RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITÉ MOHAMED BOUDIAF - M'SILA
FACULTÉ DE MATHÉMATIQUES ET DE L'INFORMATIQUE
DÉPARTEMENT DE MATHÉMATIQUES

N° d'ordre : .....

T H È S E

Présentée pour l'obtention du diplôme
de Doctorat de Troisième Cycle (LMD)

Domaine
Mathématiques et Informatique

Spécialité
Algèbre et Mathématiques Discrètes

Par
Bilel Selikh

Thème

Sur les courbes elliptiques et application à la cryptographie

Soutenue le 30/06/2022 devant le jury composé de :

Abdelmadjid Boudaoud	**Prof.**	**Université de M'sila**	**Président**
Douadi Mihoubi	**Prof.**	**Université de M'sila**	**Directeur de thèse**
Nacer Ghadbane	**MCA**	**Université de M'sila**	**Co-Directeur de thèse**
Lemnouar Noui	**Prof.**	**Université de Batna II**	**Examinateur**
Noureddine Midoune	**MCA**	**Université de M'sila**	**Examinateur**
Soheyb Milles	**MCA**	**Centre universitaire de Barika**	**Examinateur**
Lemnaouar Zedam	**Prof.**	**Université de M'sila**	**Invité**

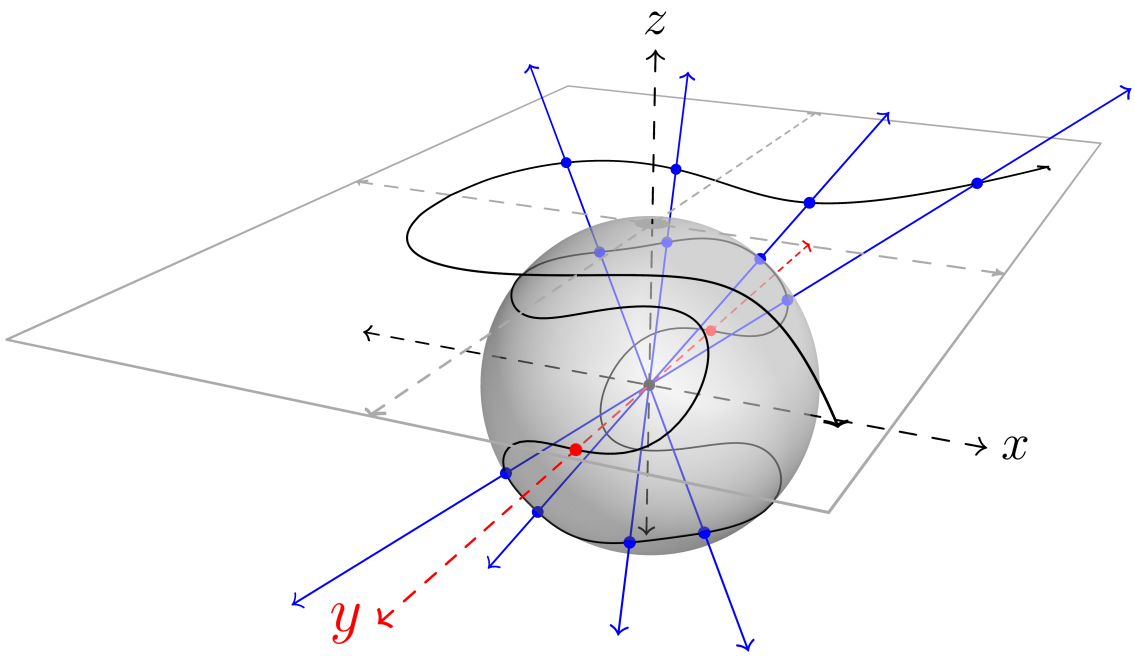
Année Universitaire : 2021/2022

A thesis submitted in fulfillment of the requirements
for the degree of Doctor of Mathematics

University of M'sila-Algeria
Faculty of Mathematics and Computer Science
Department of Mathematics

On elliptic curves and application to cryptography

By
Bilel Selikh



Academic year
2021-2022

Committee President:
Prof. Dr. Abdelmadjid Boudaoud
Faculty of Mathematics and Computer Science
Department of Mathematics
abdelmadjid.boudaoud@univ-msila.dz

Supervisor:
Prof. Dr. Douadi Mihoubi
Faculty of Mathematics and Computer Science
Department of Mathematics
douadi.mihoubi@univ-msila.dz

Co-Supervisor:
Dr. Nacer Ghadbane
Faculty of Mathematics and Computer Science
Department of Mathematics
nasser.ghedbane@univ-msila.dz

Internal Examiners:
Dr. Noureddine Midoune
Faculty of Mathematics and Computer Science
Department of Mathematics
noureddine.midoune@univ-msila.dz

External Examiners:
Prof. Dr. Lemnouar Noui
Faculty of Science
Department of Mathematics
nouilem@yahoo.fr

Dr. Soheyb Milles
Faculty of Science
Department of Mathematics and Computer Science
soheyb.milles@univ-msila.dz

Committee Invites:
Prof. Dr. Lemnaouar Zedam
Faculty of Mathematics and Computer Sceince
Department of Mathematics
lemnaouar.zedam@univ-msila.dz

Bilel Selikh
bilel.selikh@univ-msila.dz

Acknowledgements

In the beginning, I would like to praise Allah the Almighty, the Most Gracious, and the Most Merciful for His blessing given to me during my study and in completing this thesis to achieve my dream of attaining the highest qualification. May Allah's blessing goes to His final Prophet Muhammad (peace be up on him), his family and his companions. I would say thanks to my supervisor Prof. Douadi Mihoubi to guide me well throughout the research work from title's selection to finding the results. Their immense knowledge, motivation and patience have given me more power and spirit to excel in the research writing. Conducting the academic study regarding such a difficult topic couldn't be as simple as he made this for me. He is my mentor and a better advisor for my doctorate study beyond the imagination. Apart from my Supervisor, I won't forget to express the gratitude to co-supervisor: Dr. Nacer Ghadbane for giving the encouragement and sharing insightful suggestions. I am also pleased to say thank you to the man who also supported me well throughout the entire research program is Prof. Abdelhakim Chillali Their immense support actually guided me to rectify numerous things that could create major challenges in the acceptance of my paper. It wouldn't have been possible to conduct this research without their precious support. They all really mean a lot to me. They have played a major role in polishing my research writing skills. Their endless guidance is hard to forget throughout my life. I sincerely thank the chairman of the jury committee Prof. Abdelmadjid Boudaoud, and the other jury members. Finally, I wish to express my profound appreciation to my colleagues from laboratory of Pure and Applied Mathematics at M'sila university.

♡

Dedication

I am grateful to my parents (Ameur and Mina Bachiri), siblings, friends and acquaintances who remembered me in their prayers for the ultimate success. I consider myself nothing without them. They gave me enough moral support, encouragement and motivation to accomplish the personal goals. My two lifelines (my parents) have always supported me financially so that I only pay attention to the studies and achieving my objective without any obstacle on the way.

Contents

Page

List of Figures iv

List of Tables v

List of Symbols vi

List of Abbreviations ix

List of Original Papers x

General Introduction xi

Part I Arithmetic of Elliptic Curves 1

1 Elliptic curves over a field $\mathbb{K}$ 2

1.1 Affine elliptic curves . . . 3

1.1.1 Simplified Weierstrass equations . . . 5

1.1.2 The group law . . . 8

1.1.3 Isomorphism of elliptic curves . . . 13

1.1.4 Elliptic curve over a finite field . . . 15

1.2 Projective elliptic curves . . . 18

1.2.1 Projective space . . . 18

1.2.2 Arithmetic in projective coordinates . . . 20

2 Elliptic curves over a finite rings 27

2.1 Basic concepts . . . 28

2.2 Elliptic curves over the ring R . . . 29

2.3 Elliptic curve over a ring of characteristic $\neq 2, 3$ . . . 30

2.3.1 The finite ring $\mathbb{F}_q[\varepsilon], \varepsilon^4 = \varepsilon^3$ . . . 30

2.3.2 Elliptic curve over $\mathbb{F}_q[\varepsilon], \varepsilon^4 = \varepsilon^3$ . . . 35

2.3.3 Classification of elements in $E_{a,b}(\mathbb{F}_q[\varepsilon])$ . . . 43

2.4 Elliptic curve over a ring of characteristic 3 . . . 44

2.4.1 The finite ring $\mathbb{F}_{3^d}[\varepsilon], \varepsilon^4 = \varepsilon^3$ . . . 45

2.4.2 Elliptic curve over $\mathbb{F}_{3^d}[\varepsilon], \varepsilon^4 = \varepsilon^3$ . . . 48

2.4.3 Classification of elements in $E_{a,b}(\mathbb{F}_{3^d}[\varepsilon])$ . . . 52

Part II Elliptic Curves in Cryptography 54

3 Generalities on a public key cryptosystems 56

3.1 Complexity of an algorithms . . . 57

3.2 Introduction to a cryptology . . . 61
3.2.1 Cryptography . . . 62
3.2.2 Cryptanalysis . . . 69
3.3 Discrete logarithm problem . . . 70
3.4 Diffie-Hellman key exchange . . . 72
3.5 The digital signature algorithm . . . 74
3.5.1 What is digital signature? . . . 74
3.5.2 Digital signature algorithm steps . . . 76
3.6 Elliptic curves cryptography . . . 78
3.6.1 Elliptic curve discrete logarithm problem . . . 79
3.6.2 Elliptic curve Diffie-Hellman key exchange . . . 80
3.6.3 Elliptic curve digital signature algorithm . . . 82
3.6.4 ECC encryption/decryption . . . 85

4 Cryptographic applications over a non-commutative rings 88
4.1 Fully homomorphic encryption . . . 89
4.2 ECC over a non commutative ring R_p . . . 90
4.2.1 The ring R_p . . . 90
4.2.2 Cryptographic protocols . . . 92
4.2.3 Numerical example of cryptography . . . 95
4.3 FHE scheme over a non commutative ring R_m . . . 97
4.3.1 The ring R_m . . . 97
4.3.2 Encryption scheme using the ring R_m . . . 104
4.3.3 Numerical example of cryptography . . . 107

5 Encryption scheme based on a local ring 110
5.1 The finite ring A_4 . . . 111
5.2 Elliptic curve over the ring A_4 . . . 111
5.2.1 Classification of elements in $E^4_{a,b}$ . . . 111
5.2.2 The group law over $E^4_{a,b}$ . . . 112
5.3 Cryptographic protocols . . . 112
5.3.1 Exchange of secret key . . . 113
5.3.2 Encryption and decryption functions . . . 113
5.4 Cryptographic application . . . 114
5.4.1 Coding of elements of G . . . 114
5.4.2 Example for cryptography . . . 115

General conclusion and perspectives 121

Appendix A Groups, rings and fields 122
A.1 Basic definitions of the groups . . . 123
A.2 Introduction to rings . . . 124
A.3 Field extensions and finite fields . . . 126

Appendix B Algorithms **128**
B.1 Representation the elements of $\mathbb{F}_q[\varepsilon]$ 129
B.2 Representation of group $E_{a,b}(\mathbb{F}_q[\varepsilon])$ 131

Customized Index **134**

Bibliography **135**

List of Figures

1.1 A smooth curve and a singular curve. 4
1.2 Point addition $P + Q = R$. 8
1.3 Point doubling $[2]P = P + P = R$. 9
1.4 Point doubling $[2]P = \infty$. 9
1.5 Point inverse $P + Q = \infty$. 10
1.6 An elliptic curve $E : y^2 = x^3 + 3x + 5$ defined over a prime field $\mathbb{F}_{17}$. . . . 16

3.1 Characteristics of an algorithm. 57
3.2 Asymptotic notations: Big-O, Big-Omega, Big-Theta. 59
3.3 Time complexity analysis of algorithms. 60
3.4 The classification of the crypto-terminologies. 61
3.5 Communication between two parties. 62
3.6 Classification of cryptography algorithms. 64
3.7 Symmetric key cryptography. 64
3.8 Cryptographic hash functions 66
3.9 Asymmetric key cryptography. 68
3.10 Types of attacks. 70
3.11 Diffie–Hellman secret-key agreement protocol 73
3.12 Digital Signature Algorithm. 75
3.13 Elliptic curve Diffie-Hellman key exchange. 81

List of Tables

1.1 Weierstrass short forms for elliptic curves. 7
1.2 Operation count for adding and doubling points on $E/\mathbb{F}_q$. 26

2.1 The subgroup $G = \langle P \rangle$. 40

3.1 The elements of the group $G = \langle g \rangle$. 71
3.2 Comparable key sizes for equivalent security. 86

5.1 Elements of the subgroup G of order 63. 117
5.2 Code elements of the subgroup G. 118

List of Symbols

$\mathbb{K}$	Field.
$\overline{\mathbb{K}}$	Algebraic closure of a field $\mathbb{K}$.
$\mathbb{K}^*$	$\mathbb{K} - \{0\}$.
$\mathbb{K}[x, y]$	Polynomial ring of two variables.
$\mathbb{N}$	Set of natural numbers.
$\mathbb{Z}$	Set of integer numbers.
$\mathbb{Q}$	Set of rational numbers.
$\mathbb{R}$	Set of real numbers.
$\mathbb{C}$	Set of complex numbers.
$\mathbb{A}^n$	Affine space of dimension n over $\mathbb{K}$.
$(x_1, x_2, ..., x_n)$	Affine point in $\mathbb{A}^n$.
$\mathbb{A}^2$	Affine plane .
(x, y)	Affine point in $\mathbb{A}^2$.
E	Weierstrass equations.
$\triangle$	Discriminant of the elliptic curve.
$j(E)$	j-invariant of elliptic curve.
$char(\mathbb{K})$	The characteristic of a field $\mathbb{K}$.
$E(\mathbb{K})$	$\mathbb{K}$-rational points of the elliptic curve E.
$E/\mathbb{K}$	Elliptic curve over $\mathbb{K}$.
∞	The point at infinity.
$[n]$	Scalar multiplication by n on E.
$E[n]$	Set of n-torsion points of an elliptic curve E.
$\mathbb{F}_p$	The Prime finite field of order p.
$\mathbb{F}_q$	The unique finite field of order q.
$\overline{\mathbb{F}}_q$	Algebraic closure of $\mathbb{F}_q$.
$E(\mathbb{F}_q)$	$\mathbb{F}_q$-rational points on E.
$\#E(\mathbb{F}_q)$	Number of points in $E(\mathbb{F}_q)$.
ϕ_{End}	The q^{th}-power Frobenius endomorphism.
t	Trace of Frobenius.
gcd	The greatest common divisor.
$\cong$	Isomorphism.
$\mathbb{Z}/n\mathbb{Z}$	Quotient group of $\mathbb{Z}$ modulo n.
$\mathbb{K}[X_0, ..., X_n]$	Polynomial ring of n variables.
$\mathbb{K}[X, Y, Z]$	Polynomial ring of three variables.
$\mathbb{K}[X, Y, Z]_{hom}$	The set of homogeneous polynomials.
$\mathbb{P}^n$	Projective n-space .
$\mathbb{P}^2$	Projective plane .
$[X_0 : X_1 : \cdots : X_n]$	Projective point in $\mathbb{P}^n$.
$[X : Y : Z]$	Projective point in $\mathbb{P}^2$.
R	Ring.

R^*	The set of units of R.
$\mathcal{P}(R)$	The set of primitive triples of R.
$\sim_R$	The equivalence relation define on $\mathcal{P}(R)$.
$\mathbb{P}^2(R) = \mathcal{P}(R)/\sim_R$	The projection plane on R.
$\mathbb{F}_q[\varepsilon]$	The finite ring of characteristic $p \neq 2, 3$.
$(\mathbb{F}_q[\varepsilon])^\times$	The set of invertible elements in $\mathbb{F}_q[\varepsilon]$.
$\mathbb{P}^2(\mathbb{F}_q[\varepsilon])$	The projection plane on $\mathbb{F}_q[\varepsilon]$.
π_0	The canonical projection of element in $\mathbb{F}_q[\varepsilon]$.
π_1	The sum projection of coordinate of element in $\mathbb{F}_q[\varepsilon]$.
$E_{a,b}(\mathbb{F}_q[\varepsilon])$	Elliptic curve over the finite ring $\mathbb{F}_q[\varepsilon]$.
$E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$	Elliptic curve over the finite field $\mathbb{F}_q$.
$E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$	Elliptic curve over the finite field $\mathbb{F}_q$.
$[\pi_i(X) : \pi_i(Y) : \pi_i(Z)]$	Point of $\mathbb{P}^2(\mathbb{F}_q)$ where $i \in \{0, 1\}$.
$\triangle_0$	The image of the discriminant $\triangle$ by π_0.
$\triangle_1$	The image of the discriminant $\triangle$ by π_1.
j_0	The image of the j-invariant j by π_0.
j_1	The image of the j-invariant j by π_1.
φ_i	The morphism of group from $E_{a,b}(\mathbb{F}_q[\varepsilon])$ to $E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q)$ for $i \in \{0, 1\}$.
$\mathbb{F}_{3^d}[\varepsilon]$	The finite ring of characteristic 3.
$(\mathbb{F}_{3^d}[\varepsilon])^\times$	The set of invertible elements in $\mathbb{F}_{3^d}[\varepsilon]$.
$\mathbb{P}^2(\mathbb{F}_{3^d}[\varepsilon])$	The projection plane on $\mathbb{F}_{3^d}[\varepsilon]$.
Π_0	The canonical projection of element in $\mathbb{F}_{3^d}[\varepsilon]$.
Π_1	The sum projection of coordinate of element in $\mathbb{F}_{3^d}[\varepsilon]$.
$E_a, b(\mathbb{F}_{3^d}[\varepsilon])$	Elliptic curve over the finite ring $\mathbb{F}_{3^d}[\varepsilon]$.
$E_{\Pi_0(a),\Pi_0(b)}(\mathbb{F}_{3^d})$	Elliptic curve over the finite field $\mathbb{F}_{3^d}$.
$E_{\Pi_1(a),\Pi_1(b)}(\mathbb{F}_{3^d})$	Elliptic curve over the finite field $\mathbb{F}_{3^d}$.
$[\Pi_i(X) : \Pi_i(Y) : \Pi_i(Z)]$	Point of $\mathbb{P}^2(\mathbb{F}_{3^d})$ where $i \in \{0, 1\}$.
$\triangle'_0$	The image of the discriminant $\triangle$ by Π_0.
$\triangle'_1$	The image of the discriminant $\triangle$ by Π_1.
j'_0	The image of the j-invariant j by Π_0.
j'_1	The image of the j-invariant j by Π_1.
O	Big-Oh notation.
Ω	Big-Omega notation.
Θ	Big-Theta notation.
$\log_g(t)$	The discrete logarithm problem of t with respect to g.
$\mathcal{P}$	The set of plaintexts.
$\mathcal{C}$	The set of ciphertexts.
$\mathcal{K}$	Space of the keys.
$\mathcal{E}$	The set of encryption functions.
$\mathcal{D}$	The set of decryption functions.
$h(m)$	The hash value of the message m.

$\log_P(Q)$	The elliptic curve discrete logarithm problem of Q with respect to P.
K_{pub}	The public key.
K_{pr}	The private key.
$ord(P)$	The order of point P.
R_p	Non commutative polynomial ring.
R_m	Non commutative matrix ring.
$\widetilde{X}$	The tilde of matrix X.
$Encpk$	Encryption function using the ring R_p.
$Decsk$	Decryption function using the ring R_p.
E_{nc}	Encryption function using the ring R_m.
D_{ec}	Decryption function using the ring R_m.
$Z(R_m)$	The center of a ring R_m.
$R_m^{\times}$	The set of units of a ring R_m.
A_4	Local ring $\mathbb{F}_{3^d}[\varepsilon]$, where $\varepsilon^4 = 0$.
$E^4_{a,b}$	Elliptic curve over the ring A_4.
Enc	Encryption function using the ring A_4.
Dec	Decryption function using the ring A_4.

Acronyms of Abbreviations

AES	Advanced Encryption Standard.
CCA	Chosen cipertext attack.
CCP	Conjugal classical problem.
CPA	Chosen plaintext attack.
COA	Ciphertext only attack.
DES	Data encryption standard.
3DES	Triple data encryption standard.
DLP	Discrete logarithm problem.
D-H	Diffie and Hellman.
DHKE	Diffie and Hellman key exhcnage.
DSA	Digital signature algorithm.
EC	Elliptic curve.
ECC	Elliptic curve cryptography.
ECDH	Elliptic curve Diffie and Hellman.
ECDHKE	Elliptic curve Diffie and Hellman key exchange.
ECDLP	Elliptic curve discrete logarithm problem.
ECDSA	Elliptic curve digital signature.
FHE	Fully homomorphic encryption.
FIPS	Federal information processing standard.
IDEA	International data encryption algorithm.
IPSec	Internet Protocol Security.
KPA	Known plaintext attack.
RC 4-5-6	Rivest cipher 4-5-6.
MD5	Message digest.
NIST	National institute of standards and technology.
PKC	Public key cryptography.
RSA	Rivest-Shamir-Adleman.
SHA	Secure hash algorithm.
SSH	Secure Shell.
SSL	Secure Sockets Layer
TLS	Transport Layer Security.

List of Original Papers

This thesis is based on the following original publications. They will be referred to in the text by Roman numerals:

chapter 2

☞I B. Selikh, D. Mihoubi and N. Ghadbane, *Classification of elements in elliptic curve over the ring* $\mathbb{F}_q[\varepsilon]$, Discussiones Mathematicae General Algebra and Applications, 41(2) (2021), pp. 283–298.

☞II B. Selikh, *Study of elliptic curve over a finite ring* $\mathbb{F}_{3^d}[\varepsilon], \varepsilon^4 = \varepsilon^3$, Gulf Journal of Mathematics, in press.

chapter 4

☞III B. Selikh, A. Chillali, D. Mihoubi and N. Ghadbane, *A novel non-commutative cryptography scheme using a special ring* $\mathbb{F}_q[\varepsilon], \varepsilon^4 = \varepsilon^3$, manuscript submitted for publication.

☞IV B. Selikh, A. Chillali, D. Mihoubi and N. Ghadbane, *A new public key cryptosystem based on the non-commutative ring* R, Journal of Discrete Mathematical Sciences & Cryptography, in press.

chapter 5

☞V B. Selikh, A. Chillali, D. Mihoubi and N. Ghadbane, *ECC over the ring* $\mathbb{F}_{3^d}[\varepsilon]; \varepsilon^4 = 0$ *by using two methods,* Tbilisi Mathematical Journal, 14(3) (2021), pp. 213-223.

General Introduction

An elliptic curves are a special case of algebraic curve of the form $y^2 = f(x)$, where $f(x)$ is a cubic polynomial with no repeated roots. The first appearance of the elliptic curve was in the second or third century AD in the book "Arithmetica" of Diophantus, who had no idea about elliptic curves.

The problem posed in his book on the elliptic curve is as follows: " To divide a given number into two numbers such that their product is cube minus its side." And the equation that Diophantus wrote is $y(a - y) = x^3 - x$ which is actually an elliptic curve in disguise.

From the eleventh to the nineteenth centuries, elliptic curves were famous in number theory and algebraic geometry through the works of both Fibonacci, Bachet, Fermat, Euler, Newton, Jacobi, Weierstrass and Poincare.

Elliptic curves were originally created in areas related to analysis, the name “elliptic” is given because these curves arose in studying the problem of calculating integrals to finding the arc length of an ellipse, but nowadays it has come to play an important role in many areas of mathematics (number theory, algebraic geometry, coding, cryptography etc). It has many uses, including:

- Used to demonstrate of Fermat’s Great Theorem by Andrew Wiles [90].
- Used for the factorization of integers by Lenstra [47].
- Used in number theory algorithms for proofs and primality tests by Goldwasser and Kilian [27].
- Used in random bit generation framework by Kaliski [38].
- Used in coding theory by Driencourt Michon [19] et Gerard van der Geer [25].

  . . .

Information security, is the science that works to protect the information and equipment used to store, process and transmit it, from theft, intrusion, natural disasters, or all of them. It works to keep it available to authorized individuals, and the inability to obtain information, except by persons authorized to do so.
In computer science, cryptography is a way of protect information and communications between parties by using codes, so that only the parties targeted by the information can read and process it. This is done through the use of specific algorithms (which is a set of mathematical calculations) and a private key.

In cryptography, to transform messages in ways that are hard to decipher, these deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet, and protect confidential transactions such as credit card and debit card transactions and email.

In 1976, public key algorithms came in public sphere when Whitfield Diffie and Martin Hellman published their article entitled by "New Directions in Cryptography" (see [18]), this is known as the Diffie-Hellman key exchange.
The Diffie-Hellman key exchange was one of the most important developments in public key cryptography and it is still frequently implemented in a range of today is different security protocols. Diffie-Hellman and RSA cryptographic methods are based on the creation of keys by using very large prime numbers. Hence, a key generation method requires a lot computations power.

In the mid 1980, Neal Koblitz and Victor Miller independently proposed of elliptic curves in cryptography (see [42, 52]), it was approved by the US government. Elliptic curve cryptography (ECC) is a public key encryption technique (the latest family of public-key cryptosystems) based on the theory of elliptic curves that can be used to create smaller and more efficient cryptographic keys. This makes it ideal for the increasingly mobile world. ECC was proposed as an alternative to public key cryptosystems such as DH, DSA, RSA, and ElGamal. Some researchers have shown that a security level with a 164-bits key for ECC, requires a 1024-bits key for RSA. The shorter key lengths require less computing power, meaning faster, secure connections to the like of smart phone and tablets on-the-go.

Our work falls within the framework of elliptic curves and their applications in cryptography, more precisely those defined on a finite non local ring $\mathbb{F}_q[\varepsilon]$; where $\varepsilon^4 = \varepsilon^3$ of characteristic p different 2 and 3. Elliptic curves defined on a ring have been studied in different aspects.
In algebraic geometry, Joseph Hillel Silverman in his book [76] studied these curves in the case of a local ring.

In number theory, Hendrik Willem Lenstra Junior in his article [46] studied these curves on the ring $\mathbb{Z}_{pq}$ with p and q be two different prime numbers, which made it possible to factor large integers using elliptic curves. And in cryptography, Sebastia Martin in his thesis [51] studied the elliptic curves on the same ring $\mathbb{Z}_{pq}$, he built an ElGamal cryptosystem using these curves and studied the number of curve points over the rings of type $\mathbb{Z}_p^n$.

Marie Virat [88] studied the elliptic curves over the local finite ring $\mathbb{F}_q[\varepsilon]$; where $\varepsilon^2 = 0$ of characteristic $p \neq 2, 3$. This study allowed him, among other things, to create a W_{ε_0} cryptosystem, which is similar to that of ElGamal but with additional performance.

Abdelhakim Chillali [14] generalized the work of Marie Virat by extending it to the rings $\mathbb{F}_q[\varepsilon]$, with $\varepsilon^n = 0$ and $q = p^n, p \geqslant 5$ be a prime number and $n \in \mathbb{N}^*$, and created some cryptosystems based on this elliptic curve (see [13, 15]).

In 2016-2017, Aziz Boulbot et al [5, 6] were studied the classification of elements in elliptic curves over the non-local finite rings $\mathbb{F}_q[e]$; where $e^2 = e$ and $\mathbb{F}_q[e]$; where $e^3 = e^2$ of characteristics $p \neq 2, 3$. And in 2018, they studied the group law of elliptic curve over the ring $\mathbb{F}_{3^d}[e]$; where $e^2 = e$ of characteristic 3 [4]. And in 2019, they introduced a new encryption protocols based on a non commutative ring by using the elliptic curve over a ring $\mathbb{F}_q[e]$; where $e^2 = e$ [7].

In 2019, Mustapha Elhassani et al [20] were introduced a new diagram of fully homomorphic encryption based on the non commutative ring $\mathbb{F}_q[e]$; where $e^3 = e^2$.

The aim of this work is to study elliptic curves and cryptography on them, and to show the strength of data security and cryptographic algorithms built using these curves for against attacks. In this thesis, we are interested in studying elliptic curves over the rings $\mathbb{F}_q[\varepsilon]$ and $\mathbb{F}_{3^d}[\varepsilon]$; where $\varepsilon^4 = \varepsilon^3$, it is an extension of the study conducted by Aziz Boulbot et al. in their articles (see [4–6]), and the non commutative cryptography based on the ring $\mathbb{F}_q[\varepsilon]$.
In our research, we addressed three axes:

- **The algebraic axis:** we defined and studied the rings $\mathbb{F}_q[\varepsilon]$ and $\mathbb{F}_{3^d}[\varepsilon]$.
- **The algebraic geometry axis:** we defined the elliptic curve over the ring $\mathbb{F}_q[\varepsilon]$, and the group law over it.
- **The cryptography axis:** we applied the results found in the two previous axes.

This thesis is organized in two parts, the part I is a study and theoretical description of the elliptic curves and the part II is a cryptographic applications based on the elliptic curves.

The part I opens with the two chapters 1 and 2 where:

- **Chapter 1:** It is intended for basics on elliptic curves over any field $\mathbb{K}$ and is composed of two sections namely affine elliptic curves and projective elliptic curve. We recall the generalities of elliptic curves as we study the simplification of Weierstrass equations and we will give the Weierstrass equations of these elliptic curves in the certain cases of the field $\mathbb{K}$, then we define the group law geometrically and explicitly (in the affine and projective cases) on these curves.
- **Chapter 2:** We will define the rings $\mathbb{F}_q[\varepsilon]$ and $\mathbb{F}_{3^d}[\varepsilon]$, with $\varepsilon^4 = \varepsilon^3$. Furthermore, the ring $\mathbb{F}_q[\varepsilon]$ which will be the core of this thesis for cryptographic applications in chapter 4. In the sections 2.3 and 2.4 we will define the elliptic curves over these rings, denoted $E_{a,b}(\mathbb{F}_q[\varepsilon])$ and $E_{a,b}(\mathbb{F}_{3^d}[\varepsilon])$. Next, we study the classification of elements in elliptic curves over these rings [71, 80].

The part II consists of the three chapters 3, 4 and 5 where:

- **Chapter 3:** We will provide an overview of cryptography and its classifications with a focus on studying of a public key encryption and security evidence.
  In the sections 3.3, 3.4 and 3.5 are discuss some notions of an algorithms and its security: the discrete logarithm problem (DLP); the Diffie-Hellman key exchange (DH) and the digital signature algorithm (DSA). In the section 3.6, we talk about the elliptic curves cryptography by setting out the keys by using the elliptic curve Diffie-Hellman key exchange (ECDHKE), signature and verification algorithms, and encryption/decryption algorithms based on elliptic curve discrete logarithm problem (ECDLP).

- **Chapter 4:** Here, we will be interested in studying non-commutative cryptography and fully homomorphic encryption. In the sections 4.2 and 4.3, using the elliptic curve over the ring $\mathbb{F}_q[\varepsilon]$ we will make a two new fully homomorphic schemes over a special rings based on the two difficult problems; problem of conjugal and discrete logarithm problem [68, 69].

- **Chapter 5:** We will be interested in the ECC based on a local ring, where the sections 5.1 and 5.2 are fundamental results from the article of Moulay Hachim Hassib et al [32], where had constructed the ring $A_4 := \mathbb{F}_{3^d}[\varepsilon] = \mathbb{F}_{3^d}[X]/(X^4)$, with $\varepsilon^4 = 0$, defined an elliptic curve over $\mathbb{F}_{3^d}[\varepsilon]$ and they had given the classification of elements in elliptic curve $E_{a,b}(A_4)$. We will introduce both the Diffie-Hellman protocol over $E_{a,b}(A_4)$ and a cryptosystem for encryption and decryption, then we will present a cryptographic application using an encoding of the elements of a cyclic subgroup G generated by a point P of known order [70].

- **Appendix A:** This appendix is a overview of the basic concepts of groups, rings, polynomial rings, fields, finite fields and extension of fields.

- **Appendix B:** We will show the fundamental algorithms over the ring $\mathbb{F}_q[\varepsilon]$ and the group $E_{a,b}(\mathbb{F}_q[\varepsilon])$.

Part I

Arithmetic of Elliptic Curves

Chapter 1

Elliptic curves over a field $\mathbb{K}$

"Elliptic curves are a particular family of Diophantine equations which play an important role in many areas of mathematics (geometry, theory of numbers, cryptography and so on). The subject of elliptic curves is vast, and we content ourselves to studying its basic concepts (affine and projective) over any field $\mathbb{K}$ by using of Weierstrass equations."
For more information about elliptic curves, see the following books and articles:
[9, 10]; [22]; [34–37]; [42, 43, 45]; [76–78] and [82, 89].

Contents in Brief

1.1 Affine elliptic curves 3
1.1.1 Simplified Weierstrass equations 5
1.1.2 The group law 8
1.1.3 Isomorphism of elliptic curves 13
1.1.4 Elliptic curve over a finite field 15
1.2 Projective elliptic curves 18
1.2.1 Projective space 18
1.2.2 Arithmetic in projective coordinates 20

Throughout this thesis, we set the following notation: $\mathbb{K}$ be a field and $\overline{\mathbb{K}}$ its algebraic closure. We will use the following site: `https://asecuritysite.com/` in examples of this chapter to compute the group law elements.

1.1 Affine elliptic curves

In this section, we introduce the basic concepts and definitions related to space affine and affine curves. Our main objective is to study the basic notions of the affine elliptic curves over the field $\mathbb{K}$.

Definition 1.1. The affine space (over $\mathbb{K}$) of dimension n is the set of points

$$\mathbb{A}^n = \mathbb{A}^n(\overline{\mathbb{K}}) = \{(x_1, x_2, ..., x_n) \mid x_i \in \overline{\mathbb{K}}\}.$$

The set of $\mathbb{K}$-rational points of $\mathbb{A}^n(\overline{\mathbb{K}})$ is the set

$$\mathbb{A}^n(\mathbb{K}) = \{(x_1, x_2, ..., x_n) \in \mathbb{A}^n(\overline{\mathbb{K}}) \mid x_i \in \mathbb{K}\}.$$

If $n = 2$, then the affine space is called affine plane.
If $n = 1$, then the affine space is called affine line.

• An affine plane curve C over $\mathbb{K}$ is the set of zeros an irreducible polynomial $H \in \mathbb{K}[x, y]$ in the affine plane, i.e. $\{(x, y) \in \mathbb{A}^2(\mathbb{K}) \mid H(x, y) = 0\}$.

• Let C be a curve and $P = (x_1, y_1)$ be a point on C. Then P is singular on C if $\frac{\partial C}{\partial x}(x_1, y_1) = \frac{\partial C}{\partial y}(x_1, y_1) = 0$. A singular curve is a curve with at least one singular point (is not smooth).

Example 1.1. Let $C : y^2 = x^3 + 3x^2$ be a curve over $\mathbb{K} = \mathbb{R}$, and the point $P = (0, 0)$ be a point on C, we easily verify that $\frac{\partial C}{\partial x}(0, 0) = \frac{\partial C}{\partial y}(0, 0) = 0$. Then we say that the point P is a singular point (the curve C is not smooth).

