1}(S(3)) = \psi_k^{-1}(Y) = S$ of the plaintext T from the fourth column of Table 2.1.

2.4 Security Analysis and Comparison

For the proposed scheme analysis, we apply some well-known security tests including key spacing analysis, key sensitivity analysis, histogram test, information entropy analysis, ciphertext only and known-plaintext attack. Their results for the proposed scheme are explained in Sections 2.4.1-2.4.4. Furthermore, we give a detailed comparison of the security of the our scheme to a number of the currently developed text encryption schemes in Section 2.4.6.

2.4.1 Key-space Analysis

Key spacing for a cryptosystem is defined as the number of unique secret keys that it can produce. An encryption scheme is secure if its key spacing is at least 2^{100} by [37]. The proposed scheme has five secret keys, three integers k , h , and h' , a weight function w and the sequence $\sigma'(D)$, where the key $\sigma'(D)$ depends on m, h, h', k , and w , by Eq. 2.3.2. There are m choices for k and $(10^\beta)^n$ choices for w , when the plaintext is encoded to real numbers with at most $\beta \geq 14$ digits after the decimal and n is the size of the plaintext. This means that the proposed scheme's key spacing is at least $m(10^\beta)^n > 2^{100}$ for $n \geq 4$, $m \geq 1$ and $\beta \geq 14$. So, the proposed scheme satisfies key spacing analysis. In particular, when computation accuracy is 10^{-14} , $m = 5$, $\beta = 14$ and $n \geq 4$, then there are 88 choices for selecting a pair of integers h and h' such that $h' - h + 1 \leq \beta$ and there exists a restricted Pell sequence. Hence, the key spacing of the proposed scheme in this case is at least $5 \cdot 88 \cdot (10^{14})^4 > 2^{194}$.

2.4.2 Analysis of Key Sensitivity

In the next lemma, we show that for any plaintext our scheme can generate a different ciphertext when any of the secret keys k, h, h' , and w is changed.

Lemma 2.4.1. *For a size n plaintext T over size m symbol set S and $G = \sigma(c_1)\sigma(c_2) \dots \sigma(c_n)$ be a ciphertext of T that is obtained by the proposed scheme using the keys h, k, h' and weight function w .*

- (i) *The ciphertext G' generated by the proposed scheme by using $k' \neq k$, $k' \in [0, m - 1]$, h, h' , and w is not equal to G .*
- (ii) *The ciphertext G' generated by the proposed scheme by using $k, t \neq h$ or $t' \neq h'$ that satisfies conditions of step 2, and w is not equal to G .*
- (iii) *If $\alpha_i = 1$, $i \in [1, n]$, the ciphertext G' generated by the proposed scheme by using k, h, h' , and w' such that $w'(i) \neq w(i)$, for all $i \in [1, n]$, is not equal to G .*

Proof. Let $G' = \sigma(c'_1)\sigma(c'_2) \dots, \sigma(c'_n)$.

(i) The integer $k' \neq k$ used at step 1 of the proposed scheme is to shift the elements of the symbol set S . Then for all $j \in [1, n]$ it holds that $S((j + k') \pmod{m}) \neq S((j + k) \pmod{m})$. This implies that $q_{(j+k') \pmod{m}} + \alpha_i w(i) \neq q_{(j+k) \pmod{m}} + \alpha_i w(i)$ for each $i \in [1, n]$ in Eq 2.3.2, where $T(i) = S(j)$. This implies that $c'_i \neq c_i$ for each $i \in [1, n]$, and hence $G' \neq G$.

(ii) For any integer $t \neq h$ or $t' \neq h'$ that satisfies conditions of Step 2, the restricted Pell sequence $Q'_{t,t'} = q'_1 q'_2 \dots q'_n \neq Q_{h,h'} = q_1 q_2 \dots q_n$, since the length of the elements of $Q'_{t,t'}$ is different from the length of the elements of $Q_{h,h'}$. This implies that $q'_{(j+k) \pmod{m}} + \alpha_i w(i) \neq q_{(j+k) \pmod{m}} + \alpha_i w(i)$ for each $i \in [1, n]$. This implies that $c'_i \neq c_i$, and hence $\sigma(c'_i) \neq \sigma(c_i)$, $i \in [1, n]$, from which it follows that $G' \neq G$.

(iii) Since $w'(i) \neq w(i)$ and $\alpha_i = 1$ therefore $q_{(j+k) \pmod{m}} + \alpha_i w(i) \neq q_{(j+k) \pmod{m}} + \alpha_i w'(i)$ for each $i \in [1, n]$ in Eq 2.3.2, where $T(i) = S(j)$. This implies that $c'_i \neq c_i$, and hence $G' \neq G$. \square

We demonstrate Lemma 2.4.1 with an example by generating ciphertexts for the plaintext $T = \text{STAY SAFE}$ by slightly changing one key and fixing all other keys. The ciphertext for $k = 6, h = 18, h' = 22$, and weight function w is listed in Table 2.2, ordered MEC $E_{11,0,4}$ with diffusion ordering is listed in the first column of Table 2.5. The ciphertext generated by only changing the integer k to 7 following Lemma 2.4.1(i) is listed in the third column of Table 2.5. The ciphertext generated by only changing integer h' to 23 following Lemma 2.4.1(ii) is listed in the second column of Table 2.5. The ciphertext generated by only changing weight function to $w'(i) = w(i) + 10^{-4}$ following Lemma 2.4.1(iii) is listed in the fourth column of Table 2.5. The ciphertext generated by only changing EC $E_{11,0,5}$ parameter b to 5 with diffusion ordering is listed in the fifth column of Table 2.5. From Table 2.5 it is evident that the ciphertext generated by slight changes in the secret keys are totally different. Hence, the proposed scheme satisfies the key sensitivity analysis.

Table 2.5: Different ciphertexts generated by the proposed scheme for a fixed plaintext

Original ciphertext	Effect of h	Effect of k	Effect of w	Ordered EC
0.96103	0.961034	0.34106	0.64013	0.48980
0.28662	0.286624	0.95404	0.28672	1.79218
0.48980	0.489799	0.73249	-0.00761	0.28662
1.21868	1.218677	1.23643	1.21878	1.21868
1.79218	1.792177	1.80992	1.79318	1.79874
0.39322	0.393223	0.38890	0.67502	0.45662
0.38890	0.388903	0.92887	1.03900	0.96103
1.79874	1.798742	1.69988	1.79884	0.38890
0.45662	0.456624	1.12404	0.45672	0.39322

2.4.3 Statistical Analysis

A scheme is secure against statistical attacks if it can generate ciphertexts with uniform histogram and optimal entropy. In the following result, we show that for each plaintext, our scheme can generate a ciphertext with a uniform histogram and optimal entropy.

Lemma 2.4.2. *For any plaintext, there exists at least one weight function w such that the frequency of each element in the generated ciphertext is 1.*

Proof. For a size n plaintext over symbol set S , and $T(i)$, $i \in [1, n]$ be the i -th element of T . Our proof will complete if we show that there exists at least one weight function w such that for any two distinct $i, i' \in [1, n]$ it holds that the $c_i \neq c_{i'}$, where c_i and $c_{i'}$ are generated by Eq. 2.3.2. Let $g_i = q_{(j+k) \pmod{m}}$ for $i \in [1, n]$, where $T(i) = S(j)$, for some $j \in [1, m]$ and $\psi_k(S(j)) = S((j+k) \pmod{m})$. Let $g_{i'}$ be an ordering of g_1, g_2, \dots, g_n such that $g_{i'} \geq g_{i'+1}$ for $i' \in [1, n]$. Let w be a mapping such that $w(i'+1)$ is a real in the open interval $(-1, w(i'))$ and $c_{i'+1} = g_{i'+1} + w(i'+1)$ for $i' \in [1, n]$. Note that w is an injection since $w(i') > w(i'+1)$ for each $i' \in [1, n-1]$. Furthermore, for each $i' \in [1, n]$ it holds that $g_{i'} + w(i') > g_{i'+1} + w(i'+1)$, since $g_{i'} \geq g_{i'+1}$ and $w(i') > w(i'+1)$ for each $i' \in [1, n]$. This implies that $c_{i'} > c_{i'+1}$

for each $i' \in [1, n]$, and hence $c'_1 c'_2 \dots c'_n$ is a strictly decreasing sequence. This implies that $\sigma(c_i) \neq \sigma(c_j)$ for each distinct $i, j \in [1, n]$ from which the proof follows. \square

By Lemma 2.4.2, it follows that for each plaintext, the proposed scheme can generate a ciphertext with uniform histogram and optimal entropy by using the weight function w constructed in Lemma 2.4.2 and $\alpha_i = 1$ for each i . Hence the proposed scheme has provable security against statistical attacks. We demonstrate the claim in Lemma 2.4.2 in Table 2.6 by generating a ciphertext for the plaintext $T = \text{STAY SAFE}$ with secret keys $k = 6, h = 18, h' = 22$, ordered ECs $E_{11,0,4}$ with diffusion ordering and weight function w listed in Table 2.6.

Table 2.6: A ciphertext generated by the proposed scheme with uniform histogram and optimal entropy

Index i	Weight $w(i)$	Ciphertext $\sigma(c_i)$
1	-0.49751	-0.20389
2	-0.321	0.64003
3	-0.007	0.81168
4	0.163	0.65280
5	0.2817	1.19924
6	0.4	-0.10038
7	0.65	1.46868
8	0.8812	1.27010
9	0.97350	0.67492

2.4.4 Known-plaintext Attack

In our scheme, the attacker tries to generate h, h', k, w and $\sigma(D')$. The plaintext consists of symbols in S and the ciphertext consists of real numbers with at most β digits after the decimal in our scheme, and therefore there is no relationship between the plaintext and the keys h, h', k and w . Recall that $w(i) \in [-1, 1]$, and therefore it is not necessary that $h' - h + 1$

is at most the minimum number of digits after the decimal in the ciphertext. Thus, the attacker needs to try all possibilities for h, h' such that $h' - h + 1 \leq \beta$ and there exists a restricted Pell sequence of the size $|S|$, and k to know the representation of symbols in S , the weight function w to know the index of the symbols in the plaintext, and $\sigma(D')$ which depends on the latter keys. Furthermore for a given plaintext the presented scheme can generate a completely different ciphertext when keys are changed, as discussed in Section 2.4.3. The suggested system is hence extremely secure against known-plaintext attack by [61].

2.4.5 Ciphertext only Attack

In the proposed scheme, without the proposed scheme's secret keys, the cryptanalyst cannot decipher the plaintext.

Furthermore, there are at least 2^{100} keys for a fixed plaintext of size at least 4, as discussed in Section 2.4.1, and therefore the brute-force attack requires lots of time to decrypt the ciphertext without keys. Hence by [61] the proposed scheme is secure against ciphertext only attack.

2.4.6 Security Comparison

This scheme has five secret keys, the three integers h, h' and k , the weight function w , and the encoded sequence $\sigma'(D)$. The secret key depends on $\sigma'(D)$ the choice of h, h', k, w and the plaintext. The main purpose of $\sigma'(D)$ is to get the weight value $w(i)$, and hence the index i when $\alpha_i = 0$. However, if $\alpha_i = 1$ for all i , then the weight $w(i)$ are in the ciphertext by Eq. 2.3.2, and therefore the key $\sigma'(D)$ is not necessary to get the weight function. More precisely, when $\alpha_i = 1$ for all i , we solve Eq. 2.3.3 for $d = 1 - q_i$, where $q_i \in Q_{h,h'}$ to get w . This implies that in the case of $\alpha_i = 1$ for all i , k, h, h' and w are sufficient keys to decrypt a ciphertext. Note that these keys are independent of the plaintext. Also, the proposed scheme satisfies key sensitivity, spacing analysis, ciphertext-only attack, statistical analysis, and known-plaintext attack for the case of $\alpha_i = 1$ for all i as discussed in Sections 2.4.1-2.4.4.

We compared the security strength of the proposed scheme when $\alpha_i = 1$ for all i , the case where all secret keys are independent of the plaintext, and the schemes in [6–8, 38, 41, 42, 44, 45, 56–59, 61, 65] against sensitivity, spacing analysis, ciphertext-only attack, statistical analysis, and known-plaintext attack. In the Table 2.7, we write No (resp. NA) if the corresponding scheme is not secure (resp. the analysis of the scheme is not available.) From Table 2.7 observe that the security of the schemes in [6–8, 38, 41, 42, 44, 45, 56–59, 61, 65] is suspected against these analysis. Therefore from Sections 2.4.1-2.4.4, the scheme is highly secure among all schemes mentioned above.

Table 2.7: Security comparison between different schemes

Method	High key spacing	Provable key sensitivity	Provable security against statistical attack	Secure against ciphertext only attack	Secure against known-plaintext attack
Ref. [6–8, 38, 41, 44, 45, 65]	NA	No	No	NA	NA
Ref. [42]	NA	No	No	Yes	Yes
Ref. [56]	NA	No	No	NA	NA
Ref. [57]	Yes	No	No	Yes	Yes
Ref. [58, 59]	NA	No	No	NA	NA
Ref. [61]	Yes	No	No	Yes	Yes
Proposed scheme	Yes	Yes	Yes	Yes	Yes

2.5 Conclusion

We proposed a secure text encryption scheme. The scheme has three steps, first we diffuse the plaintext by permuting the symbol set to convert the plaintext into a meaningless message. Then, the diffused plaintext is encoded with real numbers based on a weight function, the Pell sequence, and a binary sequence to hide the diffused plaintext. In the third step, the scheme creates confusion in the encoded diffused plaintext by generating permutations over ECs. We analyzed the security of the proposed scheme against several modern attacks including ciphertext-only attack, key sensitivity, spacing analysis, statistical analysis, and known-plaintext attack. From the analysis it is clear that this scheme has high resistance against modern attacks. Furthermore, we compared our scheme's security strength with the existing text encryption schemes in [6–8, 38, 41, 42, 44, 45, 56–59, 61, 65]. It is visible from the comparison that this scheme is more secure than the existing scheme against modern cryptanalysis.

Chapter 3

A Novel Substitution Box

Construction Based on an EC Over a Finite Ring of Integers

3.1 Introduction

In this chapter, we present a new S-box generator that can generate a good S-box based on an EC over a finite ring of integers.

The organization of this chapter is as follows: There is some motivation and relevant work in Section 3.2. The proposed S-box generating scheme is described in Section 3.3. Section 3.4 contains analysis and comparison of the S-box generated by the proposed scheme. Section 3.5 contains a conclusion.

3.2 Motivation and Related work

Recently, S-box-based encryption algorithms have gained special attention [67]. Many authors (see, for example, [68, 69]) have observed that the S-box used to create confusion in the well-

known cryptosystems is vulnerable because a static S-box is used. Furthermore, it also has low algebraic complexity.