Definition 1.2 (See [77]). An elliptic curve E over a field $\mathbb{K}$ (denoted by $E/\mathbb{K}$) of genus [1]one is the set of solutions in the affine plane $\mathbb{A}^2(\mathbb{K})$ of Weierstrass equation of the form:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1.1}$$

where $a_1, a_2, a_3, a_4, a_6 \in \mathbb{K}$. This equation is also referred to as the long Weierstrass form. The discriminant of the curve E is defined as:

$$\triangle = -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6,$$

[1]The genus g given by $g = \frac{(d-2)(d-1)}{2} - s$, where d is the degree of irreducible plane curve, s is the number of singularities when properly counted.

where:
$$\begin{cases} d_2 = a_1^2 + 4a_2; \\ d_4 = 2a_4 + a_1a_3; \\ d_6 = a_3^2 + 4a_6; \\ d_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{cases}$$

When $\triangle \neq 0$, the j-invariant of the curve E is defined as:
$j(E) = c_4^3/\triangle$, where $c_4 = d_2^2 - 24d_4$. The j-invariant makes it possible to classify the curves by class of isomorphisms.

For example an elliptic curve over finite field $\mathbb{K} = \mathbb{F}_p$ with $p = 97$ is given by:

$$E_1 : y^2 + 4xy + 3y = x^3 + 2x^2 + 30x + 55.$$

We have, $d_2 = 24$, $d_4 = 72$, $d_6 = 35$, $d_8 = 78$, $\triangle(E_1) = 5$, $j(E_1) = 74$.

Definition 1.3. An elliptic curve E defined over $\mathbb{K}$ is a smooth curve given by a Weierstrass equation (1.1). The term "*smooth curve*" means that the following property is satisfied: if $(x, y) \in \overline{\mathbb{K}}^2$ verify equation (1.1) then the partial derivatives of the curve equation $\frac{\partial E}{\partial y}(x, y) = 2y + a_1x + a_3$ and $\frac{\partial E}{\partial x}(x, y) = 3x^2 + 2a_2x + a_4 - a_1y$ are not simultaneously zero.

Remark 1.1. The condition $\triangle \neq 0$ ensures that the elliptic curve is "*smooth*" i.e. there are no points at which the curve has two or more distinct tangent lines.

Example 1.2. Let E_1 and E_2 are two curves (over $\mathbb{K} = \mathbb{R}$) defined by $y^2 = x^3 + x$ and $y^2 = x^3 + x^2$ respectively, with $\triangle(E_1) = -4 \neq 0, J(E_1) = 1728$ and $\triangle(E_2) = 0$. We have E_1 is a smooth curve and E_2 is a singular curve as shown in the figure 1.1:

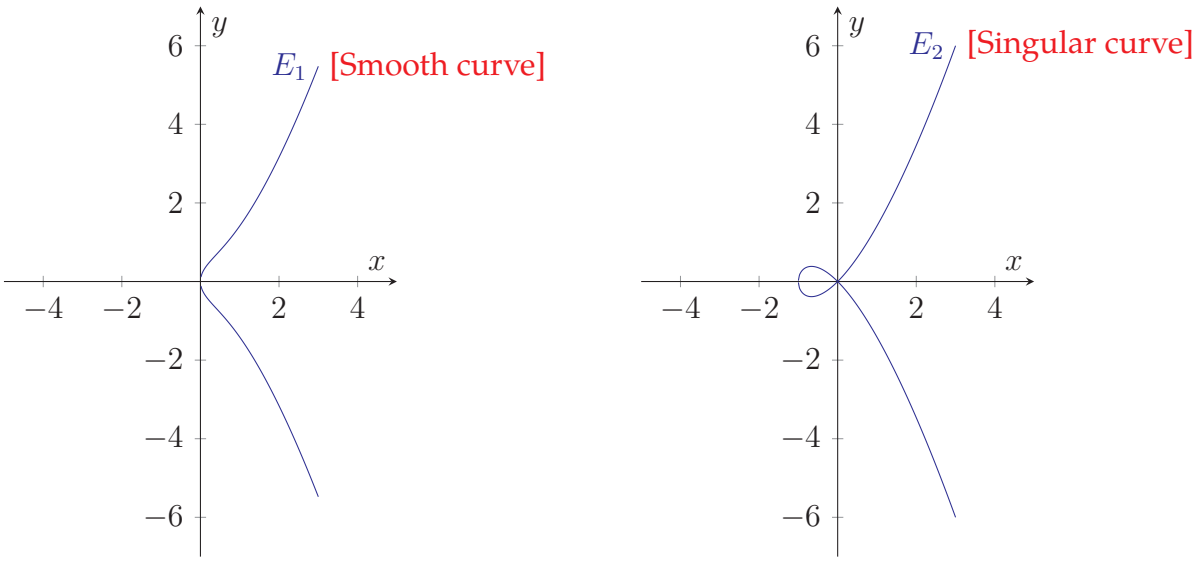


Figure 1.1: A smooth curve and a singular curve.

Proposition 1.1 (See [77]). *The curve E given by a Weierstrass equation satisfies:*

(i) It is non-singular if and only if $\triangle \neq 0$.

(ii) It has a node if and only if $\triangle = 0$ and $c_4 \neq 0$.

(iii) It has a cusp if and only if $\triangle = c_4 = 0$.

In cases (ii) and (iii), there is only the one singular point.

1.1.1 Simplified Weierstrass equations

An elliptic curve E defined by Weierstrass equation (1.1) over the field $\mathbb{K}$ with multiplicative identity $1_{\mathbb{K}}$ and addition identity $0_{\mathbb{K}}$ of the characteristic $char(\mathbb{K}) = p$.
The equation (1.1) can be simplified over $\mathbb{K}$ by the following subsitutions.

If $char(\mathbb{K}) \neq 2$

We substitute:

$$(x, y) \longmapsto \left(x, y - \frac{a_1}{2}x - \frac{a_3}{2}\right),$$

we have:

$$\left(y - \frac{a_1}{2}x - \frac{a_3}{2}\right)^2 + a_1 x\left(y - \frac{a_1}{2}x - \frac{a_3}{2}\right) + a_3\left(y - \frac{a_1}{2}x - \frac{a_3}{2}\right) = x^3 + a_2x^2 + a_4x + a_6$$

$$y^2 + \frac{a_1^2}{4}x^2 + \frac{a_3^2}{4} - a_1xy - a_3y + \frac{a_1a_3}{2}x + a_1xy - \frac{a_1^2}{2}x^2 - \frac{a_1a_3}{2}x + a_3y - \frac{a_1a_3}{2}x - \frac{a_3^2}{2}$$

$$= x^3 + a_2x^2 + a_4x + a_6$$

thus, $y^2 = x^3 + \underbrace{\left(a_2 + \frac{a_1^2}{4}\right)}_{a}x^2 + \underbrace{\left(a_4 + \frac{a_1a_3}{2}\right)}_{b}x + \underbrace{\left(a_6 + \frac{a_3^2}{4}\right)}_{c},$

transforms E to the curve:

$$E : y^2 = x^3 + ax^2 + bx + c, \tag{1.2}$$

where $a, b, c \in \mathbb{K}$.
- The discriminant of this curve is $\triangle = -64a^3c + 16a^2b^2 + 288abc - 64b^3 - 432c^2$.
- The j-invariant of this curve is $j(E) = (16a^2 - 48b)^3/\triangle$.

If $char(\mathbb{K}) \neq 2, 3$

By the equation (1.2), we substitute:

$$(x, y) \longmapsto \left(x - \frac{a_2'}{3}, y\right),$$

eliminates the x^2 term, yielding the simpler equation:

$$\begin{aligned} y^2 &= \left(x - \frac{a_2'}{3}\right)^3 + a_2'\left(x - \frac{a_2'}{3}\right)^2 + a_4'\left(x - \frac{a_2'}{3}\right) + a_6' \\ &= x^3 - \frac{a_2'^3}{27} - a_2'x^2 + \frac{a_2'^2}{3}x + a_2'x^2 + \frac{a_2'^3}{9} - \frac{2}{3}a_2'^2x + a_4'x - \frac{a_2'a_4'}{3} + a_6' \\ &= x^3 + \underbrace{\left(a_4' - \frac{a_2'^2}{3}\right)}_{a}x + \underbrace{\left(a_6' + 2\frac{a_2'^3}{27} - \frac{a_2'a_4'}{3}\right)}_{b}, \end{aligned}$$

transforms E to the curve:

$$E : y^2 = x^3 + ax + b, \tag{1.3}$$

where $a, b \in \mathbb{K}$.
- The discriminant of this curve is $\triangle = -16(4a^3 + 27b^2)$.
- The j-invariant of this curve is $j(E) = (-48a)^3/\triangle$.

If $char(\mathbb{K}) = 2$

We substitute:

$$(x, y) \longmapsto \left(a_1^2x + \frac{a_3}{a_1}, a_1^3y + \frac{a_1^2a_4 + a_3^2}{a_1^3}\right),$$

we get:

$$\begin{aligned} &\left(a_1^3y + \frac{a_1^2a_4 + a_3^2}{a_1^3}\right)^2 + a_1\left(a_1^2x + \frac{a_3}{a_1}\right)\left(a_1^3y + \frac{a_1^2a_4 + a_3^2}{a_1^3}\right) + a_3\left(a_1^3y + \frac{a_1^2a_4 + a_3^2}{a_1^3}\right) \\ &= \left(a_1^2x + \frac{a_3}{a_1}\right)^3 + a_2\left(a_1^2x + \frac{a_3}{a_1}\right)^2 + a_4\left(a_1^2x + \frac{a_3}{a_1}\right) + a_6. \end{aligned}$$

Keeping in mind that $2a_i = 0$ for all $a_i \in \mathbb{K}$ because $char(\mathbb{K}) = 2$, we find:

$$\begin{aligned} y^2 + xy = x^3 &+ \underbrace{\left(\frac{a_1a_3 + a_1^2 + a_2}{a_1^3}\right)}_{a}x^2 \\ &+ \underbrace{\left(\frac{a_1^4a_4^2 + a_3^4}{a_1^6} + \frac{a_1^2a_4 + a_3^2}{a_1^2} + \frac{a_3(a_1^2a_4 + a_3^2)}{a_1^2} + \frac{a_2a_3^2}{a_1^2} + \frac{a_4 + a_3}{a_1} + a_6\right)}_{b}, \end{aligned}$$

transforms E to the curve:

$$E : y^2 + xy = x^3 + ax^2 + b, \tag{1.4}$$

where $a, b \in \mathbb{K}$.
- The discriminant of this curve is $\triangle = b$.
- The j-invariant of this curve is $j(E) = 1/b$.

In case $char(\mathbb{K}) = 2$, if $a_1 = 0$ we can find another short form by the substitution

$$(x, y) \longmapsto (x + a_2, y),$$

transforms E to the curve:

$$E : y^2 + cy = x^3 + ax + b, \tag{1.5}$$

where $a, b, c \in \mathbb{K}$. Such a curve is said to be supersingular.
- The discriminant of this curve is $\triangle = c^4$.
- The j-invariant of this curve is $j(E) = 0$.

If $char(\mathbb{K}) = 3$

We have two cases to consider.
❖ If $a_1^2 \neq -a_2$, we substitute:

$$(x, y) \longmapsto \left(x + \frac{a_4 - a_1 a_3}{a_1^2 + a_2}, y + a_1 x + \frac{a_1(a_4 - a_1 a_3)}{a_1^2 + a_2} + a_3 \right),$$

in the same calculation method as in the previous cases, transforms E to the curve:

$$E : y^2 = x^3 + ax^2 + b, \tag{1.6}$$

where $a, b \in \mathbb{K}$. Such a curve is said to be non-supersingular.
- The discriminant of this curve is $\triangle = -a^3 b$.
- The j-invariant of this curve is $j(E) = -a^3/b$.

❖ If $a_1^2 = -a_2$, we can find another short form by the substitution

$$(x, y) \longmapsto (x, y + a_1 x + a_3),$$

transforms E to the curve:

$$E : y^2 = x^3 + ax + b, \tag{1.7}$$

where $a, b \in \mathbb{K}$. Such a curve is said to be supersingular.
- The discriminant of this curve is $\triangle = -a^3$.
- The j-invariant of this curve is $j(E) = 0$.

The following table summarizes all of the Weierstrass short forms that we found:

$char(\mathbb{K})$	Weierstrass short equation	Discriminant $\triangle$	j-invariant
$\neq 2$	$y^2 = x^3 + ax^2 + bx + c$	$-64a^3c + 16a^2b^2 + 288abc - 64b^3 - 432c^2$	$(16a^2 - 48b)^3/\triangle$
$\neq 2, 3$	$y^2 = x^3 + ax + b$	$-16(4a^3 + 27b^2)$	$(-48a)^3/\triangle$
$= 2$	$y^2 + xy = x^3 + ax^2 + b$ $y^2 + cy = x^3 + ax + b$	b c^4	$1/b$ 0
$= 3$	$y^2 = x^3 + ax^2 + b$ $y^2 = x^3 + ax + b$	$-a^3b$ $-a^3$	$-a^3/b$ 0

Table 1.1: Weierstrass short forms for elliptic curves.

1.1.2 The group law

Definition 1.4. Let E be an elliptic curve (over $\mathbb{K}$) defined by the Weierstrass equation (1.1). The set of $\mathbb{K}$-rational points on E is:

$$E(\mathbb{K}) = \{(x, y) \in \mathbb{K}^2 \mid y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0\} \cup \{\infty\}.$$

The same:

$$E(\overline{\mathbb{K}}) = \{(x, y) \in \overline{\mathbb{K}}^2 \mid y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0\} \cup \{\infty\},$$

where ∞ is the point at infinity. Note that if $\mathbb{K} \subset \mathbb{L} \subset \overline{\mathbb{K}}$ then $E(\mathbb{K}) \subset E(\mathbb{L}) \subset E(\overline{\mathbb{K}})$.

1.1.2.1 Geometric addition of points

Let E be an elliptic curve defined over the field $\mathbb{K}$. There is a chord-and-tangent rule for adding two points in $E(\mathbb{K})$ to give a third point in $E(\mathbb{K})$. Together with this addition operation, the set of points $E(\mathbb{K})$ forms an abelian group with ∞ serving as its identity. It is this group that is used in the construction of elliptic curve cryptographic systems (see [75, 82]). The addition rule is best explained geometrically. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are two distinct points on an elliptic curve E, then the sum $R = (x_3, y_3)$ of P and Q is defined as follows. First draw a line through P and Q; this line intersects the elliptic curve at a third point. Then R is the reflection of this point about the x-axis. This is depicted in the figure 1.2:

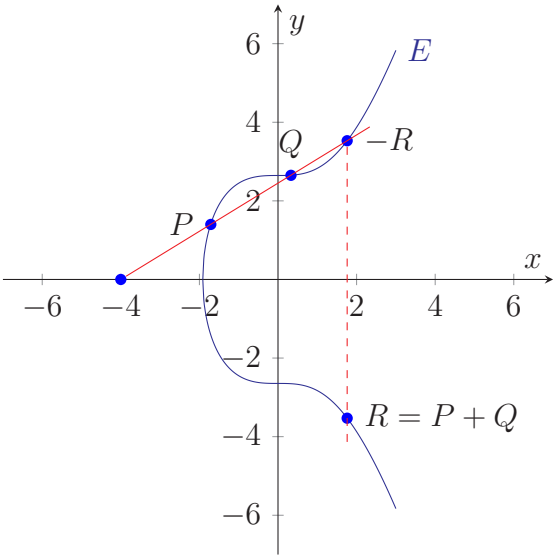


Figure 1.2: Point addition $P + Q = R$.

The double R of P is defined as follows. First draw the tangent line to the elliptic curve at the point P. This line intersects the elliptic curve at a second point. Then R is the reflection of this point about the x-axis. This is depicted in the figure 1.3:

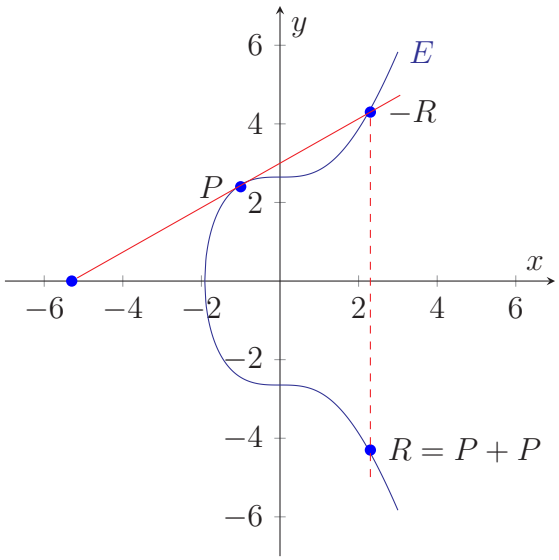


Figure 1.3: Point doubling $[2]P = P + P = R$.

If the tangent to the point is vertical, it intersects the curve at the point at infinity and $[2]P = P + P = \infty$, i.e. P is a point of order 2. This is depicted in the figure 1.4:

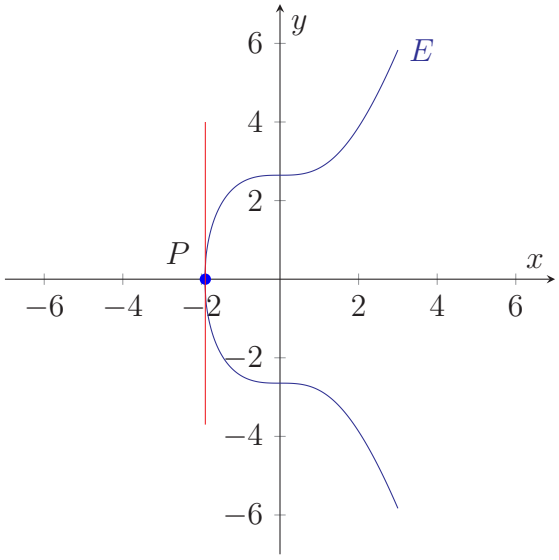


Figure 1.4: Point doubling $[2]P = \infty$.

In the case $x_1 = x_2$ but $y_1 \neq y_2$, the line through P and Q is a vertical line, which therefore intersects E in ∞. Reflecting ∞ across the x-axis yields the same point ∞ (this is why we put ∞ at both the top and the bottom of the y-axis). Therefore, in this case $P + Q = \infty$. This is depicted in the figure 1.5:

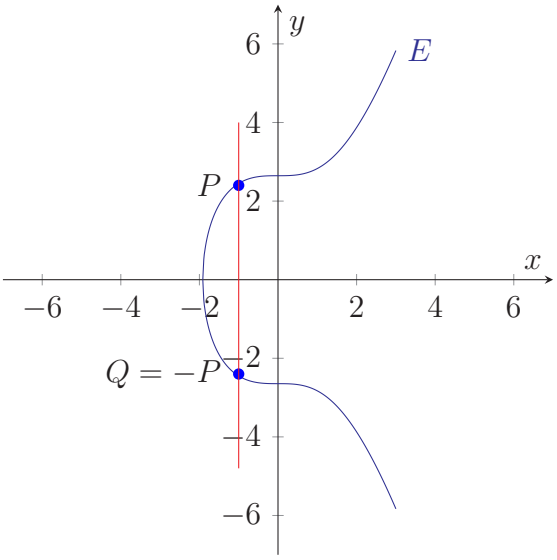


Figure 1.5: Point inverse $P + Q = \infty$.

1.1.2.2 Algebraic addition of points

Definition 1.5. We define an abelian group law $+$ on $E(\mathbb{K})$ as follows:

1. [*Identity*] $P + \infty = \infty + P = P$ for all $P \in E(\mathbb{K})$.
2. [*Inverse*] If $P \in E(\mathbb{K})$, then $(x, y) + (x, -y - a_1x - a_3) = \infty$. The point $(x, -y - a_1x - a_3)$ is denoted by $-P$ and is called the inverse of P.
3. [*Addition-Doubling*] Let $P = (x_1, y_1)$ and $Q(x_2, y_2)$ are two points in $E(\mathbb{K})$. For addition $P + Q = R = (x_3, y_3)$ we have two cases $P \neq \pm Q$ and $P = Q$.

We will show explicit formulas for adding two points (see [34]).
Let $P = (x_1, y_1) \in E(\mathbb{K})$ and $Q = (x_2, y_2) \in E(\mathbb{K})$ with $P \neq -Q$ (otherwise, Q is inverse of P and we have $P + Q = \infty$).
We take $P \neq Q$, and we compute the coordinates of $P + Q = R = (x_3, y_3)$. The line passing through P and Q has for equation $y = \lambda x + \mu$ with:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \text{ and } \mu = y_1 - \lambda x_1.$$

The intersection of the line (PQ) with the curve E is given by:

$$(\lambda x + \mu)^2 + (a_1x + a_3)(\lambda x + \mu) = x^3 + a_2x^2 + a_4x + a_6,$$

which gives the following equation:

$$z(x) = x^3 + (a_2 - \lambda^2 - a_1\lambda)x^2 + (a_4 - 2\lambda\mu - a_1\mu - a_3\lambda)x + (a_6 - \mu^2 - a_3\mu) = 0.$$

We already know two roots of $z(x)$, namely the x-coordinates of the other two points x_1 and x_2. Since

$$z(x) = (x - x_1)(x - x_2)(x - x_3).$$

Now the sum of three roots is the opposite of the coefficient of degree 2 and we therefore set:

$$\lambda^2 + a_1\lambda - a_2 = x_1 + x_2 + x_3 \text{ and } \tilde{y_3} = \lambda x_3 + \mu.$$

The point $(x_3, \tilde{y_3})$ is the third point of intersection sought. Thus, we have:

$$\begin{aligned} P + Q = (x_3, y_3) &= (\lambda^2 + a_1\lambda - a_2 - x_1 - x_2, -\lambda x_3 - \mu - a_1 x_3 - a_3) \\ &= (\lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1 - a_1 x_3 - a_3). \end{aligned}$$

Doubling $P = (x_1, y_1) = Q$. The line tangent to the curve E at point P has the equation $y = \lambda x + \mu$ with the slope λ obtain by implicit derivating. We have:

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} \text{ and } \mu = y_1 - \lambda x_1.$$

After substitution in the Weierstrass equation and with the same work we find:

$$\lambda^2 + a_1\lambda - a_2 = 2x_1 + x_3 \text{ and } \tilde{y_3} = \lambda x_3 + \mu.$$

The point $(x_3, \tilde{y_3})$ is the third point of intersection sought. Thus, we have:

$$\begin{aligned} [2]P = P + P = (x_3, y_3) &= (\lambda^2 + a_1\lambda - a_2 - 2x_1, -\lambda x_3 - \mu - a_1 x_3 - a_3) \\ &= (\lambda^2 + a_1\lambda - a_2 - 2x_1, \lambda(x_1 - x_3) - y_1 - a_1 x_3 - a_3). \end{aligned}$$

Proposition 1.2. *We have the following rules to calculate the law "+". We pose $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, then:*

- $-P = (x_1, -y_1 - a_1x_1 - a_3)$.
- $P + Q = (x_3, y_3)$ *with* $x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1 - a_1x_3 - a_3$, *where:*

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if} \quad P \neq \pm Q; \\ \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & \text{if} \quad P = Q. \end{cases}$$

If $P = Q$ and $2y_1 + a_1x_1 + a_3 = 0$ then $P + Q = P + P = \infty$.

We recall the particular cases of elliptic curves (over fields of $char(\mathbb{K}) \neq 2, 3$ and $char(\mathbb{K}) = 3$) which we will be interested hereafter.

Group law for $E/\mathbb{K}$: $y^2 = x^3 + ax + b$, $char(\mathbb{K}) \neq 2, 3$

Let $P = (x_1, y_1)$ and $Q = (x_2, y_2) \in E(\mathbb{K})$.

- The inversion of P is $-P = (x_1, -y_1)$.
- If $P \neq \pm Q$, then $P + Q = (x_3, y_3)$ with $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$, where $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$.
- If $P = Q$, then $[2]P = P + P = (x_3, y_3)$ with $x_3 = \lambda^2 - 2x_1$, $y_3 = \lambda(x_1 - x_3) - y_1$, where $\lambda = \dfrac{3x_1^2 + a}{2y_1}$.

Group law for $E/\mathbb{K}$: $y^2 = x^3 + ax^2 + b$, $char(\mathbb{K}) = 3$

Let $P = (x_1, y_1) \in E(\mathbb{K})$ and $Q = (x_2, y_2) \in E(\mathbb{K})$.

- The inversion of P is $-P = (x_1, -y_1)$.
- If $P \neq \pm Q$, then $P + Q = (x_3, y_3)$ with $x_3 = \lambda^2 - a - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$, where $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$.
- If $P = Q$, then $[2]P = P + P = (x_3, y_3)$ with $x_3 = \lambda^2 - a - 2x_1$, $y_3 = \lambda(x_1 - x_3) - y_1$, where $\lambda = \dfrac{3x_1^2 + 2ax_1}{2y_1}$.

Example 1.3. We consider $E : y^2 = x^3 + 7x + 11$ defined over $\mathbb{F}_{23}$, with $char(\mathbb{F}_{23}) \neq 2, 3$. Note that $\triangle = -4639 = 7 \not\equiv 0[23]$, so E is indeed an elliptic curve. The points of $E(\mathbb{F}_{23})$ are as follows:

$(3,6)$	$(3,17)$	$(6,4)$	$(6,19)$	$(7,9)$	$(7,14)$	$(8,2)$
$(8,21)$	$(10,0)$	$(11,4)$	$(11,19)$	$(12,12)$	$(12,11)$	$(14,1)$
$(14,22)$	$(15,8)$	$(15,15)$	$(17,12)$	$(17,11)$	$(18,9)$	$(18,14)$
$(20,3)$	$(20,20)$	$(21,9)$	$(21,14)$	$(22,16)$	$(22,7)$	∞

Examples of elliptic curve addition are $(10,0)+(7,9) = (15,15)$, and $[2](10,0) = (10,0)+(10,0) = \infty$.

Definition 1.6 (Scalar multiplication). Take $n \in \mathbb{N} \setminus \{0\}$ and let us denote the scalar multiplication by n on E by $[n]$, or $[n]_E$ to avoid confusion. Namely,

$$[n] : \left| \begin{array}{ccc} E(\mathbb{K}) & \longrightarrow & E(\mathbb{K}) \\ P & \longmapsto & [n]P = \underbrace{P + P + \cdots + P}_{n-\text{times}} \end{array} \right.$$

This definition extends trivially to all $n \in \mathbb{Z}$, setting $[0]P = \infty$ and $[n]P = [-n](-P)$ for $n < 0$.

Example 1.4. The elliptic curve $E : y^2 = x^3 + 3x + 11$ defined over $\mathbb{F}_{19}$ has $\#E(\mathbb{F}_{19}) = 25$. $E(\mathbb{F}_{19})$ is a cyclic group and any point in $E(\mathbb{F}_{19})$ except for ∞ is a generator of $E(\mathbb{F}_{19})$. The following shows that the multiples of the point $P = (3,16)$ generate all the points in $E(\mathbb{F}_{19})$.

$P=(3,16)$	$2P=(0,7)$	$3P=(6,13)$	$4P=(11,11)$	$5P=(14,17)$
$6P=(13,9)$	$7P=(9,11)$	$8P=(4,7)$	$9P=(17,15)$	$10P=(15,12)$
$11P=(18,8)$	$12P=(2,5)$	$13P=(2,14)$	$14P=(18,11)$	$15P=(15,7)$
$16P=(17,4)$	$17P=(4,12)$	$18P=(9,8)$	$19P=(13,10)$	$20P=(14,2)$
$21P=(11,8)$	$22P=(6,6)$	$23P=(0,12)$	$24P=(3,3)$	$25P=\infty$

Theorem 1.1 (See [35]). *Let E be an elliptic curve (over $\mathbb{K}$). Then the addition law on $E(\mathbb{K})$ has the following properties:*

1. *[Identity]* $P+\infty=\infty+P=P$ *for all* $P\in E(\mathbb{K})$.
2. *[Inverse]* $P+(-P)=\infty$ *for all* $P\in E(\mathbb{K})$.
3. *[Associative]* $(P+Q)+R=P+(Q+R)$ *for all* $P,Q,R\in E(\mathbb{K})$.
4. *[Commutative]* $P+Q=Q+P$ *for all* $P,Q\in E(\mathbb{K})$.

In other words, the addition law makes the points of $E(\mathbb{K})$ into an abelian group.

1.1.3 Isomorphism of elliptic curves

Theorem 1.2. *Let $E_1/\mathbb{K}$ and $E_2/\mathbb{K}$ be two elliptic curves and given by Weierstrass equations:*

$$E_1: y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6;$$
$$E_2: y^2+a_1'xy+a_3'y=x^3+a_2'x^2+a_4'x+a_6';$$

E_1 and E_2 are isomorphic if and only if there exist $u\in\mathbb{K}^*$ and $r,s,t\in\mathbb{K}$ such that the change of variables

$$\varphi: E_1\longrightarrow E_2,\ (x,y)\longmapsto(u^2x+r,u^3y+u^2sx+t),$$

transforms equation E_1 into equation E_2.
And the inverse φ^{-1} of φ given by:

$$\varphi^{-1}: E_2\longrightarrow E_1,\ (x,y)\longmapsto(u^{-2}(x-r),u^{-3}(y-sx-t+rs)),$$

transforms equation E_2 into equation E_1, with $\varphi^{-1}\circ\varphi=Id_{E_1}$ and $\varphi\circ\varphi^{-1}=Id_{E_2}$.
Furthermore, we have:

$$\begin{cases} ua_1'=a_1+2s;\\ u^2a_2'=a_2-sa_1+3r-s^2;\\ u^3a_3'=a_3+ra_1+2t;\\ u^4a_4'=a_4-sa_3+2ra_2-(t+rs)a_1+3r^2-2st;\\ u^6a_6'=a_6+ra_4-ta_3+r^2a_2-rta_1+r^3-t^2;\\ u^{12}\triangle'=\triangle;\\ j(E_1)=j(E_2). \end{cases}$$

If $char(\mathbb{K}) \neq 2, 3$

The elliptic curves equations are reduced to the short form

$$E_1 : y^2 = x^3 + ax + b;$$
$$E_2 : y^2 = x^3 + a'x + b';$$

where $a_1 = a_2 = a_3 = 0$, $a_4 = a$ and $a_6 = b$. The elliptic curves E_1 and E_2 are isomorphic if there exist $u \in \mathbb{K}^*$ such that $u^4a' = a$ and $u^6b' = b$. Furthermore, we have:

$$(x, y) \longmapsto (u^2x, u^3y).$$

- If $a = 0$ then for every $b' \in \mathbb{K}^*$ the curve E_1 is isomorphic to $E_2 : y^2 = x^3 + b'$ over $\mathbb{K}((b/b')^{1/6})$.
- If $b = 0$ then for every $a' \in \mathbb{K}^*$ the curve E_1 is isomorphic to $E_2 : y^2 = x^3 + a'x$ over $\mathbb{K}((a/a')^{1/4})$.

If $char(\mathbb{K}) = 3$

The elliptic curves equations are reduced to the short form

$$E_1 : y^2 = x^3 + ax^2 + b;$$
$$E_2 : y^2 = x^3 + a'x^2 + b';$$

where $a_1 = a_3 = a_4 = 0$, $a_2 = a$ and $a_6 = b$. The elliptic curves E_1 and E_2 are isomorphic if there exist $u \in \mathbb{K}^*$ such that $u^2a' = a$ and $u^6b' = b$. Furthermore, we have:

$$(x, y) \longmapsto (u^2x, u^3y).$$

Lemma 1.1. *Let $E_1/\mathbb{K}$ and $E_2/\mathbb{K}$ be two elliptic curves. If E_1 and E_2 are isomorphic over $\mathbb{K}$ then they have the same j-invariant. Conversely, if $j(E_1) = j(E_2)$ then E_1 and E_2 are isomorphic over $\overline{\mathbb{K}}$.*

Example 1.5. We consider the elliptic curves:

$$E_1 : y^2 = x^3 + 2x + 1;$$
$$E_2 : y^2 = x^3 + 162x + 729;$$
$$E_3 : y^2 = x^3 + 18x + 27.$$

Then we see that

- E_1 is isomorphic to E_2 over $\mathbb{Q}$, simply take $u = 3$.
- E_1 is isomorphic to E_3 over $\mathbb{Q}(\sqrt{3})$, but not over $\mathbb{Q}$, take $u = \sqrt{3}$.

Thus:

- $E_1 \cong E_2$ over $\mathbb{Q} \Longrightarrow j(E_1) = j(E_2) = \dfrac{55296}{59} = \dfrac{2^{11}3^3}{59}$.
- $E_1 \cong E_3$ over $\mathbb{Q}(\sqrt{3}) \Longleftrightarrow j(E_1) = j(E_3) = \dfrac{55296}{59} = \dfrac{2^{11}3^3}{59}$.

1.1.4 Elliptic curve over a finite field

Let E be an elliptic curve over a finite field $\mathbb{F}_q$ defined by the Weierstrass equation (1.1), where $q = p^r$ with p prime number and $r \in \mathbb{N}^*$.

Definition 1.7 (Torsion points). Let $E/\mathbb{K}$ be an elliptic curve and $n \in \mathbb{Z}$. The kernel of $[n]$ denoted by $E[n]$, and its defined by:

$$E[n] = \{P \in E(\overline{\mathbb{K}}) \mid [n]P = \infty\}.$$

An element $P \in E[n]$ is called a n-torsion point.

Example 1.6. For all point $P \in E(\mathbb{F}_{19})$ in Example 1.4 is 25-torsion point.

Lemma 1.2. *Let E be an elliptic curve defined over $\mathbb{K}$.*
If the $char(\mathbb{K}) = 0$ or $\gcd(char(\mathbb{K}), n) = 1$, then:

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Otherwise, when $char(\mathbb{K}) = p$ and $n = p^r$, then either

$$E[p^r] = \{\infty\}, \text{ for all } r \geqslant 1 \text{ or } E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}, \text{ for all } r \geqslant 1.$$

Definition 1.8. Let E be a curve defined over $\mathbb{K}$ of characteristic p. If $E[p^r] = \{\infty\}$ for one and in fact for all positive integers r, then the curve E is called supersingular . Otherwise the curve is called ordinary .

The number of points in $E(\mathbb{F}_q)$, denoted by $\#E(\mathbb{F}_q)$ and called the order of E over $\mathbb{F}_q$, it is an important aspect for the security of cryptosystems built on the elliptic curves over a finite fields, we will see this in the second part.

Theorem 1.3 (Hasse [77]). *Let E be an elliptic curve defined over $\mathbb{F}_q$. Then:*

$$|\#E(\mathbb{F}_q) - (q+1)| \leqslant 2\sqrt{q}.$$

Lemma 1.3. *The group $E(\mathbb{F}_q)$ is either cyclic or isomorphic to a product of two cyclic groups,*

$$E(\mathbb{F}_q) \cong \mathbb{Z}/d\mathbb{Z}, \text{ where } d = \#E(\mathbb{F}_q),$$

or

$$E(\mathbb{F}_q) \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}, \text{ where } d_1 \mid d_2 \text{ and } d_1 \mid q-1.$$

Example 1.7. Let E be an elliptic curve over a finite field.
❖ If $E : y^2 = x^3 + 3x + 5$ over $\mathbb{F}_{17}$. The set of $\mathbb{F}_{17}$-rational points on E is:

$$\begin{aligned} E(\mathbb{F}_{17}) = \{&(1,14),(1,3),(2,6),(2,11),(4,8),(4,9),(5,3),(5,14),(6,1),(6,16),(9,8),\\ &(9,9),(10,7),(10,10),(11,14),(11,3),(12,1),(12,16),(15,12),(15,5),\\ &(16,1),(16,16),\infty\}. \end{aligned}$$

Points of $E(\mathbb{F}_{17})$ shown in the figure 1.6:

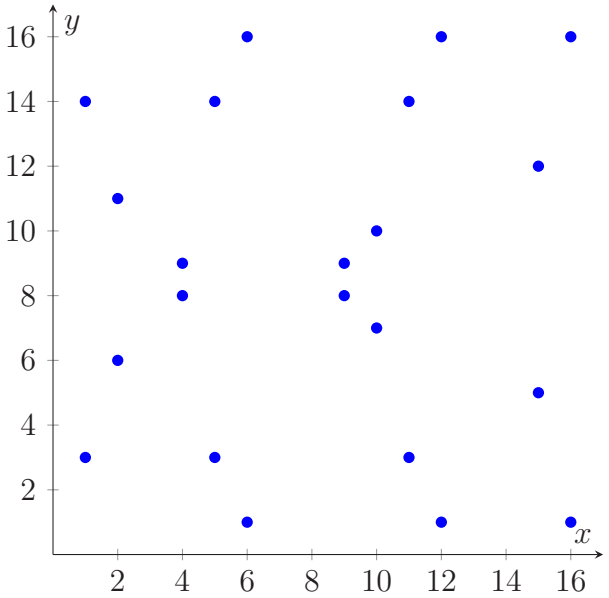


Figure 1.6: An elliptic curve $E : y^2 = x^3 + 3x + 5$ defined over a prime field $\mathbb{F}_{17}$.