In a cryptosystem, an S-box is one of the key component. Therefore, researchers are trying to generate S-boxes which are cryptographically secure. One way is to improve the security of the AES cryptosystem. That is why Cui and Cao [70] enhanced the complexity of an AES S-box in order to protect it from algebraic attacks. Similarly, an improved AES S-box that has reliable security against algebraic and differential attacks is proposed by Liu et al. [71]. Tran et al. [72] presented the Gray S-box for the AES, which is secure against algebraic and interpolation attacks. In addition to this, many other techniques are used to design S-boxes with the desired security. For example, Ibrahim and Alhabi [67] utilized a Henon map for secure and dynamic S-boxes generation. Silva-Garcia et al. [73] designed a unique chaos-based cryptosystem, which generates an S-box to resist linear attacks. Özkaynak [74] proposed robust S-boxes using different chaotic systems. Due to their higher security, EC-based cryptosystems have gained the interest of researchers. Miller [75] presented an EC-based cryptosystem with high security and a small key size. Cheon et al. [76] used hyperelliptic curves to obtain a lower bound on the nonlinearity of Boolean functions. Hayat et al. [27,77] employed ECs over finite fields and rings to design secure S-boxes. It is analyzed that the S-box generators over finite rings generate dynamic S-boxes with reasonable time complexity.

3.3 The Proposed S-box

To construct an S-box, we need the parameters n, b , and t . It is mentioned that $n = \prod_{i=1}^k p_i$, where each p_i is a prime and k is a positive integer. In principle, n may be assigned any value. We choose n as a product of primes because, in the masking phase for each prime p_i , we need the EC over the related prime field \mathbb{F}_{p_i} . The parameters n, b are used to generate the EC $E_{n,b}$ over the ring of integers \mathbb{Z}_n . Here, t is upper bound on y , means we compute such $(x, y) \in E_{n,b}$ for which $y \leq t$. The y -coordinate is kept bounded, so that we compute

$(x, y) \in E_{n,b}$ for all $x \in \mathbb{Z}_n$ and particular values of y instead of all $y \in \mathbb{Z}_n$. This is conducted in order to reduce the time of execution. After the generation of the EC $E_{n,b}$, the points of $E_{n,b}$ need to be arranged by some ordering. The points may be arranged according to any ordering. The ordering \prec_N , however, can produce S-boxes with excellent cryptographic features. Therefore, we use \prec_N to sort the points of $E_{n,b}$. Then, we construct an $m \times m$ S-box $\sigma(n, t)$ by extracting first 2^m different values $y_i < 2^m$ of the y -coordinate of the ordered $E_{n,b}$. Mathematically, the S-box is generated according to the following function:

$$\sigma(n, t) : [0, 2^m - 1] \rightarrow [0, 2^m - 1]$$

defined by:

$$\sigma(n, t)(i) = y_i,$$

where $(x, y_i) \in E_{n,b}$ for some $x \in \mathbb{Z}_n$ and $\sigma(n, t)(r) \neq y_i$ for $r < i$. The following steps provide a detailed explanation of the S-box construction.

Step 1. To generate an $m \times m$ S-box, select three integers b, n , and t such that $n > 2^m, 0 < b < n$ and $2^m \leq t \leq n$;

Step 2. Choose primes p_i for a finite $k \geq 2$ in such a way that $n = \prod_{i=1}^k p_i$;

Step 3. For each $y \in [0, t]$ and $x \in [0, n-1]$, compute all the points (x, y) such that $y^2 \equiv x^3 + b \pmod{n}$; i.e., compute $E_{n,b}$;

Step 4. If the set $[0, 2^m - 1]$ is contained in the y -coordinates of the points $(x, y) \in E_{n,b}$, then proceed to Step 5. Otherwise, change p_i for some i and repeat Steps 1–3;

Step 5. Arrange the points of $E_{n,b}$ by applying the ordering \prec_N ;

Step 6. Construct the S-box $\sigma(n, t) : [0, 2^m - 1] \rightarrow [0, 2^m - 1]$, such that $\sigma(n, t)(i) = y_i$, where $(x, y_i) \in E_{n,b}$ for some $x \in [0, n-1]$ with the constraint that $y_i < 2^m$ and $\sigma(n, t)(j) \neq \sigma(n, t)(i)$ for $j < i$.

For parameters $n = 2491, p_1 = 47, p_2 = 53, b = 716$, and $t = 255$, generation of an 8×8 S-box by using the proposed algorithm on an EC $E_{2491,716}$ is shown in Table 3.1.

Table 3.1: The S-box $\sigma(2491, 255)$ generated by the proposed algorithm.

29	221	121	55	244	223	215	53	14	115	131	96	11	143	145	238
136	3	181	138	137	248	61	189	140	64	20	182	70	134	124	49
141	50	19	191	164	125	22	179	118	237	202	66	10	167	38	83
40	193	230	234	175	9	159	158	229	34	251	205	249	180	197	81
218	110	195	116	27	150	94	87	157	62	48	226	117	75	217	99
86	1	68	90	165	130	242	163	32	203	72	51	89	235	37	120
113	77	239	188	5	201	162	60	149	192	211	59	161	88	155	6
233	222	106	8	178	245	209	123	204	199	76	153	122	194	184	100
246	228	107	142	26	207	232	104	227	198	73	154	186	172	152	12
57	56	65	58	44	69	46	74	92	101	174	160	82	220	112	200
54	103	253	41	97	4	2	224	231	133	243	236	18	91	206	23
135	177	148	147	213	24	208	129	168	35	169	30	42	144	216	127
241	255	33	95	171	7	109	170	28	247	212	98	225	210	84	31
93	47	219	119	176	108	156	240	166	196	52	36	114	190	67	173
25	71	15	139	128	39	252	151	17	105	78	80	214	254	16	111
43	13	250	85	79	183	45	21	0	146	126	102	63	187	185	132

3.4 Analysis for Evaluating the Strength of S-box

The cryptographic strength of the proposed S-box is analyzed by well-known tests, which are described as follows.

Linear Attacks

A cryptosystem is secure if it can strongly resist attackers to exploit the linear relations of inputs and outputs. The immunity of an $n \times n$ S-box S against linear attacks is evaluated by

its $NL(S)$ [78], $LAP(S)$ [79], and algebraic complexity $AC(S)$ [80].

For a chosen n , the $NL(S)$ represents the minimum Hamming distances between the S-box S and all the corresponding affine functions. Similarly, the $LAP(S)$ is the approximation of the relation lying between the inputs and outputs, and the $AC(S)$ represents the number of non-zero terms in the polynomial representation of the S-box S . The resistance of an S-box against $LAP(S)$ and $NL(S)$ is measured by 1.2.1 and 1.2.2, respectively.

The resistance to linear attacks is greater if the $LAP(S)$ is low, the $NL(S)$ is close to $2^{n-1} - 2^{(n/2)-1}$, and the $AC(S)$ tends to $2^n - 1$. For the S-box shown in Table 3.1, 254, 106, and 0.0156 are the values of the NL , AC and LAP , respectively. According to Table 3.2, the suggested S-box is very secure against linear attacks when compared to the S-boxes in [13, 53, 81–86], and comparable with the S-boxes in [74, 77, 87].

Differential Attacks

The $DAP(S)$ [88] measures the strength of an S-box S to thwart the attackers. The S-box S possesses higher security if the $DAP(S)$ is close to $1/2^n$. The DAP value of the S-box measured by 1.2.3, depicted in Table 3.1 is 0.0469. From Table 3.2, it is also evident that the DAP value of the proposed S-box and the S-boxes displayed in [77, 84, 85] is equal, and comparable to the S-boxes in [13, 53, 74, 81–83, 86, 87]. Thus, the presented S-box has comparable strength over differential attacks, against the S-boxes in [13, 53, 74, 77, 81–87].

Table 3.2: Comparison of the S-boxes generated by the proposed algorithm and some recent algorithms.

Scheme	NL	LAP	AC	DAP	SAC (min)	SAC (max)	BIC (min)	BIC (max)
Proposed	106	0.0156	254	0.0469	0.4063	0.5938	0.4688	0.5293
Ref. [53]	106	0.1484	254	0.0234	0.3906	0.6094	0.4727	0.5254
Ref. [86]	106	0.1328	253	0.0391	0.3750	0.5938	0.4688	0.5254
Ref. [81]	104	0.0469	254	0.0391	0.4063	0.6250	0.4668	0.5234
Ref. [82]	101	0.0664	254	0.0391	0.4219	0.5781	0.4668	0.5195
Ref. [83]	104	0.0625	253	0.0391	0.4219	0.5938	0.4766	0.5391
Ref. [84]	100	0.0391	253	0.0469	0.4063	0.6094	0.4473	0.5332
Ref. [74]	106	0.0703	255	0.0391	0.3906	0.6094	0.4707	0.5332
Ref. [85]	102	0.0781	254	0.0469	0.4219	0.6406	0.4766	0.5332
Ref. [13]	104	0.1328	253	0.0391	0.4063	0.5938	0.4668	0.5430
Ref. [77]	106	0.148	255	0.0470	0.4063	0.6250	0.4710	0.5390
Ref. [87]	106	0.148	254	0.0390	0.4220	0.5940	0.4710	0.5330

Analysis of Boolean Functions

The Boolean functions of an S-box are used to create confusion/diffusion in a cryptosystem. Two approaches, bit independence criterion (BIC) [89], and strict avalanche criterion (SAC) [89] are used to analyze the Boolean functions. An S-box creates enough confusion/diffusion if all off-diagonal entries of $M(S)$ and $B(S)$ are close to 0.5. The minimum (SAC (min)) 1.2.5 and maximum (SAC (max)) of the off-diagonal values of $M(S)$ for the

S displayed in Table 3.1 are 0.4063 and 0.5938, respectively. Furthermore, Table 3.2 reveals that the SAC (min) of the designed S-box is larger and the SAC (max) is less than or equal to the SAC (min) and SAC (max) values of the S-boxes designed in [53, 74, 86] and [53, 74, 77, 86], respectively. So, the S-box in Table 3.1 has a higher confusion-creation capability than the S-boxes in [53, 74, 86]. The Table 3.1 reveals that the proposed scheme generates S-boxes with higher confusion than the schemes in [77, 81, 84]. The SAC values indicate that the confusion-creation capability of the new S-box is equal to the S-box in [13] and comparable to that of [85, 87]. Now, the minimum (BIC (min)) and maximum (BIC (max)) 1.2.4 of the off-diagonal values of $B(S)$ for S in Table 3.1 are 0.4688 and 0.5293, respectively. Table 3.2 reveals that the BIC (min) of the generated S-box is equivalent to the S-boxes in [13, 53, 74, 77, 81–87], and the BIC (max) of the current S-box better than that of the S-boxes in [13, 74, 77, 83–85, 87]. Thus, the proposed scheme generates S-boxes with diffusion-creation capabilities comparable to the S-boxes in [13, 53, 74, 77, 81–87].

3.5 Conclusion

We proposed a new S-box generator by employing an EC over a ring of integers. The comparison between the S-boxes formed by the ECs over finite fields in [13, 53, 86] and the S-boxes in [81–85] shows that the given S-box is highly resistant to linear attacks. The confusion-creation capability of the newly constructed S-box is higher than that of the S-boxes in [53, 74, 86].

Chapter 4

A Novel Image Encryption Scheme Based on Elliptic Curves over Finite Rings

4.1 Introduction

The proposed encryption scheme requires an S-box generator to obtain the desired level of confusion. This chapter contains the proposed image encryption algorithm using the cryptographically strong S-box generator, constructed in 3. Unlike the case in [13, 53, 90], each input image does not need the computation of a new EC for the confusion phase. It can encrypt a number of images with better security against differential, statistical, key and plain-text attacks and the run-time of the proposed scheme to encrypt color images is very low.

The remaining chapter is organized in the following manner: Section 4.2 contains the related work and motivation of new scheme. Section 4.3 presents the proposed image encryption scheme. In Section 4.4, the decryption procedure is reported. The security analysis is conducted in Section 4.5. Lastly, the conclusion is drawn in Section 4.6.

4.2 Related work

In this modern era, the transmission of images over public networks is an indispensable task. Therefore, distributing secret images in a secure way is essential. Encryption schemes take plain-text data as an input and convert it into an unreadable form using secret keys. Then, an authorized person uses the secret keys to acquire the original data. Furthermore, the pixels have high correlation and the data size is large in an image. Many approaches, such as fuzzy theory [37] and chaotic maps [91–102], are used to develop encryption schemes.

Due to their simplicity of implementation and speed of execution, chaos-based systems have recently gained more attention [103]. Moreover, chaotic maps have certain distinctive qualities that make them ideal for use in cryptosystems, like unpredictable behavior, ergodicity, sensitivity to initial parameters, and randomness [104]. Therefore, several image encryption algorithms are put forth that are based on cat maps [105], sine maps [106, 107], and other chaotic maps [108].

Ye et al. [109] designed an effective and secure image cryptosystem based on the RSA technique and a fractional-order chaotic system. On the other hand, there exist chaotic encryption schemes which are not secure. Elliptic curves (ECs), like chaotic maps, are extremely sensitive to the initial parameters, and several EC-based algorithms have been constructed [10, 15, 52, 53, 75, 87, 110–118].

Abdelfatah [52] used the group law for a digital signature scheme and the generation of a public key and encrypted digital images with the combination of chaotic system and elliptic curve cryptography (ECC) is presented by Zhang and Wang [112]. Abbas et al. [113] proposed a chaotic encryption algorithm using an addition operator over the points of the EC. El-Latif et al. [51] used an EC-based sequence and a chaotic sequence combination to generate a keystream for encryption. Toughi et al. [54] generated keys of encryption algorithm with a sequence of numbers, using ECs. Hayat et al. [13] developed a twofold image encryption scheme over EC. Reyad et al. [119] modulated random sequences using ECs and chaotic maps. It is experimentally proved that all the above schemes are highly secure. In addition, ECs

provide more security to a cryptosystem than chaotic maps [120, 121], but it is important to mention that the scheme in [51] first generates a sequence of scalars. Each scalar is then mapped to a scalar multiple of a point of a cyclic EC. To compute a scalar multiple of a point lying on an EC is not simple; it involves the group law, consisting of many complex calculations. Due to the group law usage, the schemes of [51, 52, 112, 113, 115, 119] time-consuming. To generate ECs, the method in [13] ignores the group law, however each plain image demands the construction of two ECs. Moreover, trials are required for the generation of ECs to ensure the encryption of an image because the said scheme does not output an S-box for all parameters. These facts slow the execution time of the scheme. The algorithm in [53] does not create triads for all the same size images but generates an EC for each image, which enhances the execution time. In all the above-discussed EC-based schemes, finite fields are used to obtain the desired security. The security of such cryptosystems based on ECs over finite fields essentially depends on the computational cost for solving the discrete logarithm problem [122]. Diaz et al. [122] pointed out that the ECs over finite rings based cryptosystems are more secure than the ECs over finite fields based cryptosystems. Their claim follows from the fact that the computational cost of breaking such cryptosystems based on ECs over finite rings depends on fixing the discrete logarithm problem and the factorization problem [16]. Our research contribution aims to develop a cryptosystem that is based on a ring of integers and that has higher resistance against modern attacks than the existing schemes of ECs over finite fields.

4.3 The Proposed Encryption Scheme

Suppose we want to encrypt an image I of size $u \times v$ over the symbol set $[0, 2^m - 1]$, and $I(i, j)$ represents the pixel lying at the intersection of the i -th row and the j -th column. Furthermore, for the sum of all pixel values of I denoted by \mathcal{S}_I , the proposed encryption scheme consists of the following steps.

4.3.1 Generation of Keys

To encrypt an image of size $u \times v$, we need to generate an EC $E_{n,b}$, over a ring \mathbb{Z}_n , for $n = \prod_{i=1}^k p_i$. For the sake of convenience, we take $k = 2$ and $n \geq uv$, so that we choose primes p_1, p_2 and integers $b, t \in \mathbb{Z}_n$ to generate $E_{n,b}$. Thus, p_1, p_2, b and t are chosen in such a way that there exists at least uv points $(x, y) \in E_{n,b}$, where y is attaining each value in the interval $[0, 2^m - 1]$. This condition is imposed to ensure the S-box construction using points of the EC $E_{n,b}$. We further choose an integer value ℓ_1 as a key. The use of the key ℓ_1 is explained in Section 4.3.4(i). The parameters p_1, p_2, b, t , and ℓ_1 are all secret keys.

4.3.2 Masking Phase

Before masking an image I , we first arrange the points of the EC $E_{n,b}$ according to the ordering \prec_D . After ordering, we assume that $(x_i, y_i) \in E_{n,b}$ stands for the i -th point of the EC $E_{n,b}$. The reason for this is that the \prec_D diffuses the y -coordinates of the points, because, over a ring of integers \mathbb{Z}_n , if $(x, y) \in E_{n,b}$, then, for such an x , there are at least two values y_1, y_2 of y in \mathbb{Z}_n , such that $(x, y_1), (x, y_2) \in E_{n,b}$. The masking phase of an image I takes place as follows:

- (i) Generate a row matrix M from $(x_i, y_i) \in E_{n,b}$ of length $2(\#E_{n,b})$ such that, for $1 \leq i \leq \#E_{n,b}$, we have:

$$M(j) = \begin{cases} x_i, & \text{if } j \text{ is odd} \\ x_i + y_i, & \text{otherwise} \end{cases}$$

The purpose of constructing matrix M is to design a sequence from both coordinates of $E_{n,b}$. The elements of the said sequence are used to hide the pixel values of an image I ;

- (ii) Choose a submatrix N , which consists of the first uv entries of the matrix M because only the uv values are needed to hide the pixel values. The chosen n should not be less than uv ; otherwise, in Section 4.3.3(i), the construction of M_2 with size $u \times v$ will not

be possible;

- (iii) The sensitivity to the plain image is necessary for a secure cryptosystem. For this purpose, transform the entries of N by the pixel value $I(1, 1)$ to obtain the matrix B , given by:

$$B(i) = N(i) + I(1, 1). \quad (4.3.1)$$

There is no restrictions on pixel or the number of pixels. Any number of arbitrary pixels may be used for transformation. For the sake of convenience, only one pixel value $I(1, 1)$ is fixed;

- (iv) For the sake of simplicity, reshape the matrix B to construct a matrix with u rows and v columns. By reshaping B , we mean that B is divided into v blocks such that each block contains u entries and the i -th block represents the i -th column of the matrix B , so that the corresponding values of both B and I are combined to hide the pixel values of the image I ;

- (v) To obtain the masked image M_I , mask the pixels of image I using Equation (4.3.2):

$$M_I(i, j) = I(i, j) + B(i, j) \pmod{2^m}. \quad (4.3.2)$$

Since there is a one–one correspondence between $E_{n,b}$ and $E_{p_1,b} \times E_{p_2,b}$, $E_{n,b}$ may be mapped onto $E_{p_1,b}$ and $E_{p_2,b}$, respectively, via the following maps:

$$(x, y) \rightarrow (x \pmod{p_1}, y \pmod{p_1}), \quad (4.3.3)$$

$$(x, y) \rightarrow (x \pmod{p_2}, y \pmod{p_2}). \quad (4.3.4)$$

These two ECs, $E_{p_1,b}$ and $E_{p_2,b}$, are used to alter the pixels of an image. The S-box generated on $E_{n,b}$ is used to create the confusion in the encrypted image. The steps of the said procedure are explained in the following phase.

4.3.3 Diffusion Phase

The steps of this phase are explained as follows:

- (i) For $1 \leq i \leq \#E_{n,b}$, construct two row matrices, $M_k, k = 1, 2$, due to the all points $(x_{ik}, y_{ik}) \in E_{p_k, b}$ for both primes $p_k, k = 1, 2$, respectively, such that:

$$M_1(j) = \begin{cases} x_{i1}, & \text{if } j \text{ is odd} \\ x_{i1} + y_{i1}, & \text{otherwise,} \end{cases}$$

and:

$$M_2(j) = y_{i2}.$$

In fact, we want to generate two sequences using ECs $E_{p_1, b}$ and $E_{p_2, b}$. Both sequences consist of integer values, which are further used to alter the pixel values of the masked image M_I in Section 4.3.3(v) and to permute the image P in Section 4.3.4(iii), respectively;

- (ii) Take submatrices $N_k, k = 1, 2$ containing the first uv entries of $M_k, k = 1, 2$, respectively, so as to choose the sequences of length that are equal to that of the number of pixels in the image I ;
- (iii) Modify the sizes of above constructed matrices, so that $N_k, k = 1, 2$ has u rows and v columns. The reason for generating such matrices has been explained previously;
- (iv) Apply the modulo 2^m operator to $N_k, k = 1, 2$ to generate the matrices $B_k, k = 1, 2$, consisting of m -bit integers. Since for encrypting m -bit images, m -bit sequences are needed;
- (v) Convert the elements of M_I and $B_k, k = 1, 2$ into the binary format and generate the

image X_1 by diffusing the pixels of M_I by the following equation:

$$X_1(i, j) = M_I \oplus B_1(i, j), \quad (4.3.5)$$

where \oplus is a logical operator (XOR operation by binary bit) known as exclusive disjunction.

4.3.4 Confusion Phase

For a secure cryptographic algorithm, it is necessary to have a desired level of confusion. For the current cryptosystem, the confusion phase consists of the following steps:

- (i) Choose a secret key ℓ_1 to construct a shifting parameter ℓ_2 , such that $\ell_2 = \mathcal{S}_I + \ell_1 \pmod{2^m}$; then, give a circular shift to the S-box $\sigma(n, t)$ to design a new S-box $\sigma(n, t, \ell_2)$. The shifting parameter, the secret key ℓ_1 , and \mathcal{S}_I are linked in order to enhance the sensitivity to the plain image I ;
- (ii) Permute the pixels of the image X_1 using the S-box $\sigma(n, t, \ell_2)$ as follows:

$$P(i, j) = \sigma(n, t, \ell_2)X_1(i, j). \quad (4.3.6)$$

In the coming encryption of 4×4 hypothetical image, the first entry of X_1 is 2. Then, $\sigma(n, t, \ell_2)(2)$ represents the third entry of the S-box $\sigma(n, t, \ell_2)$, which is 1. That is, $\sigma(n, t, \ell_2)(r)$ stands for the $(r + 1)$ -th element of the S-box $\sigma(n, t, \ell_2)$;

- (iii) In order to obtain the scrambled image X_2 , repeat Section 4.3.3(v) using P in place of M_I , and replacing $B_1(i, j)$ with $B_2(i, j)$, such that:

$$X_2(i, j) = P \oplus B_2(i, j); \quad (4.3.7)$$

- (iv) Finally, to obtain the encrypted image C with the desired level of confusion, permute

the image X_2 as follows:

$$C(i, j) = \sigma(n, t, \ell_2)X_2(i, j). \quad (4.3.8)$$

The flowchart of the proposed encryption scheme is shown in Figure 4.1. We theoretically

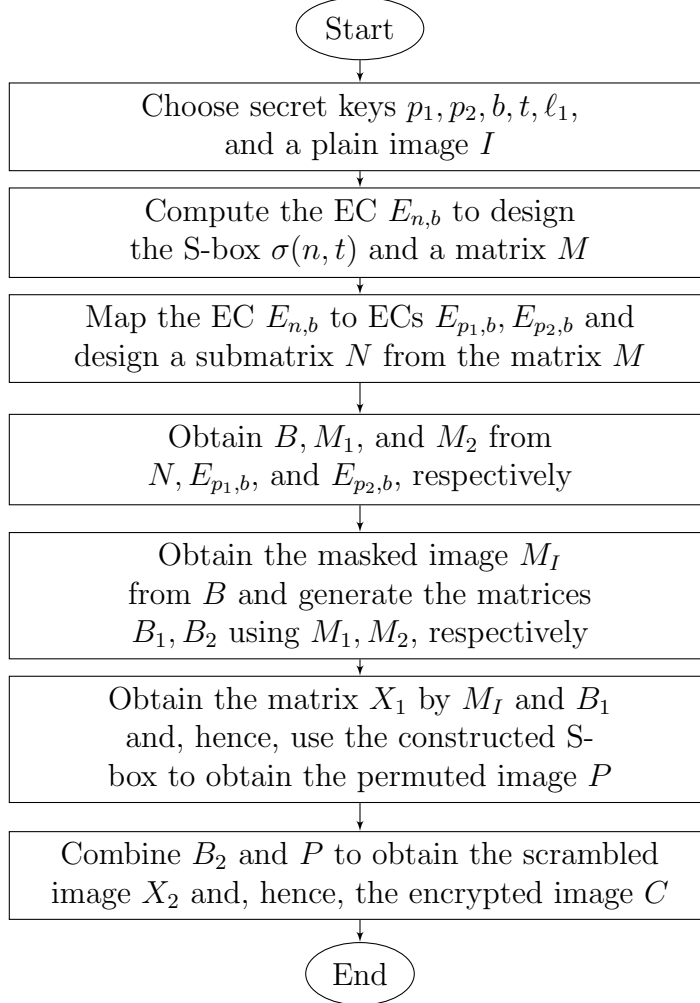


Figure 4.1: Flowchart of the encryption scheme.

derive the presented scheme's run-time complexity in Theorem 4.3.1.

Theorem 4.3.1. *Let I be a plain image of size $u \times v$, and let $n \geq uv$ be a positive integer; then, for the proposed scheme, $\mathcal{O}(\max\{nt, (\#E_{n,b}) \log(\#E_{n,b})\})$ is the time complexity, where $t \leq n$ is an integer such that $E_{n,b}$ is computed for all $x \in [0, n - 1]$ and $y \leq t$.*

Proof. In the key generation phase (Section 4.3.1), to compute all $(x, y) \in E_{n,b}$, we need to check for each $x \in [0, n - 1]$, t values of $y \in [0, t - 1]$, such that $y^2 \equiv x^3 + b \pmod{n}$. Thus, the computation of $E_{n,b}$ takes $\mathcal{O}(nt)$ time. Further, the ordering of the points of the EC $E_{n,b}$ needs $\mathcal{O}((\#E_{n,b}) \log(\#E_{n,b}))$ time. In Section 4.3.2(i), we can see that $\#M = 2(\#E_{n,b})$; therefore, M can be constructed in $\mathcal{O}(n)$ time. As $\#N = \#B = uv$, we can design N, B by a for loop, executing uv times. Furthermore, B can be reshaped by two nested loops, such that one loop executes u times, while the other executes v times. In a similar way, we can add two matrices of the same order by two nested loops. Thus, the time complexity of Section 4.3.2(ii)–(v) is $\mathcal{O}(uv)$. From the chosen keys, we have $n \geq uv$ and $\#E_{n,b} \leq n$, so that the complexity of the masking phase is $\mathcal{O}(\max\{nt, (\#E_{n,b}) \log(\#E_{n,b})\})$.

Now, we can map the EC $E_{n,b}$ on the ECs $E_{p_1,b}, E_{p_2,b}$ in $\mathcal{O}(n)$ time. In the diffusion phase (Section 4.3.3(i)), $\#M_k = 2(\#E_{n,b})$ and $\#N_k = \#B_k = uv$ for $k = 1, 2$. Therefore, Section 4.3.3(i)–(v) takes $\mathcal{O}(\#E_{n,b})$ and $\mathcal{O}(uv)$ time, respectively.

In the confusion phase (Section 4.3.4(i)), the time required to compute \mathcal{S}_I is $\mathcal{O}(uv)$ and ℓ_2 can be computed in constant time. Since X_1 has uv entries, we can implement Section 4.3.4(ii)–(iv) in $\mathcal{O}(uv)$ time, using two nested loops executing u and v times, respectively.

Clearly, $nt > n$ and $n \geq uv$; thus, the above discussion implies that the time complexity for the presented scheme is $\mathcal{O}(\max\{nt, (\#E_{n,b}) \log(\#E_{n,b})\})$. \square

As the time complexity is dependent on the parameter t , that is, the time is controllable with t , the current scheme is effective, particularly when a large dataset of images is to be encrypted.

The whole process is illustrated by the encryption of a 4-bit hypothetical image, as shown in Figure 4.2.

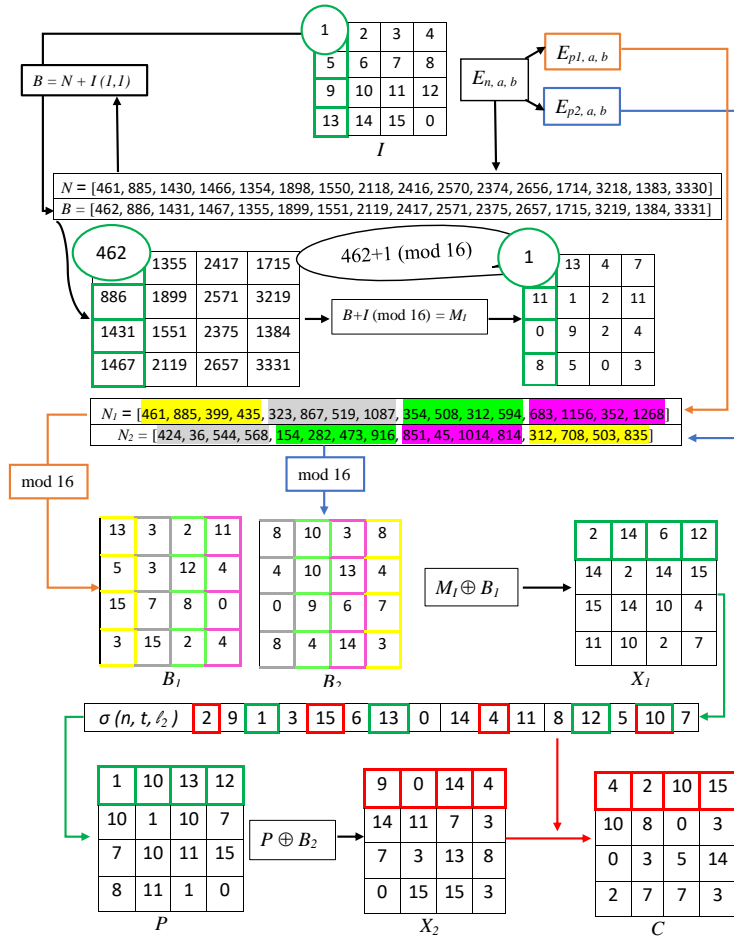


Figure 4.2: Encryption of a 4×4 image by the proposed scheme.