The group $E(\mathbb{F}_{17})$ is cyclic for all $P \in E(\mathbb{F}_{17})$ $(\#E(\mathbb{F}_{17}) = 23)$, and we have:

$$|\#E(\mathbb{F}_{17}) - (17+1)| \leqslant 2\sqrt{17} \text{ and } E(\mathbb{F}_{17}) \cong \mathbb{Z}/23\mathbb{Z}.$$

❖ If $E : y^2 = x^3 + 10$ over $\mathbb{F}_{13}$. The set of $\mathbb{F}_{13}$-rational points on E is:

$$E(\mathbb{F}_{13}) = \{(0,7),(0,6),(4,3),(4,10),(10,3),(10,10),(12,3),(12,10),\infty\}.$$

The group $E(\mathbb{F}_{13})$ is not cyclic $(\#E(\mathbb{F}_{13}) = 9)$, and we have:

$$|\#E(\mathbb{F}_{13}) - (13+1)| \leqslant 2\sqrt{13} \text{ and } E(\mathbb{F}_{13}) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

Definition 1.9 (Isogenies). Two curves $E_1/\mathbb{K}$ and $E_2/\mathbb{K}$ are isogenous over $\mathbb{K}$ if there exists a morphism $\varphi : E_1 \longrightarrow E_2$ with coefficients in $\mathbb{K}$ mapping the neutral element of E_1 to the neutral element of E_2. From this simple property, it is possible to show that φ is a group homomorphism from $E_1(\mathbb{K})$ to $E_2(\mathbb{K})$.

Proposition 1.3. *Two elliptic curves E_1 and E_2 defined over $\mathbb{F}_q$ are isogenous over $\mathbb{F}_q$ if and only if $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$.*

Theorem 1.4 (See [78]). *Let $E/\mathbb{F}_q$ be an elliptic curve, let*

$$\phi_{End} : \begin{cases} E(\overline{\mathbb{F}}_q) & \longrightarrow & E(\overline{\mathbb{F}}_q) \\ (x,y) & \longmapsto & (x^q, y^q) \\ \infty & \longmapsto & \infty \end{cases}$$

be the q^{th}-power Frobenius endomorphism, and let $t = q + 1 - \#E(\mathbb{F}_q)$. The integer t is called the trace of Frobenius and satisfies $-2\sqrt{q} \leqslant t \leqslant 2\sqrt{q}$.

1. *Let $\alpha, \beta \in \mathbb{C}$ be the roots of the polynomial $T^2 - tT + q$. Then α and β are complex conjugates satisfying $|\alpha| = |\beta| = \sqrt{q}$, and for every $n \geqslant 1$,*

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - \alpha^n - \beta^n.$$

2. *The trace of Frobenius t and the Frobenius endomorphism ϕ_{End} will play a fundamental role in our study of elliptic curves, they are related by the equation:*

$$\phi^2_{End}(P) - [t]\phi_{End}(P) + [q]P = \infty, \qquad (\phi^2_{End} = \phi_{End} \circ \phi_{End})$$

that is for any point $P = (x_1, y_1) \in E(\overline{\mathbb{F}}_q)$, we have:

$$(x_1^{q^2}, y_1^{q^2}) - [t](x_1^q, y_1^q) + [q](x_1, y_1) = \infty,$$

where addition and subtraction denote curve operations.

Example 1.8. Using the previous Example 1.7, we have:
let E be an elliptic curve defined by the equation $y^2 = x^3 + 3x + 5$ over $\mathbb{F}_{17}$ of the cardinal 23.
So, the trace $t = q + 1 - \#E(\mathbb{F}_{17}) = 17 + 1 - 23 = -5$.
Let $\alpha, \beta \in \mathbb{C}$ be two roots of the polynomial $T^2 - tT + q = T^2 + 5T + 17$, where $\alpha = -\frac{5}{2} + \frac{\sqrt{43}}{2}i$ and $\beta = -\frac{5}{2} - \frac{\sqrt{43}}{2}i$.
For $n = 2$, we deduce that we have:

$$\#E(\mathbb{F}_{17^2}) = \#E(\mathbb{F}_{289}) = 17^2 + 1 - \alpha^2 - \beta^2 = 299.$$

For $n = 5$, we deduce that we have:

$$\#E(\mathbb{F}_{17^5}) = \#E(\mathbb{F}_{1419857}) = 17^5 + 1 - \alpha^5 - \beta^5 = 1419583.$$

All elements of $E(\mathbb{F}_{17})$ are fixed by ϕ^2_{End} and ϕ_{End}, then the point $P = (x, y) \in E(\mathbb{F}_{17})$ we have: $\phi^2_{End}(x,y) - [t]\phi_{End}(x,y) + [q](x,y) = (x,y) + 5(x,y) + 17(x,y) = 23(x,y) = \infty$.
For $P = (6,1) \in E(\mathbb{F}_{17})$, we have: $(6,1) + 5(6,1) + 17(6,1) = 23(6,1) = \infty$.

Proposition 1.4. *Let E be a curve defined over a field $\mathbb{F}_q$ of characteristic p. The curve E is supersingular if and only if the trace t of the Frobenius satisfies $t \equiv 0[p]$.*

1.2 Projective elliptic curves

In this section we describe, the projective space, homogeneous polynomial, homogeneous Weierstrass equations and projective coordinates of elliptic curves.

1.2.1 Projective space

Projective space is the collection of the points in affine space together with the points at infinity. The points at infinity are constructed by asserting that in each direction there lies a unique point at infinity. By convention, directions that are $180°$ apart define the same point at infinity; otherwise parallel lines would intersect at two points instead of just one.

Definition 1.10 (Homogeneous polynomial). A polynomial $F \in \overline{\mathbb{K}}[X_0, ..., X_n]$ is homogeneous of degree d if

$$F(\lambda X_0, ..., \lambda X_n) = \lambda^d F(X_0, ..., X_n), \text{for all } \lambda \in \overline{\mathbb{K}}.$$

For example, the polynomial $F(X, Y) = X^4+3X^2Y^2+5XY^3 \in \mathbb{R}[X, Y]$ is homogeneous of degree 4.

Definition 1.11. Projective space (over $\mathbb{K}$) of demension n, denoted by $\mathbb{P}^n$ or $\mathbb{P}^n(\overline{\mathbb{K}})$, is the set of all $(n + 1)$-tuples $(X_0, ..., X_n) \in \mathbb{A}^{n+1}$, such that at least one X_i is nonzero, modulo the equivalence relation $(X_0, ..., X_n) \sim (Y_0, ..., Y_n)$ if and only if: there exists a $\lambda \in \overline{\mathbb{K}}^*$, such that $X_i = \lambda Y_i$ for all $0 \leqslant i \leqslant n$. An equivalence class is:

$$[X_0 : \cdots : X_n] = \{(\lambda Y_0, ..., \lambda Y_n) \mid \lambda \in \overline{\mathbb{K}}^*\},$$

and the individual $X_0, ..., X_n$ are called homogeneous coordinates for the corresponding point in $\mathbb{P}^n$.
The set of $\mathbb{K}$-rational points in $\mathbb{P}^n$ is the set:

$$\mathbb{P}^n(\mathbb{K}) = \{[X_0 : \cdots : X_n] \in \mathbb{P}^n \mid X_i \in \mathbb{K}\}.$$

- If $n = 2$, then the projective space is called projective plane.
- If $n = 1$, then the projective space is called projective line.

For example, let $\mathbb{K} = \mathbb{F}_{11}$ be a finite field of eleven elements, then the two points $(6, 4, 10)$ and $(2, 5, 7)$ are equivalent, so that:

$$(6, 4, 10) \sim (2, 5, 7) \Longleftrightarrow \exists \lambda = 3 \in \mathbb{F}_{11}, (6, 4, 10) = 3(2, 5, 7).$$

Theorem 1.5 (Bézout's theorem [22]). *Let C_1 and C_2 are plane curves of degree m and m' respectively, then the number of points of intersection of C_1 and C_2 is mm'.*

Remark 1.2. In generally, Bézout's theorem is not true in affine space, because two parallel lines that do not intersect at any point. On the other hand, it is always true for projective planes (not true for other projective spaces), then two parallel lines will meet at a point at infinity.

Proposition 1.5. *The map*

$$\varphi : \left| \begin{array}{ccc} \mathbb{A}^2(\mathbb{K}) & \longrightarrow & \mathbb{P}^2(\mathbb{K}) \\ (x,y) & \longmapsto & [x:y:1] \end{array} \right.$$

is one-to-one and the complement of the image of φ is the line at infinity.
The projective plane space is the set $\mathbb{P}^2(\mathbb{K}) = \mathbb{A}^2(\mathbb{K}) \cup \{$ the set of points at infinity $\}$.

• A polynomial $F(X,Y) \in \mathbb{K}[X,Y]$ can be homogenised by defining

$$F^*(X,Y,Z) = Z^d F\left(\frac{X}{Z}, \frac{Y}{Z}\right) \in \mathbb{K}[X,Y,Z],$$

where d is the degree of F.
For example, if $F(X,Y) = X^3 + XY + 5$ of degree 3, then $F^*(X,Y,Z) = X^3 + XYZ + 5Z^3$.

• A homogeneous polynomial $F^*(X,Y,Z) \in \mathbb{K}[X,Y,Z]$ can be dehomogenised by defining

$$F(X,Y) = F^*(X,Y,1) \in \mathbb{K}[X,Y].$$

• A projective plane curve is the set of zeros in the projective plane of an irreducible homogeneous polynomial $F(X,Y,Z) \in \mathbb{K}[X,Y,Z]_{hom}$ ($\mathbb{K}[X,Y,Z]_{hom}$ the set of homogeneous polynomials) in the projective plane, i.e. $\{[X:Y:Z] \in \mathbb{P}^2(\mathbb{K}) \mid F(X,Y,Z) = 0\}$.
• A point $P = (X_1, Y_1, Z_1)$ on $F(X,Y,Z)$ is singular if

$$\frac{\partial F(X_1,Y_1,Z_1)}{\partial X} = \frac{\partial F(X_1,Y_1,Z_1)}{\partial Y} = \frac{\partial F(X_1,Y_1,Z_1)}{\partial Z} = 0.$$

Definition 1.12. An elliptic curve E over $\mathbb{K}$ given by a homogeneous equation $E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$, defined by:

$$E(\mathbb{K}) = \{[X:Y:Z] \in \mathbb{P}^2(\mathbb{K}) \mid Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3\},$$

with $a_1, a_2, a_3, a_4, a_6 \in \mathbb{K}$, in this case the point at infinity is $\infty = [0:1:0]$.
Its discriminant $\triangle$ and its j-invariant are as in the Definition 1.2.

- ❖ If $char(\mathbb{K}) \neq 2, 3$, we have $E(\mathbb{K}) = \{[X:Y:Z] \in \mathbb{P}^2(\mathbb{K}) \mid Y^2Z = X^3 + aXZ^2 + bZ^3\}$.
- ❖ If $char(\mathbb{K}) = 3$, we have $E(\mathbb{K}) = \{[X:Y:Z] \in \mathbb{P}^2(\mathbb{K}) \mid Y^2Z = X^3 + aX^2Z + bZ^3\}$.

Where $(a, b) \in \mathbb{K}^2$.

• The elliptic curve E is a smooth if the partial derivatives of the curve equation are not simultaneously zero, i.e. $\left(\frac{\partial E}{\partial X}, \frac{\partial E}{\partial Y}, \frac{\partial E}{\partial Z}\right) \neq (0, 0, 0)$.
• Let E and E' are two curves defined by projective Weierstrass equations

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3;$$
$$E' : Y^2Z + a'_1XYZ + a'_3YZ^2 = X^3 + a'_2X^2Z + a'_4XZ^2 + a'_6Z^3;$$

E and E' are isomorphic if E' can be obtained from E by a change of variables of the form

$$(X, Y, Z) \longrightarrow (u^2X, u^3Y + u^2sX + tZ, Z),$$

where $(u, r, s, t) \in \mathbb{K}^* \times \mathbb{K}^3$ (and dividing the resulting equation by u^6). The corresponding transformation is referred to as an admissible change of variables.

Proposition 1.6 (See [22]). *Any projective Weierstrass equation is irreducible. It contains the unique infinite point $\infty = [0 : 1 : 0]$, and is singular if and only if $\triangle = 0$.*

1.2.2 Arithmetic in projective coordinates

One of the problems the formulae for the group laws is that at some stage they involve a division operation. Division in finite fields is considered as an expensive operation. To avoid these division operations one can use projective coordinates (see [78]).
In subsection 1.1.2, we explained the group law in general case and in particular cases ($char(\mathbb{K}) \neq 2, 3$ and $char(\mathbb{K}) = 3$) by using the affine points. Here, we shall give formulas for the adding and doubling of two projective points in elliptic curve over finite field $\mathbb{F}_q$ with cases $char(\mathbb{F}_q) \neq 2, 3$ and $char(\mathbb{F}_q) = 3$.

- ❖ Addition of two projective points P and $Q \in E(\mathbb{F}_q)$ provided $P \neq \pm Q$.
- ❖ Doubling of P.

Projective coordinates for $char(\mathbb{F}_q) \neq 2, 3$

In projective coordinates, the equation of elliptic curve is $E : Y^2Z = X^3 + aXZ^2 + bZ^3$. The point $[X_1 : Y_1 : Z_1]$ on E corresponds to the affine point $(X_1/Z_1, Y_1/Z_1)$ when $Z_1 \neq 0$, and to the point at infinity $\infty = [0 : 1 : 0]$. Otherwise, the opposite of $[X_1 : Y_1 : Z_1]$ is $[X_1 : -Y_1 : Z_1]$.

Addition of P and Q:

The affine form test $x_1 = x_2$ corresponds to the projective form test $X_1/Z_1 = X_2/Z_2$. This

is equivalent to $X_1Z_2 = X_2Z_1$, via cross multiplication. For the interesting case where $P = (X_1, Y_1, Z_1), Q = (X_2, Y_2, Z_2)$ and $X_1Z_2 \neq X_2Z_1$, let's convert the affine arithmetic to projective arithmetic.
Expand and simplify:

$$\begin{aligned}\lambda &= \frac{y_2 - y_1}{x_2 - x_1} = \frac{Y_2/Z_2 - Y_1/Z_1}{X_2/Z_2 - X_1/Z_1} \\ &= \frac{Y_2/Z_2 - Y_1/Z_1}{X_0/Z_2 - X_1/Z_1} \cdot \frac{Z_2Z_1}{Z_2Z_1} \\ &= \frac{Y_2Z_1 - Y_1Z_2}{X_2Z_1 - X_1Z_2}.\end{aligned}$$

Let $T_0 = Y_2Z_1$, $T_1 = Y_1Z_2$, $T = T_0 - T_1$, $U_0 = X_2Z_1$, $U_1 = X_1Z_2$ and $U = U_0 - U_1$.
Substitute $\lambda = \frac{T}{U}$.
Expand and simplify:

$$\begin{aligned}x_3 = \lambda^2 - x_2 - x_1 &= \left(\frac{T}{U}\right)^2 - \frac{X_2}{Z_2} - \frac{X_1}{Z_1} \\ &= \frac{T^2}{U^2} \cdot \frac{Z_2Z_1}{Z_2Z_1} - \frac{X_2}{Z_2} \cdot \frac{U^2Z_1}{U^2Z_1} - \frac{X_1}{Z_1} \cdot \frac{U^2Z_2}{U^2Z_2} \\ &= \frac{T^2Z_2Z_1 - U^2X_2Z_1 - U^2X_1Z_2}{U^2Z_2Z_1} \\ &= \frac{T^2Z_2Z_1 - U^2\left(U_0 + U_1\right)}{U^2Z_2Z_1}.\end{aligned}$$

Let $U_2 = U^2$, $V = Z_2Z_1$ and $W = T^2V - U_2\left(U_0 + U_1\right)$.
Substitute $x_3 = \frac{W}{U_2V}$.
Expand and simplify:

$$\begin{aligned}y_3 = \lambda\left(x_1 - x_3\right) - y_1 &= \frac{T}{U}\left(\frac{X_1}{Z_1} - \frac{W}{U_2V}\right) - \frac{Y_1}{Z_1} \\ &= \frac{T}{U}\left(\frac{X_1}{Z_1} \cdot \frac{U_2Z_2}{U_2Z_2} - \frac{W}{U_2V}\right) - \frac{Y_1}{Z_1} \\ &= \frac{T}{U}\left(\frac{U_1U_2}{U_2V} - \frac{W}{U_2V}\right) - \frac{Y_1}{Z_1} \\ &= \frac{T\left(U_1U_2 - W\right)}{UU_2V} - \frac{Y_1}{Z_1} \\ &= \frac{T\left(U_1U_2 - W\right)}{UU_2V} - \frac{Y_1}{Z_1} \cdot \frac{UU_2Z_2}{UU_2Z_2} \\ &= \frac{T\left(U_1U_2 - W\right)}{UU_2V} - \frac{UU_2Y_1Z_2}{UU_2V} \\ &= \frac{T\left(U_1U_2 - W\right) - T_1UU_2}{UU_2V}.\end{aligned}$$

Let $U_3 = UU_2$.
Substitute: $y_3 = \dfrac{T\left(U_1U_2 - W\right) - T_1U_3}{U_3V}$.
Adjust denominator: $x_3 = \dfrac{W}{U_2V} \cdot \dfrac{U}{U} = \dfrac{UW}{UU_2V} = \dfrac{UW}{U_3V}$.
Now that x_3 and y_3 have the same denominator, we can write:

$$\begin{aligned} X_3 &= UW. \\ Y_3 &= T\left(U_1U_2 - W\right) - T_1U_3. \\ Z_3 &= U_3V. \end{aligned}$$

Doubling of P:

The affine form test $y_1 = 0$ corresponds to the projective form test $Y_1/Z_1 = 0$, this is equivalent to $Y_1 = 0$, since $Z_1 \neq 0$.
For the interesting case where $P = (X_1, Y_1, Z_1)$ and $Y_1 \neq 0$, let's convert the affine arithmetic to projective arithmetic.
Expand and simplify:

$$\begin{aligned} \lambda &= \frac{3x_1^2 + a}{2y_1} \\ &= \frac{3(X_1/Z_1)^2 + a}{2(Y_1/Z_1)} \\ &= \frac{3(X_1/Z_1)^2 + a}{2(Y_1/Z_1)} \cdot \frac{Z_1^2}{Z_1^2} \\ &= \frac{3X_1^2 + aZ_1^2}{2Y_1Z_1}. \end{aligned}$$

Let $T = 3X_1^2 + aZ_1^2$ and $U = 2Y_1Z_1$.
Substitute $\lambda = \dfrac{T}{U}$.
Expand and simplify:

$$\begin{aligned} x_3 = \lambda^2 - 2x_1 &= \left(\frac{T}{U}\right)^2 - 2\frac{X_1}{Z_1} \\ &= \frac{T^2}{U^2} - \frac{2X_1}{Z_1} \cdot \frac{4Y_1^2Z_1}{4Y_1^2Z_1} \\ &= \frac{T^2}{U^2} - \frac{8X_1Y_1^2Z_1}{4Y_1^2Z_1^2} \\ &= \frac{T^2}{U^2} - \frac{4UX_1Y_1}{U^2} \\ &= \frac{T^2 - 4UX_1Y_1}{U^2}. \end{aligned}$$

Let $V = 2UX_1Y_1$ and $W = T^2 - 2V$.
Substitute $x_3 = \dfrac{W}{U^2}$.

Expand and simplify:

$$\begin{aligned}
y_3 = \lambda(x_1 - x_3) - y_1 &= \frac{T}{U}\left(\frac{X_1}{Z_1} - \frac{W}{U^2}\right) - \frac{Y_1}{Z_1} \\
&= \frac{T}{U}\left(\frac{X_1}{Z_1}\cdot\frac{4Y_1^2Z_1}{4Y_1^2Z_1} - \frac{W}{U^2}\right) - \frac{Y_1}{Z_1} = \frac{T}{U}\left(\frac{4X_1Y_1^2Z_1}{4Y_1^2Z_1^2} - \frac{W}{U^2}\right) - \frac{Y_1}{Z_1} \\
&= \frac{T}{U}\left(\frac{V}{U^2} - \frac{W}{U^2}\right) - \frac{Y_1}{Z_1} = \frac{T}{U}\left(\frac{V-W}{U^2}\right) - \frac{Y_1}{Z_1} \\
&= \frac{T(V-W)}{U^3} - \frac{Y_1}{Z_1} = \frac{T(V-W)}{U^3} - \frac{Y_1}{Z_1}\cdot\frac{8Y_1^3Z_1^2}{8Y_1^3Z_1^2} \\
&= \frac{T(V-W)}{U^3} - \frac{8Y_1^4Z_1^2}{8Y_1^3Z_1^3} = \frac{T(V-W)}{U^3} - \frac{2U^2Y_1^2}{U^3} \\
&= \frac{T(V-W) - 2U^2Y_1^2}{U^3} = \frac{T(V-W) - 2(UY_1)^2}{U^3}.
\end{aligned}$$

Adjust denominator: $x_3 = \frac{W}{U^2}\cdot\frac{U}{U} = \frac{UW}{U^3}$.
Now that x_3 and y_3 have the same denominator, we can write:

$$\begin{aligned}
X_3 &= UW. \\
Y_3 &= T(V-W) - 2(UY_1)^2. \\
Z_3 &= U^3.
\end{aligned}$$

Projective coordinates for $char(\mathbb{F}_q) = 3$

In projective coordinates, the equation of elliptic curve is $E : Y^2Z = X^3 + aX^2Z + bZ^3$. The point $[X_1 : Y_1 : Z_1]$ on E corresponds to the affine point $(X_1/Z_1, Y_1/Z_1)$ when $Z_1 \neq 0$ and to the point at infinity $\infty = [0 : 1 : 0]$. Otherwise, the opposite of $[X_1 : Y_1 : Z_1]$ is $[X_1 : -Y_1 : Z_1]$.

Addition of P and Q:

The affine form test $x_1 = x_2$ corresponds to the projective form test $X_1/Z_1 = X_2/Z_2$. This is equivalent to $X_1Z_2 = X_2Z_1$, via cross multiplication. For the interesting case where $P = (X_1, Y_1, Z_1), Q = (X_2, Y_2, Z_2)$ and $X_1Z_2 \neq X_2Z_1$, let's convert the affine arithmetic to projective arithmetic. Expand and simplify:

$$\begin{aligned}
\lambda = \frac{y_2 - y_1}{x_2 - x_1} &= \frac{Y_2/Z_2 - Y_1/Z_1}{X_2/Z_2 - X_1/Z_1} \\
&= \frac{Y_2/Z_2 - Y_1/Z_1}{X_0/Z_2 - X_1/Z_1}\cdot\frac{Z_2Z_1}{Z_2Z_1} \\
&= \frac{Y_2Z_1 - Y_1Z_2}{X_2Z_1 - X_1Z_2}.
\end{aligned}$$

Let $T_0 = Y_2Z_1$, $T_1 = Y_1Z_2$, $T = T_0 - T_1$, $U_0 = X_2Z_1$, $U_1 = X_1Z_2$ and $U = U_0 - U_1$.
Substitute $\lambda = \dfrac{T}{U}$.
Expand and simplify:

$$\begin{aligned} x_3 = \lambda^2 - a - x_2 - x_1 &= \left(\frac{T}{U}\right)^2 - a - \frac{X_2}{Z_2} - \frac{X_1}{Z_1} \\ &= \frac{T^2}{U^2} \cdot \frac{Z_2Z_1}{Z_2Z_1} - a \cdot \frac{U^2Z_2Z_1}{U^2Z_2Z_1} - \frac{X_2}{Z_2} \cdot \frac{U^2Z_1}{U^2Z_1} - \frac{X_1}{Z_1} \cdot \frac{U^2Z_2}{U^2Z_2} \\ &= \frac{T^2Z_2Z_1 - U^2aZ_2Z_1 - U^2X_2Z_1 - U^2X_1Z_2}{U^2Z_2Z_1} \\ &= \frac{T^2Z_2Z_1 - U^2\left(aZ_2Z_1 + U_0 + U_1\right)}{U^2Z_2Z_1}. \end{aligned}$$

Let $U_2 = U^2$, $V = Z_2Z_1$ and $W = T^2V - U_2\left(aV + U_0 + U_1\right)$.
Substitute $x_3 = \dfrac{W}{U_2V}$.
Expand and simplify:

$$\begin{aligned} y_3 = \lambda\left(x_1 - x_3\right) - y_1 &= \frac{T}{U}\left(\frac{X_1}{Z_1} - \frac{W}{U_2V}\right) - \frac{Y_1}{Z_1} \\ &= \frac{T}{U}\left(\frac{X_1}{Z_1} \cdot \frac{U_2Z_2}{U_2Z_2} - \frac{W}{U_2V}\right) - \frac{Y_1}{Z_1} = \frac{T}{U}\left(\frac{U_1U_2}{U_2V} - \frac{W}{U_2V}\right) - \frac{Y_1}{Z_1} \\ &= \frac{T\left(U_1U_2 - W\right)}{UU_2V} - \frac{Y_1}{Z_1} = \frac{T\left(U_1U_2 - W\right)}{UU_2V} - \frac{Y_1}{Z_1} \cdot \frac{UU_2Z_2}{UU_2Z_2} \\ &= \frac{T\left(U_1U_2 - W\right)}{UU_2V} - \frac{UU_2Y_1Z_2}{UU_2V} \\ &= \frac{T\left(U_1U_2 - W\right) - T_1UU_2}{UU_2V}. \end{aligned}$$

Let $U_3 = UU_2$.
Substitute: $y_3 = \dfrac{T\left(U_1U_2 - W\right) - T_1U_3}{U_3V}$.
Adjust denominator: $x_3 = \dfrac{W}{U_2V} \cdot \dfrac{U}{U} = \dfrac{UW}{UU_2V} = \dfrac{UW}{U_3V}$.
Now that x_3 and y_3 have the same denominator, we can write:

$$\begin{aligned} X_3 &= UW. \\ Y_3 &= T\left(U_1U_2 - W\right) - T_1U_3. \\ Z_3 &= U_3V. \end{aligned}$$

Doubling of P:

The affine form test $y_1 = 0$ corresponds to the projective form test $Y_1/Z_1 = 0$, this is equivalent to $Y_1 = 0$, since $Z_1 \neq 0$.
For the interesting case where $P = (X_1, Y_1, Z_1)$ and $Y_1 \neq 0$, let's convert the affine arithmetic to projective arithmetic.

Expand and simplify:

$$\lambda = \frac{3x_1^2 + 2ax_1}{2y_1} = \frac{3(X_1/Z_1)^2 + 2a(X_1/Z_1)}{2(Y_1/Z_1)}$$
$$= \frac{3(X_1/Z_1)^2 + 2a(X_1/Z_1)}{2(Y_1/Z_1)} \cdot \frac{Z_1^2}{Z_1^2} = \frac{3X_1^2 + 2aX_1Z_1}{2Y_1Z_1}.$$

Let $T = 3X_1^2 + 2aX_1Z_1$ and $U = 2Y_1Z_1$.
Substitute $\lambda = \frac{T}{U}$.
Expand and simplify:

$$x_3 = \lambda^2 - a - 2x_1 = \left(\frac{T}{U}\right)^2 - a - 2\frac{X_1}{Z_1}$$
$$= \frac{T^2}{U^2} - a \cdot \frac{4Y_1^2Z_1^2}{4Y_1^2Z_1^2} - \frac{2X_1}{Z_1} \cdot \frac{4Y_1^2Z_1}{4Y_1^2Z_1}$$
$$= \frac{T^2}{U^2} - \frac{4aY_1^2Z_1^2}{4Y_1^2Z_1^2} - \frac{8X_1Y_1^2Z_1}{4Y_1^2Z_1^2} = \frac{T^2}{U^2} - \frac{aU^2}{U^2} - \frac{4UX_1Y_1}{U^2}$$
$$= \frac{T^2 - aU^2 - 4UX_1Y_1}{U^2}.$$

Let $V = 2UX_1Y_1$ and $W = T^2 - aU^2 - 2V$.
Substitute $x_3 = \frac{W}{U^2}$.
Expand and simplify:

$$y_3 = \lambda(x_1 - x_3) - y_1 = \frac{T}{U}\left(\frac{X_1}{Z_1} - \frac{W}{U^2}\right) - \frac{Y_1}{Z_1}$$
$$= \frac{T}{U}\left(\frac{X_1}{Z_1} \cdot \frac{4Y_1^2Z_1}{4Y_1^2Z_1} - \frac{W}{U^2}\right) - \frac{Y_1}{Z_1} = \frac{T}{U}\left(\frac{4X_1Y_1^2Z_1}{4Y_1^2Z_1^2} - \frac{W}{U^2}\right) - \frac{Y_1}{Z_1}$$
$$= \frac{T}{U}\left(\frac{V}{U^2} - \frac{W}{U^2}\right) - \frac{Y_1}{Z_1} = \frac{T}{U}\left(\frac{V - W}{U^2}\right) - \frac{Y_1}{Z_1}$$
$$= \frac{T(V-W)}{U^3} - \frac{Y_1}{Z_1} = \frac{T(V-W)}{U^3} - \frac{Y_1}{Z_1} \cdot \frac{8Y_1^3Z_1^2}{8Y_1^3Z_1^2}$$
$$= \frac{T(V-W)}{U^3} - \frac{8Y_1^4Z_1^2}{8Y_1^3Z_1^3} = \frac{T(V-W)}{U^3} - \frac{2U^2Y_1^2}{U^3}$$
$$= \frac{T(V-W) - 2U^2Y_1^2}{U^3} = \frac{T(V-W) - 2(UY_1)^2}{U^3}.$$

Adjust denominator: $x_3 = \frac{W}{U^2} \cdot \frac{U}{U} = \frac{UW}{U^3}$.
Now that x_3 and y_3 have the same denominator, we can write:

$$X_3 = UW.$$
$$Y_3 = T(V-W) - 2(UY_1)^2.$$
$$Z_3 = U^3.$$

The table 1.2 shows the computation times for the addition-doubling formulas in affine and projective coordiantes. For simplicity, we neglect addition, subtraction and multiplication by a small constant in $\mathbb{F}_q$ because they are much faster than multiplication and inversion in $\mathbb{F}_q$. Let's represent multiplication, inverse and squaring in $\mathbb{F}_q$ by M, I and S respectively.

Coordinates / $char(\mathbb{F}_q)$	Projective		Affine	
	Addition	Doubling	Addition	Doubling
$\neq 2, 3$	12M+2S	7M+5S	I+2M+S	I+2M+2S
$= 3$	13M+2S	8M+4S	I+2M+S	I+2M+2S

Table 1.2: Operation count for adding and doubling points on $E/\mathbb{F}_q$.

Chapter 2

Elliptic curves over a finite rings

"Elliptic curves are of great importance in mathematics areas in particular number theory and algebraic geometry, which have become a major area of current research. In this chapter, we present an elliptic curves over the two finite rings $\mathbb{F}_q[\varepsilon]$ and $\mathbb{F}_{3^d}[\varepsilon]$, where $\varepsilon^4 = \varepsilon^3$ of characteristics $p \neq 2, 3$ and $p = 3$ respectively, and we focus on study the classification of elements in elliptic curves over these rings [71, 80]."
For more information about elliptic curves over a finite rings, see the following thesis and articles: [4–6]; [12–14]; [30–32] and [85, 86, 88].

Contents in Brief

2.1 Basic concepts **28**
2.2 Elliptic curves over the ring R **29**
2.3 Elliptic curve over a ring of characteristic $\neq 2, 3$ **30**
2.3.1 The finite ring $\mathbb{F}_q[\varepsilon], \varepsilon^4 = \varepsilon^3$ 30
2.3.2 Elliptic curve over $\mathbb{F}_q[\varepsilon], \varepsilon^4 = \varepsilon^3$ 35
2.3.3 Classification of elements in $E_{a,b}(\mathbb{F}_q[\varepsilon])$ 43
2.4 Elliptic curve over a ring of characteristic 3 . . . . . **44**
2.4.1 The finite ring $\mathbb{F}_{3^d}[\varepsilon], \varepsilon^4 = \varepsilon^3$ 45
2.4.2 Elliptic curve over $\mathbb{F}_{3^d}[\varepsilon], \varepsilon^4 = \varepsilon^3$ 48
2.4.3 Classification of elements in $E_{a,b}(\mathbb{F}_{3^d}[\varepsilon])$ 52

2.1 Basic concepts

Quotient ring $\mathbb{K}[\varepsilon]$

❖ Let $\mathbb{K}$ be a field. Define the polynomial ring

$$\mathbb{K}[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^d \mid a_i \in \mathbb{K}, d \in \mathbb{N}\}.$$

For $f \in \mathbb{K}[x]$ of degree n and (f) be the ideal generated by f of $\mathbb{K}[x]$, define $\mathbb{K}[x]/(f) := \mathbb{K}[x]/\sim$, where $\sim$ is the equivalence relation defined by $g \sim h$ if $f|g-h$ with $g, h \in \mathbb{K}[x]$.
❖ We denote the set of all congruence classes of $\mathbb{K}[x]$ modulo f by $\mathbb{K}[x]/(f)$, and we write:

$$\begin{aligned}\mathbb{K}[x]/(f) &= \{\overline{g(x)} \mid g(x) \in \mathbb{K}[x]\}\\ &= \{g(x) + (f) \mid g(x) \in \mathbb{K}[x]\}\\ &= \{a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + (f) \mid a_i \in \mathbb{K}, n = \deg(f)\}\\ &= \{g(x) + (f) \mid g(x) \in \mathbb{K}[x], \deg(g) < \deg(f) = n\}.\end{aligned}$$

❖ Let $\overline{g(x)}$, $\overline{h(x)}$ in $\mathbb{K}[x]/(f)$ and $\lambda \in \mathbb{K}$, we have:

$$\overline{g(x)} + \overline{h(x)} = \overline{g(x) + h(x)};$$

$$\lambda \cdot \overline{g(x)} = \overline{\lambda \cdot g(x)}.$$

Then the set $\mathbb{K}[x]/(f)$ has a natural ring structure called the quotient ring of $\mathbb{K}[x]$ by the ideal (f).
❖ The base of $\mathbb{K}[x]/(f)$:

$$\begin{aligned}\mathbb{K}[x]/(f) &= \{\overline{a_0 \cdot 1 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}} \mid a_i \in \mathbb{K}\}\\ &= \{a_0\overline{1} + a_1\overline{x} + a_2\overline{x}^2 + \cdots + a_{n-1}\overline{x}^{n-1} \mid a_i \in \mathbb{K}\}.\end{aligned}$$

If we pose $\varepsilon = \overline{x}$, we have:

$$\mathbb{K}[\varepsilon] = \mathbb{K}[x]/(f) = \{a_0 + a_1\varepsilon + a_2\varepsilon^2 + \cdots + a_{n-1}\varepsilon^{n-1} \mid a_i \in \mathbb{K}\}.$$

Then the ring $\mathbb{K}[\varepsilon]$ is a vector space over $\mathbb{K}$ of dimension $n = \deg(f)$, and have $\{1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{n-1}\}$ as basis.
- If the field $\mathbb{K}$ is finite, then we call $\mathbb{K}[\varepsilon]$ is a finite ring.
- If f is irreducible polynomial in $\mathbb{K}[x]$ then $\mathbb{K}[\varepsilon]$ is a field.

Local ring

Definition 2.1 (Local ring). A ring R is local if it has a unique maximal ideal I_m.

Proposition 2.1 (See [30]). *A ring R is local if and only if the set of its non-invertible elements is an ideal.*

Lemma 2.1 (See [30]). *Let R be a local ring of maximal ideal I_m. Then the set of non-invertible elements of R is I_m.*

2.2 Elliptic curves over the ring R

In the previous chapter, we discussed on elliptic curves over any field $\mathbb{K}$ and in particular cases of $char(\mathbb{K}) \neq 2, 3$ and $char(\mathbb{K}) = 3$. In this section, we will focus on the definition of an elliptic curve over a finite ring, the restrictions that Lenstra [46] made for this definition and how these restrictions do not pose problems in characteristics $p \neq 2, 3$ and $p = 3$, which constitutes the object of our research.

Just like on a field, an elliptical curve can also be defined on a ring under some conditions, represented as follows::

1. The element 6 is invertible in R, as Lenstra indicates in [46] is not needed for this definition, but just to use a precise form of the elliptic curve equation.

2. Any projective R-module of rank 1 is free, is on the other hand necessary, it is verified by the finished rings. This is therefore a sufficient condition to be able to define an elliptic curve over a ring, while preserving the group law defined geometrically by the secant and the tangent.

Definition 2.2 (Primitive triplet [46]). Let R be a ring. A primitive triplet of R is a triplet $(x_1, x_2, x_3) \in R^3$ such that $\sum_{i=1}^{3} x_i R = R$, i.e. if there exist $(a_1, a_2, a_3) \in R^3$, such that $\sum_{i=1}^{3} a_i x_i = 1$. We denote by $\mathcal{P}(R)$, the set of primitive triplets of R.

Definition 2.3 (Projective plane over R). Let R be a ring, $\mathcal{P}(R)$ the set of primitive elements of R, R^* the set of units of R, and $\sim_R$ the equivalence relation defined on $\mathcal{P}(R)$ by:

$$(X, Y, Z) \sim_R (X', Y', Z') \Longleftrightarrow \exists u \in R^*, \text{ such that } (X, Y, Z) = (uX', uY', uZ').$$

We call a projective plane on R, and we denote by $\mathbb{P}^2(R) = \mathcal{P}(R)/\sim_R$. We will denote the projective points on R by $[X : Y : Z]$.

Definition 2.4. Let R be a finite unitary commutative ring.

- If $char(R) \neq 2, 3$, then we define the elliptic curves over the ring R by the homogeneous equation of Weierstrass $Y^2Z = X^3 + aXZ^2 + bZ^3$, where $a, b \in R$ for which $4a^3 + 27b^2 \in R^*$. And we denote the set of rational points by $E_{a,b}(R)$:

$$E_{a,b}(R) = \{[X : Y : Z] \in \mathbb{P}^2(R) \mid Y^2Z - X^3 - aXZ^2 - bZ^3 = 0\} \cup \{\infty\}.$$

- If $char(R) = 3$, then we define the elliptic curves over the ring R by the homogeneous equation of Weierstrass $Y^2Z = X^3 + aX^2Z + bZ^3$, where $a, b \in R$ for which $-a^3b \in R^*$. And we denote the set of rational points by $E_{a,b}(R)$:

$$E_{a,b}(R) = \{[X : Y : Z] \in \mathbb{P}^2(R) \mid Y^2Z - X^3 - aX^2Z - bZ^3 = 0\} \cup \{\infty\}.$$

Proposition 2.2 (Group law for $E_{a,b}(R)$). *Let R be a finite unitary commutative ring. The method of the secant-tangent known over a field, defines a group law on the elliptic curve $E_{a,b}(R)$ and admits as neutral element the point $[0 : 1 : 0]$.*

Proof. The ring R is finite, therefore according to Lenstra [46] condition (2) is satisfied and this allows to conclude the proposition. □

2.3 Elliptic curve over a ring of characteristic $\neq 2, 3$

In this section, we study the elliptic curve over the finite ring $\mathbb{F}_q[\varepsilon]$, where $\varepsilon^4 = \varepsilon^3$ of characteristic $p \neq 2, 3$ given by homogeneous Weierstrass equation of the form

$$Y^2Z = X^3 + aXZ^2 + bZ^3, \text{ where } a, b \in \mathbb{F}_q[\varepsilon].$$

Such that we study the arithmetic operation of this ring and define the elliptic curve over it. Next, we show that $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$ and $E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$ are two elliptic curves over the finite field $\mathbb{F}_q$, such that π_0 is a canonical projection and π_1 is a sum projection of coordinate of element in $\mathbb{F}_q[\varepsilon]$, and we conclude by given a classification of elements in elliptic curve over the finite ring $\mathbb{F}_q[\varepsilon]$. This section is important for the applications of cryptography in the chapter 4.

2.3.1 The finite ring $\mathbb{F}_q[\varepsilon], \varepsilon^4 = \varepsilon^3$

We follow the approach in [4–6]. The ring $\mathbb{F}_q[\varepsilon]$, $\varepsilon^4 = \varepsilon^3$ can be constructed by using the quotient ring of $\mathbb{F}_q[X]$ by the polynomial $X^4 - X^3$. $\mathbb{F}_q$ is a finite field of order q, where

q is a power of a prime number p, $p \geq 5$. An element X in $\mathbb{F}_q[\varepsilon]$ written in the form $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3$ where $(x_0, x_1, x_2, x_3) \in \mathbb{F}_q^4$.

2.3.1.1 Arithmetic operations

The arithmetic operations in $\mathbb{F}_q[\varepsilon]$ can be decomposed into operations in $\mathbb{F}_q$ and they are computed as follows:

$X + Y = (x_0 + y_0) + (x_1 + y_1)\varepsilon + (x_2 + y_2)\varepsilon^2 + (x_3 + y_3)\varepsilon^3$, and

$$X \cdot Y = x_0y_0 + (x_0y_1 + x_1y_0)\varepsilon + (x_0y_2 + x_1y_1 + x_2y_0)\varepsilon^2 + ((x_0 + x_1 + x_2 + x_3)y_3 + (x_1 + x_2 + x_3)y_2 + (x_2 + x_3)y_1 + x_3y_0)\varepsilon^3,$$

where $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3$ and $Y = y_0 + y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3$.

Example 2.1. Let $X, Y \in \mathbb{F}_7[\varepsilon]$, where $X = 2 + \varepsilon + 3\varepsilon^2 + 4\varepsilon^3$ and $Y = 1 + 5\varepsilon^2 + 3\varepsilon^3$, we have: $X + Y = 3 + \varepsilon + \varepsilon^3$ and $X \cdot Y = 2 + \varepsilon + 6\varepsilon^2 + 4\varepsilon^3$.

Lemma 2.2. *$(\mathbb{F}_q[\varepsilon], +, \cdot)$ is a finite unitary commutative ring isomorphic to the quotient ring $\mathbb{F}_q[X]/(X^4 - X^3)$.*

Lemma 2.3. *The ring $\mathbb{F}_q[\varepsilon]$ is a vector space over $\mathbb{F}_q$ of dimension 4. And have $\{1, \varepsilon, \varepsilon^2, \varepsilon^3\}$ as basis, then: $\mathbb{F}_q[\varepsilon] = \mathbb{F}_q + \mathbb{F}_q\varepsilon + \mathbb{F}_q\varepsilon^2 + \mathbb{F}_q\varepsilon^3$.*

Proof. Let $X = \sum_{i=0}^{3} x_i\varepsilon^i$ and $Y = \sum_{i=0}^{3} y_i\varepsilon^i$ be two elements of $\mathbb{F}_q[\varepsilon]$ and k in $\mathbb{F}_q$, we have:

- $X + Y = (x_0 + y_0) + (x_1 + y_1)\varepsilon + (x_2 + y_2)\varepsilon^2 + (x_3 + y_3)\varepsilon^3$.
- $k \cdot X = k\sum_{i=0}^{3} x_i\varepsilon^i = \sum_{i=0}^{3} kx_i\varepsilon^i = kx_0 + kx_1\varepsilon + kx_2\varepsilon^2 + kx_3\varepsilon^3$.

□

Proposition 2.3. *The product operation in $\mathbb{F}_q[\varepsilon]$ can be written as:*

$$X \cdot Y = x_0y_0 + \Theta_{XY}\varepsilon + \Omega_{XY}\varepsilon^2 + ((x_0 + x_1 + x_2 + x_3)(y_0 + y_1 + y_2 + y_3) - x_0y_0 - \Theta_{XY} - \Omega_{XY})\varepsilon^3,$$

where:

$$\Theta_{XY} = (x_0 + x_1)(y_0 + y_1) - x_0y_0 - x_1y_1 = x_0y_1 + x_1y_0 \text{ and}$$

$$\Omega_{XY} = (x_0 + x_1 + x_2)(y_0 + y_1 + y_2) - x_0(y_0 + y_1) - x_1(y_0 + y_2) - x_2(y_1 + y_2) = x_0y_2 + x_1y_1 + x_2y_0.$$

Proof. We have:

$(x_0 + x_1 + x_2 + x_3)(y_0 + y_1 + y_2 + y_3) - x_0y_0 - \Theta_{XY} - \Omega_{XY}$
$= (x_0 + x_1 + x_2 + x_3)y_3 + (x_1 + x_2 + x_3)y_2 + (x_2 + x_3)y_1 + x_3y_0.$ □

Corollary 2.1. *Let* $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 \in \mathbb{F}_q[\varepsilon]$. *We have:*
$X^2 = x_0^2 + \Theta_{X^2}\varepsilon + \Omega_{X^2}\varepsilon^2 + ((x_0 + x_1 + x_2 + x_3)^2 - x_0^2 - x_1^2 - 2x_0x_1 - 2x_0x_2)\varepsilon^3$,
$X^3 = x_0^3 + \Theta_{X^3}\varepsilon + \Omega_{X^3}\varepsilon^2 + ((x_0 + x_1 + x_2 + x_3)^3 - x_0^3 - 3(x_0x_1^2 + x_2x_0^2 + x_1x_0^2))\varepsilon^3$,
where:
$\Theta_{X^2} = (x_0 + x_1)^2 - x_0^2 - x_1^2$,
$\Omega_{X^2} = (x_0 + x_1 + x_2)^2 - x_0^2 - x_2^2 - 2x_0x_1 - 2x_1x_2$,
$\Theta_{X^3} = (x_0 + x_1)^3 - x_0^3 - x_1^3 - 3x_0x_1^2$ *and*
$\Omega_{X^3} = (x_0 + x_1 + x_2)^3 - x_0^3 - x_1^3 - x_2^3 - 3(x_0x_2^2 + x_1x_2^2 + x_1x_0^2 + x_2x_1^2) - 6x_0x_1x_2$.

The next proposition characterize the set $(\mathbb{F}_q[\varepsilon])^\times$ of invertible elements in $\mathbb{F}_q[\varepsilon]$.

Proposition 2.4. *Let* $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 \in \mathbb{F}_q[\varepsilon]$. *The element* X *is invertible if and only if* x_0 *and* $x_0 + x_1 + x_2 + x_3$ *are invertible in* $\mathbb{F}_q$. *The inverse of* X *is given by:*
$X^{-1} = x_0^{-1} - x_1x_0^{-2}\varepsilon + (x_1^2x_0^{-3} - x_2x_0^{-2})\varepsilon^2$
$\quad + ((x_0 + x_1 + x_2 + x_3)^{-1} + x_1x_0^{-2} + x_2x_0^{-2} - x_1^2x_0^{-3} - x_0^{-1})\varepsilon^3$.

Proof. Let $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3$ and $Y = y_0 + y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3$ be two elements of $\mathbb{F}_q[\varepsilon]$. We have:
$X \cdot Y = x_0y_0 + \Theta_{XY}\varepsilon + \Omega_{XY}\varepsilon^2$
$\quad + ((x_0 + x_1 + x_2 + x_3)(y_0 + y_1 + y_2 + y_3) - x_0y_0 - \Theta_{XY} - \Omega_{XY})\varepsilon^3$.
Where $\Theta_{XY} = x_0y_1 + x_1y_0$ and $\Omega_{XY} = x_0y_2 + x_1y_1 + x_2y_0$. Then:

$$X \cdot Y = 1 \iff \begin{cases} x_0y_0 = 1; \\ \Theta_{XY} = 0; \\ \Omega_{XY} = 0; \\ (x_0 + x_1 + x_2 + x_3)(y_0 + y_1 + y_2 + y_3) - x_0y_0 - \Theta_{XY} - \Omega_{XY} = 0. \end{cases}$$

$$\iff \begin{cases} x_0y_0 = 1; \\ x_0y_1 + x_1y_0 = 0; \\ x_0y_2 + x_1y_1 + x_2y_0 = 0; \\ (x_0 + x_1 + x_2 + x_3)(y_0 + y_1 + y_2 + y_3) = 1. \end{cases}$$

$$\iff \begin{cases} y_0 = x_0^{-1}; \\ y_1 = -x_1x_0^{-2}; \\ y_2 = -x_2x_0^{-2} + x_1^2x_0^{-3}; \\ y_3 = (x_0 + x_1 + x_2 + x_3)^{-1} + x_1x_0^{-2} + x_2x_0^{-2} - x_1^2x_0^{-3} - x_0^{-1}. \end{cases}$$

So, the element $X \in (\mathbb{F}_q[\varepsilon])^\times$ if and only if $x_0 \not\equiv 0[p]$ and $x_0 + x_1 + x_2 + x_3 \not\equiv 0[p]$.
In this case we have:
$X^{-1} = x_0^{-1} - x_1x_0^{-2}\varepsilon + (x_1^2x_0^{-3} - x_2x_0^{-2})\varepsilon^2$
$\quad + ((x_0 + x_1 + x_2 + x_3)^{-1} + x_1x_0^{-2} + x_2x_0^{-2} - x_1^2x_0^{-3} - x_0^{-1})\varepsilon^3$. □

Corollary 2.2. *Let* $X \in \mathbb{F}_q[\varepsilon]$, *then* X *is not invertible if and only if* $x_0 \equiv 0[p]$ *or* $x_0 + x_1 + x_2 + x_3 \equiv 0[p]$, *where* $(x_0, x_1, x_2, x_3) \in \mathbb{F}_q^4$.

Example 2.2. Let $X = 2+\varepsilon+\varepsilon^2+3\varepsilon^3 \in \mathbb{F}_5[\varepsilon]$, we have $x_0 = 2 \not\equiv 0[5]$ and $x_0+x_1+x_2+x_3 = 2 \not\equiv 0[5]$ then X is invertible in $\mathbb{F}_5[\varepsilon]$. The inverse of X is $X^{-1} = 3 + \varepsilon + 3\varepsilon^2 + \varepsilon^3$.

Lemma 2.4. *$\mathbb{F}_q[\varepsilon]$ is a non local ring.*

Proof. We consider the two ideals of $\mathbb{F}_q[\varepsilon]$ defined by:

$$J_0 = \{x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 \mid (x_1, x_2, x_3) \in \mathbb{F}_q^3\}, \text{ and}$$
$$J_1 = \{x_0 + x_1\varepsilon + x_2\varepsilon^2 - (x_0 + x_1 + x_2)\varepsilon^3 \mid (x_0, x_1, x_2) \in \mathbb{F}_q^3\},$$

it's clear that $J_0 \cup J_1$ is the set of non invertible elements in $\mathbb{F}_q[\varepsilon]$, and for all $x_0, x_1, x_2, x, y,$ and z in $\mathbb{F}_q$ we have: $x_0 + x_1\varepsilon + x_2\varepsilon^2 - (x_0 + x_1 + x_2)\varepsilon^3 = x\varepsilon + y\varepsilon^2 + z\varepsilon^3$
$\Longrightarrow x_0 + (x_1 - x)\varepsilon + (x_2 - y)\varepsilon^2 - (x_0 + x_1 + x_2 + z)\varepsilon^3 = 0$

$$\Longrightarrow \begin{cases} x_0 = 0; \\ x_1 - x = 0; \\ x_2 - y = 0; \\ x_0 + x_1 + x_2 + z = 0. \end{cases} \Longrightarrow \begin{cases} x_0 = 0; \\ x_1 = x; \\ x_2 = y; \\ x_1 + x_2 = -z. \end{cases}$$

We have $J_0 \cap J_1 = \{x\varepsilon + y\varepsilon^2 - z\varepsilon^3 \mid (x, y, z) \in \mathbb{F}_q^3\}$ then J_0 and J_1 are two distinct ideals of $\mathbb{F}_q[\varepsilon]$, so $J_0 \cup J_1$ is not ideal. Finally, the ring $\mathbb{F}_q[\varepsilon]$ is not local. □

Definition 2.5. Let π_0 be a canonical projection and π_1 be a sum projection of coordinate of element in $\mathbb{F}_q[\varepsilon]$ defined as given below:

$$\pi_0 : \left| \begin{array}{ccc} \mathbb{F}_q[\varepsilon] & \longrightarrow & \mathbb{F}_q \\ X = \sum_{i=0}^{3} x_i\varepsilon^i & \longmapsto & x_0 \end{array} \right. \text{ and } \pi_1 : \left| \begin{array}{ccc} \mathbb{F}_q[\varepsilon] & \longrightarrow & \mathbb{F}_q \\ X = \sum_{i=0}^{3} x_i\varepsilon^i & \longmapsto & \sum_{i=0}^{3} x_i \end{array} \right.$$

Lemma 2.5. *The mappings π_0 and π_1 are two surjective morphisms of rings.*

Proof. Let $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3$ and $Y = y_0 + y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3$ be two elements of $\mathbb{F}_q[\varepsilon]$. From the definition of the sum and product operation in $\mathbb{F}_q[\varepsilon]$, we have:

$$\pi_0(X + Y) = x_0 + y_0 = \pi_0(X) + \pi_0(Y), \text{ and}$$
$$\pi_0(X \cdot Y) = x_0 \cdot y_0 = \pi_0(X) \cdot \pi_0(Y).$$

So, π_0 is morphism of rings.

$$\begin{aligned} \pi_1(X + Y) &= x_0 + y_0 + x_1 + y_1 + x_2 + y_2 + x_3 + y_3 \\ &= \pi_1(X) + \pi_1(Y), \text{ and} \\ \pi_1(X \cdot Y) &= (x_0 + x_1 + x_2 + x_3) \cdot (y_0 + y_1 + y_2 + y_3) \\ &= \pi_1(X) \cdot \pi_1(Y). \end{aligned}$$

So, π_1 is morphism of rings.
Finally, for all $x \in \mathbb{F}_q \subset \mathbb{F}_q[\varepsilon]$, we have $\pi_0(x) = \pi_1(x) = x$, so π_0 and π_1 are two surjective morphisms. □

Lemma 2.6. *Let $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 \in \mathbb{F}_q[\varepsilon]$. If X is invertible in $\mathbb{F}_q[\varepsilon]$, then:*

$$\pi_0(X^{-1}) = (\pi_0(X))^{-1} \text{ and } \pi_1(X^{-1}) = (\pi_1(X))^{-1}.$$

Proof. Let $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 \in \mathbb{F}_q[\varepsilon]$. By using the Proposition 2.4, we have:

$$\begin{aligned}\pi_0(X^{-1}) &= x_0^{-1} = (\pi_0(X))^{-1} \text{ and}\\ \pi_1(X^{-1}) &= (x_0 + x_1 + x_2 + x_3)^{-1} = (\pi_1(X))^{-1}.\end{aligned}$$

□

Remark 2.1. The kernel of π_0 and π_1 is an ideal such that:

$$\begin{aligned}\ker \pi_0 &= \{X \in \mathbb{F}_q[\varepsilon] \mid \pi_0(X) = 0\},\\ \ker \pi_1 &= \{X \in \mathbb{F}_q[\varepsilon] \mid \pi_1(X) = 0\}.\end{aligned}$$

Corollary 2.3. *For all $i \in \{0, 1\}$, the mapping $\widetilde{\pi_i}$ given by:*

$$\widetilde{\pi_i} : \left| \begin{array}{ccc} \mathbb{F}_q[\varepsilon]/\ker \pi_i & \longrightarrow & \operatorname{Im} \pi_i = \pi_i(\mathbb{F}_q[\varepsilon]) \\ \overline{X} = X + \ker \pi_i & \longmapsto & \pi_i(X) \end{array} \right.$$

is an isomorphism.

Proof. For $i \in \{0, 1\}$, we have π_i is a ring morphism and $\ker \pi_i$ is an ideal. The mapping $\widetilde{\pi_i}$ is well defined, let $\overline{X}, \overline{X'} \in \mathbb{F}_q[\varepsilon]/\ker \pi_i$, such that $\widetilde{\pi_i}(\overline{X}) = \pi_i(X)$ and $\widetilde{\pi_i}(\overline{X'}) = \pi_i(X')$

$$\begin{aligned}\overline{X} = \overline{X'} &\iff X - X' \in \ker \pi_i\\ &\iff \pi_i(X - X') = \pi_i(X) - \pi_i(X') = 0\\ &\iff \pi_i(X) = \pi_i(X')\\ &\iff \widetilde{\pi_i}(\overline{X}) = \widetilde{\pi_i}(\overline{X'}).\end{aligned}$$

$\widetilde{\pi_i}$ is a ring morphism:

$$\begin{aligned}\widetilde{\pi_i}(\overline{X} + \overline{X'}) &= \widetilde{\pi_i}(\overline{X + X'})\\ &= \pi_i(X + X')\\ &= \pi_i(X) + \pi_i(X')\\ &= \widetilde{\pi_i}(\overline{X}) + \widetilde{\pi_i}(\overline{X'}).\end{aligned}$$

and

$$\begin{aligned}\widetilde{\pi_i}(\overline{X} \cdot \overline{X'}) &= \widetilde{\pi_i}(\overline{X \cdot X'})\\ &= \pi_i(X \cdot X')\\ &= \pi_i(X) \cdot \pi_i(X')\\ &= \widetilde{\pi_i}(\overline{X}) \cdot \widetilde{\pi_i}(\overline{X'}).\end{aligned}$$

$\widetilde{\pi_i}$ is a surjective:
If for every $y \in \operatorname{Im} \pi_i = \pi_i(\mathbb{F}_q[\varepsilon])$, there exists $X \in \mathbb{F}_q[\varepsilon]$ with $y = \pi_i(X)$, then $\exists \overline{X} \in \mathbb{F}_q[\varepsilon]/\ker \pi_i$ such that $y = \widetilde{\pi_i}(\overline{X})$.

$\widetilde{\pi_i}$ is a injective:

$$\begin{aligned}\widetilde{\pi_i}(\overline{X}) = \widetilde{\pi_i}(\overline{X'}) &\iff \pi_i(X) = \pi_i(X')\\ &\iff \pi_i(X) - \pi_i(X') = 0\\ &\iff \pi_i(X - X') = 0\\ &\iff X - X' \in \ker \pi_i\\ &\iff \overline{X} = \overline{X'}.\end{aligned}$$

Finally, $\mathbb{F}_q[\varepsilon]/\ker \pi_i \cong \operatorname{Im} \pi_i$ for all $i \in \{0, 1\}$. □

Corollary 2.4. *The mapping $\widetilde{\pi_i}$ is an isomorphism for $i \in \{0, 1\}$, in particular we have:*

$$\frac{\#\mathbb{F}_q[\varepsilon]}{\#\ker \pi_i} = \#\mathbb{F}_q[\varepsilon]/\ker \pi_i = \#\operatorname{Im} \pi_i.$$

2.3.1.2 Costs of arithmetic operations

Let s, m and i denote the costs of addition, multiplication and inversion in $\mathbb{F}_q$ respectively and let S, M and I denote the costs of addition, multiplication and inversion in $\mathbb{F}_q[\varepsilon]$ respectively. We have: $S = 4s$, $M = 11s+8m$ and $I = 7s+3m+4i$ where M is calculated by the Propsition 2.3.

2.3.2 Elliptic curve over $\mathbb{F}_q[\varepsilon], \varepsilon^4 = \varepsilon^3$

In this subsection, we consider X, Y, Z, a and b are elements of the ring $\mathbb{F}_q[\varepsilon]$ fixed by $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3$, $Y = y_0 + y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3$, $Z = z_0 + z_1\varepsilon + z_2\varepsilon^2 + z_3\varepsilon^3$, $a = a_0 + a_1\varepsilon + a_2\varepsilon^2 + a_3\varepsilon^3$ and $b = b_0 + b_1\varepsilon + b_2\varepsilon^2 + b_3\varepsilon^3$, with the prime number p is greater than or equal to 5.
The discriminant of elliptic curve over the ring $\mathbb{F}_q[\varepsilon]$ is $\triangle := -16(4a^3 + 27b^2)$ and we denoted by $\triangle_0$ and $\triangle_1$ the images of the discriminant $\triangle$ by π_0 and π_1 the morphisms respectively,

$$\begin{aligned}\triangle_0 &= \pi_0(\triangle) = \pi_0(-16(4a^3 + 27b^2)) = -16(\pi_0(4a^3) + \pi_0(27b^2))\\ &= -16(4(\pi_0(a))^3 + 27(\pi_0(b))^2) = -16(4a_0^3 + 27b_0^2) \text{ and}\\ \triangle_1 &= \pi_1(\triangle) = \pi_1(-16(4a^3 + 27b^2)) = -16(\pi_1(4a^3) + \pi_1(27b^2))\\ &= -16(4(\pi_1(a))^3 + 27(\pi_1(b))^2) = -16(4(a_0 + a_1 + a_2 + a_3)^3 + 27(b_0 + b_1 + b_2 + b_3)^2).\end{aligned}$$

The j-invariant of elliptic curve over the ring $\mathbb{F}_q[\varepsilon]$ is $j := \dfrac{(-48a)^3}{\triangle}$ and we denoted by j_0 and j_1 the images of the j-invariant j by π_0 and π_1 the morphisms respectively.

By using the Lemma 2.6, we have:

$$j_0 = \pi_0(j) = \pi_0\left(\frac{-48^3a^3}{\triangle}\right) = \pi_0(-48^3a^3\triangle^{-1}) = \pi_0(-48^3a^3)\pi_0(\triangle^{-1})$$
$$= (-48\pi_0(a))^3(\pi_0(\triangle))^{-1} = -48^3a_0^3\triangle_0^{-1} = \frac{-48^3a_0^3}{\triangle_0} \text{ and}$$
$$j_1 = \pi_1(j) = \pi_1\left(\frac{-48^3a^3}{\triangle}\right) = \pi_1((-48a)^3\triangle^{-1}) = \pi_1(-48^3a^3)\pi_1(\triangle^{-1})$$
$$= (-48\pi_1(a))^3(\pi_1(\triangle))^{-1} = -48^3(a_0+a_1+a_2+a_3)^3\triangle_1^{-1} = \frac{-48^3(a_0^3+a_1^3+a_2^3+a_3^3)}{\triangle_1}.$$

Definition 2.6. We define an elliptic curve over the ring $\mathbb{F}_q[\varepsilon]$, as a curve in the projective space $\mathbb{P}^2(\mathbb{F}_q[\varepsilon])$, which is given by the homogeneous equation of the degree 3, $Y^2Z = X^3 + aXZ^2 + bZ^3$ where a and b in $\mathbb{F}_q[\varepsilon]$ such that the discriminant $\triangle$ is invertible in $\mathbb{F}_q[\varepsilon]$. In this case, we denote the elliptic curve over $\mathbb{F}_q[\varepsilon]$ by $E_{a,b}(\mathbb{F}_q[\varepsilon])$, and we write:

$$E_{a,b}(\mathbb{F}_q[\varepsilon]) = \{[X:Y:Z] \in \mathbb{P}^2(\mathbb{F}_q[\varepsilon]) \mid Y^2Z = X^3 + aXZ^2 + bZ^3\}.$$

Proposition 2.5. *The discriminant $\triangle$ is invertible in the ring $\mathbb{F}_q[\varepsilon]$ if and only if $\triangle_0$ and $\triangle_1$ are invertible in the field $\mathbb{F}_q$.*

Proof. We show easily that $\triangle = \triangle_0 + \Theta\varepsilon + \Omega\varepsilon^2 + (\triangle_1 - \triangle_0 - \Theta - \Omega)\varepsilon^3$, where $\Theta = 4\Theta_{a^3} + 27\Theta_{b^2}$ and $\Omega = 4\Omega_{a^3} + 27\Omega_{b^2}$, then from the Proposition 2.4 we deduce the result. □

Corollary 2.5. *If the discriminant $\triangle$ is invertible in $\mathbb{F}_q[\varepsilon]$, then we can talk about the elliptic curves $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$ and $E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$ defined over the finite field $\mathbb{F}_q$ by:*

$$E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q) = \{[x:y:z] \in \mathbb{P}^2(\mathbb{F}_q) |\ y^2z = x^3 + a_0xz^2 + b_0z^3\} \text{ and}$$
$$E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q) = \{[x:y:z] \in \mathbb{P}^2(\mathbb{F}_q) |\ y^2z = x^3 + (\sum_{i=0}^{3} a_i)xz^2 + (\sum_{i=0}^{3} b_i)z^3\}.$$

Proposition 2.6. *Let X, Y and Z in $\mathbb{F}_q[\varepsilon]$, then $[X:Y:Z]$ is a point of $\mathbb{P}^2(\mathbb{F}_q[\varepsilon])$ if and only if $[\pi_i(X):\pi_i(Y):\pi_i(Z)]$ is a point of $\mathbb{P}^2(\mathbb{F}_q)$, where $i \in \{0,1\}$.*

Proof. Suppose that $[X:Y:Z] \in \mathbb{P}^2(\mathbb{F}_q[\varepsilon])$, then there exist the triple $(\alpha,\beta,\gamma) \in (\mathbb{F}_q[\varepsilon])^3$ such that $\alpha X + \beta Y + \gamma Z = 1$. Hence, we have:

$$\pi_0(\alpha)\pi_0(X) + \pi_0(\beta)\pi_0(Y) + \pi_0(\gamma)\pi_0(Z) = 1 \text{ and}$$
$$\pi_1(\alpha)\pi_1(X) + \pi_1(\beta)\pi_1(Y) + \pi_1(\gamma)\pi_1(Z) = 1.$$

So, $(\pi_0(X),\pi_0(Y),\pi_0(Z)) \neq (0,0,0)$ and $(\pi_1(X),\pi_1(Y),\pi_1(Z)) \neq (0,0,0)$, which proves that $[\pi_i(X):\pi_i(Y):\pi_i(Z)] \in \mathbb{P}^2(\mathbb{F}_q)$ for $i \in \{0,1\}$.

Reciprocally, let $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \in \mathbb{P}^2(\mathbb{F}_q)$ where $i \in \{0, 1\}$. Suppose that $x_0 \not\equiv 0[p]$, then we distinguish between two cases of $x_0 + x_1 + x_2 + x_3$:

1. $x_0 + x_1 + x_2 + x_3 \not\equiv 0[p]$: then X is invertible in $\mathbb{F}_q[\varepsilon]$, so the projective point $[X : Y : Z] \in \mathbb{P}^2(\mathbb{F}_q[\varepsilon])$.

2. $x_0 + x_1 + x_2 + x_3 \equiv 0[p]$: then $y_0 + y_1 + y_2 + y_3 \not\equiv 0[p]$ or $z_0 + z_1 + z_2 + z_3 \not\equiv 0[p]$.

   (i) If $y_0 + y_1 + y_2 + y_3 \not\equiv 0[p]$ then:
   $x_0 + x_1\varepsilon + x_2\varepsilon^2 + (y_0 + y_1 + y_2 + y_3 - x_0 - x_1 - x_2)\varepsilon^3$
   $= x_0 + x_1\varepsilon + x_2\varepsilon^2 - (x_0 + x_1 + x_2)\varepsilon^3 + (y_0 + y_1 + y_2 + y_3)\varepsilon^3$
   $= X + \varepsilon^3 Y \in (\mathbb{F}_q[\varepsilon])^\times$,
   so there exist $\Psi \in \mathbb{F}_q[\varepsilon]$: $\Psi X + \varepsilon^3 \Psi Y = 1$, hence $[X : Y : Z] \in \mathbb{P}^2(\mathbb{F}_q[\varepsilon])$.

   (ii) If $z_0 + z_1 + z_2 + z_3 \not\equiv 0[p]$ then:
   $x_0 + x_1\varepsilon + x_2\varepsilon^2 + (z_0 + z_1 + z_2 + z_3 - x_0 - x_1 - x_2)\varepsilon^3$
   $= x_0 + x_1\varepsilon + x_2\varepsilon^2 - (x_0 + x_1 + x_2)\varepsilon^3 + (z_0 + z_1 + z_2 + z_3)\varepsilon^3$
   $= X + \varepsilon^3 Z \in (\mathbb{F}_q[\varepsilon])^\times$,
   so there exist $\Phi \in \mathbb{F}_q[\varepsilon]$: $\Phi X + \varepsilon^3 \Phi Z = 1$, hence $[X : Y : Z] \in \mathbb{P}^2(\mathbb{F}_q[\varepsilon])$.

In the case where $y_0 \not\equiv 0[p]$ or $z_0 \not\equiv 0[p]$, we follow the same proof. □

Example 2.3. Let $X = 3+\varepsilon+2\varepsilon^2+\varepsilon^3$, $Y = 1+\varepsilon^2+4\varepsilon^3$ and $Z = \varepsilon+3\varepsilon^3$ be three elements in $\mathbb{F}_5[\varepsilon]$, then $[X : Y : Z]$ is a point of $\mathbb{P}^2(\mathbb{F}_5[\varepsilon]) \iff [\pi_0(X) : \pi_0(Y) : \pi_0(Z)] = [3 : 1 : 0]$ and $[\pi_1(X) : \pi_1(Y) : \pi_1(Z)] = [2 : 1 : 4]$ are two points of $\mathbb{P}^2(\mathbb{F}_5)$.