4.4 Decryption

The decryption process takes place by reversing all the encryption process steps. To generate the inverse of the S-box, the receiver will need the keys p_1, p_2, b, t , and $\ell_1 \sigma^{-1}(n, t, \ell_2)$ and the matrices $B_k, k = 1, 2$. Then, by the use of Equations (4.3.1), (4.3.2), and (4.3.5)–(4.3.8), one can obtain the original image I .

4.5 Security Analysis

In this section, some well-known metrics are described, which are generally used to measure the security level of new algorithms. The security of the proposed encryption scheme is evaluated by performing experiments on all-gray images of different sizes, taken from the USC-SIPI database [123] of square images of size $w \times w$, $w = 256, 512, 1024$. The plain images of Lena and Clock, along with their encrypted images, are shown in Figure 4.3. The experiments are performed by taking the parameters $p_1 = p_2 = 1031, b = 7, t = 1031^2$ and $\ell_1 = 80 - \mathcal{S}_I$, using MATLAB 2016a on a personnel machine equipped with a 6 GB RAM, Windows 10 operating system, and 1.8 GHz processor. The security strength of the encryption algorithm is analyzed in the following subsections.

4.5.1 Differential Attacks Analysis

Two metrics are used to assess a cryptographic scheme's resistance against differential attacks: the unified average changing intensity (UACI) and the number of pixels' change rate (NPCR). In an encryption algorithm, the change of one pixel of a plain image has an influence on the encrypted image. The NPCR is a criterion used to measure the influence of a change in a plain image on the ciphers. The UACI criterion measures the average intensity difference between two different images.

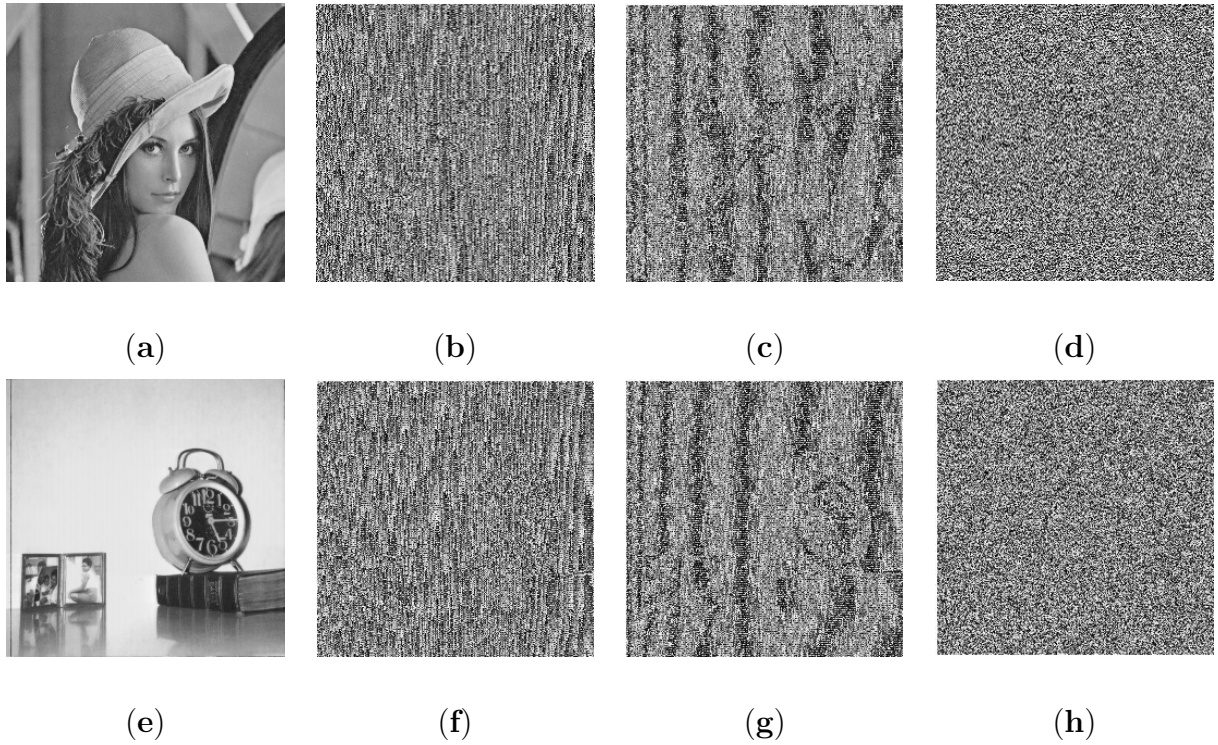


Figure 4.3: (a,e) Plain images; (b,f) masked images; (c,g) diffused images; (d,h) encrypted images of Lena and Clock, respectively.

If I and I' are any two plain images of the same dimension $u \times v$, and C_I and $C_{I'}$ are the respective cipher images of I and I' . For 8-bit images with $w = 256, 512, 1024$, the theoretical values of NPCR calculated by Equation (1.2.9), are 99.5693, 99.5893, 99.5994, respectively. Unlike NPCR, the expected ranges of UACI calculated by Equation (1.2.8), are [33.2824, 33.6447], [33.3730, 33.5541], and [33.4183, 33.5088], respectively [95]. We randomly choose i and j , and a random value is assigned to the pixel $I(i, j)$ for each image I of the database. The random values of i, j and $I(i, j)$ for images of size $w = 256$ are shown in Figure 4.4(a). Then, the UACI and NPCR results for the proposed algorithm are computed for each image; shown in Figure 4.4(c,d), where the average values of UACI and NPCR are 33.32 and 99.60, respectively.

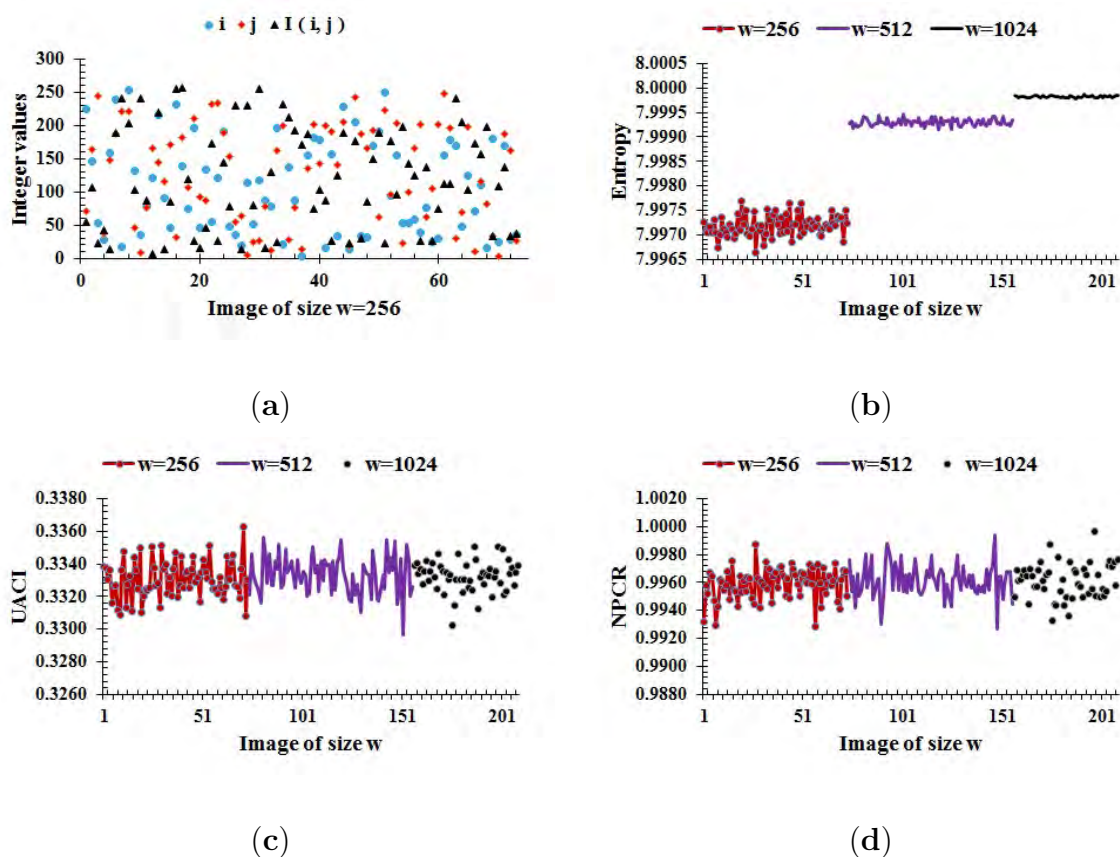


Figure 4.4: (a) Random values of i, j and $I(i, j)$; (b–d) for the whole image database, entropy, UACI, and NPCR results, respectively.

Also, After changing one pixel of some images, compared the results of both tests with the results of the recent schemes in [13, 90–95, 106, 124, 125], as shown in Tables 4.1 and 4.2, respectively. It follows that the proposed scheme has better performance against differential attacks than the schemes in [13, 90–94, 106], and has comparable performance to the schemes in [95, 125].

Table 4.1: Comparison of NPCR results due to the proposed algorithm and some other schemes, where the bold value shows that the corresponding image passed the test.

File Name	Proposed	Ref. [125]	Ref. [91]	Ref. [106]	Ref. [92]	Ref. [93]	Ref. [94]	Ref. [95]	Ref. [90]	Ref. [13]	Ref. [124]
5.1.10	99.5911	99.6095	99.6353	99.6154	99.5513	99.5803	99.6459	99.6397	99.6094	99.6399	99.61
5.1.11	99.6155	99.6133	99.6277	99.6244	99.53	99.6215	99.5803	99.6018	99.5926	99.5605	99.64
5.1.12	99.6292	99.6123	99.5351	99.5703	99.5789	99.6231	99.6154	99.6321	99.6063	99.5972	99.60
5.1.13	99.5972	99.6050	99.617	99.6109	99.2706	99.5971	99.44	99.6351	99.6201	99.6201	99.63
5.1.14	99.6323	99.6210	99.6109	99.6364	99.5986	99.6353	99.5803	99.6063	99.5941	99.6017	99.62
7.1.02	99.6277	99.6117	99.6124	99.6075	99.4747	99.6097	99.5544	99.6584	99.6044	99.6021	99.62
7.1.06	99.6376	99.6064	99.6078	99.6272	99.5506	99.6086	99.5925	99.6291	99.6147	99.6346	99.61
5.3.01	99.6292	99.6095	99.6099	99.5931	99.5977	99.6242	99.6091	99.6128	99.6024	99.6059	99.60
5.3.02	99.6571	99.6095	99.6076	99.6128	99.5534	99.6125	99.6033	99.6159	99.6100	99.6027	99.62
Pass/All	9/9	9/9	8/9	8/9	2/9	9/9	7/9	9/9	9/9	8/9	9/9

Table 4.2: Comparison of UACI results due to the proposed algorithm and some other schemes, where the bold value shows that the corresponding image passed the test.

File Name	Proposed	Ref. [125]	Ref. [91]	Ref. [106]	Ref. [92]	Ref. [93]	Ref. [94]	Ref. [95]	Ref. [90]	Ref. [13]	Ref. [124]
5.1.10	33.3765	33.4663	33.4478	33.3640	30.1968	33.6559	32.4913	33.3592	33.2932	33.2502	33.24
5.1.11	33.4904	33.4554	33.5105	33.5293	31.7477	33.2149	32.9639	33.4603	33.3983	33.3431	33.72
5.1.12	33.5736	33.4604	33.4483	33.3835	33.5818	33.3513	33.4799	33.4650	33.3457	33.2988	33.56
5.1.13	33.4112	33.4601	33.5006	33.4355	40.1144	33.4222	33.5458	33.5112	33.2842	33.3081	33.77
5.1.14	33.5087	33.4606	33.4946	33.4754	30.0463	33.5030	32.6501	33.3569	33.3674	33.2394	33.21
7.1.02	33.3974	33.4563	33.5150	33.5432	29.3539	33.4345	31.9622	33.4765	33.2943	33.2690	33.53
7.1.06	33.4346	33.4515	33.3860	33.5144	29.8338	33.4610	32.3346	33.3988	33.3885	33.3408	33.30
5.3.01	33.4680	33.4511	33.4744	33.4981	32.4783	33.4344	33.0525	33.4723	33.3002	33.3506	33.42
5.3.02	33.4337	33.4536	33.4877	33.4800	30.4249	33.4542	32.6017	33.4906	33.3224	33.3033	33.29
Pass/All	9/9	9/9	9/9	9/9	1/9	6/9	2/9	9/9	6/9	3/9	2/9

4.5.2 Information Entropy

For an 8-bit encrypted image, the ideal value of entropy is 8, which corresponds to the highest level of uncertainty. Thus, for a cryptographically strong encryption scheme, the value of $H(I)$ should be close to 8. The entropy results for the current scheme are computed for each image of the database as shown in Figure 4.4(d). The entropy for images of size $w = 256, 512, 1024$ are lying in the ranges $[7.9966, 7.9977]$, $[7.9991, 7.9995]$, and $[7.9998, 7.99987]$, respectively. In all cases, the entropy approaches the optimal value. Consequently, the proposed encryption scheme is capable of providing high randomness in a cipher.

The comparison of the entropy results is carried out in Table 4.3. It is clear from Table 4.3 that the information entropy for the presented scheme is higher than that of [13, 90, 92–94, 96, 97, 106, 117] and comparable to that of the schemes in [52, 91, 95, 126]. Thus, our scheme generates encrypted images having more randomness than the techniques in [13, 90, 92–94, 96, 97, 106, 117].

Table 4.3: Comparison of entropy results due to the proposed algorithm and some other schemes.

File Name	Proposed	[91]	[106]	[92]	[93]	[94]	[95]	[96]	[97]	[90]	[13]	[117]	[126]	[52]
Lena	7.9994	7.9993	7.9993	7.9634	7.9992	7.9976	7.9994	7.9993	7.9972	7.9993	7.9991	7.9894	7.9993	7.9994
Barbara	7.9993	7.9994	7.9992	7.9667	7.9993	7.9979	7.9993	7.9992	-	7.9991	7.9993	-	7.9993	7.9994

4.5.3 Histogram

A histogram of an image represents the frequency distribution of the gray values. If each pixel value occurs with almost equal frequency in an image, then the histogram of that image is said to be uniform. The histogram of an ordinary image is always highly nonuniform, while a properly encrypted image has a uniform histogram. Figure 4.5(a,c) depicts the histograms of the plain images in Figure 4.3(a,e), respectively, and Figure 4.5(b,d) shows the histograms of the cipher images in Figure 4.3(d,h), respectively.

It is evident from the histograms that the proposed scheme encrypts an image in such a way that it does not reveal any secret information of the former.