Proposition 2.7. *Let X, Y and Z in $\mathbb{F}_q[\varepsilon]$, if the point $[X : Y : Z]$ is a solution of the Weierstrass equation in $E_{a,b}(\mathbb{F}_q[\varepsilon])$ then $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)]$, where $i \in \{0, 1\}$ is a solution of the same equation in $E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q)$.*

Proof. From the Proposition 2.3 and the Corollary 2.1, we have:

$$Y^2 = y_0^2 + \Theta_{Y^2}\varepsilon + \Omega_{Y^2}\varepsilon^2 + ((\sum_{i=0}^{3} y_i)^2 - y_0^2 - \Theta_{Y^2} - \Omega_{Y^2})\varepsilon^3.$$

$$Z^2 = z_0^2 + \Theta_{Z^2}\varepsilon + \Omega_{Z^2}\varepsilon^2 + ((\sum_{i=0}^{3} z_i)^2 - z_0^2 - \Theta_{Z^2} - \Omega_{Z^2})\varepsilon^3.$$

$$aX = a_0x_0 + \Theta_{aX}\varepsilon + \Omega_{aX}\varepsilon^2 + ((\sum_{i=0}^{3} a_i)(\sum_{i=0}^{3} x_i) - a_0x_0 - \Theta_{aX} - \Omega_{aX})\varepsilon^3.$$

$$Z^3 = z_0^3 + \Theta_{Z^3}\varepsilon + \Omega_{Z^3}\varepsilon^2 + ((\sum_{i=0}^{3} z_i)^3 - z_0^3 - \Theta_{Z^3} - \Omega_{Z^3})\varepsilon^3.$$

Then:

$$Y^2Z = y_0^2z_0 + \Theta_{Y^2Z}\varepsilon + \Omega_{Y^2Z}\varepsilon^2 + ((\sum_{i=0}^{3} y_i)^2(\sum_{i=0}^{3} z_i) - y_0^2z_0 - \Theta_{Y^2Z} - \Omega_{Y^2Z})\varepsilon^3,$$

$$X^3 = x_0^3 + \Theta_{X^3}\varepsilon + \Omega_{X^3}\varepsilon^2 + ((\sum_{i=0}^{3} x_i)^3 - x_0^3 - \Theta_{X^3} - \Omega_{X^3})\varepsilon^3,$$

$$aXZ^2 = a_0x_0z_0^2 + \Theta_{aXZ^2}\varepsilon + \Omega_{aXZ^2}\varepsilon^2 + ((\sum_{i=0}^{3} a_i)(\sum_{i=0}^{3} x_i)(\sum_{i=0}^{3} z_i)^2 - a_0x_0z_0^2 - \Theta_{aXZ^2} - \Omega_{aXZ^2})\varepsilon^3,$$

$$bZ^3 = b_0z_0^3 + \Theta_{bZ^3}\varepsilon + \Omega_{bZ^3}\varepsilon^2 + ((\sum_{i=0}^{3} b_i)(\sum_{i=0}^{3} z_i)^3 - b_0z_0^3 - \Theta_{bZ^3} - \Omega_{bZ^3})\varepsilon^3.$$

$$\text{Hence, } Y^2Z = X^3+aXZ^2+bZ^3 \Longleftrightarrow \begin{cases} y_0^2z_0 = x_0^3 + a_0x_0z_0^2 + b_0z_0^3; \\ \Theta_{Y^2Z} = \Theta_{X^3} + \Theta_{aXZ^2} + \Theta_{bZ^3}; \\ \Omega_{Y^2Z} = \Omega_{X^3} + \Omega_{aXZ^2} + \Omega_{bZ^3}; \\ (\sum_{i=0}^{3} y_i)^2(\sum_{i=0}^{3} z_i) = (\sum_{i=0}^{3} x_i)^3 + (\sum_{i=0}^{3} a_i)(\sum_{i=0}^{3} x_i)(\sum_{i=0}^{3} z_i)^2 \\ \qquad\qquad + (\sum_{i=0}^{3} b_i)(\sum_{i=0}^{3} z_i)^3. \end{cases}$$

Which proves that for $i \in \{0,1\}$, $[\pi_i(X) : \pi_i(y) : \pi_i(Z)]$ is a solution of the Weierstrass equation in $E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q)$. □

Example 2.4. Let $E_{a,b} : Y^2Z = X^3+aXZ^2+bZ^3$, where $a = 1+2\varepsilon^3$ and $b = 1+\varepsilon+3\varepsilon^2+2\varepsilon^3$ in $\mathbb{F}_5[\varepsilon]$, the discriminant $\triangle = 4+\varepsilon+\varepsilon^2+3\varepsilon^3$ is invertible in $\mathbb{F}_5[\varepsilon]$ because $\pi_0(\triangle) = 4 \not\equiv 0[5]$ and $\pi_1(\triangle) = 4 \not\equiv 0[5]$, then $E_{a,b}(\mathbb{F}_5[\varepsilon])$ is an elliptic curve.
Let $X = 2+\varepsilon+3\varepsilon^2+\varepsilon^3$, $Y = 1+2\varepsilon+2\varepsilon^2+\varepsilon^3$ and $Z = 1$ in $\mathbb{F}_5[\varepsilon]$, the point $[X : Y : Z]$ is a solution of the Weierstrass equation $E_{a,b}$, then $[\pi_0(X) : \pi_0(Y) : \pi_0(Z)] = [x, y, z] = [2 : 1 : 1]$ and $[\pi_1(X) : \pi_1(Y) : \pi_1(Z)] = [x, y, z] = [2 : 1 : 1]$ are a solutions of equations $E_{\pi_0(a),\pi_0(b)}$ and $E_{\pi_1(a),\pi_1(b)}$ respectively, where:

$$E_{\pi_0(a),\pi_0(b)} : y^2z = x^3 + \pi_0(a)xz^2 + \pi_0(b)z^3 = x^3 + xz^2 + z^3,$$
$$E_{\pi_1(a),\pi_1(b)} : y^2z = x^3 + \pi_1(a)xz^2 + \pi_1(b)z^3 = x^3 + 3xz^2 + 2z^3.$$

Theorem 2.1. *Let $a = \tilde{a}+a_3\varepsilon^3$, $b = \tilde{b}+b_3\varepsilon^3$, $X = \widetilde{X}+x_3\varepsilon^3$, $Y = \widetilde{Y}+y_3\varepsilon^3$, and $Z = \widetilde{Z}+z_3\varepsilon^3$, the elements of $\mathbb{F}_q[\varepsilon]$, which satisfied the Weierstrass equation $Y^2Z = X^3 + aXZ^2 + bZ^3$, then:*

$$\widetilde{Y}^2\widetilde{Z} = \widetilde{X}^3 + \tilde{a}\widetilde{X}\widetilde{Z}^2 + \tilde{b}\widetilde{Z}^3 + (D - (Ax_3 + By_3 + Cz_3))\varepsilon^3,$$

where:

$$\begin{cases} D = a_3(x_0 + x_1 + x_2)(z_0 + z_1 + z_2)^2 + b_3(z_0 + z_1 + z_2)^3 \\ \quad + 3x_3^2(x_0 + x_1 + x_2) + x_3^3 - y_3^2(z_0 + z_1 + z_2 + z_3) \\ \quad + z_3^2((x_0 + x_1 + x_2 + x_3)(a_0 + a_1 + a_2 + a_3) + 3(z_0 + z_1 + z_2)(b_0 + b_1 + b_2 + b_3)); \\ A = -3(x_0 + x_1 + x_2)^2 - (z_0 + z_1 + z_2)^2(a_0 + a_1 + a_2 + a_3); \\ B = 2(y_0 + y_1 + y_2)(z_0 + z_1 + z_2 + z_3); \\ C = -2(z_0 + z_1 + z_2)(x_0 + x_1 + x_2 + x_3)(a_0 + a_1 + a_2 + a_3) \\ \quad - 3(z_0 + z_1 + z_2)^2(b_0 + b_1 + b_2 + b_3) + (y_0 + y_1 + y_2)^2. \end{cases}$$

Proof. We have:

$$Y^2 = (\widetilde{Y} + y_3\varepsilon^3)^2 = \widetilde{Y}^2 + 2\widetilde{Y}y_3\varepsilon^3 + y_3^2\varepsilon^3 = \widetilde{Y}^2 + (2y_3(y_0 + y_1 + y_2) + y_3^2)\varepsilon^3.$$
$$\begin{aligned} Y^2Z &= (\widetilde{Y} + y_3\varepsilon^3)^2(\widetilde{Z} + z_3\varepsilon^3) = (\widetilde{Y}^2 + (2y_3(y_0 + y_1 + y_2) + y_3^2)\varepsilon^3)(\widetilde{Z} + z_3\varepsilon^3) \\ &= \widetilde{Y}^2\widetilde{Z} + (z_3(y_0 + y_1 + y_2)^2 + 2y_3(y_0 + y_1 + y_2)(z_0 + z_1 + z_2 + z_3) \\ &\quad + y_3^2(z_0 + z_1 + z_2 + z_3))\varepsilon^3. \end{aligned}$$

$$\begin{aligned}
X^3 &= (\widetilde{X} + x_3\varepsilon^3)^3 = \widetilde{X}^3 + 3\widetilde{X}^2 x_3\varepsilon^3 + 3\widetilde{X}x_3^2\varepsilon^3 + x_3^3\varepsilon^3 \\
&= \widetilde{X}^3 + (3\widetilde{X}^2 x_3 + 3\widetilde{X}x_3^2 + x_3^3)\varepsilon^3 \\
&= \widetilde{X}^3 + (3x_3(x_0 + x_1 + x_2)^2 + 3x_3^2(x_0 + x_1 + x_2) + x_3^3)\varepsilon^3. \\
aXZ^2 &= (\tilde{a} + a_3\varepsilon^3)(\widetilde{X} + x_3\varepsilon^3)(\tilde{Z} + z_3\varepsilon^3)^2 \\
&= (\tilde{a} + a_3\varepsilon^3)(\widetilde{X}\tilde{Z}^2 + (x_3(z_0 + z_1 + z_2)^2 \\
&+ 2z_3(z_0 + z_1 + z_2)(x_0 + x_1 + x_2 + x_3) + z_3^2(x_0 + x_1 + x_2 + x_3))\varepsilon^3) \\
&= \tilde{a}\widetilde{X}\tilde{Z}^2 + (x_3(z_0 + z_1 + z_2)^2(a_0 + a_1 + a_2 + a_3) \\
&+ 2z_3(z_0 + z_1 + z_2)(x_0 + x_1 + x_2 + x_3)(a_0 + a_1 + a_2 + a_3) \\
&+ z_3^2(x_0 + x_1 + x_2 + x_3)(a_0 + a_1 + a_2 + a_3) + a_3(x_0 + x_1 + x_2)(z_0 + z_1 + z_2)^2)\varepsilon^3. \\
bZ^3 &= (\tilde{b} + b_3\varepsilon^3)(\tilde{Z} + z_3\varepsilon^3)^3 \\
&= (\tilde{b} + b_3\varepsilon^3)(\tilde{Z}^3 + (3z_3(z_0 + z_1 + z_2)^2 + 3z_3^2(z_0 + z_1 + z_2) + z_3^3)\varepsilon^3) \\
&= \tilde{b}\tilde{Z}^3 + (3z_3(z_0 + z_1 + z_2)^2(b_0 + b_1 + b_2 + b_3) \\
&+ 3z_3^2(z_0 + z_1 + z_2)(b_0 + b_1 + b_2 + b_3) + b_3(z_0 + z_1 + z_2)^3)\varepsilon^3.
\end{aligned}$$

Since $Y^2Z = X^3 + aXZ^2 + bZ^3$ then:

$$\tilde{Y}^2\tilde{Z} = \widetilde{X}^3 + \tilde{a}\widetilde{X}\tilde{Z}^2 + \tilde{b}\tilde{Z}^3 + (D - (Ax_3 + By_3 + Cz_3))\varepsilon^3,$$

where:

$$\begin{cases}
D = a_3(x_0 + x_1 + x_2)(z_0 + z_1 + z_2)^2 + b_3(z_0 + z_1 + z_2)^3 \\
\quad + 3x_3^2(x_0 + x_1 + x_2) + x_3^3 - y_3^2(z_0 + z_1 + z_2 + z_3) \\
\quad + z_3^2((x_0 + x_1 + x_2 + x_3)(a_0 + a_1 + a_2 + a_3) + 3(z_0 + z_1 + z_2)(b_0 + b_1 + b_2 + b_3)); \\
A = -3(x_0 + x_1 + x_2)^2 - (z_0 + z_1 + z_2)^2(a_0 + a_1 + a_2 + a_3); \\
B = 2(y_0 + y_1 + y_2)(z_0 + z_1 + z_2 + z_3); \\
C = -2(z_0 + z_1 + z_2)(x_0 + x_1 + x_2 + x_3)(a_0 + a_1 + a_2 + a_3) \\
\quad - 3(z_0 + z_1 + z_2)^2(b_0 + b_1 + b_2 + b_3) + (y_0 + y_1 + y_2)^2.
\end{cases}$$

Then, we deduce the theorem. □

Corollary 2.6. *If $D = Ax_3 + By_3 + Cz_3$ then $\tilde{a}, \tilde{b}, \widetilde{X}, \widetilde{Y}$ and $\widetilde{Z}$ are satisfies the equation of Weierstrass $\widetilde{Y}^2\widetilde{Z} = \widetilde{X}^3 + \tilde{a}\widetilde{X}\widetilde{Z}^2 + \tilde{b}\widetilde{Z}^3$.*

From the propositions 2.5, 2.6 and 2.7, we deduce the theorem:

Theorem 2.2. *Let X, Y and Z in $\mathbb{F}_q[\varepsilon]$. If $[X : Y : Z] \in E_{a,b}(\mathbb{F}_q[\varepsilon])$ then $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \in E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q)$, where $i \in \{0, 1\}$.*

Theorem 2.3. *The set $E_{a,b}(\mathbb{F}_q[\varepsilon])$ is abelian group, written additively. And has $[0 : 1 : 0]$ as its zero element, and for all $P = [X_1 : Y_1 : Z_1]$ and $Q = [X_2 : Y_2 : Z_2]$ in $E_{a,b}(\mathbb{F}_q[\varepsilon])$ we have $P + Q = [X_3 : Y_3 : Z_3]$, where:*

- ❖ *If $P \neq Q$, then:*

$$X_3 = Y_1^2X_2Z_2 - Z_1X_1Y_2 - a(Z_1X_2 + X_1Z_2)(Z_1X_2 - X_1Z_2) + (2Y_1Y_2 - 3bZ_1Z_2)(Z_1X_2 - X_1Z_2).$$
$$Y_3 = Y_1Y_2(Z_2Y_1 - Z_1Y_2) - a(X_1Y_1Z_2^2 - Z_1^2X_2Y_2) + (-2aZ_1Z_2 - 3X_1X_2)(X_2Y_1 - X_1Y_2) - 3bZ_1Z_2(Z_2Y_1 - Z_1Y_2).$$
$$Z_3 = (Z_1Y_2 + Z_2Y)(Z_2Y_1 - Z_1Y_2) + (3X_1X_2 + aZ_1Z_2)(Z_1X_2 - X_1Z_2).$$

❖ *If $P = Q$, then:*

$$X_3 = (Y_1Y_2 - 6bZ_1Z_2)(X_2Y_1 + X_1Y_2) + (a^2Z_1Z_2 - 2aX_1X_2)(Z_1Y_2 + Z_2Y_1) - 3b(X_1Y_1Z_2^2 + Z_1^2X_2Y_2) - a(Y_1Z_1X_2^2 + X_1^2Y_2Z_2).$$
$$Y_3 = Y_1^2Y_2^2 + 3aX_1^2X_2^2 + (-a^3 - 9b^2)Z_1^2Z_2^2 - a^2(Z_1X_2 + X_1Z_2^2)^2 - 2a^2Z_1X_1Z_2X_2 + (9bX_1X_2 - 3abZ_1Z_2)(Z_1X_2 + X_1Z_2).$$
$$Z_3 = (Y_1Y_2 + 3bZ_1Z_2)(Z_1Y_2 + Z_2Y_1) + (3X_1X_2 + 2aZ_1Z_2)(X_2Y_1 + X_1Y_2) + a(X_1Y_1Z_2^2 + Z_1^2X_2Y_2).$$

Proof. The ring $\mathbb{F}_q[\varepsilon]$ is a finite, therefore according to Lenstra [46] conditions (1) and (2) is satisfied. So, using the explicit formulae of W. Bosma and H. W. Lenstra article, see [8][page: 236-238], we prove the theorem. □

Example 2.5. Let $P = [3\varepsilon^3 + 2\varepsilon + 2 : 1 : 2\varepsilon^2 + 3\varepsilon + 1]$ be a point in $E_{a,b}(\mathbb{F}_5[\varepsilon])$, where $a = 2\varepsilon^3 + 1$ and $b = 2\varepsilon^3 + 3\varepsilon^2 + \varepsilon + 1$ in $\mathbb{F}_5[\varepsilon]$. And G is the subgroup of elliptic curve $E_{a,b}(\mathbb{F}_5[\varepsilon])$ generated by the point P of order $n = 15$.
The elements of a subgroup $G = \langle P \rangle$ is shown in the table 2.1:

n	nP	n	nP
1	$[3\varepsilon^3 + 2\varepsilon + 2 : 1 : 2\varepsilon^2 + 3\varepsilon + 1]$	9	$[4\varepsilon^3 + 4\varepsilon : 1 : 4\varepsilon^3]$
2	$[\varepsilon^3 + 3 : 1 : 4\varepsilon^3 + \varepsilon + 4]$	10	$[2\varepsilon^3 + 3\varepsilon^2 + 3\varepsilon + 2 : 1 : 4\varepsilon^2 + 1]$
3	$[3\varepsilon^3 + 3\varepsilon : 1 : \varepsilon^3]$	11	$[\varepsilon^3 + 2\varepsilon^2 + \varepsilon + 3 : 1 : 4\varepsilon^3 + 3\varepsilon + 4]$
4	$[4\varepsilon^3 + 3\varepsilon^2 + 4\varepsilon + 2 : 1 : \varepsilon^3 + 2\varepsilon + 1]$	12	$[2\varepsilon^3 + 2\varepsilon : 1 : 4\varepsilon^3]$
5	$[3\varepsilon^3 + 2\varepsilon^2 + 2\varepsilon + 3 : 1 : \varepsilon^2 + 4]$	13	$[4\varepsilon^3 + 2 : 1 : \varepsilon^3 + 4\varepsilon + 1]$
6	$[\varepsilon^3 + \varepsilon 1 : \varepsilon^3]$	14	$[2\varepsilon^3 + 3\varepsilon + 3 : 1 : 3\varepsilon^2 + 2\varepsilon + 4]$
7	$[2\varepsilon^3 + 4\varepsilon^2 + \varepsilon + 2 : 1 : 3\varepsilon^3 + 4\varepsilon^2 + \varepsilon + 1]$	15	$[0 : 1 : 0] = \infty$
8	$[3\varepsilon^3 + \varepsilon^2 + 4\varepsilon + 3 : 1 : 2\varepsilon^3 + \varepsilon^2 + 4\varepsilon + 4]$		

Table 2.1: The subgroup $G = \langle P \rangle$.

Corollary 2.7. *For $i \in \{0, 1\}$, the mapping φ_i given by:*

$$\varphi_i : \begin{array}{ccc} E_{a,b}(\mathbb{F}_q[\varepsilon]) & \longrightarrow & E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q) \\ [X : Y : Z] & \longmapsto & [\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \end{array}$$

is well defined.

Proof. Let $[X : Y : Z] \in E_{a,b}(\mathbb{F}_q[\varepsilon])$. From the previous Theorem 2.2, we have $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \in E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q)$, where $i \in \{0, 1\}$.

If $[X : Y : Z] = [X' : Y' : Z']$ then there exist $\Phi \in (\mathbb{F}_q[\varepsilon])^\times$ such that: $X' = \Phi X$, $Y' = \Phi Y$ and $Z' = \Phi Z$, then:

$$\begin{aligned}\varphi_i([X' : Y' : Z']) &= [\pi_i(X') : \pi_i(Y') : \pi_i(Z')] \\ &= [\pi_i(\Phi X) : \pi_i(\Phi Y) : \pi_i(\Phi Z)] \\ &= \underbrace{[\pi_i(\Phi)\pi_i(X) : \pi_i(\Phi)\pi_i(Y) : \pi_i(\Phi)\pi_i(Z)]}_{\pi_i(\Phi)\in\mathbb{F}_q^*} \\ &= [\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \\ &= \varphi_i([X : Y : Z]).\end{aligned}$$

So, the mapping φ_i is well defined where $i \in \{0, 1\}$. □

Corollary 2.8. *The mapping φ_i is a morphism of group, where $i \in \{0, 1\}$.*

Proof. Let $[X_1 : Y_1 : Z_1]$, $[X_2 : Y_2 : Z_2] \in E_{a,b}(\mathbb{F}_q[\varepsilon])$,

$$\begin{aligned}\varphi_i([X_1 : Y_1 : Z_1] + [X_2 : Y_2 : Z_2]) &= \varphi_i([X_3 : Y_3 : Z_3]) \\ &= [\pi_i(X_3) : \pi_i(Y_3) : \pi_i(Z_3)],\end{aligned}$$

by the Theorem 2.3 and π_i is a morphism of ring, we have:

$$\begin{aligned}[\pi_i(X_3) : \pi_i(Y_3) : \pi_i(Z_3)] &= [\pi_i(X_1) : \pi_i(Y_1) : \pi_i(Z_1)] + [\pi_i(X_2) : \pi_i(Y_2) : \pi_i(Z_2)] \\ &= \varphi_i([X_1 : Y_1 : Z_1]) + \varphi_i([X_2 : Y_2 : Z_2]),\end{aligned}$$

then $\varphi_i([X_1 : Y_1 : Z_1] + [X_2 : Y_2 : Z_2]) = \varphi_i([X_1 : Y_1 : Z_1]) + \varphi_i([X_2 : Y_2 : Z_2])$.
So, the mapping φ_i is a morphism of group, where $i \in \{0, 1\}$. □

Corollary 2.9. *The mapping φ_0 is a surjective.*

Proof. Let $[x : y : z] \in E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$, then:

- If $y \not\equiv 0[p]$ then $[x : y : z] \sim [x : 1 : z]$ hence $[x(1 - \varepsilon - \varepsilon^2 + \varepsilon^3) : 1 : z(1 - \varepsilon - \varepsilon^2 + \varepsilon^3)]$ is an antecedent of $[x : 1 : z]$.
- If $y \equiv 0[p]$ then $z \not\equiv 0[p]$ and $[x : y : z] \sim [x : 0 : 1]$ hence $[x(1 - \varepsilon - \varepsilon^2 + \varepsilon^3) : \varepsilon + \varepsilon^2 + \varepsilon^3 : 1 - \varepsilon - \varepsilon^2 + \varepsilon^3]$ is an antecedent of $[x : 0 : 1]$.

□

Corollary 2.10. *The mapping φ_1 is a surjective.*

Proof. Let $[x : y : z] \in E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$, then:

- If $y \not\equiv 0[p]$ then $[x : y : z] \sim [x : 1 : z]$ hence $[x(\varepsilon - \varepsilon^2 + \varepsilon^3) : 1 : z(\varepsilon - \varepsilon^2 + \varepsilon^3)]$ is an antecedent of $[x : 1 : z]$.

❖ If $y \equiv 0[p]$ then $z \not\equiv 0[p]$ and $[x : y : z] \sim [x : 0 : 1]$ hence $[x(\varepsilon - \varepsilon^2 + \varepsilon^3) : 1 + \varepsilon - \varepsilon^2 - \varepsilon^3 : \varepsilon - \varepsilon^2 + \varepsilon^3]$ is an antecedent of $[x : 0 : 1]$.

□

Lemma 2.7. *The kernel of φ_i is a subgroup, such that:*

$$\ker \varphi_i = \{[X : Y : Z] \in E_{a,b}(\mathbb{F}_q[\varepsilon]) \mid [\pi_i(X) : \pi_i(Y) : \pi_i(Z)] = [0 : 1 : 0]\},$$

where $i \in \{0, 1\}$.

Proposition 2.8. *The mapping $\overline{\varphi_i}$ where $i \in \{0, 1\}$ given by:*

$$\overline{\varphi_i} : \left| \begin{array}{ccc} E_{a,b}(\mathbb{F}_q[\varepsilon])/\ker \varphi_i & \longrightarrow & \operatorname{Im} \varphi_i = E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q) \\ [X : Y : Z] + \ker \varphi_i & \longmapsto & [\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \end{array} \right.$$

is an isomorphism of group.

Proof. Let $\overline{P}, \overline{Q} \in E_{a,b}(\mathbb{F}_q[\varepsilon])/\ker \varphi_i$ such that $\overline{P} = P + \ker \varphi_i$ and $\overline{Q} = Q + \ker \varphi_i$ where $P = [X_1 : Y_1 : Z_1]$ and $Q = [X_2 : Y_2 : Z_2]$. For all $i \in \{0, 1\}$, we have:

$$\overline{\varphi_i}(\overline{P}) = \varphi_i(P) \text{ and } \overline{\varphi_i}(\overline{Q}) = \varphi_i(Q).$$

$\overline{\varphi_i}$ is well defined:

$$\begin{aligned} \overline{P} = \overline{Q} &\iff P - Q \in \ker \varphi_i \\ &\iff \varphi_i(P - Q) = \varphi_i(P) - \varphi_i(Q) = [0 : 1 : 0] \quad (\varphi_i \text{ is a morphism group}) \\ &\iff \varphi_i(P) = \varphi_i(Q) \\ &\iff \overline{\varphi_i}(\overline{P}) = \overline{\varphi_i}(\overline{Q}). \end{aligned}$$

$\overline{\varphi_i}$ is a morphism of group:

$$\begin{aligned} \overline{\varphi_i}(\overline{P} + \overline{Q}) &= \overline{\varphi_i}(\overline{P + Q}) \\ &= \varphi_i(P + Q) = \varphi_i(P) + \varphi_i(Q) \\ &= \overline{\varphi_i}(\overline{P}) + \overline{\varphi_i}(\overline{Q}). \end{aligned}$$

$\overline{\varphi_i}$ is a surjective:

If for every $M \in \operatorname{Im} \varphi_i = E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q)$, there exists at least one $P \in E_{a,b}(\mathbb{F}_q[\varepsilon])$ with $M = \varphi_i(P)$, then $\exists \overline{P} \in E_{a,b}(\mathbb{F}_q[\varepsilon])/\ker \varphi_i$ such that $M = \overline{\varphi_i}(\overline{P})$.

$\overline{\varphi_i}$ is an injective:

$$\begin{aligned} \overline{\varphi_i}(\overline{P}) = \overline{\varphi_i}(\overline{Q}) &\iff \varphi_i(P) = \varphi_i(Q) \\ &\iff \varphi_i(P) - \varphi_i(Q) = \varphi_i(P - Q) = [0 : 1 : 0] \\ &\iff P - Q \in \ker \varphi_i \iff \overline{P} = \overline{Q}. \end{aligned}$$

Finally, $E_{a,b}(\mathbb{F}_q[\varepsilon])/\ker\varphi_i \cong \operatorname{Im}\varphi_i$, for all $i \in \{0,1\}$. □

Corollary 2.11. *The mapping $\overline{\varphi_i}$ is an isomorphism for $i \in \{0,1\}$, in particular we have:*

$$\frac{\#E_{a,b}(\mathbb{F}_q[\varepsilon])}{\#\ker\varphi_i} = \#E_{a,b}(\mathbb{F}_q[\varepsilon])/\ker\varphi_i = \#\operatorname{Im}\varphi_i = \#E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q).$$

2.3.3 Classification of elements in $E_{a,b}(\mathbb{F}_q[\varepsilon])$

In this subsection, we will classify the elements of the elliptic curve $E_{a,b}(\mathbb{F}_q[\varepsilon])$ into three types, depending on whether the third projective coordinate Z is invertible or not. The result is in the following proposition.

Proposition 2.9. *Every element of the elliptic curve $E_{a,b}(\mathbb{F}_q[\varepsilon])$ has one of the forms:*

1. $[X : Y : 1]$, *where* $X, Y \in \mathbb{F}_q[\varepsilon]$.
2. $[x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 : 1 : z_1\varepsilon + z_2\varepsilon^2 + z_3\varepsilon^3]$, *such that* $[x_1 + x_2 + x_3 : 1 : z_1 + z_2 + z_3]$ *in* $E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$.
3. $[x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 : 1 + y_1\varepsilon + y_2\varepsilon^2 - (1 + y_1 + y_2)\varepsilon^3 : z_1\varepsilon + z_2\varepsilon^2 + z_3\varepsilon^3]$, *such that* $[x_1 + x_2 + x_3 : 0 : z_1 + z_2 + z_3]$ *in* $E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$.
4. $[x_0 + x_1\varepsilon + x_2\varepsilon^2 - \sum_{i=0}^{2} x_i\varepsilon^3 : 1 : z_0 + z_1\varepsilon + z_2\varepsilon^2 - \sum_{i=0}^{2} z_i\varepsilon^3]$, *such that* $[x_0 : 1 : z_0]$ *in* $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$.
5. $[x_0 + x_1\varepsilon + x_2\varepsilon^2 - \sum_{i=0}^{2} x_i\varepsilon^3 : y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3 : z_0 + z_1\varepsilon + z_2\varepsilon^2 - \sum_{i=0}^{2} z_i\varepsilon^3]$, *such that* $y_1 + y_2 + y_3 \not\equiv 0[p]$ *and* $[x_0 : 0 : 1]$ *in* $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$.

Proof. Let $\Gamma = [X : Y : Z] \in E_{a,b}(\mathbb{F}_q[\varepsilon])$, we have three cases of third projective coordinate Z:

1. If Z is invertibe, then: $[X : Y : Z] \sim [X : Y : 1]$.
2. If $Z = z_1\varepsilon + z_2\varepsilon^2 + z_3\varepsilon^3$ where $(z_1, z_2, z_3) \in (\mathbb{F}_q)^3$, then $\varphi_0([X : Y : Z]) = [x_0 : y_0 : 0]$ so $x_0 \equiv 0[p]$ and $y_0 \not\equiv 0[p]$, hence $[X : Y : Z] = [x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 : 1 + y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3 : z_1\varepsilon + z_2\varepsilon^2 + z_3\varepsilon^3]$ and there are two sub-cases of $y_1 + y_2 + y_3 \in \mathbb{F}_q$:
   (i) $y_1 + y_2 + y_3 \not\equiv -1[p]$ then $1 + y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3$ is invertible in $\mathbb{F}_q[\varepsilon]$, so we have: $[X : Y : Z] \sim [x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 : 1 : z_1\varepsilon + z_2\varepsilon^2 + z_3\varepsilon^3]$, where $[x_1 + x_2 + x_3 : 1 : z_1 + z_2 + z_3] \in E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$.

(ii) $y_1 + y_2 + y_3 \equiv -1[p]$, then $1 + y_1\varepsilon + y_2\varepsilon^2 - (1 + y_1 + y_2)\varepsilon^3$ is not invertible in $\mathbb{F}_q[\varepsilon]$, so we have:
$[X : Y : Z] = [x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 : 1 + y_1\varepsilon + y_2\varepsilon^2 - (1 + y_1 + y_2)\varepsilon^3 : z_1\varepsilon + z_2\varepsilon^2 + z_3\varepsilon^3]$,
where $[x_1 + x_2 + x_3 : 0 : z_1 + z_2 + z_3] \in E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$.

3. If $Z = z_0 + z_1\varepsilon + z_2\varepsilon^2 - (z_0 + z_1 + z_2)\varepsilon^3$ where $(z_0, z_1, z_2) \in (\mathbb{F}_q)^3$, then:
$\varphi_1([X : Y : Z]) = [x_0 + x_1 + x_2 + x_3 : y_0 + y_1 + y_2 + y_3 : 0]$, so $x_0 + x_1 + x_2 + x_3 \equiv 0[p]$ and $y_0 + y_1 + y_2 + y_3 \not\equiv 0[p]$, hence
$[X : Y : Z] = [x_0 + x_1\varepsilon + x_2\varepsilon^2 - \sum_{i=0}^{2} x_i\varepsilon^3 : y_0 + y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3 : z_0 + z_1\varepsilon + z_2\varepsilon^2 - \sum_{i=0}^{2} z_i\varepsilon^3]$,
so we have two sub-cases of $y_0 \in \mathbb{F}_q$:

(i) $y_0 \not\equiv 0[P]$, then $y_0 + y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3$ is invertible in $\mathbb{F}_q[\varepsilon]$, then:
$[X : Y : Z] \sim [x_0 + x_1\varepsilon + x_2\varepsilon^2 - \sum_{i=0}^{2} x_i\varepsilon^3 : 1 : z_0 + z_1\varepsilon + z_2\varepsilon^2 - \sum_{i=0}^{2} z_i\varepsilon^3]$, where
$[x_0 : 1 : z_0] \in E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$.

(ii) $y_0 \equiv 0[P]$, then $Y = y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3$ is not invertible in $\mathbb{F}_q[\varepsilon]$, so we have:
$[X : Y : Z] = [x_0 + x_1\varepsilon + x_2\varepsilon^2 - \sum_{i=0}^{2} x_i\varepsilon^3 : y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3 : z_0 + z_1\varepsilon + z_2\varepsilon^2 - \sum_{i=0}^{2} z_i\varepsilon^3]$, where $[x_0 : 0 : z_0] \in E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$, then necessary $z_0 \not\equiv 0[p]$ and
$[X : Y : Z] = [x_0 + x_1\varepsilon + x_2\varepsilon^2 - \sum_{i=0}^{2} x_i\varepsilon^3 : y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3 : 1 + \alpha\varepsilon + \beta\varepsilon^2 - (1 + \alpha + \beta)\varepsilon^3]$, where $y_1 + y_2 + y_3 \not\equiv 0[p]$ and $[x_0 : 0 : 1] \in E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$.

Which proves the proposition. □

2.4 Elliptic curve over a ring of characteristic 3

In this section, we study the elliptic curve over the finite ring $\mathbb{F}_{3^d}[\varepsilon]$, where $\varepsilon^4 = \varepsilon^3$ of characteristic 3 given by the homogeneous Weierstrass equation of the form

$$Y^2Z = X^3 + aX^2Z + bZ^3, \text{ where } a, b \in \mathbb{F}_{3^d}[\varepsilon].$$

Such that we study the arithmetic operations of this ring and define the elliptic curve over it. Next, we show that $E_{\Pi_0(a),\Pi_0(b)}(\mathbb{F}_{3^d})$ and $E_{\Pi_1(a),\Pi_1(b)}(\mathbb{F}_{3^d})$ are two elliptic curves over the finite field $\mathbb{F}_{3^d}$, such that Π_0 is a canonical projection and Π_1 is a sum projection of coordinate of element in $\mathbb{F}_{3^d}[\varepsilon]$ and we conclude by given a classification of elements in elliptic curve over the finite ring $\mathbb{F}_{3^d}[\varepsilon]$.

2.4.1 The finite ring $\mathbb{F}_{3^d}[\varepsilon], \varepsilon^4 = \varepsilon^3$

We will follow the approach in the previous section. The ring $\mathbb{F}_{3^d}[\varepsilon]$, where $\varepsilon^4 = \varepsilon^3$ can be constructed by using the quotient ring of $\mathbb{F}_{3^d}[X]$ by the polynomial $X^4 - X^3$. $\mathbb{F}_{3^d}$ is a finite field of order 3^d where d is a positive integer. Every element $X \in \mathbb{F}_{3^d}[\varepsilon]$ written in the form $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3$ where $(x_0, x_1, x_2, x_3) \in \mathbb{F}_{3^d}^4$.

2.4.1.1 Arithmetic operations

The arithmetic operations in $\mathbb{F}_{3^d}[\varepsilon]$ can be decomposed into operations in $\mathbb{F}_{3^d}$ and they are computed as follows:
$X + Y = (x_0 + y_0) + (x_1 + y_1)\varepsilon + (x_2 + y_2)\varepsilon^2 + (x_3 + y_3)\varepsilon^3$ and

$$\begin{aligned} X \cdot Y &= (x_0y_0) + (x_0y_1 + x_1y_0)\varepsilon + (x_0y_2 + x_1y_1 + x_2y_0)\varepsilon^2 \\ &\quad + ((x_0 + x_1 + x_2 + x_3)y_3 + (x_1 + x_2 + x_3)y_2 + (x_2 + x_3)y_1 + x_3y_0)\varepsilon^3, \end{aligned}$$

where $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3$ and $Y = y_0 + y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3$ with $x_i, y_i \in \mathbb{F}_{3^d}$ and $0 \leq i \leq 3$.