4.5.4 Correlation

A good encryption scheme breaks the correlation among the pixels of an encrypted image. The correlation coefficient between two datasets of the same size, x and y , is determined by 1.2.7. The correlation coefficients in all directions of each image in the database encrypted by the proposed scheme are computed as shown in Figure 4.6. The average values of correlation in Figure 4.6(a–d) are -0.00012 , -0.00038 , -0.00026 , and -0.00004 , respectively. Based on

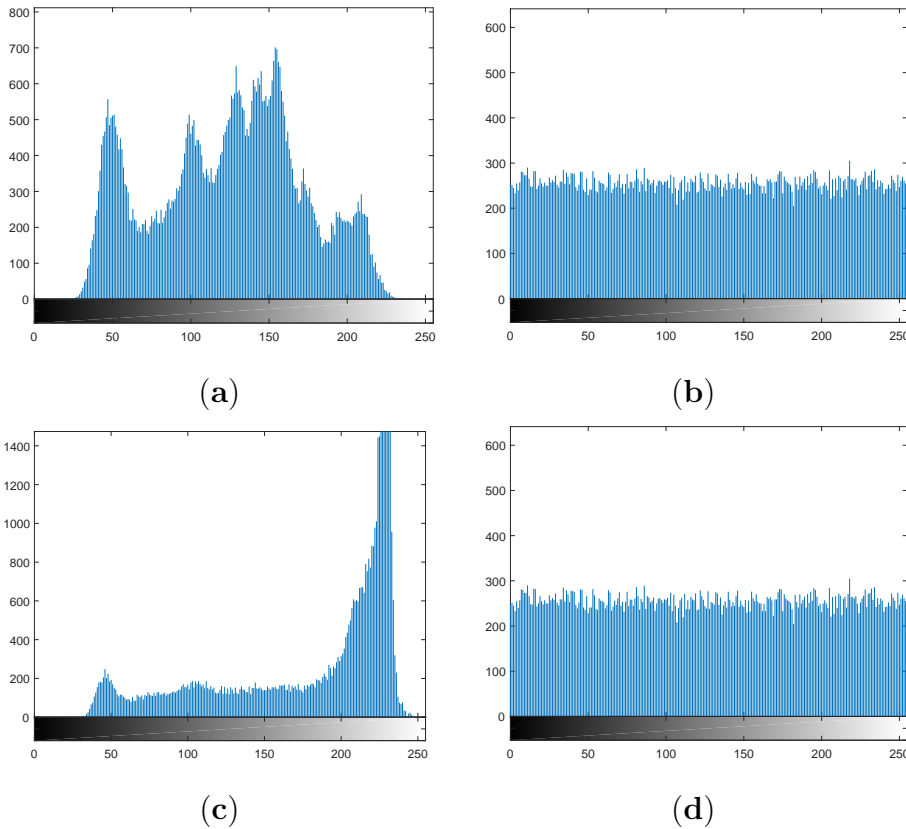


Figure 4.5: Histograms of plain and encrypted images: **(a,c)** histogram of the plain images in Figure 4.3(a,e), respectively; **(b,d)** histogram of the encrypted images in Figure 4.3(d,h), respectively.

these results, the proposed scheme makes the correlation close to zero in all directions. So, the proposed method is capable of disrupting the correlation of pixels in ciphers.

In addition, a random sample of 2560 pairs of pixels is selected along the vertical, horizontal, diagonal, and off-diagonal directions from both the plain image and the cipher image of $\text{Lena}_{512 \times 512}$. The correlation distribution between the adjacent gray values before and after encryption is shown in Figure 4.7.

It follows From Figure 4.7(a–d) that adjacent pixels of the plain image are in high correlation, but Figure 4.7(e–h) indicates that the proposed scheme successfully weakens the correlation of the pixels.

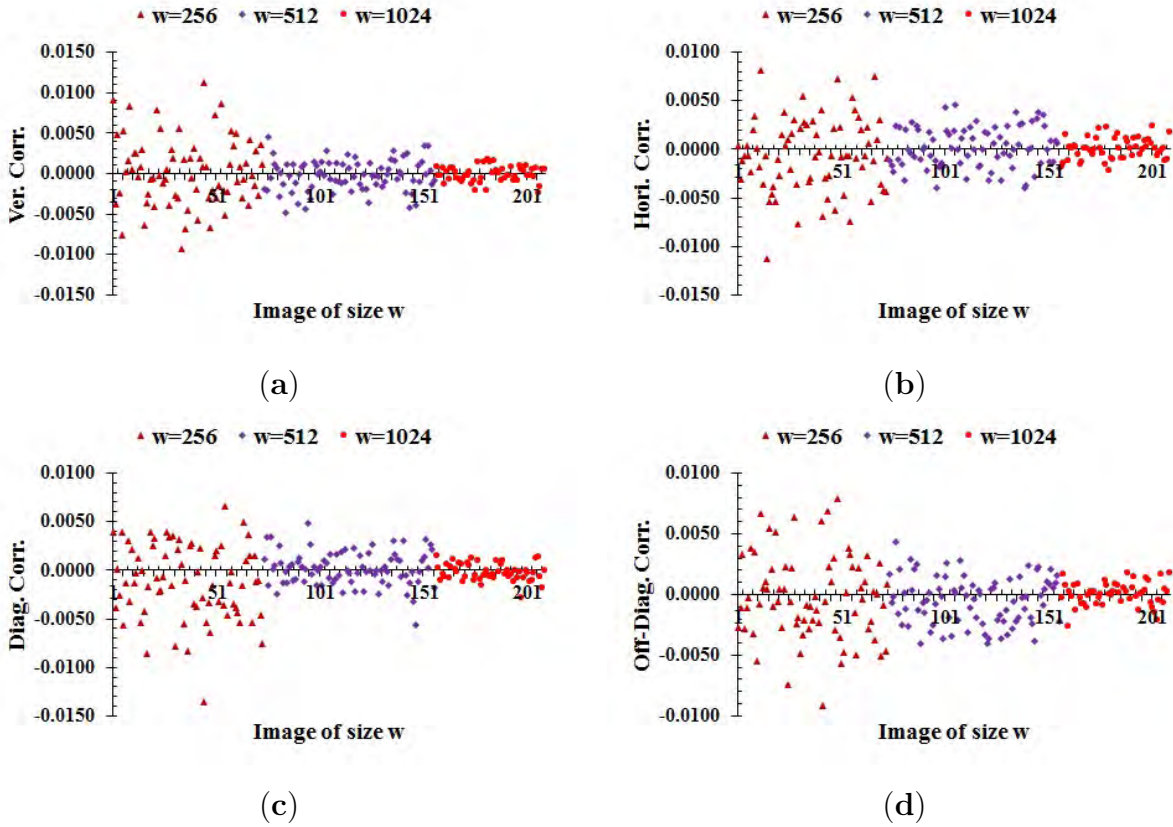


Figure 4.6: Correlation among the adjacent pixels of each encrypted image in the databases: (a) vertical; (b) horizontal; (c) diagonal; (d) off-diagonal correlation.

The correlation results for encrypted image of $\text{Lena}_{512 \times 512}$ and $\text{Barbara}_{512 \times 512}$ are compared with other schemes in Table 4.4. It can be observed that the results for the Lena image of the current scheme are better than all the compared schemes. Similarly, the results for the newly encrypted Barbara image are better than the schemes in [13, 52, 96, 126], and comparable to the results of [90, 93]. Thus, our scheme generates encrypted images with more randomness than the other techniques listed in Table 4.4.

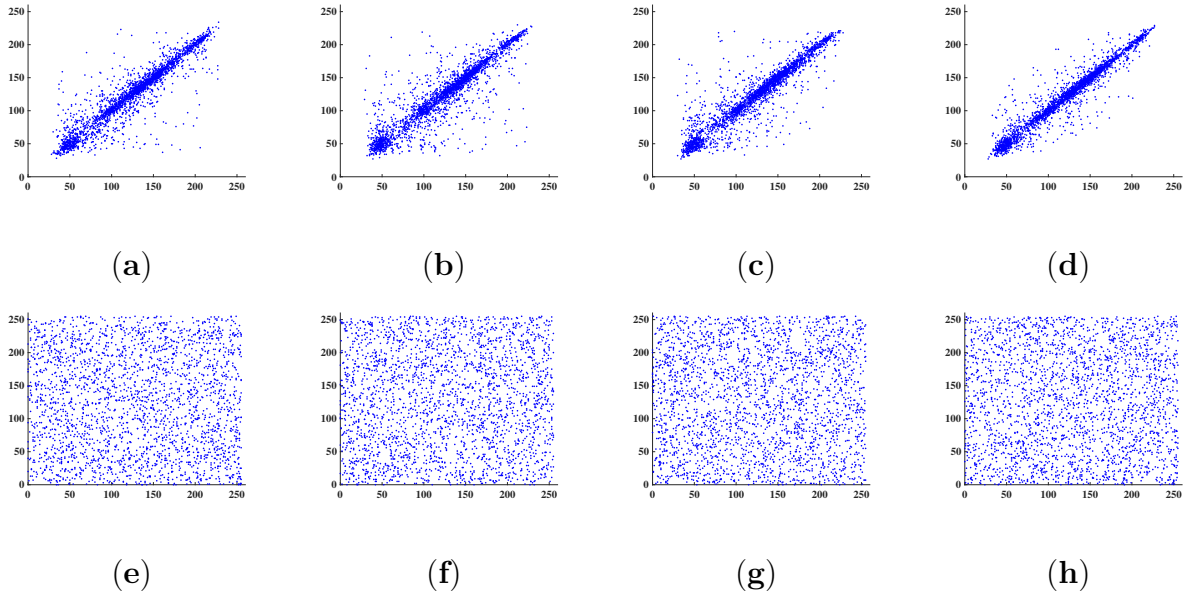


Figure 4.7: Correlation distribution of adjacent pixels of plain image along the (a) horizontal, (b) diagonal, (c) off-diagonal, and (d) vertical directions, respectively; correlation distribution of adjacent pixels of cipher image along the (e) horizontal, (f) diagonal, (g) off-diagonal, and (h) vertical directions, respectively.

4.5.5 Key Space

Key space is a set consisting of the all possible secret keys for a cryptosystem. Generally, for a good cryptosystem, the size of a key space should be at least 2^{128} . The five keys p_1, p_2, b, t , and ℓ_1 are introduced by the proposed scheme. The least number of bits to store a key required by the proposed algorithm is 29. Thus, the size of our key space is 2^{145} , which is much larger than 2^{128} . Hence, the described scheme has the capability to resist brute-force attacks in an efficient way.

4.5.6 Key Sensitivity

This is an important feature of a cryptographically strong cryptosystem. Key sensitivity is also necessary to resist brute-force attacks. If a small change in a key leads to a significant

Table 4.4: Comparison of correlation results along all the three directions for the Lena and Barbara images, due to the proposed algorithm and some other schemes.

Scheme	Lena			Barbara		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Proposed	-0.0006	-0.00009	-0.0005	0.0007	0.0014	-0.0005
Ref. [91]	-0.0026	-0.0054	0.0082	-	-	-
Ref. [106]	-0.0353	0.0286	-0.0249	-	-	-
Ref. [92]	-0.0011	-0.0020	0.0064	-	-	-
Ref. [93]	0.0027	0.0003	0.0012	0.0005	0.0068	0.0003
Ref. [94]	-0.0005	-0.0011	-0.0015	-	-	-
Ref. [95]	0.0039	0.0059	-0.0050	-	-	-
Ref. [96]	-0.0013	0.0080	-0.0094	-0.0047	0.0007	0.0060
Ref. [97]	-0.0005	0.0012	0.0007	-	-	-
Ref. [13]	0.0009	0.0097	-0.0013	-0.0016	0.0038	0.0014
Ref. [90]	-0.0003	-0.0005	0.0005	-0.0002	0.0003	-0.0006
Ref. [117]	0.0023	0.0029	0.0021	-	-	-
Ref. [126]	0.0019	-0.0024	0.0011	-0.0024	0.0031	-0.0013
Ref. [52]	0.0019	-0.0006	-0.0014	-0.00007	-0.0022	0.0007

change in the cipher, then the cryptosystem is said to be sensitive to the keys. For this purpose, we decrypted the Lena image by changing a single key; the results are shown in Figure 4.8(b-d).

Moreover, slightly changing the keys b and p change the coordinates of the ECs $E_{257,1}$, $E_{257,2}$, and $E_{257,1}$, $E_{263,1}$; these are shown in Figure 4.9(a,b), respectively.

Figure 4.9 shows the sensitivity of the masking phase to the parameters of the ECs. From Figures 4.8 and 4.9, it follows that slight changes in a key lead to very different results. Hence, our proposed scheme is highly sensitive to the keys.

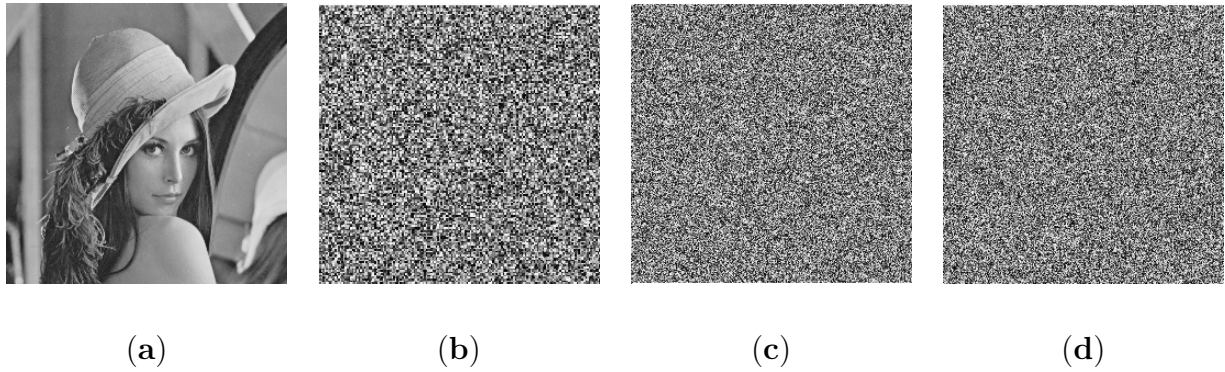


Figure 4.8: Decrypted image with (a) actual keys; (b) $p_1 = p_2 = 257$; (c) $b = 8$; (d) $\ell_1 = \ell_1 + 1$.