Example 2.6. Let $X = 1 + \varepsilon + \varepsilon^2 + 2\varepsilon^3$ and $Y = 2 + \varepsilon^2 + \varepsilon^3$ are two elements in $\mathbb{F}_3[\varepsilon]$, we have:

$$X + Y = \varepsilon + 2\varepsilon^2, \text{ and } X \cdot Y = 2 + 2\varepsilon + \varepsilon^3.$$

Lemma 2.8. *$(\mathbb{F}_{3^d}[\varepsilon], +, \cdot)$ is a finite unitary commutative ring isomorphic to the quotient ring $\mathbb{F}_{3^d}[X]/(X^4 - X^3)$.*

Lemma 2.9. *The ring $\mathbb{F}_{3^d}[\varepsilon]$ is a vector space over $\mathbb{F}_{3^d}$ of dimension 4. And have $\{1, \varepsilon, \varepsilon^2, \varepsilon^3\}$ as basis, then: $\mathbb{F}_{3^d}[\varepsilon] = \mathbb{F}_{3^d} + \mathbb{F}_{3^d}\varepsilon + \mathbb{F}_{3^d}\varepsilon^2 + \mathbb{F}_{3^d}\varepsilon^3$.*

Proof. Let X and Y in $\mathbb{F}_{3^d}[\varepsilon]$ and k in the ring $\mathbb{F}_{3^d}$, we have:

- $X + Y = (x_0 + y_0) + (x_1 + y_1)\varepsilon + (x_2 + y_2)\varepsilon^2 + (x_3 + y_3)\varepsilon^3$.
- $k \cdot X = k\sum_{i=0}^{3} x_i\varepsilon^i = \sum_{i=0}^{3} kx_i\varepsilon^i = kx_0 + kx_1\varepsilon + kx_2\varepsilon^2 + kx_3\varepsilon^3$.

□

Proposition 2.10. *The product law in $\mathbb{F}_{3^d}[\varepsilon]$ can be written as:*

$$\begin{aligned} X \cdot Y &= x_0y_0 + \Theta_{XY}\varepsilon + \Omega_{XY}\varepsilon^2 \\ &\quad + ((x_0 + x_1 + x_2 + x_3)(y_0 + y_1 + y_2 + y_3) - x_0y_0 - \Theta_{XY} - \Omega_{XY})\varepsilon^3, \end{aligned}$$

where:

$$\Theta_{XY} = (x_0 + x_1)(y_0 + y_1) - x_0y_0 - x_1y_1 = x_0y_1 + x_1y_0 \text{ and}$$

$$\begin{aligned} \Omega_{XY} &= (x_0 + x_1 + x_2)(y_0 + y_1 + y_2) - x_0(y_0 + y_1) - x_1(y_0 + y_2) - x_2(y_1 + y_2) \\ &= x_0y_2 + x_1y_1 + x_2y_0. \end{aligned}$$

Proof. We have:
$(x_0+x_1+x_2+x_3)(y_0+y_1+y_2+y_3)-x_0y_0-\Theta_{XY}-\Omega_{XY}$
$=(x_0+x_1+x_2+x_3)y_3+(x_1+x_2+x_3)y_2+(x_2+x_3)y_1+x_3y_0.$ □

Corollary 2.12. *Let $X=x_0+x_1\varepsilon+x_2\varepsilon^2+x_3\varepsilon^3\in\mathbb{F}_{3^d}[\varepsilon]$, we have:*
$X^2=x_0^2+\Theta_{X^2}\varepsilon+\Omega_{X^2}\varepsilon^2+((x_0+x_1+x_2+x_3)^2-x_0^2-x_1^2+x_0x_1+x_0x_2)\varepsilon^3,$
$X^3=x_0^3+(x_1^3+x_2^3+x_3^3)\varepsilon^3,$
where: $\Theta_{X^2}=(x_0+x_1)^2-x_0^2-x_1^2$ *and* $\Omega_{X^2}=(x_0+x_1+x_2)^2-x_0^2-x_2^2+x_0x_1+x_1x_2.$

The next proposition characterize the set $(\mathbb{F}_{3^d}[\varepsilon])^\times$of invertible elements in $\mathbb{F}_{3^d}[\varepsilon]$.

Proposition 2.11. *Let $X=x_0+x_1\varepsilon+x_2\varepsilon^2+x_3\varepsilon^3\in\mathbb{F}_{3^d}[\varepsilon]$. The element X is invertible if and only if x_0 and $x_0+x_1+x_2+x_3$ are invertible in $\mathbb{F}_{3^d}$. The inverse of X is given by:*
$X^{-1}=x_0^{-1}-x_1x_0^{-2}\varepsilon+(x_1^2x_0^{-3}-x_2x_0^{-2})\varepsilon^2$
$\quad+((x_0+x_1+x_2+x_3)^{-1}+x_1x_0^{-2}+x_2x_0^{-2}-x_1^2x_0^{-3}-x_0^{-1})\varepsilon^3.$

Proof. Let $X=x_0+x_1\varepsilon+x_2\varepsilon^2+x_3\varepsilon^3$ and $Y=y_0+y_1\varepsilon+y_2\varepsilon^2+y_3\varepsilon^3$ be two elements of $\mathbb{F}_{3^d}[\varepsilon]$, we have:
$$\begin{aligned}X\cdot Y &= x_0y_0+\Theta_{XY}\varepsilon+\Omega_{XY}\varepsilon^2\\ &+ ((x_0+x_1+x_2+x_3)(y_0+y_1+y_2+y_3)-x_0y_0-\Theta_{XY}-\Omega_{XY})\varepsilon^3,\end{aligned}$$
where $\Theta_{XY}=x_0y_1+x_1y_0$ and $\Omega_{XY}=x_0y_2+x_1y_1+x_2y_0$. Then:
$$X\cdot Y=1 \iff \begin{cases} x_0y_0=1;\\ \Theta_{XY}=0;\\ \Omega_{XY}=0;\\ (\sum_{i=0}^{3}x_i)(\sum_{i=0}^{3}y_i)-x_0y_0-\Theta_{XY}-\Omega_{XY}=0.\end{cases}$$
$$\iff \begin{cases} x_0y_0=1;\\ x_0y_1+x_1y_0=0;\\ x_0y_2+x_1y_1+x_2y_0=0;\\ (\sum_{i=0}^{3}x_i)(\sum_{i=0}^{3}y_i)=1.\end{cases}$$
$$\iff \begin{cases} y_0=x_0^{-1}, \text{ and } x_0\not\equiv 0[3];\\ y_1=-x_1x_0^{-2};\\ y_2=-x_2x_0^{-2}+x_1^2x_0^{-3};\\ y_3=(\sum_{i=0}^{3}x_i)^{-1}+x_1x_0^{-2}+x_2x_0^{-2}-x_1^2x_0^{-3}-x_0^{-1}, \text{ and } \sum_{i=0}^{3}x_i\not\equiv 0[3].\end{cases}$$
So, $X\in(\mathbb{F}_{3^d}[\varepsilon])^\times$ if and only if $x_0\not\equiv 0[3]$ and $x_0+x_1+x_2+x_3\not\equiv 0[3]$.
In this case, we have:
$X^{-1}=x_0^{-1}-x_1x_0^{-2}\varepsilon+(x_1^2x_0^{-3}-x_2x_0^{-2})\varepsilon^2$
$\quad+((x_0+x_1+x_2+x_3)^{-1}+x_1x_0^{-2}+x_2x_0^{-2}-x_1^2x_0^{-3}-x_0^{-1})\varepsilon^3.$ □

Corollary 2.13. *Let $X\in\mathbb{F}_{3^d}[\varepsilon]$, then is not invertible if and only if $x_0\equiv 0[3]$ or $x_0+x_1+x_2+x_3\equiv 0[3]$, where $(x_0,x_1,x_2,x_3)\in\mathbb{F}_{3^d}^4$.*

Example 2.7. Let $X = 1 + 2\varepsilon + \varepsilon^3 \in \mathbb{F}_3[\varepsilon]$, we have $x_0 = 1 \not\equiv 0[3]$ and $x_0 + x_1 + x_2 + x_3 = 1 \not\equiv 0[3]$ then X is invertible in $\mathbb{F}_3[\varepsilon]$. The inverse of X is $X^{-1} = 1 + \varepsilon + \varepsilon^2 + \varepsilon^3$.

Lemma 2.10. *$\mathbb{F}_{3^d}[\varepsilon]$ is a non local ring.*

Proof. Let $X \in \mathbb{F}_{3^d}[\varepsilon]$, then the element X is not invertible if and only if $X = x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3$ or $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 - (x_0 + x_1 + x_2)\varepsilon^3$, such that $(x_0, x_1, x_2, x_3) \in \mathbb{F}_{3^d}^4$.
Now, we consider I_0, I_1 be two ideals of $\mathbb{F}_{3^d}[\varepsilon]$ defined by:

$$I_0 = \{x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 \mid (x_1, x_2, x_3) \in \mathbb{F}_{3^d}^3\} \text{ and}$$
$$I_1 = \{x_0 + x_1\varepsilon + x_2\varepsilon^2 - (x_0 + x_1 + x_2)\varepsilon^3 \mid (x_0, x_1, x_2) \in \mathbb{F}_{3^d}^3\},$$

it's clear that $I_0 \cup I_1$ is the set of non invertible elements in $\mathbb{F}_{3^d}[\varepsilon]$, and for all x_0, x_1, x_2, a, b and c in $\mathbb{F}_{3^d}$, we have:
$x_0 + x_1\varepsilon + x_2\varepsilon^2 - (x_0 + x_1 + x_2)\varepsilon^3 = a\varepsilon + b\varepsilon^2 + c\varepsilon^3$
$\Longrightarrow x_0 + (x_1 - a)\varepsilon + (x_2 - b)\varepsilon^2 - (x_0 + x_1 + x_2 + c)\varepsilon^3 = 0,$

$$\Longrightarrow \begin{cases} x_0 = 0; \\ x_1 - a = 0; \\ x_2 - b = 0; \\ x_0 + x_1 + x_2 + c = 0. \end{cases} \qquad \Longrightarrow \begin{cases} x_0 = 0; \\ x_1 = a; \\ x_2 = b; \\ x_1 + x_2 = -c. \end{cases}$$

We have $I_0 \cap I_1 = \{a\varepsilon + b\varepsilon^2 - c\varepsilon^3 \mid (a, b, c) \in \mathbb{F}_{3^d}^3\}$ then I_0 and I_1 are two distinct ideals of $\mathbb{F}_{3^d}[\varepsilon]$, so $I_0 \cup I_1$ is not ideal. Finally, the ring $\mathbb{F}_{3^d}[\varepsilon]$ is not local. □

Definition 2.7. Let Π_0 be a canonical projection and Π_1 be a sum projection of coordinate of element in $\mathbb{F}_{3^d}[\varepsilon]$ defined as given below:

$$\Pi_0 : \left| \begin{array}{ccc} \mathbb{F}_{3^d}[\varepsilon] & \longrightarrow & \mathbb{F}_{3^d} \\ X = \sum_{i=0}^{3} x_i\varepsilon^i & \longmapsto & x_0 \end{array} \right. \text{ and } \Pi_1 : \left| \begin{array}{ccc} \mathbb{F}_{3^d}[\varepsilon] & \longrightarrow & \mathbb{F}_{3^d} \\ X = \sum_{i=0}^{3} x_i\varepsilon^i & \longmapsto & \sum_{i=0}^{3} x_i \end{array} \right.$$

Lemma 2.11. *The mappings Π_0 and Π_1 are two surjective morphisms of rings.*

Proof. Let $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3$ and $Y = y_0 + y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3$ be two elements of $\mathbb{F}_{3^d}[\varepsilon]$. From the definition of the sum and product law in $\mathbb{F}_{3^d}[\varepsilon]$, we have:

$$\Pi_0(X + Y) = x_0 + y_0 = \Pi_0(X) + \Pi_0(Y), \text{ and}$$
$$\Pi_0(X \cdot Y) = x_0 \cdot y_0 = \Pi_0(X) \cdot \Pi_0(Y).$$

So, Π_0 is morphism of rings.

$$\Pi_1(X + Y) = x_0 + y_0 + x_1 + y_1 + x_2 + y_2 + x_3 + y_3$$
$$= \Pi_1(X) + \Pi_1(Y), \text{ and}$$

$$\begin{aligned}\Pi_1(X\cdot Y) &= (x_0+x_1+x_2+x_3)\cdot(y_0+y_1+y_2+y_3)\\ &= \Pi_1(X)\cdot\Pi_1(Y).\end{aligned}$$

So, Π_1 is morphism of rings.
Finally, for all $x \in \mathbb{F}_{3^d} \subset \mathbb{F}_{3^d}[\varepsilon]$, we have $\Pi_0(x) = \Pi_1(x) = x$, so Π_0 and Π_1 are two surjective morphisms. □

Lemma 2.12. *Let $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 \in \mathbb{F}_{3^d}[\varepsilon]$. If X is invertible in $\mathbb{F}_{3^d}[\varepsilon]$, then:*

$$\Pi_0(X^{-1}) = (\Pi_0(X))^{-1} \text{ and } \Pi_1(X^{-1}) = (\Pi_1(X))^{-1}.$$

Proof. Let $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 \in \mathbb{F}_{3^d}[\varepsilon]$. By using the Proposition 2.11, we have:

$$\begin{aligned}\Pi_0(X^{-1}) &= x_0^{-1}\\ &= (\Pi_0(X))^{-1},\end{aligned} \quad \text{and} \quad \begin{aligned}\Pi_1(X^{-1}) &= (x_0+x_1+x_2+x_3)^{-1}\\ &= (\Pi_1(X))^{-1}.\end{aligned}$$

□

2.4.2 Elliptic curve over $\mathbb{F}_{3^d}[\varepsilon], \varepsilon^4 = \varepsilon^3$

In this subsection, we consider X, Y, Z, a and b are elements of the ring $\mathbb{F}_{3^d}[\varepsilon]$ fixed by $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3$, $Y = y_0 + y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3$, $Z = z_0 + z_1\varepsilon + z_2\varepsilon^2 + z_3\varepsilon^3$, $a = a_0 + a_1\varepsilon + a_2\varepsilon^2 + a_3\varepsilon^3$ and $b = b_0 + b_1\varepsilon + b_2\varepsilon^2 + b_3\varepsilon^3$, with d is a positive integer.
The discriminant of elliptic curve over the ring $\mathbb{F}_{3^d}[\varepsilon]$ is $\triangle := -a^3b$, and we denoted by $\triangle_0'$ and $\triangle_1'$ the images of the discriminant $\triangle$ by Π_0 and Π_1 the morphisms respectively,

$$\begin{aligned}\triangle_0' &= \Pi_0(\triangle) = \Pi_0(-a^3b) = \Pi_0(-a^3)\Pi_0(b) = -a_0^3b_0, \text{ and}\\ \triangle_1' &= \Pi_1(\triangle) = \Pi_1(-a^3b) = \Pi_1(-a^3)\Pi_1(b) = -(a_0+a_1+a_2+a_3)^3(b_0+b_1+b_2+b_3)\\ &= -(a_0^3+a_1^3+a_2^3+a_3^3)(b_0+b_1+b_2+b_3).\end{aligned}$$

The j-invariant of elliptic curve over the ring $\mathbb{F}_{3^d}[\varepsilon]$ is $j := \dfrac{-a^3}{b}$, and we denoted by j_0' and j_1' the images of the j-invariant j by Π_0 and Π_1 the morphisms respectively.
By using the Lemma 2.12, we have:

$$\begin{aligned}j_0' &= \Pi_0(j) = \Pi_0\left(\frac{-a^3}{b}\right) = \Pi_0(-a^3b^{-1}) = \Pi_0(-a^3)\Pi_0(b^{-1}) = (-\Pi_0(a))^3(\Pi_0(b))^{-1}\\ &= -a_0^3b_0^{-1} = \frac{-a_0^3}{b_0}, \text{ and}\\ j_1' &= \Pi_1(j) = \Pi_1\left(\frac{-a^3}{b}\right) = \Pi_1(-a^3b^{-1}) = \Pi_1(-a^3)\Pi_1(b^{-1}) = (-\Pi_1(a))^3(\Pi_1(b))^{-1}\\ &= -(a_0+a_1+a_2+a_3)^3(b_0+b_1+b_2+b_3)^{-1} = \frac{-(a_0^3+a_1^3+a_2^3+a_3^3)}{(b_0+b_1+b_2+b_3)}.\end{aligned}$$

Definition 2.8. We define an elliptic curve over the ring $\mathbb{F}_{3^d}[\varepsilon]$, as a curve in the projective space $\mathbb{P}^2(\mathbb{F}_{3^d}[\varepsilon])$, which is given by the homogeneous equation of the degree 3, $Y^2Z = X^3 + aX^2Z + bZ^3$, where a and b in $\mathbb{F}_{3^d}[\varepsilon]$ such that the discriminant $\triangle$ is invertible in the ring $\mathbb{F}_{3^d}[\varepsilon]$. In this case, we denote the elliptic curve over $\mathbb{F}_{3^d}[\varepsilon]$ by $E_{a,b}(\mathbb{F}_{3^d}[\varepsilon])$, and we write:

$$E_{a,b}(\mathbb{F}_{3^d}[\varepsilon]) = \{[X : Y : Z] \in \mathbb{P}^2(\mathbb{F}_{3^d}[\varepsilon]) \mid Y^2Z = X^3 + aX^2Z + bZ^3\}.$$

Proposition 2.12. *The discriminant $\triangle$ is invertible in $\mathbb{F}_{3^d}[\varepsilon]$ if and only if $\triangle'_0 \not\equiv 0[3]$ and $\triangle'_1 \not\equiv 0[3]$.*

Proof. We show easily that $\triangle = \triangle'_0 + A\varepsilon + B\varepsilon^2 + (\triangle'_1 - \triangle'_0 - A - B)\varepsilon^3$ where $A = -a_0^3 b_1$ and $B = -a_0^3 b_2$, then from the Proposition 2.11 we deduce the result. □

Corollary 2.14. *If the discriminant $\triangle$ is invertible in $\mathbb{F}_{3^d}[\varepsilon]$, then we can talk about the elliptic curves $E_{\Pi_0(a),\Pi_0(b)}(\mathbb{F}_{3^d})$ and $E_{\Pi_1(a),\Pi_1(b)}(\mathbb{F}_{3^d})$ defined over the finite field $\mathbb{F}_{3^d}$ by:*

$$E_{\Pi_0(a),\Pi_0(b)}(\mathbb{F}_{3^d}) = \{[x : y : z] \in \mathbb{P}^2(\mathbb{F}_{3^d}) |\ y^2z = x^3 + a_0x^2z + b_0z^3\},\ \textit{and}$$
$$E_{\Pi_1(a),\Pi_1(b)}(\mathbb{F}_{3^d}) = \{[x : y : z] \in \mathbb{P}^2(\mathbb{F}_{3^d}) |\ y^2z = x^3 + (\sum_{i=0}^{3} a_i)x^2z + (\sum_{i=0}^{3} b_i)z^3\}.$$

Proposition 2.13. *Let X, Y and Z be three elements in the ring $\mathbb{F}_{3^d}[\varepsilon]$, then $[X : Y : Z]$ is a point of $\mathbb{P}^2(\mathbb{F}_{3^d}[\varepsilon])$ if and only if $[\Pi_i(X) : \Pi_i(Y) : \Pi_i(Z)]$ is a point of $\mathbb{P}^2(\mathbb{F}_{3^d})$, where $i \in \{0, 1\}$.*

Proof. Suppose that $[X : Y : Z] \in \mathbb{P}^2(\mathbb{F}_{3^d}[\varepsilon])$, then there exist the triple $(\alpha_1, \alpha_2, \alpha_3) \in (\mathbb{F}_{3^d}[\varepsilon])^3$ such that $\alpha_1X + \alpha_2Y + \alpha_3Z = 1$. Hence, we have:

$$\Pi_0(\alpha_1)\Pi_0(X) + \Pi_0(\alpha_2)\Pi_0(Y) + \Pi_0(\alpha_3)\Pi_0(Z) = 1, \text{ and}$$
$$\Pi_1(\alpha_1)\Pi_1(X) + \Pi_1(\alpha_2)\Pi_1(Y) + \Pi_1(\alpha_3)\Pi_1(Z) = 1.$$

So, $(\Pi_0(X), \Pi_0(Y), \Pi_0(Z)) \neq (0, 0, 0)$ and $(\Pi_1(X), \Pi_1(Y), \Pi_1(Z)) \neq (0, 0, 0)$, which proves that $[\Pi_i(X) : \Pi_i(Y) : \Pi_i(Z)] \in \mathbb{P}^2(\mathbb{F}_{3^d})$ for $i \in \{0, 1\}$.
Reciprocally, let $[\Pi_i(X) : \Pi_i(Y) : \Pi_i(Z)] \in \mathbb{P}^2(\mathbb{F}_{3^d})$ where $i \in \{0, 1\}$. Suppose that $x_0 \not\equiv 0[3]$, then we distinguish between two cases of $\Pi_1(X) = x_0 + x_1 + x_2 + x_3$:

1. $\Pi_1(X) \not\equiv 0[3]$: then X is invertible in $\mathbb{F}_{3^d}[\varepsilon]$, so the projective point $[X : Y : Z] \in \mathbb{P}^2(\mathbb{F}_{3^d}[\varepsilon])$.

2. $\Pi_1(X) \equiv 0[3]$: then $\Pi_1(Y) \not\equiv 0[3]$ or $\Pi_1(Z) \not\equiv 0[3]$.

   (i) If $\Pi_1(Y) \not\equiv 0[3]$ then:
   $x_0 + x_1\varepsilon + x_2\varepsilon^2 + (y_0 + y_1 + y_2 + y_3 - x_0 - x_1 - x_2)\varepsilon^3$
   $= x_0 + x_1\varepsilon + x_2\varepsilon^2 - (x_0 + x_1 + x_2)\varepsilon^3 + (y_0 + y_1 + y_2 + y_3)\varepsilon^3$
   $= X + \varepsilon^3 Y \in (\mathbb{F}_{3^d}[\varepsilon])^\times$,
   so there exist $\Phi \in \mathbb{F}_{3^d}[\varepsilon]$: $\Phi X + \varepsilon^3 \Phi Y = 1$, hence $[X : Y : Z] \in \mathbb{P}^2(\mathbb{F}_{3^d}[\varepsilon])$.

(ii) If $\Pi_1(Z) \not\equiv 0[3]$ then:
$x_0 + x_1\varepsilon + x_2\varepsilon^2 + (z_0 + z_1 + z_2 + z_3 - x_0 - x_1 - x_2)\varepsilon^3$
$= x_0 + x_1\varepsilon + x_2\varepsilon^2 - (x_0 + x_1 + x_2)\varepsilon^3 + (z_0 + z_1 + z_2 + z_3)\varepsilon^3$
$= X + \varepsilon^3 Z \in (\mathbb{F}_{3^d}[\varepsilon])^\times$,
so there exist $\Phi' \in \mathbb{F}_{3^d}[\varepsilon]$: $\Phi' X + \varepsilon^3 \Phi' Z = 1$, hence $[X : Y : Z] \in \mathbb{P}^2(\mathbb{F}_{3^d}[\varepsilon])$.

In the case where $\Pi_0(Y) \not\equiv 0[3]$ or $\Pi_0(Z) \not\equiv 0[3]$, we follow the same proof. □

Example 2.8. Let $X = 1 + \varepsilon + \varepsilon^2 + 2\varepsilon^3$, $Y = 1 + 2\varepsilon + \varepsilon^3$ and $Z = 2 + \varepsilon + \varepsilon^2$ in $\mathbb{F}_3[\varepsilon]$, then $[X : Y : Z]$ is a point of $\mathbb{P}^2(\mathbb{F}_3[\varepsilon]) \iff [\Pi_0(X) : \Pi_0(Y) : \Pi_0(Z)] = [1 : 1 : 2]$ and $[\Pi_1(X) : \Pi_1(Y) : \Pi_1(Z)] = [2 : 1 : 1]$ are two points of $\mathbb{P}^2(\mathbb{F}_3)$.

Proposition 2.14. *Let X, Y and Z in $\mathbb{F}_{3^d}[\varepsilon]$, if the point $[X : Y : Z]$ is a solution of the Weierstrass equation in $E_{a,b}(\mathbb{F}_{3^d}[\varepsilon])$ then $[\Pi_i(X) : \Pi_i(Y) : \Pi_i(Z)]$ is a solution of the same equation in $E_{\Pi_i(a),\Pi_i(b)}(\mathbb{F}_{3^d})$, where $i \in \{0, 1\}$.*

Proof. From the Proposition 4.2 and the Corollary 2.12, we have:

$$Y^2 = y_0^2 + \Theta_{Y^2}\varepsilon + \Omega_{Y^2}\varepsilon^2 + ((\sum_{i=0}^{3} y_i)^2 - y_0^2 - \Theta_{Y^2} - \Omega_{Y^2})\varepsilon^3,$$

$$Z^2 = z_0^2 + \Theta_{Z^2}\varepsilon + \Omega_{Z^2}\varepsilon^2 + ((\sum_{i=0}^{3} z_i)^2 - z_0^2 - \Theta_{Z^2} - \Omega_{Z^2})\varepsilon^3,$$

$$aX^2 = a_0x_0^2 + \Theta_{aX^2}\varepsilon + \Omega_{aX^2}\varepsilon^2 + ((\sum_{i=0}^{3} a_i)(\sum_{i=0}^{3} x_i)^2 - a_0x_0^2 - \Theta_{aX^2} - \Omega_{aX^2})\varepsilon^3,$$

$$Z^3 = z_0^3 + (\sum_{i=1}^{3} z_i^3)\varepsilon^3.$$

Then:

$$Y^2Z = y_0^2z_0 + \Theta_{Y^2Z}\varepsilon + \Omega_{Y^2Z}\varepsilon^2 + ((\sum_{i=0}^{3} y_i)^2(\sum_{i=0}^{3} z_i) - y_0^2z_0 - \Theta_{Y^2Z} - \Omega_{Y^2Z})\varepsilon^3,$$

$$X^3 = x_0^3 + (\sum_{i=1}^{3} x_i^3)\varepsilon^3,$$

$$aX^2Z = a_0x_0^2z_0 + \Theta_{aX^2Z}\varepsilon + \Omega_{aX^2Z}\varepsilon^2 + ((\sum_{i=0}^{3} a_i)(\sum_{i=0}^{3} x_i)^2(\sum_{i=0}^{3} z_i) - a_0x_0^2z_0 - \Theta_{aX^2Z} - \Omega_{aX^2Z})\varepsilon^3,$$

$$bZ^3 = b_0z_0^3 + b_1Z_0^3\varepsilon + b_2Z_0^3\varepsilon^2 + ((\sum_{i=0}^{3} b_i)(\sum_{i=0}^{3} z_i^3) - b_0z_0^3 - b_1Z_0^3 - b_2Z_0^3)\varepsilon^3.$$

Hence,

$$Y^2Z = X^3 + aX^2Z + bZ^3 \iff \begin{cases} y_0^2z_0 = x_0^3 + a_0x_0^2z_0 + b_0z_0^3; \\ \Theta_{Y^2Z} = \Theta_{aX^2Z} + b_1Z_0^3; \\ \Omega_{Y^2Z} = \Omega_{aX^2Z} + b_2Z_0^3; \\ (\sum_{i=0}^{3} y_i)^2(\sum_{i=0}^{3} z_i) = (\sum_{i=1}^{3} x_i^3) + (\sum_{i=0}^{3} a_i)(\sum_{i=0}^{3} x_i)^2(\sum_{i=0}^{3} z_i) \\ \qquad\qquad + (\sum_{i=0}^{3} b_i)(\sum_{i=0}^{3} z_i^3). \end{cases}$$

Which proves that for $i \in \{0,1\}$, $[\Pi_i(X) : \Pi_i(y) : \Pi_i(Z)]$ is a solution of the Weierstrass equation in $E_{\Pi_i(a),\Pi_i(b)}(\mathbb{F}_{3^d}[\varepsilon])$. □

Example 2.9. Let $E_{a,b} : Y^2Z = X^3+aX^2Z+bZ^3$, where $a = 2+\varepsilon+\varepsilon^2$ and $b = 1+2\varepsilon^2+\varepsilon^3$ in $\mathbb{F}_3[\varepsilon]$, the discriminant $\triangle = -a^3b = 1 + 2\varepsilon^2 + 2\varepsilon^3$ is invertible in $\mathbb{F}_3[\varepsilon]$, because $\Pi_0(\triangle) = 1 \not\equiv 0[3]$ and $\Pi_1(\triangle) = 2 \not\equiv 0[3]$ then $E_{a,b}(\mathbb{F}_3[\varepsilon])$ is an elliptic curve.
Let $X = 1 + \varepsilon$, $Y = 1 + \varepsilon$ and $Z = 1$ in $\mathbb{F}_3[\varepsilon]$, the point $[X : Y : Z]$ is a solution of the Weierstrass equation $E_{a,b}$, then $[\Pi_0(X) : \Pi_0(Y) : \Pi_0(Z)] = [x, y, z] = [1 : 1 : 1]$ is a solution of equation:

$$E_{\Pi_0(a),\Pi_0(b)} : y^2z = x^3 + \Pi_0(a)x^2z + \Pi_0(b)z^3 = x^3 + 2x^2z + z^3,$$

and $[\Pi_1(X) : \Pi_1(Y) : \Pi_1(Z)] = [x, y, z] = [2 : 2 : 1]$ is a solution of equation:

$$E_{\Pi_1(a),\Pi_1(b)} : y^2z = x^3 + \Pi_1(a)x^2z + \Pi_1(b)z^3 = x^3 + x^2z + z^3.$$

From the propositions 2.12, 2.13 and 2.14, we deduce the theorem:

Theorem 2.4. *Let X, Y and Z in $\mathbb{F}_{3^d}[\varepsilon]$. If $[X : Y : Z] \in E_{a,b}(\mathbb{F}_{3^d}[\varepsilon])$ then $[\Pi_i(X) : \Pi_i(Y) : \Pi_i(Z)] \in E_{\Pi_i(a),\Pi_i(b)}(\mathbb{F}_{3^d})$, where $i \in \{0,1\}$.*

Corollary 2.15. *The mappings $\overline{\Pi}_0$ and $\overline{\Pi}_1$ are well defined, where $\overline{\Pi}_i$ for $i \in \{0,1\}$ is given by:*

$$\overline{\Pi}_i : \left| \begin{array}{ccc} E_{a,b}(\mathbb{F}_{3^d}[\varepsilon]) & \longrightarrow & E_{\Pi_i(a),\Pi_i(b)}(\mathbb{F}_{3^d}) \\ [X : Y : Z] & \longmapsto & [\Pi_i(X) : \Pi_i(Y) : \Pi_i(Z)] \end{array} \right.$$

Proof. Let $[X : Y : Z] \in E_{a,b}(\mathbb{F}_{3^d}[\varepsilon])$. From the previous theorem 2.4, we have $[\Pi_i(X) : \Pi_i(Y) : \Pi_i(Z)] \in E_{\Pi_i(a),\Pi_i(b)}(\mathbb{F}_{3^d})$ where $i \in \{0,1\}$.
If $[X : Y : Z] = [X' : Y' : Z']$ then there exist $\Psi \in (\mathbb{F}_{3^d}[\varepsilon])^\times$ such that: $X' = \Psi X$, $Y' = \Psi Y$ and $Z' = \Psi Z$, then:

$$\begin{aligned} \overline{\Pi}_i([X' : Y' : Z']) &= [\Pi_i(X') : \Pi_i(Y') : \Pi_i(Z')] \\ &= [\Pi_i(\Psi X) : \Pi_i(\Psi Y) : \Pi_i(\Psi Z)] \\ &= \underbrace{[\Pi_i(\Psi)\Pi_i(X) : \Pi_i(\Psi)\Pi_i(Y) : \Pi_i(\Psi)\Pi_i(Z)]}_{\Pi_i(\Psi)\in\mathbb{F}_{3^d}^*} \\ &= [\Pi_i(X) : \Pi_i(Y) : \Pi_i(Z)] \\ &= \overline{\Pi}_i([X : Y : Z]). \end{aligned}$$

So, the mapping $\overline{\Pi}_i$ is well defined with $i \in \{0,1\}$. □

Corollary 2.16. *The mapping $\overline{\Pi}_0$ is a surjective.*

Proof. Let $[x : y : z] \in E_{\Pi_0(a),\Pi_0(b)}(\mathbb{F}_{3^d})$, then:

- If $y \not\equiv 0[3]$ then $[x : y : z] \sim [x : 1 : z]$ hence $[x(1 + 2\varepsilon + 2\varepsilon^2 + \varepsilon^3) : 1 : z(1 + 2\varepsilon + 2\varepsilon^2 + \varepsilon^3)]$ is an antecedent of $[x : 1 : z]$.
- If $y \equiv 0[3]$ then $z \not\equiv 0[3]$ and $[x : y : z] \sim [x : 0 : 1]$ hence $[x(1 + 2\varepsilon + 2\varepsilon^2 + \varepsilon^3) : \varepsilon + \varepsilon^2 + \varepsilon^3 : 1 + 2\varepsilon + 2\varepsilon^2 + \varepsilon^3]$ is an antecedent of $[x : 0 : 1]$.

□

Corollary 2.17. *The mapping $\overline{\Pi}_1$ is a surjective.*

Proof. Let $[x : y : z] \in E_{\Pi_1(a),\Pi_1(b)}(\mathbb{F}_{3^d})$ then:

- If $y \not\equiv 0[3]$ then $[x : y : z] \sim [x : 1 : z]$ hence $[x(\varepsilon + 2\varepsilon^2 + \varepsilon^3) : 1 : z(\varepsilon + 2\varepsilon^2 + \varepsilon^3)]$ is an antecedent of $[x : 1 : z]$.
- If $y \equiv 0[3]$ then $z \not\equiv 0[3]$ and $[x : y : z] \sim [x : 0 : 1]$ hence $[x(\varepsilon + 2\varepsilon^2 + \varepsilon^3) : 1 + \varepsilon + 2\varepsilon^2 - \varepsilon^3 : \varepsilon + 2\varepsilon^2 + \varepsilon^3]$ is an antecedent of $[x : 0 : 1]$.

□

2.4.3 Classification of elements in $E_{a,b}(\mathbb{F}_{3^d}[\varepsilon])$

In this subsection, we will classify the elements of the elliptic curve $E_{a,b}(\mathbb{F}_{3^d}[\varepsilon])$ into three types, depending on whether the third projective coordinate Z is invertible or not. The result is in the following proposition.

Proposition 2.15. *Every element of the elliptic curve $E_{a,b}(\mathbb{F}_{3^d}[\varepsilon])$ has one of the forms:*

1. $[X : Y : 1]$, *where* $X, Y \in \mathbb{F}_{3^d}[\varepsilon]$.
2. $[x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 : 1 : z_1\varepsilon + z_2\varepsilon^2 + z_3\varepsilon^3]$, *such that* $[x_1 + x_2 + x_3 : 1 : z_1 + z_2 + z_3]$ *in* $E_{\Pi_1(a),\Pi_1(b)}(\mathbb{F}_{3^d})$.
3. $[x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 : 1 + y_1\varepsilon + y_2\varepsilon^2 - (1 + y_1 + y_2)\varepsilon^3 : z_1\varepsilon + z_2\varepsilon^2 + z_3\varepsilon^3]$, *such that* $[x_1 + x_2 + x_3 : 0 : z_1 + z_2 + z_3]$ *in* $E_{\Pi_1(a),\Pi_1(b)}(\mathbb{F}_{3^d})$.
4. $[x_0 + x_1\varepsilon + x_2\varepsilon^2 - \sum_{i=0}^{2} x_i\varepsilon^3 : 1 : z_0 + z_1\varepsilon + z_2\varepsilon^2 - \sum_{i=0}^{2} z_i\varepsilon^3]$, *such that* $[x_0 : 1 : z_0]$ *in* $E_{\Pi_0(a),\Pi_0(b)}(\mathbb{F}_{3^d})$.
5. $[x_0 + x_1\varepsilon + x_2\varepsilon^2 - \sum_{i=0}^{2} x_i\varepsilon^3 : y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3 : z_0 + z_1\varepsilon + z_2\varepsilon^2 - \sum_{i=0}^{2} z_i\varepsilon^3]$, *such that* $y_1 + y_2 + y_3 \not\equiv 0[3]$ *and* $[x_0 : 0 : 1]$ *in* $E_{\Pi_0(a),\Pi_0(b)}(\mathbb{F}_{3^d})$.

Proof. Let $\mathcal{T} = [X : Y : Z]$ be a point in $E_{a,b}(\mathbb{F}_{3^d}[\varepsilon])$, we have three cases of third projective coordinate Z:

1. If Z is invertibe, then: $[X:Y:Z] \sim [X:Y:1]$.

2. If $Z = z_1\varepsilon + z_2\varepsilon^2 + z_3\varepsilon^3$ where $(z_1, z_2, z_3) \in \mathbb{F}_{3^d}^3$, then:
   $\overline{\Pi}_0([X:Y:Z]) = [\Pi_0(X):\Pi_0(Y):\Pi_0(Z)] = [x_0:y_0:0]$, so $x_0 \equiv 0[3]$ and $y_0 \not\equiv 0[3]$, hence
   $[X:Y:Z] = [x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 : 1 + y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3 : z_1\varepsilon + z_2\varepsilon^2 + z_3\varepsilon^3]$, and there are two sub-cases of $y_1 + y_2 + y_3 \in \mathbb{F}_{3^d}$:

   (i) $y_1 + y_2 + y_3 \not\equiv 0[3]$, then $1 + y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3$ is invertible in $\mathbb{F}_{3^d}[\varepsilon]$, so we have:
   $[X:Y:Z] \sim [x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 : 1 : z_1\varepsilon + z_2\varepsilon^2 + z_3\varepsilon^3]$, where
   $[x_1 + x_2 + x_3 : 1 : z_1 + z_2 + z_3] \in E_{\Pi_1(a),\Pi_1(b)}(\mathbb{F}_{3^d})$.

   (ii) $y_1 + y_2 + y_3 \equiv 0[3]$, then $1 + y_1\varepsilon + y_2\varepsilon^2 - (1 + y_1 + y_2)\varepsilon^3$ is not invertible in $\mathbb{F}_{3^d}[\varepsilon]$, so we have:
   $[X:Y:Z] = [x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 : 1 + y_1\varepsilon + y_2\varepsilon^2 - (1 + y_1 + y_2)\varepsilon^3 : z_1\varepsilon + z_2\varepsilon^2 + z_3\varepsilon^3]$, where $[x_1 + x_2 + x_3 : 0 : z_1 + z_2 + z_3] \in E_{\Pi_1(a),\Pi_1(b)}(\mathbb{F}_{3^d})$, then necessary $z_1 + z_2 + z_3 \not\equiv 0[3]$.

3. If $Z = z_0 + z_1\varepsilon + z_2\varepsilon^2 - (z_0 + z_1 + z_2)\varepsilon^3$ where $(z_0, z_1, z_2) \in \mathbb{F}_{3^d}^3$, then:
   $\overline{\Pi}_1([X:Y:Z]) = [\Pi_1(X):\Pi_1(Y):\Pi_1(Z)] = [x_0 + x_1 + x_2 + x_3 : y_0 + y_1 + y_2 + y_3 : 0]$, so $x_0 + x_1 + x_2 + x_3 \equiv 0[3]$ and $y_0 + y_1 + y_2 + y_3 \not\equiv 0[3]$, hence
   $[X:Y:Z] = [x_0 + x_1\varepsilon + x_2\varepsilon^2 - \sum_{i=0}^{2} x_i\varepsilon^3 : y_0 + y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3 : z_0 + z_1\varepsilon + z_2\varepsilon^2 - \sum_{i=0}^{2} z_i\varepsilon^3]$, so we have two sub-cases of $y_0 \in \mathbb{F}_{3^d}$:

   (i) $y_0 \not\equiv 0[3]$, then $y_0 + y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3$ is invertible in $\mathbb{F}_{3^d}[\varepsilon]$, then:
   $[X:Y:Z] \sim [x_0 + x_1\varepsilon + x_2\varepsilon^2 - \sum_{i=0}^{2} x_i\varepsilon^3 : 1 : z_0 + z_1\varepsilon + z_2\varepsilon^2 - \sum_{i=0}^{2} z_i\varepsilon^3]$, where
   $[x_0 : 1 : z_0] \in E_{\Pi_0(a),\Pi_0(b)}(\mathbb{F}_{3^d})$.

   (ii) $y_0 \equiv 0[3]$, then $y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3$ is not invertible in $\mathbb{F}_{3^d}[\varepsilon]$, so we have:
   $[X:Y:Z] = [x_0 + x_1\varepsilon + x_2\varepsilon^2 - \sum_{i=0}^{2} x_i\varepsilon^3 : y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3 : z_0 + z_1\varepsilon + z_2\varepsilon^2 - \sum_{i=0}^{2} z_i\varepsilon^3]$, where $[x_0 : 0 : z_0] \in E_{\Pi_0(a),\Pi_0(b)}(\mathbb{F}_{3^d})$, then necessary $z_0 \not\equiv 0[3]$ and
   $[X:Y:Z] = [x_0 + x_1\varepsilon + x_2\varepsilon^2 - \sum_{i=0}^{2} x_i\varepsilon^3 : y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3 : 1 + \alpha\varepsilon + \beta\varepsilon^2 - (1 + \alpha + \beta)\varepsilon^3]$, where $y_1 + y_2 + y_3 \not\equiv 0[3]$ and $[x_0 : 0 : 1] \in E_{\Pi_0(a),\Pi_0(b)}(\mathbb{F}_{3^d})$.

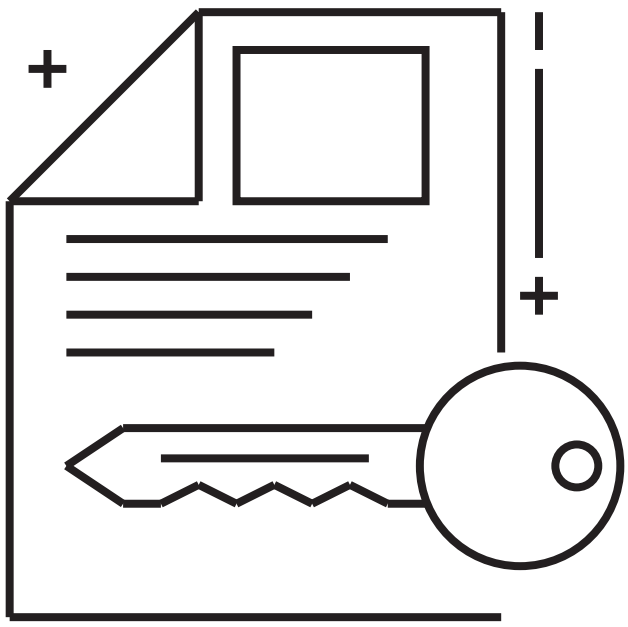
Which proves the proposition. □

Part II

Elliptic Curves in Cryptography

Kerckhoff's Principle

A cryptosystem should be secure even if details of encryption and decryption algorithms about the system is publically known. Only the secret key need to be secret [39].



Chapter 3

Generalities on a public key cryptosystems

"Elliptic curve cryptography (ECC) appeared in the mid-1980s and is a member of the asymmetric family of algorithms. ECC is based on a generalized discrete logarithm problem and has a high level of security with a shorter keys length compared to the RSA and Diffie-Hellman algorithms. This chapter begins with a description of complexity of an algorithms. Next, we describe in generally the cryptology (cryptography and cryptanalysis). Moreover, the use of public-key algorithms is examined (DLP, D-H and the DSA). Finally, we focus on the elliptic curve cryptography and the most important functions of cryptosystems based on elliptic curves." For more information about ECC, see the following books and articles: [3]; [9]; [10]; [22]; [75] and [87].

Contents in Brief

3.1 Complexity of an algorithms **57**
3.2 Introduction to a cryptology **61**
3.2.1 Cryptography 62
3.2.2 Cryptanalysis 69
3.3 Discrete logarithm problem **70**
3.4 Diffie-Hellman key exchange **72**
3.5 The digital signature algorithm **74**
3.5.1 What is digital signature? 74
3.5.2 Digital signature algorithm steps 76
3.6 Elliptic curves cryptography **78**
3.6.1 Elliptic curve discrete logarithm problem 79
3.6.2 Elliptic curve Diffie-Hellman key exchange 80
3.6.3 Elliptic curve digital signature algorithm 82
3.6.4 ECC encryption/decryption 85

3.1 Complexity of an algorithms

What is an algorithm?

An algorithm is a finite and unambiguous sequences of instructions and operations for solving a problem or performing a computation.

Characteristics of an algorithm:
An algorithm generally have the following characteristics:

1. **Input:** an algorithm has receives input values from a specified set.
2. **Output:** an algorithm produces output values from each set of input values from a specified set. Moreover, the output values are the solutions of the given problems.
3. **Definiteness:** the steps of an algorithm must be defined precisely, each instruction must be clear and unambiguous.
4. **Finiteness:** an algorithm should produce the desired output after a finite number of steps for any input in the set.
5. **Effectiveness:** it must be possible to perform each step of an algorithm exactly and in finite time limit.

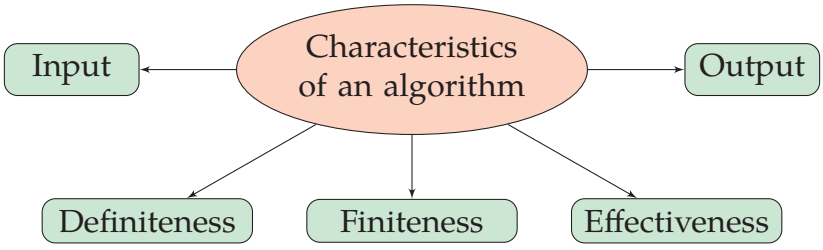


Figure 3.1: Characteristics of an algorithm.

Complexity of an algorithms

Complexity of an algorithm is a function which gives the running time and storage requirement of the algorithm in terms of size or the input data (see [63]). There are two main complexity measures of the efficiency of an algorithm:

- **Space complexity:** is defined as the process of determining a formula for prediction of how much memory space will be required for the successful execution of the algorithm.
- **Time complexity:** is defined as the process of determining a formula for total time required towards execution of that algorithm.

Cases of time complexity

There are three important cases about the time complexity of an algorithm, but it is very difficult to determine the exact time complexity of an algorithm (see [44]).

1. **Best case time:** is the minimum number of steps that can be executed for the given parameters.
2. **Worst case time:** is the maximum number of steps that can be executed for the given parameters.
3. **Average case time:** is the average of steps that can be.

Asymptotic notations

They are used to make meaningful statements about the efficiency of algorithms. These notations help us to make approx, but meaningful assumptions about the time and space complexity. Commonly used asymptotic notations to compute the running time complexity of an algorithm are Big-Oh notation (O), Big-Omega notation (Ω) and Big-Theta notation (Θ) (see [28, 42, 63]).

Definition 3.1 (Big-Oh notation (O)). Let f and g be two functions from $\mathbb{N} \to \mathbb{R}^+$. The function $f(n) = O(g(n))$ if there exist two positive constants c and n_0 such that:

$$f(n) \leq cg(n) \text{ for all } n \geq n_0.$$

It is used to find an asymptotic *"upper bounds"*.

Example 3.1. Let $f : \mathbb{N} \to \mathbb{R}^+$ defined by:

a) Let $f(n) = 7n + 3$, we have $7n + 3 \leq 8n$ for all $n \geq 4$. Therefore $7n + 3 = O(n)$ for all $n \geq 4$. Here $c = 8$ and $n_0 = 4$.

b) Let $f(n) = 20n^2 + 2n + 1$, we have $20n^2 + 2n + 1 \leq 21n^2$ for all $n \geq 3$. Therefore $20n^2 + 2n + 1 = O(n^2)$ for all $n \geq 3$. Here $c = 21$ and $n_0 = 3$.

c) Let $f(n) = 7n + 5 \neq O(1)$ as $7n + 5$ is not less or equal to c any constant c and all $n \geq n_0$.

Definition 3.2 (Big-Omega notation (Ω)). Let f and g be two functions from $\mathbb{N} \to \mathbb{R}^+$. The function $f(n) = \Omega(g(n))$ if and only if there exist two positive constants c and n_0 such that:

$$f(n) \geq cg(n) \text{ for all } n \geq n_0.$$

It is used to find an asymptotic *" lower bounds"*.

Example 3.2. Let $f : \mathbb{N} \to \mathbb{R}^+$ defined by:

a) Let $f(n) = 7n + 3$, we have $7n + 3 \geq 7n$ for all $n \geq 1$. Therefore $7n + 3 = \Omega(n)$ for all $n \geq 1$.

b) Let $f(n) = 20n^2 + 2n + 1$, we have $20n^2 + 2n + 1 \geq 20n^2$ for all $n \geq 1$. Therefore $20n^2 + 2n + 1 = \Omega(n^2)$ for all $n \geq 1$.

c) $7 \times 2^n + n^2 \geq 2^n$ for all $n \geq 1$. Therefore $7 \times 2^n + n^2 = \Theta(2^n)$.

Definition 3.3 (Big-Theta notation (Θ)). Let f and g be two functions from $\mathbb{N} \to \mathbb{R}^+$. The function $f(n) = \Theta(g(n))$ if and only if there exist three positive constants c_1 and c_2 and n_0 such that:

$$c_1 g(n) \leq f(n) \leq c_2 g(n) \text{ for all } n \geq n_0.$$

It is used to find an asymptotic *"tight bounds"*.

Example 3.3. Let $f : \mathbb{N} \to \mathbb{R}^+$ defined by:

a) We have $7n \leq f(n) = 7n+3 \leq 8n$ for all $n \geq 3$. Then the function $f(n) = 7n+3 = \Theta(n)$ for all $n \geq 3$.

b) We have $20n^2 \leq f(n) = 20n^2 + 2n + 1 \leq 21n^2$ for all $n \geq 3$. Then the function $f(n) = 20n^2 + 2n + 1 = \Theta(n^2)$ for all $n \geq 3$.

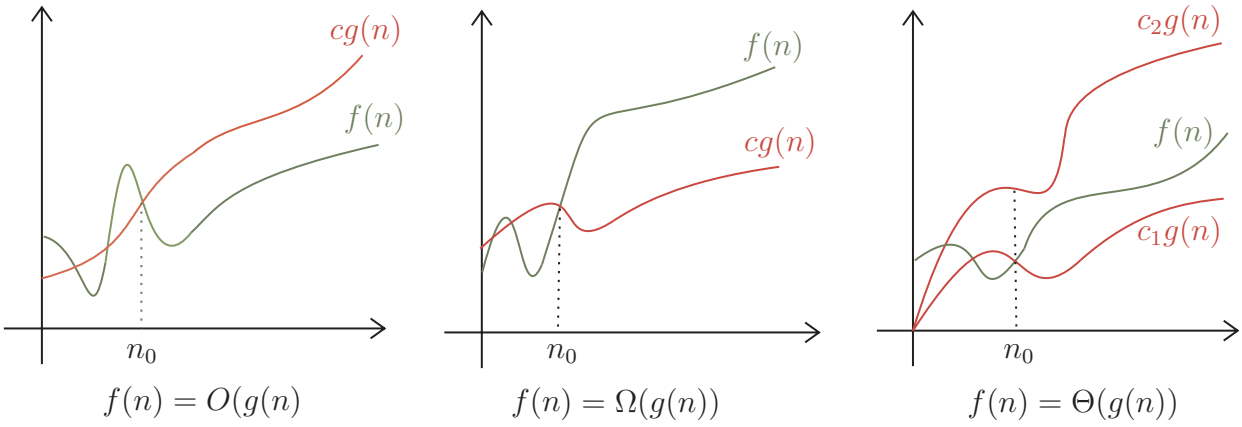


Figure 3.2: Asymptotic notations: Big-O, Big-Omega, Big-Theta.

Properties of asymptotic notations

After defining these three notations (Big-Oh; Big-Omega; Big-Theta), let us discuss here some important properties of those notations.

- If $f(n) = O(g(n))$ then $\alpha f(n) = O(g(n))$, where α is constant. This property is satisfies for both Ω and Θ notations.
- If $f(n) = O(g(n))$ and $f(n) = \Omega(g(n))$ then $f(n) = \Theta(g(n))$.
- If $f(n) = O(g(n))$ and $h(n) = \Omega(s(n))$ then $f(n) + h(n) = O(\max(g(n), s(n)))$.
- If $f(n) = O(g(n))$ and $h(n) = \Omega(s(n))$ then $f(n)h(n) = O(g(n)s(n))$.

- (Reflexive) If $f(n)$ is given then $f(n) = O(f(n))$. This property is satisfies for both Ω and Θ notations.
- (Transitive) If $f(n) = O(g(n))$ and $g(n) = O(h(n))$ then $f(n) = O(h(n))$. This property is satisfies for both Ω and Θ notations.
- (Symmetric) If $f(n) = \Theta(g(n))$ then $g(n) = \Theta(f(n))$. This property only satisfies for Θ notation.
- (Transpose symmetric) If $f(n) = O(g(n))$ then $g(n) = \Omega(f(n))$. This property only satisfies for O and Ω notations.

How to find time complexity of an algorithms?

The performance of the algorithms is classified from best to worst as follows (see [34]):

- Constant-$O(1)$: runtime does not depend on input size, e.g. addition, assignment.
- Logarithmic-$O(\log(n))$: runtime grows slower than input size, e.g. Binary Search.
- Linear-$O(n)$: runtime grows at the same rate as input, e.g. unsorted list search.
- Linear-logarithmic-$O(n \log n)$: an operation of $\log(n)$ complexity for each input value, e.g. Merge Sort, Heap Sort.
- Polynomial-$O(n^k)$ with $k > 1$: runtime grows quicker than previous all based on n, e.g. Bubble Sort, Strassen's Matrix Multiplication, Insertion Sort, Selection Sort, Bucket Sort.
- Exponential-$O(a^n)$ with $a > 1$: runtime grows even faster than polynomial algorithm based on n, e.g. Tower of Hanoi.
- Factorial-$O(n!)$: runtime grows the fastest and becomes quickly unusable for even small values of n, e.g. Brute force Search algorithm for Traveling Salesman Problem, Determinant Expansion by Minors.

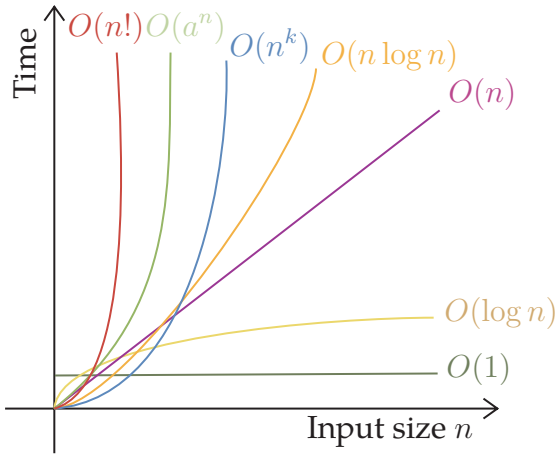


Figure 3.3: Time complexity analysis of algorithms.

3.2 Introduction to a cryptology

Cryptology is from the Greek word Kryptos (hidden) and logos (science). Literally means science of secrecy. This science, born several millennia ago and its purpose is to hide information in a message. It is a branch of security, mainly includes two fields of study, cryptography and cryptanalysis. The figure below is the diagram of classification of the crypto-terminologies.

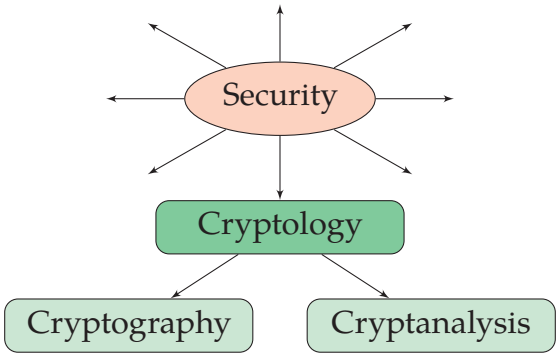


Figure 3.4: The classification of the crypto-terminologies.

Elements of communication process

Communication is a process in which messages in the form of thoughts, feelings and opinions are transmitted between two or more parties with the intention of creating a common understanding and it is a two-way process.
The communication process consists of the following elements:

- **Sender:** the sender or communicator is the main source and component of the communication process, who initiates the conversation by creating a message containing ideas, opinions, images etc., with the aim of transmitting it to others (individual or group) to share ideas and trends with them.

- **Message:** it is an essential axis in the communication process, as it consists of information, ideas, tone of voice, gestures and an impression shown by the sender and transmitted between the sender and the receiver during the communication process, and it is the point that brings together the sender and receiver, so it is important to choose phrases and symbols carefully, and there are different images of the message, including: words, gestures, tone of voice, outward appearance, and movements.

- **Encoding:** it is the process of converting the message into communication symbols such as words, pictures, gestures etc.

- **Communication channel:** it is the channel through which the message is transmitted between the sender and the receiver, and the success of the communication process is closely related to the success of the sender by choosing the appropriate means of communication.
- **Decoding:** it is the process of converting encoded symbols of the sender.
- **Receiver:** he is the one who receives the message, decodes it, translates it, then analyzes and interprets it to arrive at what the sender intends, and from here the receiver may be a real or legal personality, and in the event that he receives the message, he will exchange roles with the sender.
- **Feedback:** it is the reaction or response of the receiver. The process of communication gets completed when receiver gives feedback to the sender.

The following figure shows the process of communication between two parties:

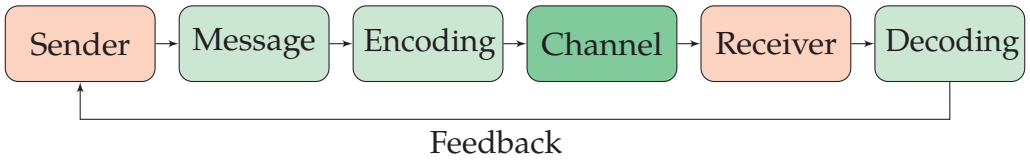


Figure 3.5: Communication between two parties.

3.2.1 Cryptography

Cryptography is technique to protect data, information and communications from theft or change by converting plain text into incomprehensible text using symbols so that no one can understand and process it except for authorized persons.
The techniques used to protect information depend on algorithms, which enable us to transmit messages in ways that make it difficult to decipher them.
These algorithms are used for key generation of cryptography and digital signature, verification to protect data privacy, and confidential transactions (debit card and credit card) and web browsing etc., this is what we will present in the following sections.

Cryptographic terminology

- **Plaintext:** original data before being transformation.
- **Ciphertext:** the scrambled data after transformation.
- **Cipher:** the algorithm used for transforming plaintext to ciphertext.
- **Key:** a secret value used during the encryption and decryption process.

- ❖ **Encryption:** process of transforming plaintext into an unreadable format.
- ❖ **Decryption:** process of transforming the ciphertext back to its original form.

Definition 3.4 (See [35]). A cryptosystem is a five-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, where:

- $\mathcal{P}$ is the set of plaintext strings.
- $\mathcal{C}$ is the set of ciphertext strings.
- $\mathcal{K}$ is space of the keys (the set of all possible keys).
- $\mathcal{E}$ is the set of encryption functions.
- $\mathcal{D}$ is the set of decryption functions.

We denote by E_k the encryption function in $\mathcal{E}$ corresponding to the key $k \in \mathcal{K}$ and D_k the decryption function in $\mathcal{D}$ that decrypts ciphertext that was encrypted using E_k, that is $D_k(E_k(m)) = m$, for all plaintext strings $m \in \mathcal{P}$.

Features of cryptography

The framework for using cryptographic processes is not limited to encryption and therefore to the sole guarantee of confidentiality of messages. We can in fact distinguish between four primitive functionalities that we wish to ensure by the use of a cryptographic: *confidentiality, integrity, non-repudiation and authenticity*, each of these features represents a defense, a security against a certain type of attack (see [44]).

- ❖ **Confidentiality:** confidentiality helps ensure that an encrypted message is understandable only by the legitimate parties to a cryptographic communication. An attacker who intercepts an encoded message must be unable to decrypt it.
- ❖ **Integrity:** in communications (encrypted or not) we obviously hope that the recipient receives the message as it was sent, that is to say without modification of any kind. Also, if the received message is different from the sent message, then the recipient should be aware of this. We summarize this by saying that we want to guarantee integrity of messages against modifications.
- ❖ **Non-repudiation:** non-repudiation is the means that prevents the recipient of a message from denying having received it or the sender from denying having sent it. This protection is fundamental, for example, in the context of a commercial transaction on the Internet.
- ❖ **Authenticity:** the task of authentication is to ensure that the received message actually comes from the entity that claims to have sent it. If an adversary sends a message to the recipient pretending to be the sender, the authenticity of the message must be questioned by the authentication service. Otherwise, the recipient, believing that he is talking to the sender, can send confidential information later fall into the hands of the enemy.

Classification of cryptography algorithms

In general, there are three types of cryptography:

1. Symmetric key cryptography.
2. Hash functions.
3. Asymmetric key cryptography.

The types of cryptography are shown in the figure 3.6.

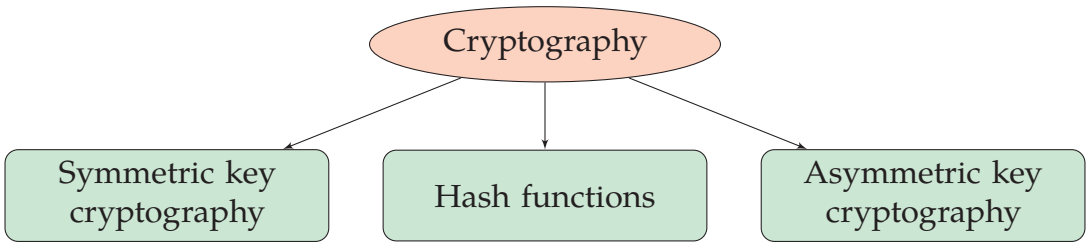


Figure 3.6: Classification of cryptography algorithms.

3.2.1.1 Symmetric key cryptography

In symmetric encryption, the same key k is used for both encryption and decryption. In this method, the original message is converted into an unrecognizable message. This converted message (by the sender Alice) is called the ciphertext, this is done using a key and encryption algorithm (see [35]).
At the receiving end (the receiver is Bob), the ciphertext is converted to the original message using the same key and decryption algorithm. As shown in the figure 3.7.

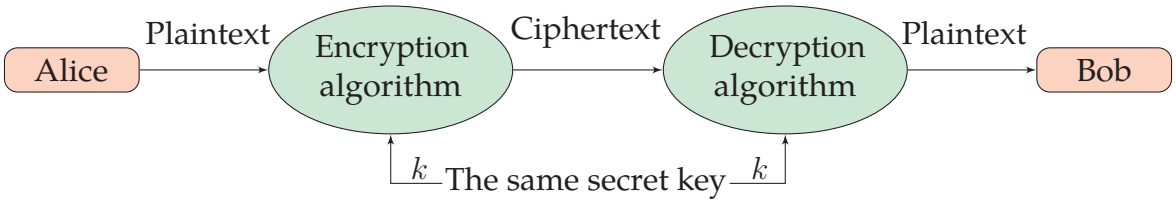


Figure 3.7: Symmetric key cryptography.

Since both parties use the same key, symmetric encryption is much faster. On the other hand, the key must be available to decrypt the message. Therefore, a secure channel is required to transmit the key.
In general, symmetric encryption is a straightforward method and does not require much time to complete.

There are two types of symmetric encryption algorithms:
Block ciphers: encrypt a fixed number of bits as a single chunk.
Stream ciphers: encrypt one bit or one byte at a time when encryption/ decryption.

Advantages/Disadvantages of symmetric-key encryption

Advantages:
Given that only one key is used in the encryption process, it can generally be said that speed is an advantage of symmetric encryption.
Disadvantages:
Symmetric cryptosystems have a problem of key transportation. The secret key is to be transmitted to the receiving system before the actual message is to be transmitted. All means of electronic communication is insecure as it is impossible to guarantee that no one will be able to tap communication channels. So the only secure way of exchanging keys would be exchanging them personally.

Popular symmetric encryption algorithms

Some examples of symmetric encryption algorithms include:

- **AES** (Advanced Encryption Standard), has a key length of 128-bits, 192-bits, and 256-bits.
- **DES** (Data Encryption Standard), has a key length of 56-bits.
- **3DES** (Triple Data Encryption Standard), has a key length of 168-bits (three 56-bit DES keys).
- **IDEA** (International Data Encryption Algorithm), has a key length of 128-bits.
- **Blowfish** (Drop-in replacement for DES or IDEA), has a variable key length from 32-bits up to 448-bits
- **RC6** (Rivest Cipher 6), has a variable key length from 128, 192, and 256-bits up to 2040-bits.
- **RC5** (Rivest Cipher 5), has a variable block size (32, 64 or 128-bits), key length from 0 bit up to 2040-bits.
- **RC4** (Rivest Cipher 4), has a variable key length from 1 bit up to 256-bits.

AES, DES, 3DES, IDEA, Blowfish, RC6 and RC5 are block ciphers, RC4 is stream cipher.

Example 3.4. Let's encrypt the message "How are you ?" by using AES.
Key size in bits: 128-bits.
Secret key: azertyuiopqsdfgh
Output text format: hexadecimal.
AES encrypted output: "698F154A3C9F833C1E01C4A1BFDDED63".

Let's decrypt the message "177C1A81C2D94F9D6BFC1DBAFB3F99371C4D6BAE7E2CB790FE4A95249DCD6FC0" by using AES.
Input text format: hexadecimal.
Key size in bits: 128-bits.
Secret key: azertyuiopqsdfgh
AES decrypted output: I am fine thank you.

3.2.1.2 Hash functions

Definition 3.5 (See [35, 59]). Let f is a function defined from E to F, then f is one-way if easy to compute $f(x)$ for $x \in E$, but the computation its inverse $f^{-1}(x)$ is infeasible. On other hand, the function f is trapdoor one-way function if its easy to compute $f(x)$ for $x \in E$ and the computation of its inverse $f^{-1}(x)$ is infeasible unless certain some secret information is known.

A cryptographic hash function h is a mathematical algorithm that takes data of arbitrary length bit-strings as input and produces a fixed length bit-strings as output. This output is often called a message digest, a hash value or a hash code (see [23, 78]).

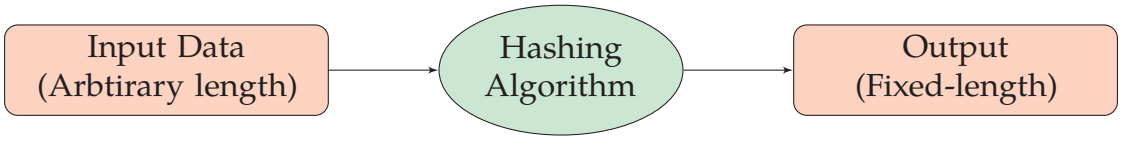


Figure 3.8: Cryptographic hash functions

More formally, a hash function is a map $h : E \longrightarrow F$ between two sets E and F, where E is the set of arbitrary finite length bit-strings by $\{0,1\}^*$ and F is the set of fixed length bit-strings by $\{0,1\}^n$, where $n \in \mathbb{N}^*$.

Example 3.5. The hash function h counts the number of zeros in the input. Then output 0 if the number of zeros is odd, and 1 if even.

$$h : \{0,1\}^* \longrightarrow \{0,1\}^1$$

Input	h(Input)=Output
0101	1
00101010	0
010010	1

A cryptographic hash function has four main advantages:

- ❖ A digest can be easily calculated for any given message.

- ❖ It is not possible to generate a message from a given digest.
- ❖ Any change in the message leads to a change in its digest.
- ❖ It is not possible to generate two messages with the same digest.

Cryptographic hash functions have many applications in the field of information security, especially in digital signatures, message authentication, one-way password file, intrusion detection, virus detection and pseudorandom number generation etc.

Properties of hash functions

A hash functions it must resist all known cryptanalysis attack types (which will be mentioned later). At a minimum, it should have the following properties (see [23]):

- ❖ **Preimage resistant:** for essentially all outputs $y \in F$ it is computationally infeasible to find any $x \in E$ such that $y = h(x)$. This property is related to a one-way or non-invertible function.
- ❖ **Second-preimage resistant:** for any given $x_1 \in E$ it is computationally infeasible to find a different $x_2 \in E$ such that $h(x_1) = h(x_2)$.
- ❖ **Collision resistant:** it is computationally infeasible to find any distinct inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

Popular hash functions

Some examples of popular hash functions:

- ❖ **MD5 (Message Digest):** is a widely used cryptographic hash function that results in a 128-bits hash value.
- ❖ **SHA-1 (Secure Hash Algorithm):** is a widely used cryptographic hash function that results in a 160-bits hash value.
- ❖ **SHA-2 (Secure Hash Algorithm):** is a widely used cryptographic hash function, it is actually a family of hashes (SHA-224, SHA-256, SHA-384 and SHA-512), and comes in a variety of lengths (224, 256, 384, 512-bits respectively), the most popular being 256-bits.

Example 3.6. We will hash the following message "I'm going to university"
The hash values of message are:

- **MD5:** "5A85A6BECC5918737A475E98A768E708".
- **SHA-1:** "FC767ED679F116ABC538718F766FC04D0A4820D5"
- **SHA-256:** "D9729EF0E53B31CFA617FC699A50B3D0E70FF180490DD75E604F879A 21513 19C".

- **SHA-384:** "A5E28045AA46867FB2C2397D99CA121D0CA664E3EA66F44ED4FE06 3B6D8 8094044476AE0058710E7BA1325B50CB0F404".
- **SHA-512:** "69B68615266D59DFE70E1C8DD3F6324734B0E3E7A4FA43F858920E2FB F835850D4581EF01255D8A3F8B86D394BC70D0E4BE141BCEBB8924BB7635E9FF9 60EF25".

3.2.1.3 Asymmetric key cryptography

Asymmetric key cryptography (or asymmetric key encryption) is a method of encrypting data with two different keys that are matches to each other, and making one of the keys available for anyone to use called the public key and the other key is known as the private key. Together, they are used to encrypt and decrypt data. If you encrypt a data using a person's public key, they can only decrypt it using their matching private key. Asymmetric key cryptography is also known as public key cryptography (see [40,83]).