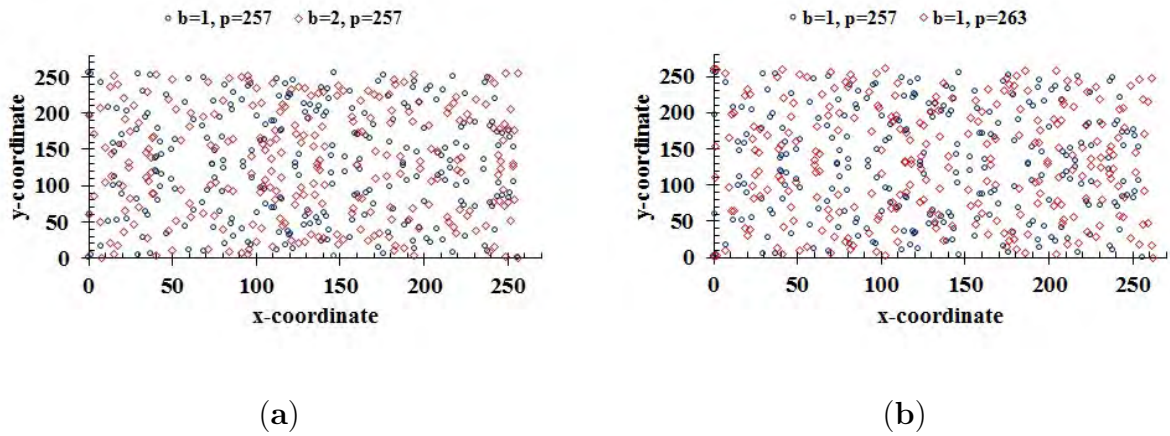


Figure 4.9: (a) Two ECs generated for a small change in the key b ; (b) points of ECs for two different primes.

4.5.7 Plaintext Attacks

There are two types of plaintext attacks, i.e., known plain-text attacks and chosen plaintext attacks. In known plain-text attacks, the attacker knows about a string of the plaintext, along with the relevant string of the cipher text. In chosen plain-text attacks, the adversary has a partial access to the encryption scheme. That is, the adversary can obtain the ciphered string for a chosen plain-text string. For this purpose, attackers use all-black or all-white images to obtain information about the encryption scheme [54], so that a secure encryption scheme

encrypts all-black and all-white images with optimal results. The efficiency of the current scheme is visible from Table 4.5 and Figure 4.10.

Table 4.5: Analysis of the proposed encryption technique against plain-text attacks.

Plain Image	NPCR (%)	UACI (%)	Correlation of Cipher Image			Entropy
			Hori.	Ver.	Diag.	
All-black	99.62	33.42	0.0046	0.0036	-0.0040	7.9974
All-white	99.62	33.49	0.0062	0.0037	0.0012	7.9974

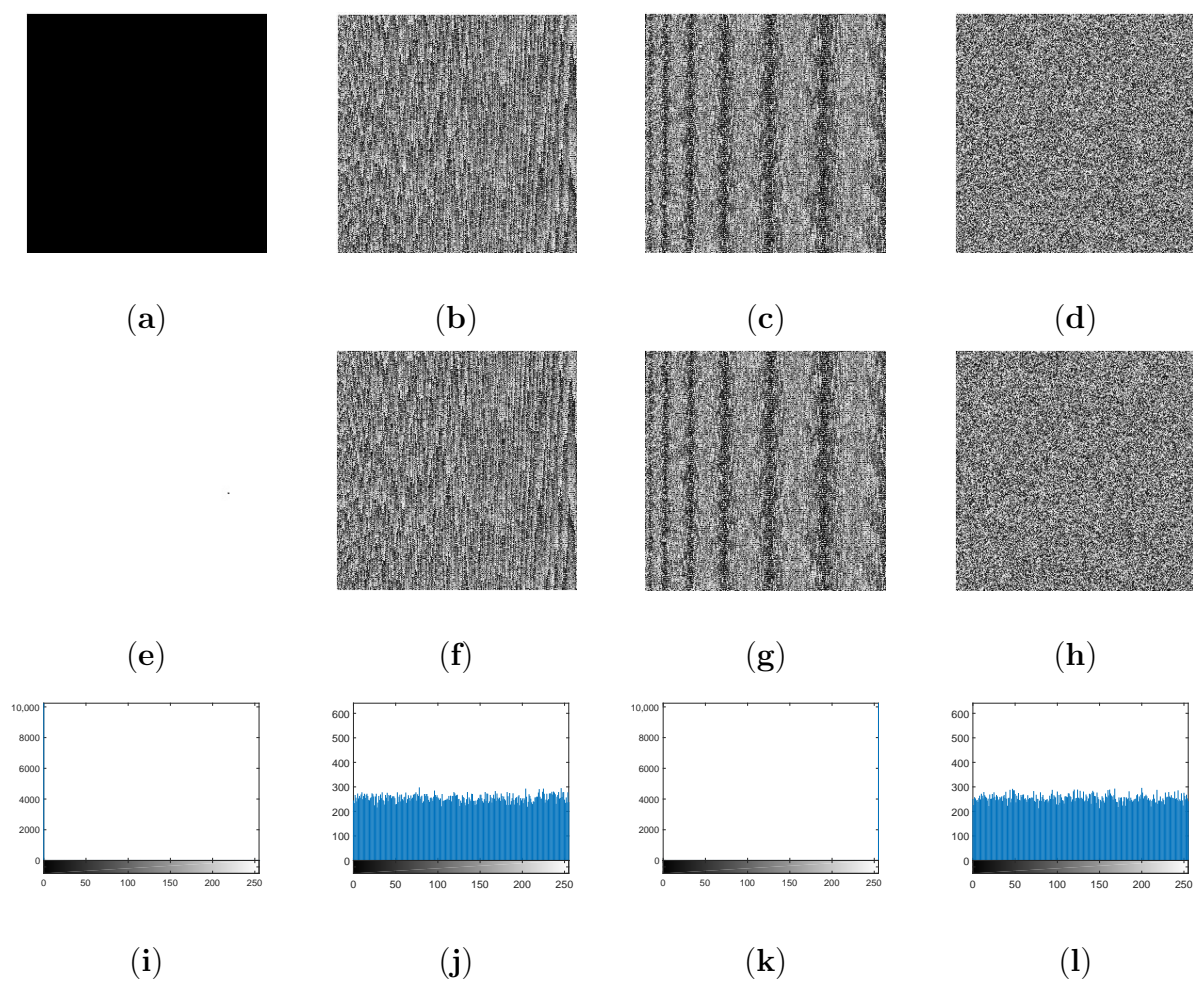


Figure 4.10: (a,e) Plain images; (b,f) masked images; (c,g) diffused images; (d,h) encrypted images of all-black and all-white images, respectively; (i,k) histograms of (a,e), respectively; (j,l) histograms of (d,h), respectively.

The histograms of the channels of the plain $\text{Lena}_{512 \times 512}$ and the encrypted $\text{Lena}_{512 \times 512}$ are shown in Figure 4.11(a–c) and Figure 4.11(d–f), respectively.

Figure 4.11 confirms that the histograms of the encrypted channels are uniform and, hence, the presented scheme encrypts color images having high resistance against the statistical attacks.

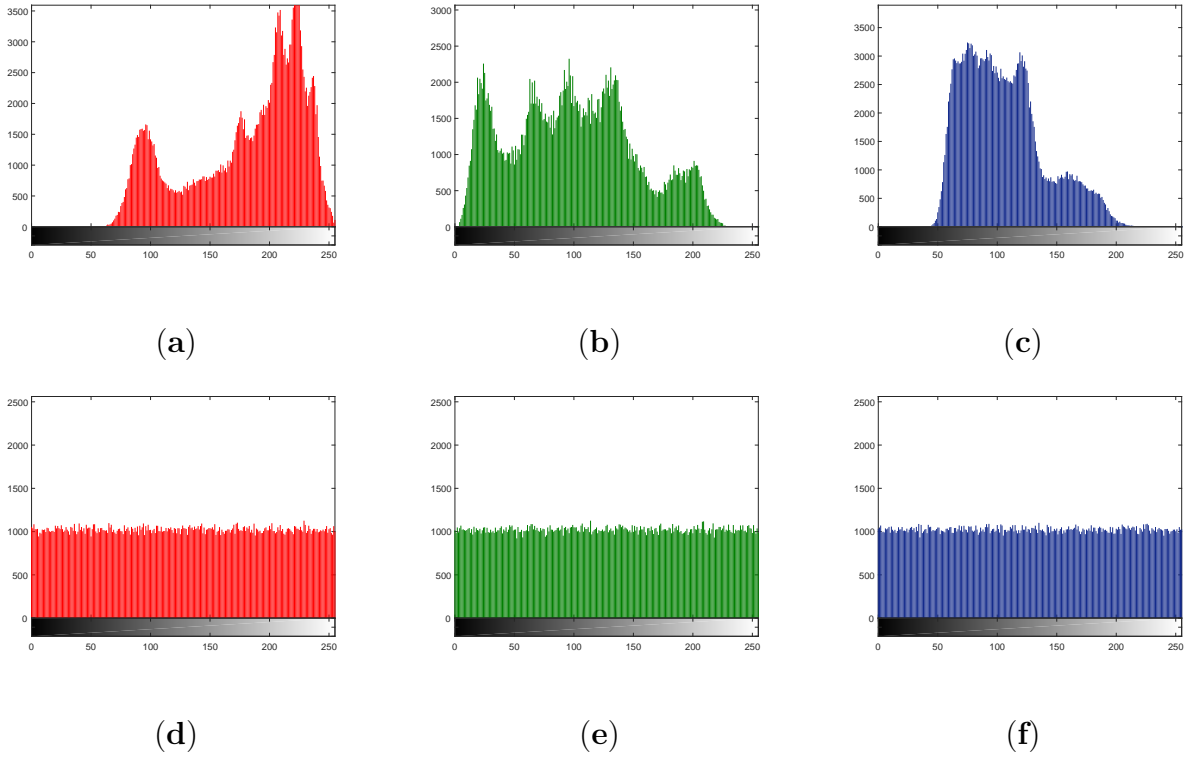


Figure 4.11: (a–c) Histogram of the plain R, G, and B channels of the color $Lena_{512 \times 512}$, respectively; (d–f) histogram of the encrypted R, G, and B channels of the color $Lena_{512 \times 512}$, respectively.

In Table 4.6, the correlation of the adjacent pixels of three different encrypted images with different sizes is shown. It is clear that the presented scheme encrypts any image in such a way that it weakens the correlation between two adjacent pixels of any channel.

Table 4.6: Correlation coefficients of two adjacent pixels in encrypted color images.

Image	Size	Correlation								
		Horizontal			Diagonal			Vertical		
		R	G	B	R	G	B	R	G	B
Female	256×256	-0.00177	0.00240	0.00253	0.00143	-0.00256	-0.00354	-0.00097	0.00113	-0.00027
Lena	512×512	0.00035	-0.00221	0.00084	0.00108	0.00002	0.00007	0.00200	0.00133	-0.00026
San Francisco	1024×1024	-0.00059	-0.00067	0.00125	0.00083	-0.00013	0.00002	0.00158	-0.00031	0.00120

Along with other properties, a good encryption scheme should be highly efficient. Different color images with different sizes are encrypted using the current scheme. To demonstrate the efficiency of the current scheme, the encryption times (sec) for the said three images are computed, since we use a pre-computed EC over the ring of integers as an input for all input images. While computing the encryption time, the time taken by the inputs is not taken under the consideration. The encryption time of the current scheme is compared with the time of some recent schemes [106, 127, 128], as shown in Figure 4.12. The results for the schemes in [106, 127, 128] are available in Table 3 of [129].

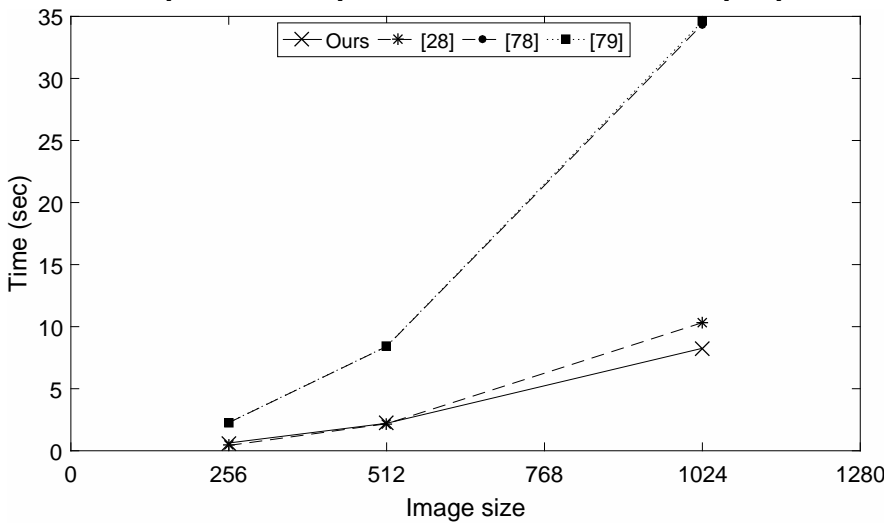


Figure 4.12: Encryption time for color images according to different encryption schemes.

For images of size $w = 256, 512$, the performance of our scheme is comparable with that of [106], and for $w = 1024$, the new scheme is highly efficient, compared to the scheme of [106]. Similarly, in Figure 4.12, the plots of [127, 128] are overlapping, but our scheme is more efficient than [127, 128] for images of all sizes.

Thus, the presented scheme is capable of efficiently encrypting color images as well, and can be used for the good encryption of color images.

4.6 Conclusions

Our proposed encryption scheme has better performance against differential attacks than that of the EC-based schemes [13, 90] and the schemes in [91–94, 106], and provides encrypted images with higher randomness than the schemes in [13, 90, 92–94, 96, 97, 106]. The current scheme is also used for different color images. The presented scheme is able to encrypt color images with low run-times and higher security when compared with [127, 128], while the scheme in [13] discusses the novelty regarding only gray images. Furthermore, as compared to the schemes in [106, 127, 128], the run-time of the current scheme is very low for relatively large images.

Chapter 5

Summary and Future Directions

Text encryption based on ECs is becoming more popular in cryptography because, in contrast to well-known cryptosystems, it offers great security with a relatively small key size. This chapter provides an overview of the research work conducted in this thesis and proposes a few possible paths for further research.

In this PhD thesis,

- i. A three-step text encryption scheme using mathematical structures such as pell sequences and elliptic curves presented.
- ii. The newly constructed text encryption system is secure against computing attacks like key and statistical attacks.
- iii. A new S-box generator that generates a good S-box based on an EC over a finite ring is proposed.
- iv. It avoids the traditional way (group law) of generating an EC. Furthermore, it imposes a bound on the y -coordinate of the EC and one does not have to check all the possible values over the underlying structure. So, the current S-box generator is comparatively efficient for a possible S-box.

- v. An image encryption algorithm is constructed using the aforementioned S-box generator. This proposed scheme can encrypt a number of images with better security against differential, statistical, key and plain-text attacks and run-time of the proposed scheme to encrypt color images is very low.

The future directions consist of the following works:

- i. To generate binary sequence and weight function by using ordered EC and propose an text encryption scheme that can provide provable confidentiality and integrity.
- ii. To improve the proposed image encryption scheme for the simultaneous encryption of all channels of a color image.
- iii. To optimize the image encryption scheme for a text-encryption algorithm
- iv. To generate random numbers based on ECs over rings and employ the sequence of random numbers in text encryption
- v. To generate random binary sequences using ECs over a ring of integers and experimentally prove their cryptographic strength.

Bibliography

- [1] C. E. Shannon, “Communication theory of secrecy systems,” *The Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.
- [2] t. Gary C. Kessler
- [3] L. C. Washington, *Elliptic curves: number theory and cryptography*. CRC press, 2008.
- [4] B. Schneier, “Description of a new variable-length key, 64-bit block cipher (Blowfish),” in *International Workshop on Fast Software Encryption*, pp. 191–204, Springer, 1993.
- [5] K. H. Rahouma, “A block cipher technique for security of data and computer networks,” in *1999 Internet Workshop. IWS99.(Cat. No. 99EX385)*, pp. 25–31, IEEE, 1999.
- [6] V. Gupta, G. Singh, and R. Gupta, “Advance cryptography algorithm for improving data security,” *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, no. 1, pp. 1–6, 2012.
- [7] S. Pattanayak and D. Dey, “Text encryption and decryption with extended euclidean algorithm and combining the features of linear congruence generator,” *International Journal of Development Research*, vol. 6, no. 07, pp. 8753–8756, 2016.
- [8] K. Abdullah, S. A. Bakar, N. H. Kamis, and H. Aliamis, “Rsa cryptosystem with fuzzy set theory for encryption and decryption,” in *AIP Conference Proceedings*, vol. 1905, p. 030001, AIP Publishing LLC, 2017.

- [9] N. Koblitz, A. Menezes, and S. Vanstone, “The state of elliptic curve cryptography,” *Designs, codes and cryptography*, vol. 19, no. 2, pp. 173–193, 2000.
- [10] M. Amara and A. Siad, “Elliptic curve cryptography and its applications,” in *International workshop on systems, signal processing and their applications, WOSSPA*, pp. 247–250, IEEE, 2011.
- [11] G. Ganapathy and K. Mani, “Maximization of speed in elliptic curve cryptography using fuzzy modular arithmetic over a micro-controller based environment,” in *Proceedings of the World Congress on Engineering and Computer Science*, vol. 1, Citeseer, 2009.
- [12] R. Balamurugan, V. Kamalakannan, G. D. Rahul, and S. Tamilselvan, “Enhancing security in text messages using matrix based mapping and elgamal method in elliptic curve cryptography,” in *2014 International Conference on Contemporary Computing and Informatics (IC3I)*, pp. 103–106, IEEE, 2014.
- [13] U. Hayat and N. A. Azam, “A novel image encryption scheme based on an elliptic curve,” *Signal Processing*, vol. 155, pp. 391–402, 2019.
- [14] N. A. Azam, U. Hayat, and I. Ullah, “Efficient construction of a substitution box based on a mordell elliptic curve over a finite field,” *Frontiers of Information Technology and Electronic Engineering*, vol. 20, no. 10, pp. 1378–1389, 2019.
- [15] N. A. Azam, U. Hayat, and I. Ullah, “An injective s-box design scheme over an ordered isomorphic elliptic curve and its characterization,” *Security and communication networks*, vol. 2018, 2018.
- [16] B. Meyer and V. Müller, “A public key cryptosystem based on elliptic curves over \mathbb{F}_n equivalent to factoring,” in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 49–59, Springer, 1996.
- [17] “NIST. FIPS Pub. 197: Specification for the AES,” 2011.

- [18] “National bureau of standards FIPS publication 46: Data Encryption Standard (DES),” 1977.
- [19] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, *The Twofish encryption algorithm: a 128-bit block cipher*. John Wiley & Sons, Inc., 1999.
- [20] T. Koshy, *Pell and Pell-Lucas numbers with applications*, vol. 431. Springer, 2014.
- [21] A. Razaq, H. Alolaiyan, M. Ahmad, M. A. Yousaf, U. Shuaib, W. Aslam, and M. Alawida, “A novel method for generation of strong substitution-boxes based on coset graphs and symmetric groups,” *Ieee Access*, vol. 8, pp. 75473–75490, 2020.
- [22] M. A. Yousaf, H. Alolaiyan, M. Ahmad, M. Dilbar, and A. Razaq, “Comparison of pre and post-action of a finite abelian group over certain nonlinear schemes,” *IEEE Access*, vol. 8, pp. 39781–39792, 2020.
- [23] M. Khan and N. A. Azam, “Right translated aes gray s-boxes,” *Security and Communication Networks*, vol. 8, no. 9, pp. 1627–1635, 2015.
- [24] M. Khan and N. A. Azam, “S-boxes based on affine mapping and orbit of power function,” *3D Research*, vol. 6, no. 2, pp. 1–15, 2015.
- [25] Ö. Koruoğlu and R. Şahin, “Generalized fibonacci sequences related to the extended hecke groups and an application to the extended modular group,” *Turkish Journal of Mathematics*, vol. 34, no. 3, pp. 325–332, 2010.
- [26] S. Ullah, L. Zhang, M. W. Sardar, and M. T. Hussain, “ τ -access policy: Attribute-based encryption scheme for social network based data trading,” *China Communications*, vol. 18, no. 8, pp. 183–198, 2021.
- [27] U. Hayat, N. A. Azam, and M. Asif, “A method of generating 8×8 substitution boxes based on elliptic curves,” *Wireless Personal Communications*, vol. 101, no. 1, pp. 439–451, 2018.

- [28] A. A. Khan, V. Kumar, and M. Ahmad, “An elliptic curve cryptography based mutual authentication scheme for smart grid communications using biometric approach,” *Journal of King Saud University-Computer and Information Sciences*, 2019.
- [29] V. Kumar, M. Ahmad, A. Kumari, S. Kumari, and M. K. Khan, “Sebap: a secure and efficient biometric-assisted authentication protocol using ecc for vehicular cloud computing,” *International Journal of Communication Systems*, vol. 34, no. 2, p. e4103, 2021.
- [30] Z. E. Dawahdeh, S. N. Yaakob, and R. R. bin Othman, “A new image encryption technique combining elliptic curve cryptosystem with hill cipher,” *Journal of King Saud University-Computer and Information Sciences*, vol. 30, no. 3, pp. 349–355, 2018.
- [31] Z. Hua, S. Yi, and Y. Zhou, “Medical image encryption using high-speed scrambling and pixel adaptive diffusion,” *Signal Processing*, vol. 144, pp. 134–144, 2018.
- [32] J. M. Vilaridy O, L. Barba J, and C. O. Torres M, “Image encryption and decryption systems using the jigsaw transform and the iterative finite field cosine transform,” in *Photonics*, vol. 6, p. 121, MDPI, 2019.
- [33] D. Lambić, A. Janković, and M. Ahmad, “Security analysis of the efficient chaos pseudo-random number generator applied to video encryption,” *Journal of Electronic Testing*, vol. 34, no. 6, pp. 709–715, 2018.
- [34] H. A. Ahmed, M. F. Zolkipli, and M. Ahmad, “A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map,” *Neural Computing and Applications*, vol. 31, no. 11, pp. 7201–7210, 2019.
- [35] M. Ahmad, S. Khurana, S. Singh, and H. D. AlSharari, “A simple secure hash function scheme using multiple chaotic maps,” *3D Research*, vol. 8, no. 2, pp. 1–15, 2017.

- [36] M. Ahmad, M. N. Doja, and M. M. S. Beg, "Security analysis and enhancements of an image cryptosystem based on hyperchaotic system," *Journal of King Saud University-Computer and Information Sciences*, vol. 33, no. 1, pp. 77–85, 2021.
- [37] N. A. Azam, "A novel fuzzy encryption technique based on multiple right translated aes gray s-boxes and phase embedding," *Security and Communication Networks*, vol. 2017, 2017.
- [38] E. Agrawal and P. R. Pal, "A secure and fast approach for encryption and decryption of message communication," *Int. J. Eng. Sci*, vol. 11481, 2017.
- [39] A. Luma and B. Raufi, "Relationship between fibonacci and lucas sequences and their application in symmetric cryptosystems," in *4th International Conference on Circuits, Systems and Signals*, vol. 146, p. 150, 2010.
- [40] A. Overmars and S. Venkatraman, "An efficient golden ratio method for secure cryptographic applications," *Mathematical and Computational Applications*, vol. 23, no. 4, p. 58, 2018.
- [41] P. Agarwal, N. Agarwal, and R. Saxena, "Data encryption through fibonacci sequence and unicode characters," *MIT International Journal of Computer Science and Information Technology*, vol. 5, no. 2, pp. 79–82, 2015.
- [42] C. T. Clelland, V. Risca, and C. Bancroft, "Hiding messages in dna microdots," *Nature*, vol. 399, no. 6736, pp. 533–534, 1999.
- [43] M. Borda and O. Tornea, "Dna secret writing techniques," in *2010 8th International Conference on Communications*, pp. 451–456, IEEE, 2010.
- [44] M. R. Abbasy, A. A. Manaf, and S. MA, "Data hiding method based on dna basic characteristics," in *International Conference on Digital Enterprise and Information Systems*, pp. 53–62, Springer, 2011.

- [45] M. Murillo-Escobar, F. Abundiz-Pérez, C. Cruz-Hernández, and R. López-Gutiérrez, “A novel symmetric text encryption algorithm based on logistic map,” in *Proceedings of the international conference on communications, signal processing and computers*, vol. 4953, 2014.
- [46] E. A. H. Díaz, H. M. P. Meana, and V. M. S. García, “Encryption of rgb images by means of a novel cryptosystem using elliptic curves and chaos,” *IEEE Latin America Transactions*, vol. 18, no. 08, pp. 1407–1415, 2020.
- [47] I. Hussain, N. A. Azam, and T. Shah, “Stego optical encryption based on chaotic s-box transformation,” *Optics & Laser Technology*, vol. 61, pp. 50–56, 2014.
- [48] M. Ahmad and M. S. Alam, “A new algorithm of encryption and decryption of images using chaotic mapping,” *International Journal on computer science and engineering*, vol. 2, no. 1, pp. 46–50, 2009.
- [49] X. Zhang, Y. Mao, and Z. Zhao, “An efficient chaotic image encryption based on alternate circular s-boxes,” *Nonlinear Dynamics*, vol. 78, no. 1, pp. 359–369, 2014.
- [50] M. Ahmad, M. N. Doja, and M. M. S. Beg, “Security analysis and enhancements of an image cryptosystem based on hyperchaotic system,” *Journal of King Saud University-Computer and Information Sciences*, vol. 33, no. 1, pp. 77–85, 2021.
- [51] A. A. Abd El-Latif and X. Niu, “A hybrid chaotic system and cyclic elliptic curve for image encryption,” *AEU-International Journal of Electronics and Communications*, vol. 67, no. 2, pp. 136–143, 2013.
- [52] R. I. Abdelfatah, “Secure image transmission using chaotic-enhanced elliptic curve cryptography,” *IEEE Access*, vol. 8, pp. 3875–3890, 2019.
- [53] I. Ullah, U. Hayat, and M. D. Bustamante, “Image encryption using elliptic curves and rossby/drift wave triads,” *Entropy*, vol. 22, no. 4, p. 454, 2020.

- [54] S. Toughi, M. H. Fathi, and Y. A. Sekhavat, “An image encryption scheme based on elliptic curve pseudo random and advanced encryption system,” *Signal processing*, vol. 141, pp. 217–227, 2017.
- [55] L. D. Singh and K. M. Singh, “Image encryption using elliptic curve cryptography,” *Procedia Computer Science*, vol. 54, pp. 472–481, 2015.
- [56] S. T. Suneetha CH and N. CH, “Implementation of double fold text encryption based on elliptic curve cryptography (ecc) with digital signature,” *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, 2020.
- [57] M. A. Najji, D. A. Hammood, H. A. Atee, R. S. Jebur, H. A. Rahim, and R. B. Ahmad, “Cryptanalysis cipher text using new modeling: Text encryption using elliptic curve cryptography,” in *AIP Conference Proceedings*, vol. 2203, p. 020003, AIP Publishing LLC, 2020.
- [58] K. Agrawal and A. Gera, “Elliptic curve cryptography with hill cipher generation for secure text cryptosystem,” *International journal of computer applications*, vol. 106, no. 1, 2014.
- [59] K. Keerthi and B. Surendiran, “Elliptic curve cryptography for secured text encryption,” in *2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT)*, pp. 1–5, IEEE, 2017.
- [60] A. Kumar, S. Tyagi, M. Rana, N. Aggarwal, and P. Bhadana, “A comparative study of public key cryptosystem based on ecc and rsa,” in *International Journal on Computer Science and Engineering (IJCSE)*, Citeseer, 2011.
- [61] L. D. Singh and K. M. Singh, “Implementation of text encryption using elliptic curve cryptography,” *Procedia Computer Science*, vol. 54, pp. 73–82, 2015.

- [62] S. Ullah, X.-Y. Li, and L. Zhang, “A review of signcryption schemes based on hyper elliptic curve,” in *2017 3rd International Conference on Big Data Computing and Communications (BIGCOM)*, pp. 51–58, IEEE, 2017.
- [63] S. Ullah, X.-Y. Li, and Z. Lan, “A novel trusted third party based signcryption scheme,” *Multimedia Tools and Applications*, vol. 79, no. 31, pp. 22749–22769, 2020.
- [64] S. Ullah and N. Din, “Blind signcryption scheme based on hyper elliptic curves cryptosystem,” *Peer-to-Peer Networking and Applications*, vol. 14, no. 2, pp. 917–932, 2021.
- [65] S. E. Ghrare, H. A. Barghi, and N. R. Madi, “New text encryption method based on hidden encrypted symmetric key,” 2018.
- [66] V. Muñoz, “Everyday cryptography: fundamental principles and applications [book review],” 2013.
- [67] S. Ibrahim and A. Alharbi, “Efficient image encryption scheme using henon map, dynamic s-boxes and elliptic curve cryptography,” *IEEE Access*, vol. 8, pp. 194289–194302, 2020.
- [68] S. Murphy and M. J. Robshaw, “Essential algebraic structure within the aes,” in *Annual International Cryptology Conference*, pp. 1–16, Springer, 2002.
- [69] J. Rosenthal, “A polynomial description of the rijndael advanced encryption standard,” *Journal of Algebra and its Applications*, vol. 2, no. 02, pp. 223–236, 2003.
- [70] L. Cui and Y. Cao, “A new s-box structure named affine-power-affine,” *International Journal of Innovative Computing, Information and Control*, vol. 3, no. 3, pp. 751–759, 2007.
- [71] J. Liu, B. Wei, X. Cheng, and X. Wang, “An aes s-box to increase complexity and cryptographic analysis,” in *19th International Conference on Advanced Information*

- Networking and Applications (AINA'05) Volume 1 (AINA papers)*, vol. 1, pp. 724–728, IEEE, 2005.
- [72] M. T. Tran, D. K. Bui, and A. D. Duong, “Gray s-box for advanced encryption standard,” in *2008 international conference on computational intelligence and security*, vol. 1, pp. 253–258, IEEE, 2008.
- [73] V. M. Silva-Garcia, R. Flores-Carapia, M. D. González-Ramírez, E. Vega-Alvarado, and M. G. Villarreal-Cervantes, “Cryptosystem based on the elliptic curve with a high degree of resistance to damage on the encrypted images,” *IEEE Access*, vol. 8, pp. 218777–218792, 2020.
- [74] F. Özkaynak, “Construction of robust substitution boxes based on chaotic systems,” *Neural Computing and Applications*, vol. 31, no. 8, pp. 3317–3326, 2019.
- [75] V. S. Miller, “Use of elliptic curves in cryptography,” in *Conference on the theory and application of cryptographic techniques*, pp. 417–426, Springer, 1985.
- [76] J. H. Cheon, S. Chee, and C. Park, “S-boxes with controllable nonlinearity,” in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 286–294, Springer, 1999.
- [77] U. Hayat, N. A. Azam, H. R. Gallegos-Ruiz, S. Naz, and L. Batool, “A truly dynamic substitution box generator for block ciphers based on elliptic curves over finite rings,” *Arabian Journal for Science and Engineering*, vol. 46, no. 9, pp. 8887–8899, 2021.
- [78] C. Adams and S. Tavares, “The structured design of cryptographically good s-boxes,” *Journal of cryptology*, vol. 3, no. 1, pp. 27–41, 1990.
- [79] M. Matsui, “Workshop on the theory and application of of cryptographic techniques,” 1993.

- [80] M. T. Sakallı, B. Aslan, E. Buluş, A. Ş. Mesut, F. Büyüksaraçoğlu, and O. Karaahmetoğlu, “On the algebraic expression of the aes s-box like s-boxes,” in *International Conference on Networked Digital Technologies*, pp. 213–227, Springer, 2010.
- [81] T. Ye and L. Zhimao, “Chaotic s-box: Six-dimensional fractional lorenz–duffing chaotic system and o-shaped path scrambling,” *Nonlinear Dynamics*, vol. 94, no. 3, pp. 2115–2126, 2018.
- [82] F. Özkaynak, V. Çelik, and A. B. Özer, “A new s-box construction method based on the fractional-order chaotic chen system,” *Signal, Image and Video Processing*, vol. 11, no. 4, pp. 659–664, 2017.
- [83] Ü. Çavuşoğlu, A. Zengin, I. Pehlivan, and S. Kaçar, “A novel approach for strong s-box generation algorithm design based on chaotic scaled zhongtang system,” *Nonlinear dynamics*, vol. 87, no. 2, pp. 1081–1094, 2017.
- [84] A. Belazi and A. A. Abd El-Latif, “A simple yet efficient s-box method based on chaotic sine map,” *Optik*, vol. 130, pp. 1438–1444, 2017.
- [85] L. Liu, Y. Zhang, and X. Wang, “A novel method for constructing the s-box based on spatiotemporal chaotic dynamics,” *applied sciences*, vol. 8, no. 12, p. 2650, 2018.
- [86] N. A. Azam, U. Hayat, and I. Ullah, “Efficient construction of a substitution box based on a mordell elliptic curve over a finite field,” *Frontiers of Information Technology & Electronic Engineering*, vol. 20, no. 10, pp. 1378–1389, 2019.
- [87] G. Murtaza, N. A. Azam, and U. Hayat, “Designing an efficient and highly dynamic substitution-box generator for block ciphers based on finite elliptic curves,” *Security and Communication Networks*, vol. 2021, 2021.
- [88] E. Biham and A. Shamir, “Differential cryptanalysis of des-like cryptosystems,” *Journal of CRYPTOLOGY*, vol. 4, no. 1, pp. 3–72, 1991.

- [89] A. Webster and S. E. Tavares, “On the design of s-boxes,” in *Conference on the theory and application of cryptographic techniques*, pp. 523–534, Springer, 1985.
- [90] N. A. Azam, I. Ullah, and U. Hayat, “A fast and secure public-key image encryption scheme based on mordell elliptic curves,” *Optics and Lasers in Engineering*, vol. 137, p. 106371, 2021.
- [91] L. Liu and S. Miao, “A new simple one-dimensional chaotic map and its application for image encryption,” *Multimedia Tools and Applications*, vol. 77, no. 16, pp. 21445–21462, 2018.
- [92] L. Liu, S. Miao, H. Hu, and M. Cheng, “N-phase logistic chaotic sequence and its application for image encryption,” *IET Signal Processing*, vol. 10, no. 9, pp. 1096–1104, 2016.
- [93] X. Wang, L. Feng, R. Li, and F. Zhang, “A fast image encryption algorithm based on non-adjacent dynamically coupled map lattice model,” *Nonlinear Dynamics*, vol. 95, no. 4, pp. 2797–2824, 2019.
- [94] J. Tang, Z. Yu, and L. Liu, “A delay coupling method to reduce the dynamical degradation of digital chaotic maps and its application for image encryption,” *Multimedia Tools and Applications*, vol. 78, no. 17, pp. 24765–24788, 2019.
- [95] M. Z. Talhaoui, X. Wang, and M. A. Midoun, “Fast image encryption algorithm with high security level using the bülbán chaotic map,” *Journal of Real-Time Image Processing*, vol. 18, no. 1, pp. 85–98, 2020.
- [96] S. M. Ismail, L. A. Said, A. G. Radwan, A. H. Madian, and M. F. Abu-Elyazeed, “Generalized double-humped logistic map-based medical image encryption,” *Journal of advanced research*, vol. 10, pp. 85–98, 2018.

- [97] M. Wang, X. Wang, T. Zhao, C. Zhang, Z. Xia, and N. Yao, “Spatiotemporal chaos in improved cross coupled map lattice and its application in a bit-level image encryption scheme,” *Information Sciences*, vol. 544, pp. 1–24, 2020.
- [98] Z. Hua, Y. Zhou, and H. Huang, “Cosine-transform-based chaotic system for image encryption,” *Information Sciences*, vol. 480, pp. 403–419, 2019.
- [99] D. Lambić, A. Janković, and M. Ahmad, “Security analysis of the efficient chaos pseudo-random number generator applied to video encryption,” *Journal of Electronic Testing*, vol. 34, no. 6, pp. 709–715, 2018.
- [100] M. Ahmad, M. Z. Alam, Z. Umayya, S. Khan, and F. Ahmad, “An image encryption approach using particle swarm optimization and chaotic map,” *International Journal of Information Technology*, vol. 10, no. 3, pp. 247–255, 2018.
- [101] Y. Zhang, “A new unified image encryption algorithm based on a lifting transformation and chaos,” *Information Sciences*, vol. 547, pp. 307–327, 2020.
- [102] Y. Zhang, “The fast image encryption algorithm based on lifting scheme and chaos,” *Information sciences*, vol. 520, pp. 177–194, 2020.
- [103] X. J. Tong, Z. Wang, M. Zhang, Y. Liu, H. Xu, and J. Ma, “An image encryption algorithm based on the perturbed high-dimensional chaotic map,” *Nonlinear Dynamics*, vol. 80, no. 3, pp. 1493–1508, 2015.
- [104] X. Wang, J. Zhao, and Z. Zhang, “A chaotic cryptosystem based on multi-one-dimensional maps,” *Modern Physics Letters B*, vol. 23, no. 02, pp. 183–189, 2009.
- [105] G. Chen, Y. Mao, and C. K. Chui, “A symmetric image encryption scheme based on 3d chaotic cat maps,” *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749–761, 2004.
- [106] Z. Hua, F. Jin, B. Xu, and H. Huang, “2d logistic-sine-coupling map for image encryption,” *Signal Processing*, vol. 149, pp. 148–161, 2018.

- [107] Z. Hua, Y. Zhou, C.-M. Pun, and C. P. Chen, “2d sine logistic modulation map for image encryption,” *Information Sciences*, vol. 297, pp. 80–94, 2015.
- [108] L. Sui, K. Duan, J. Liang, and X. Hei, “Asymmetric double-image encryption based on cascaded discrete fractional random transform and logistic maps,” *Optics express*, vol. 22, no. 9, pp. 10605–10621, 2014.
- [109] G. Ye, K. Jiao, H. Wu, C. Pan, and X. Huang, “An asymmetric image encryption algorithm based on a fractional-order chaotic system and the rsa public-key cryptosystem,” *International Journal of Bifurcation and Chaos*, vol. 30, no. 15, p. 2050233, 2020.
- [110] S. B. Sadkhan and N. F. Hameed, “Proposed developments of elliptic curves cryptosystem,” *J. Qadisiyah Pure Sci*, vol. 15, pp. 79–86, 2019.
- [111] Z. K. Obaid and N. F. H. Al Saffar, “Image encryption based on menezes vanstone elliptic curve cryptosystem,” *Solid State Technology*, vol. 63, no. 3, pp. 5256–5265, 2020.
- [112] X. Zhang and X. Wang, “Digital image encryption algorithm based on elliptic curve public cryptosystem,” *IEEE Access*, vol. 6, pp. 70025–70034, 2018.
- [113] A. M. Abbas, A. A. Alharbi, and S. Ibrahim, “A novel parallelizable chaotic image encryption scheme based on elliptic curves,” *IEEE Access*, vol. 9, pp. 54978–54991, 2021.
- [114] E. A. H. Díaz, H. M. P. Meana, and V. M. S. García, “Encryption of rgb images by means of a novel cryptosystem using elliptic curves and chaos,” *IEEE Latin America Transactions*, vol. 18, no. 08, pp. 1407–1415, 2020.
- [115] T. S. Ali and R. Ali, “A novel medical image signcryption scheme using tlts and henon chaotic map,” *IEEE Access*, vol. 8, pp. 71974–71992, 2020.

- [116] A. Shafique, J. Ahmed, M. U. Rehman, and M. M. Hazzazi, “Noise-resistant image encryption scheme for medical images in the chaos and wavelet domain,” *IEEE Access*, vol. 9, pp. 59108–59130, 2021.
- [117] X. Li, D. Xiao, H. Mou, D. Lu, and M. Peng, “A compressive sensing based image encryption and compression algorithm with identity authentication and blind signcryption,” *IEEE Access*, vol. 8, pp. 211676–211690, 2020.
- [118] S. Azhar, N. A. Azam, and U. Hayat, “Text encryption using pell sequence and elliptic curves with provable security,” *Comput. Contin.*, vol. 71, pp. 4972–4989, 2022.
- [119] O. Reyad, Z. Kotulski, and W. Abd-Elhafiez, “Image encryption using chaos-driven elliptic curve pseudo-random number generators,” *Appl. Math. Inf. Sci.*, vol. 10, no. 4, pp. 1283–1292, 2016.
- [120] T. M. Cover, *Elements of information theory*. John Wiley and Sons, 2012.
- [121] N. Jia, S. Liu, Q. Ding, S. Wu, and X. Pan, “A new method of encryption algorithm based on chaos and ecc.,” *J. Inf. Hiding Multim. Signal Process.*, vol. 7, no. 3, pp. 637–644, 2016.
- [122] R. Duran Diaz, L. Hernandez Encinas, and J. Munoz Masque, “A group law on the projective plane with applications in public key cryptography,” *Mathematics*, vol. 8, no. 5, p. 734, 2020.
- [123] “USC-SIPI Image Database.”
- [124] Y. Zhou, L. Bao, and C. P. Chen, “Image encryption using a new parametric switching chaotic system,” *Signal processing*, vol. 93, no. 11, pp. 3039–3052, 2013.
- [125] Y. Xian and X. Wang, “Fractal sorting matrix and its application on chaotic image encryption,” *Information Sciences*, vol. 547, pp. 1154–1169, 2021.

- [126] Y. Luo, X. Ouyang, J. Liu, and L. Cao, “An image encryption method based on elliptic curve elgamal encryption and chaotic systems,” *IEEE Access*, vol. 7, pp. 38507–38522, 2019.
- [127] X. Chai, Y. Chen, and L. Broyde, “A novel chaos-based image encryption algorithm using dna sequence operations,” *Optics and Lasers in engineering*, vol. 88, pp. 197–213, 2017.
- [128] Y. Zhou, L. Bao, and C. P. Chen, “A new 1d chaotic system for image encryption,” *Signal processing*, vol. 97, pp. 172–182, 2014.
- [129] Z. Hua, Z. Zhu, S. Yi, Z. Zhang, and H. Huang, “Cross-plane colour image encryption using a two-dimensional logistic tent modular map,” *Information Sciences*, vol. 546, pp. 1063–1083, 2021.

Turnitin Originality Report

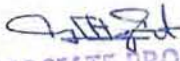
Cryptosystems based on Elliptic Curves and Recurrent Sequences
From PhD (PhD DRSMML)


by Sumaira Azhar, Turnitin

- Processed on 11-Aug-2023 14:48 PKT
- ID: 2144372908
- Word Count: 23028

Similarity Index
19%
Similarity by Source

Internet Sources: 13%
Publications: 16%
Student Papers: 2%


ASSOCIATE PROFESSOR
Department of Mathematics
Quaid-i-Azam University
Islamabad


Focal Person (Turnitin)
Quaid-i-Azam University
Islamabad

sources:

- 1 1% match ()
[Ullah, Ikram, Azam, Naveed Ahmed, Hayat, Umar. "Efficient and Secure Substitution Box and Random Number Generators Over Mordell Elliptic Curves". 2019](#)

- 2 < 1% match (Internet from 30-Jan-2023)
https://www.researchgate.net/publication/321258125_RSA_cryptosystem_with_fuzzy_set_theory_for_encryption_and_decryption

- 3 < 1% match (Internet from 18-Feb-2023)
https://www.researchgate.net/publication/321116532_A_Review_of_Signcryption_Schemes_Based_on_Hyoeer_Elliptic_Curve

- 4 < 1% match (Internet from 24-Aug-2022)
https://www.researchgate.net/publication/273510741_An_image_encryption_algorithm_based_on_the_perturbed_high-dimensional_chaotic_map

- 5 < 1% match (Internet from 30-Jan-2023)
https://www.researchgate.net/publication/272555992_An_efficient_chaotic_image_encryption_based_on_alternate_circular_S-boxes

- 6 < 1% match (Internet from 21-Feb-2023)
https://www.researchgate.net/publication/343163452_A_new_hybrid_text_encryption_approach_over_mobile_ad_hoc_network

- 7 < 1% match (Internet from 07-Oct-2022)
https://www.researchgate.net/publication/338485665_Cryptanalysis_cipher_text_using_new_modeling_Text_encryption_using_elliptic_cur

- 8 < 1% match (Internet from 02-Feb-2023)
https://www.researchgate.net/publication/338961360_An_Image_Encryption_Scheme_Based_on_DNA_Computing_and_Multiple_Chaotic

- 9 < 1% match (Internet from 25-Aug-2022)
https://www.researchgate.net/publication/334140258_A_new_image_encryption_algorithm_with_nonlinear-diffusion_based_on_Multiple_coupled_map_lattices

- 10 < 1% match (Internet from 05-May-2022)
https://link.springer.com/article/10.1007/s13369-021-05866-9?code=80b38703-1467-4b92-b5e5-45671075da48&error=cookies_not_supported

- 11 < 1% match (Internet from 23-Mar-2023)
https://link.springer.com/article/10.1007/s13369-022-07383-3?code=7d53aafb-5908-4ec3-ad61-69ee698a72f3&error=cookies_not_supported

- 12 < 1% match (Internet from 11-Dec-2022)
https://link.springer.com/article/10.1140/epjp/s13360-020-00187-0?code=c0908540-5b5d-4a28-a7d5-163d66867164&error=cookies_not_supported

- 13 < 1% match (Internet from 27-Aug-2019)