If Alice (sender) uses public key cryptography (PKC), she encrypts the message using Bob's (receiver) public key and Bob will be able to decrypt it using his private key, asymmetric encryption therefore provides a higher level of security because even if someone intercepts their messages and finds Bob's public key, they will not be able to decrypt the message or understand its content. The process of asymmetric encryption between Alice and Bob is shown in the following figure 3.9.

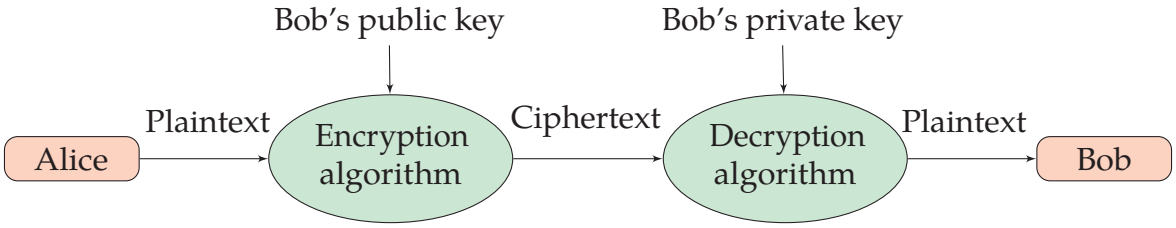


Figure 3.9: Asymmetric key cryptography.

Popular asymmetric encryption algorithms

The following encryption algorithms make use of asymmetric encryption:

- ❖ Rivest-Shamir-Adleman (RSA).
- ❖ Digital Signature Algorithm (DSA).
- ❖ El Gamal algorithm.
- ❖ Diffie-Hellman algorithm (D-H).
- ❖ Elliptic Curve Cryptography (ECC).

Asymmetric encryption has many applications are:
confidentiality of data, authenticity using digital signatures, integrity of information exchange and non-repudiation.

Advantages/Disadvantages of public-key encryption

Advantages: in public key, cryptography there is no need for exchanging keys, thus eliminating the key distribution problem.
Disadvantages: a disadvantage of using public-key cryptography for encryption is speed: there are popular symmetric key encryption methods which are significantly faster than any currently available public-key encryption method.

3.2.2 Cryptanalysis

Cryptanalysis is the study of analyzing information systems in order to study the hidden aspects of the systems. It is used to break cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown.

Principles of a cryptosystem design

The following principles should be followed when designing a cryptographic system. The principles are simple and should form the basis of any cryptanalysis procedure (see [53]):

- The adversary should not be underestimated.
- A cryptographic system can be evaluated by a cryptanalyst.
- Before evaluating the cryptographic system, the adversary's knowledge of the assessed cryptosystem is taken into account.
- The secrecy of the cryptographic system relies on the key.
- All elements within the system such as key distribution, cryptographic content, and so on must be taken into account in the cryptographic system evaluation process

Types of cryptanalysis attacks

There are four generic types of cryptanalysis, characterized by what the cryptanalyst knows (see [3, 40, 83])

❖ **Ciphertext-Only Attack (COA):** The attacker has knowledge of some ciphertexts but not the plaintexts nor the key. In this case, recovering the plaintext (without the key) may be a successful attack.

- **Known-Plaintext Attack (KPA):** The attacker has knowledge of some ciphertexts and corresponding plaintexts, encrypted under the unknown key.

- **Chosen-Plaintext Attack (CPA):** Model of cryptanalysis which assumes that the attacker can choose random plaintexts to be encrypted and obtain the corresponding ciphertexts. The goal of attacker is to gain further info which reduces the security of encryption scheme. In the worst case, this attack can expose the secret information after calculating the secret key.

- **Chosen-Cipertext Attack (CCA):** Attacker can analyze any ciphertext and gets their corresponding decryptions-plaintexts. This goal is to require a secret key or to get as many info about the attacked system as possible. The attacker has capability to make the victim decrypt any ciphertext and send him back the result. Thus by analyzing the chosen ciphertext and the corresponding received plaintext, the introder tries to guess the secret key.

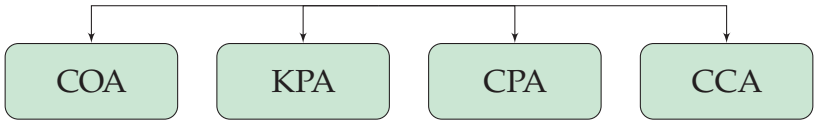


Figure 3.10: Types of attacks.

3.3 Discrete logarithm problem

The security of public-key cryptosystems is based on one-way functions, such as factoring (for RSA) and the discrete logarithm problem (denoted by DLP). The discrete logarithms are fundamental to a number of public-key algorithms, including Diffie-Hellman key exchange, Elgamal encryption and the digital signature algorithm (see [34,60,78]).

Definition 3.6 (Discrete Logarithm Problem (DLP) in $\mathbb{Z}_p^*$). Given is the finite cyclic group $\mathbb{Z}_p^*$ of order $p-1$ and a primitive element $g \in \mathbb{Z}_p^*$ and another element $t \in \mathbb{Z}_p^*$. The DLP is the problem of determining the integer $1 \leqslant \alpha \leqslant p-1$ such that:

$$g^{\alpha} \equiv t \bmod p.$$

We call α the discrete logarithm of t with respect to the base g, and denote it by:

$$\alpha \equiv \log_g(t) \bmod p.$$

Definition 3.7 (Generalized Discrete Logarithm Problem). Let G be a finite cyclic group with multiplicative operation "$\circ$" and cardinality n. We consider a primitive

element $g \in G$ and another element $t \in G$. The discrete logarithm problem is finding the integer α, where $1 \leqslant \alpha \leqslant n$, such that:

$$t = \underbrace{g \circ g \circ ... \circ g}_{\alpha-\text{times}} = g^{\alpha}.$$

In additive operation this means $t = \underbrace{g + g + ... + g}_{\alpha-\text{times}} = \alpha g$.

Example 3.7. Let $G = (\mathbb{Z}_7, +)$ is a finite cyclic group with the primitive element $g = 3$.

α	0	1	2	3	4	5	6
$\alpha g = \alpha 3$	0	3	6	2	5	1	4

Table 3.1: The elements of the group $G = \langle g \rangle$.

Let's solve the DLP for the element $t = 5$ i.e. $\alpha 3 = \underbrace{3 + 3 + ... + 3}_{\alpha-\text{times}} \equiv 5 \bmod 7$ in G. In order to solve for α, we simply have to invert the primitive element g:

$$\alpha \equiv 3^{-1}5 \bmod 7.$$

Using, the extended Euclidean algorithm, we can compute $3^{-1} \equiv 5 \bmod 7$ from which the discrete logarithm follows as:

$$\alpha \equiv 3^{-1}5 \equiv 4 \bmod 7.$$

The problem of calculating the discrete logarithm is generally a difficult problem (more or less depending on the group G). For suitable group G, like $(\mathbb{Z}/n\mathbb{Z})^{\times}$ this is considered to be a hard problem.

Remark 3.1. We see that for the additive group of $\mathbb{Z}/n\mathbb{Z}$ the DLP is easy to solve. A much better choice are the multiplicative groups $(\mathbb{Z}/n\mathbb{Z})^{\times}$, which are cyclic if and only if $n = 2, 4, p^r$ or $2p^r$, where $p > 2$ is a prime and $r \geqslant 1$.

Attacks against DLP

Generic Algorithms: work in any cyclic group [78, 89].

- *Shank's Baby-Step Giant-Step method:* the algorithm is based on a space-time-tradeoff for brute force, this algorithm has a running time $O\left(\sqrt{|G|}\right)$.
- *Pollard's ρ method:* similar to Pollard's ρ factorization, this algorithm is the best method to solve DLP and has a running time exponential similar to Baby-Step Giant-Step method $O\left(\sqrt{|G|}\right)$.

- *Pohlig-Hellman method:* uses prime factorization $|G| = \prod_i p_i^{e_i}$, this algorithm has a running time $O\left(\sum e_i(\log|G| + \sqrt{p_i})\right)$.

Non-generic Algorithms: work only in specific groups, in particular in $\mathbb{Z}_p$ [78,89].

- *The index calculus method:* similar to sieving based factorization methods, uses factor bases requires prime elements, this algorithm has a running subexponential time $O\left(\exp^{(\sqrt{2}+O(1)\sqrt{\log|G|\cdot\log\log|G|)}}\right)$.

3.4 Diffie-Hellman key exchange

Whitfield Diffie and Martin Hellman published their paper "New Directions in Cryptography" In 1976 (see [18]) proposed first public key type encryption. The Diffie-Hellman (D-H) algorithm widely known as key exchange algorithm or key agreement algorithm. The purpose of D-H key exchange algorithm is to enable two users to exchange a key securely that can be used for subsequent encryption of message. By this method each user of the network has a personalized private key and a public key. They exchange their public keys, each user then combines its private key with the other party's public key to compute the shared secret key.

Exchange of secret key

Suppose Alice and Bob are two parties who want to create a shared secret key by using Diffie-Hellman protocol (see [18,35]).

1. Alice and Bob publically agree on a prime modulus number p, and a generator number g, where both p and g are prime numbers and $p > g$.
2. Verify that p and g are co-primes, i.e. $\gcd(p, g) = 1$.
3. Alice chooses a private key X_A such that $X_A < p$, then calculates a public key $Y_A \equiv g^{X_A} \bmod p$.
4. Bob chooses a private key X_B such that $X_B < p$, then calculates a public key $Y_B \equiv g^{X_B} \bmod p$.
5. Alice sends Bob the public key Y_A, and Bob sends Alice the public key Y_B.
6. Alice computes $K_1 \equiv (Y_B)^{X_A} \bmod p$.
7. Bob computes $K_2 \equiv (Y_A)^{X_B} \bmod p$.
8. Verify that $K = K_1 = K_2$, where K_1 and K_2 are the calculated shared secret key.

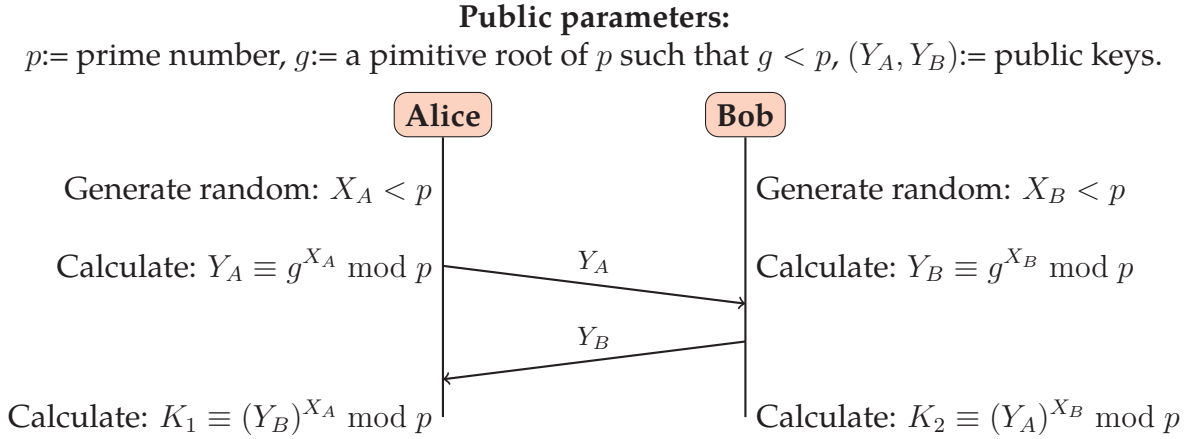


Figure 3.11: Diffie–Hellman secret-key agreement protocol

Proof. (**Correctness of the D-H algorithm**). To prove the D-H protocol requires showing that $K_1 = K_2$, we have:
Alice computes:

$$Y_A \equiv g^{X_A} \bmod p.$$

Bob Computes:

$$Y_B \equiv g^{X_B} \bmod p.$$

Then

$$\begin{aligned} K_1 &\equiv (Y_B)^{X_A} \bmod p \\ &\equiv (g^{X_B} \bmod p)^{X_A} \bmod p \\ &\equiv (g^{X_B})^{X_A} \bmod p \\ &\equiv g^{X_B X_A} \bmod p \\ &\equiv (g^{X_A})^{X_B} \bmod p \\ &\equiv (g^{X_A} \bmod p)^{X_B} \bmod p \\ &\equiv (Y_A)^{X_B} \bmod p = K_2. \end{aligned}$$

Therefore: $K = K_1 = K_2$. □

Example 3.8. Suppose Alice and Bob are two users, to exchange the secret key between them, you must follow these steps:

1. Alice and Bob agree on:
   a prime number $p = 1523$ and a primitive root of 1523, in this case $g = 499$.

2. Alice and Bob select secret keys $X_A = 14 < 1523$ and $X_B = 10 < 1523$, respectively.

3. Each user computes his public key:
   Alice computes $Y_A \equiv g^{X_A} \bmod 1523 \equiv 499^{14} \bmod 1523 = 641$.
   Bob computes $Y_B \equiv g^{X_B} \bmod 1523 \equiv 499^{10} \bmod 1523 = 1104$.

4. After the public keys are exchanged, both can compute the common secret key:
   Alice computes $K \equiv (Y_B)^{X_A} \bmod 1523 \equiv 1104^{14} \bmod 1523 = 504$.
   Bob computes $K \equiv (Y_A)^{X_B} \bmod 1523 \equiv 641^{10} \bmod 1523 = 504$.

Security of the D-H algorithm

The Diffie-Hellman protocol is safe against hackers because it based on a discrete logarithm problem. Computing discrete logarithms modulo a prime is a very hard problem if the parameters are sufficiently large. Since exponentiation modulo a prime is computationally easy, this forms a one-way function (see [59]).

3.5 The digital signature algorithm

Digital signatures algorithm (DSA) is a Federal Information Processing Standard (FIPS) for digital signatures. It was proposed in 1991 and globally standardized in 1994 by the National Institute of Standards and Technology (NIST). NIST chose to base their signature scheme on the discrete logarithm problem in a prime finite field $\mathbb{F}_p$, which are difficult to compute (see [89]).

3.5.1 What is digital signature?

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message or digital document. A digital signature is defined the signature generated electronically from the digital computer to ensure the identity of the sender and content of the message cannot be modified during transmission process.

Purpose of digital signature

- ❖ Concept of digital signature is that of a message uses a signing key (private key) to sign the message and send that message and its digital signature.
- ❖ The receiver uses a verification key (public key) of the sender only to verify the origin of the message and make sure that it has not been tempered with while in transmission.
- ❖ Digital signature techniques achieve the authenticity and integrity of the data internet.

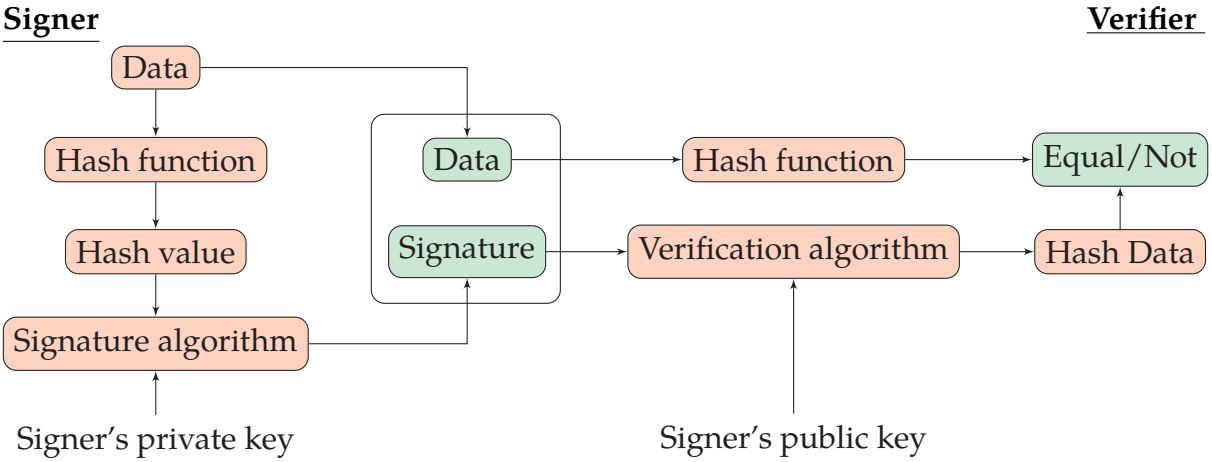


Figure 3.12: Digital Signature Algorithm.

Properties of digital signature

In situations where, there is no complete trust between sender and receiver, something more than authentication is needed. The most attractive solution to this problem is the digital signature (see [83]). The digital signature must have the following properties:

1. It must verify the author and the date and the time of the signature.
2. It must authenticate the contents at the time of the signature.
3. It must be verifiable by third parties, to resolve disputes.

Thus, the digital signature function includes the authentication function.

Advantages/Disadvantages of digital signatue

Advantages:

- *Authentication:* Identification of person that signs.
- *Integrity of data:* Every change will be detected.
- *Non repudiation:* Author cannot be denied of his work.
- *Imposter prevention:* No one else can forge your digital signature or submit an electronic document falsely claiming it was signed by you.
- *Security:* The use of digital signatures and electronic documents reduces risks of documents being intercepted, read, destroyed, or altered while in transit.

Disadvantages:

- *Expiry:* In this era of fast technology, many of these tech products have a short life.

- *Certificates:* In order to effectively use of digital signatures, both senders and receivers may have to buy digital certificates.
- *Software:* To work with digital certificates/digital signatures, senders and receivers have to buy verification software or pay to third party for verification.

3.5.2 Digital signature algorithm steps

Process of digital signature

Hash value of a message when encrypted with the private key of a user is, his digital signature on that e-document. Digital signature is an example of asymmetric key cryptography which uses three different algorithms to complete the process [59, 83]:

1. **First step** *(key generation algorithm)*: is key generation algorithm which generates private key and a corresponding public key.
2. **Second step** *(signature generation algorithm)*: is signing algorithm which selects sending both of the message and the signature using a private key generated in the first step and hash function.
3. **Third step** *(signature verification algorithm)*: is signature verifying algorithm which verifies the authenticity of sending message using a public key.

Key generation algorithm

The keys for Digital Signature Algorithm are computed as follows:

- Generate a prime number p, where $2^{L-1} < p < 2^L$ for $512 \leq L \leq 1024$ and L a multiple of 64 i.e., $L \in \{512, 576, 640, 704, 768, 832, 896, 960, 1024\}$.
- Find a prime divisor q of $(p-1)$, with $2^{159} < q < 2^{160}$.
- Choose an integer g $(1 < g < p)$, satisfying the two conditions $g^q \bmod p = 1$ and $g \equiv h^{(p-1)/q} \bmod p$, where h is any integer with $1 < h < p-1$ such that $h^{(p-1)/q} \bmod p > 1$

The algorithm parameters (p, q, g) may be shared between different users of the system. The second phase computes private and public keys for a single user:

1. Choose a random integer x, such that $0 < x < q$.
2. Compute $y \equiv g^x \bmod p$.
3. The keys are now: $\begin{cases} \text{the public key is } K_{pub} = (p, q, g, y). \\ \text{the private key is } K_{pr} = x. \end{cases}$

Signature generation algorithm

Let m be a message and $h(m)$ be a hash value of m. The signature generation process is as follows:

1. Choose a random per-message secret number k, where $0 < k < q$.
2. Compute $r \equiv (g^k \bmod p) \bmod q$.
3. Compute $s \equiv [k^{-1}(h(m) + xr)] \bmod q$.
4. If $r = 0$ or $s = 0$ then go to step 1.
5. Sends the message m and the signature (r, s) to receiver.

Signature verification algorithm

The signature verification process is as follows:

1. Verify that: $0 < r < q$ and $0 < s < q$.
2. Compute $w \equiv s^{-1} \bmod q$.
3. Compute $u_1 \equiv [h(m)w] \bmod q$.
4. Compute $u_2 \equiv rw \bmod q$.
5. Compute $v \equiv [(g^{u_1} y^{u_2}) \bmod p] \bmod q$.
6. The verification: $v \begin{cases} \equiv r \bmod q \implies \text{valid signature.} \\ \not\equiv r \bmod q \implies \text{invalid signature and rejects the signature.} \end{cases}$

Proof. (**Correctness of the DSA algorithm**). To prove the DSA algorithm requires showing that a signature (r, s) satisfies the verification condition $v \equiv r \bmod q$.
The signer computes:

$$s \equiv [k^{-1}(h(m) + xr)] \bmod q.$$

Thus

$$\begin{aligned} k &\equiv h(m)s^{-1} + xrs^{-1} \bmod q \\ &\equiv h(m)w + xrw \bmod q. \end{aligned}$$

Since g has order $q \bmod p$ we have:

$$\begin{aligned} g^k &\equiv g^{h(m)w} g^{xrw} \bmod q \\ &\equiv g^{h(m)w} y^{rw} \bmod q \\ &\equiv g^{u_1} y^{u_2} \bmod q. \end{aligned}$$

Finally, the correctness of DSA follows from

$$\begin{aligned} r &\equiv (g^k \bmod p) \bmod q \\ &\equiv (g^{u_1} y^{u_2} \bmod p) \bmod q \\ &\equiv v \bmod q. \end{aligned}$$

□

Example 3.9. Alice and Bob are two users, Alice wants to send a message m to Bob which is to be signed with the DSA. Suppose the hash value of m is $h(m) = 30$.
Then the signature and verification process is as follows:
Alice

- *Key generation:*
  Choose: $p = 61, q = 5, g = 9$.
  Choose private key: $x = 4$.
  Compute: $y \equiv g^x \bmod 61 = 34$.
  Public key: $(p, q, g, y) = (61, 5, 9, 34)$.
- *Sign:*
  Compute hash of message: $h(m) = 30$.
  Choose ephemeral key: $k = 3$.
  Compute: $r \equiv (9^4 \bmod 61) \bmod 5 = 3$.
  Compute: $s \equiv [2 \cdot (30 + 4 \cdot 3)] \bmod 5 = 4$.
  Sends to Bob: $(m, (r, s)) = (m, (3, 4))$.

Bob

- *Verify:*
  Compute: $w = 4^{-1} \equiv 4 \bmod 5$.
  Compute: $u_1 = 4 \cdot 30 \equiv 0 \bmod 5$.
  Compute: $u_2 = 3 \cdot 4 \equiv 2 \bmod 5$.
  Verification: $v \equiv [9^0 \cdot 34^2 \bmod 61] \bmod 5 = 3$.
  $v \equiv r \bmod 5 \Longrightarrow$ valid signature.

3.6 Elliptic curves cryptography

Elliptic curves cryptosystems (ECC) have several advantages over RSA and over DL schemes (Elgamal or DSA). In particular, in absence of strong attacks against ECC, bit

lengths in the range of 160–256 bits can be chosen which provide security equivalent to 1024–3072-bits RSA and DL schemes.

An elliptic curves can be defined over any field (e.g., $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$). However, elliptic curves used in cryptography are mainly defined over finite fields.

3.6.1 Elliptic curve discrete logarithm problem

The discrete logarithm problem on elliptic curve groups is believed to be more difficult than the corresponding problem in (the multiplicative group of nonzero elements of) the underlying finite field (see [34, 60, 78]).

Definition 3.8. Let E be an elliptic curve over a finite field $\mathbb{F}_p$. We consider P, Q be two points in $E(\mathbb{F}_p)$, where P a primitive element of a cyclic subgroup of $E(\mathbb{F}_p)$. The elliptic curve discrete logarithm problem (ECDLP) is finding the integer n, where $1 \leqslant n \leqslant \#E$, such that:

$$nP = \underbrace{P + P + \cdots + P}_{n-\text{times}} = Q.$$

By analogy with the discrete logarithm problem for $\mathbb{F}_p^*$, we denote this integer n by $n = \log_P(Q)$, and we call n the ECDLP of Q with respect to P.

Some remarks about ECDLP

- $\log_P(Q)$ may not be defined: there may be points P and Q, such that Q is not a scalar multiple of P.
- There is one value of n satisfying $Q = nP$.
  - There exists a positive integer s such that $sP = \infty$.
  - Since there are finite points on the elliptic curve, from the points in list $P, 2P, 3P, 4P, \ldots$ there must be i and j are two integers, such that $iP = jP, i > j$. Let $s = (i - j)$ and the smallest such $s \geqslant 1$ is called the order of P.
  - Thus, if n_0 is an integer such that $Q = n_0P$, then for any integer i, $n = n_0 + is$, satisfies the equation $Q = nP$.
  - This means that the value of $\log_P(Q)$ is really an element of $\mathbb{Z}/s\mathbb{Z}$.

Example 3.10. Let E be an elliptic curve over the finite field $\mathbb{F}_{29}$ defined by the equation:

$$E : y^2 \equiv x^3 + 7x + 5 (\mathrm{mod} 29).$$

Let the point $P = (5, 7) \in E(\mathbb{F}_{29})$ which generates a cyclic subgroup G in $E(\mathbb{F}_{29})$ of order $\#G = 11$.

The elements of G are:

$P = (5, 7)$ $2P = (3, 13)$ $3P = (1, 10)$ $4P = (0, 11)$ $5P = (20, 5)$ $6P = (20, 24)$
$7P = (0, 18)$ $8P = (1, 19)$ $9P = (3, 16)$ $10P = (5, 22)$ $11P = \infty$

We want to compute $6P = \underbrace{P + P + \cdots + P}_{6-\text{times}} = Q$, In this case, we can simply use the points that were calculated: $6P = (20, 24) = Q$.
Therefore, $\log_P(Q) = 6$.

How hard is ECDLP?

The ECDLP is based on the discrete logarithm problem (DLP) and does not pursue any polynomial time algorithm. In ECDLP, two elements P and Q are taken from a random instance $(P, Q) \in G \times G$, where G is a cyclic group of order n. It is impossible to find an integer t (with $0 < t < n$) such that $Q = tP$ by a polynomial time bounded algorithm where P is the generator for the cyclic group G (see [58]).

3.6.2 Elliptic curve Diffie-Hellman key exchange

In complete analogy to the conventional Diffie-Hellman key exchange (DHKE) presented in section 3.4. The elliptic curve Diffie-Hellman (ECDH) distincts from the general Diffie-Hellman (D-H) in the way that it is based on the elliptic curve discrete logarithm problem (ECDLP) instead of the discrete logarithm problem (DLP) (see [60, 89]).

The elliptic curve Diffie-Hellman key exhcange (ECDHKE) works as follows:

1. Alice and Bob agree on a prime number p, a point P generating a cyclic subgroup of known order of the elliptic curve E.
2. Alice chooses a private random integer $K_A < ord(P)$, and sends $Y_A = K_A P$ to Bob.
3. Bob chooses a private random integer $K_B < ord(P)$, and sends $Y_B = K_B P$ to Alice.
4. Alice computes $K_1 = K_A Y_B$.
5. Bob computes $K_2 = K_B Y_A$.
6. The secret key is $K = K_1 = K_2$.

The ECDHKE is shown in the following figure:

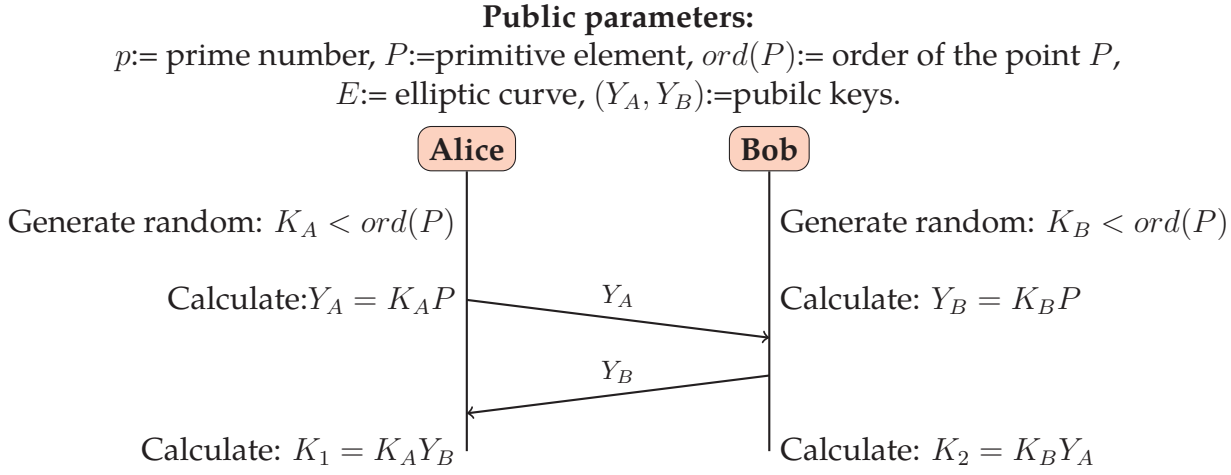


Figure 3.13: Elliptic curve Diffie-Hellman key exchange.

Proof. (**Correctness of the ECDH algorithm**). To prove the ECDH protocol requires showing that $K_1 = K_2$, we have:
Alice computes:

$$Y_A = K_A P.$$

Bob Computes:

$$Y_B = K_B P.$$

Then

$$\begin{aligned} K_1 &= K_A Y_B \\ &= K_A K_B P \\ &= K_B K_A P \quad \text{(point addition is associative)} \\ &= K_B Y_A = K_2. \end{aligned}$$

Therefore: $K = K_1 = K_2$. □

Example 3.11. We consider the public parameters of ECDH, the elliptic curve is $E : y^2 = x^3 + 15x + 6$ over the finite field $\mathbb{F}_{61}$, which forms a cyclic subgroup $G = \langle P \rangle$ generated by $P = (7, 37)$ of order $\#G = 19$.
The elements of G are:

$P = (7, 37)$	$2P = (46, 26)$	$3P = (54, 31)$	$4P = (45, 60)$	$5P = (10, 27)$
$6P = (28, 33)$	$7P = (1, 49)$	$8P = (57, 2)$	$9P = (53, 44)$	$10P = (53, 17)$
$11P = (57, 59)$	$12P = (1, 12)$	$13P = (28, 28)$	$14P = (10, 34)$	$15P = (45, 1)$
$16P = (54, 30)$	$17P = (46, 35)$	$18P = (7, 24)$	$19P = \infty$	

The elliptic curve Diffie-Hellman key exchange between Alice and Bob as follows:

- Alice and Bob select secret keys $K_A = 9 < ord(P) = 19$ and $K_B = 12 < ord(P) = 19$, respectively.

- Each user computes his public key:
  Alice computes $Y_A = K_A P = 9P = (53, 44)$.
  Bob computes $Y_B = K_B P = 12P = (1, 12)$.
- After the public keys are exchanged, both can compute the common secret key:
  Alice computes $K = K_A Y_B = 9(1, 12) = 13P = (28, 28)$.
  Bob computes $K = K_B Y_A = 12(53, 44) = 13P = (28, 28)$.

Security for ECDH

In ECDH, we have $E, P, ord(P)$ and the two points $Y_A = K_A P$ and $Y_B = K_B P$ are public. Computation of the ECDH problem is based to solve ECDLP in group $G = \langle P \rangle$ by finding the private keys K_A and K_B for get the secret key $K = K_A K_B P$. Anyhow, for the ECDH problem to have a high degree of security, it is essential that the corresponding ECDLP has a high degree of security (see [83]).

Applications of ECDH in network protocols

The elliptic curve Diffie-Hellman is currently used in many network protocols, such as:

- Secure Sockets Layer (SSL)
- Transport Layer Security (TLS).
- Internet Protocol Security (IPSec).
- Secure Shell (SSH).

3.6.3 Elliptic curve digital signature algorithm

The shorter bit length of ECC often results in shorter processing time and in shorter signatures. For these reasons, the elliptic curve digital signature algorithm (ECDSA) was standardized in the US by the American National Standards Institute (ANSI) in 1998. The steps in the elliptic curve digital signature algorithm (ECDSA) standard are conceptionally closely related to the DSA scheme (it was discussed in the section 3.5). In the ECDSA, Alice generates the signature with her secret-key and Bob verifies the signature with Alice's public-key.
This protocol consists of three parts: *key generation algorithm, signature generation algorithm and signature verification algorithm* (see [34, 59, 89]).

The ECDSA protocol it is shown below which Alice signs the message m and Bob verifies Alice's signature.

Key generation algorithm

Used to generate the public and private key of the users.

1. Use an elliptic curve E over finite field $\mathbb{F}_p$ with p a prime number, and choose a point $P \in E(\mathbb{F}_p)$ which generates a cyclic group of a prime order n.
2. Choose a random integer d with $0 < d < n$.
3. Compute $Q = dP$.
4. The keys are now: $\begin{cases} \text{the public key is } K_{pub} = (p, n, Q, P). \\ \text{the private key is } K_{pr} = d. \end{cases}$

Signature generation algorithm

Used by Alice to generate the signature for the message m using private key and hash function h.

1. Select a random or pseudorandom integer k, $0 < k < n$.
2. Compute $B = kP = (x_B, y_B)$.
3. Compute $r \equiv x_B \bmod n$.
4. If $r = 0$ then go to step 1.
5. Compute hash value of the message $h(m)$.
6. Compute $s \equiv [k^{-1}(h(m) + dr)] \bmod n$.
7. If $s = 0$ then go to step 1.
8. The signature of m is (r, s).
9. Sends the message m and the signature (r, s) to Bob.

Signature verification algorithm

Used by the Bob to verify Alice's signature for accepts or rejects the message m using public key and hash function h.

1. Verify that: $0 < r < n$ and $0 < s < n$.
2. Compute hash value of the message m and convert this bit string $h(m)$ to an integer e.
3. Compute $w \equiv s^{-1} \bmod n$.
4. Compute $u_1 \equiv [h(m)w] \bmod n$ and $u_2 \equiv rw \bmod n$.
5. Compute $A = u_1P + u_2Q = (x_A, y_A)$.

6. The verfication: $x_A \begin{cases} \equiv r \bmod n \Longrightarrow \text{valid signature.} \\ \not\equiv r \bmod n \Longrightarrow \text{invalid signature and rejects the signature.} \end{cases}$

Proof. (**Correctness of the ECDSA algorithm**). To prove the ECDSA algorithm requires showing that a signature (r, s) satisfies the verification condition $x_A \equiv r \bmod n$.
The signer computes

$$s \equiv [k^{-1}(h(m) + dr)] \bmod n.$$

Thus

$$\begin{aligned} k &\equiv h(m)s^{-1} + drs^{-1} \bmod n \\ &\equiv h(m)w + drw \bmod n. \end{aligned}$$

Since P has order n we have:

$$\begin{aligned} kP &\equiv (h(m)w + drw)P \bmod n \\ &\equiv (h(m)w)P + (drw)P \bmod n \\ &\equiv u_1P + u_2dP \bmod n \\ &\equiv u_1P + u_2Q \bmod n. \end{aligned}$$

Finally, what we showed so far is that the expression $u_1P + u_2Q$ is equal to kP if the correct signature and key (and message) have been used. But this is exactly the condition that we check in the verification process by comparing the x-coordinates of $A = u_1P + u_2Q$ and $B = kP$. □

Example 3.12. Using the elliptic curve from example 3.10, we apply a simple ECDSA example. Alice wants to send a message m to Bob that is to be signed with the ECDSA protocol. The signing and verification process is as follows:
Alice

- *Key generation:*
  Choose: elliptic curve E with parameters $a = 7, b = 5, p = 29$,
  and $P = (5, 7)$ with $n = 11$.
  Choose private key: $d = 5$.
  Compute: $Q = dP = 5(5, 7) = (20, 5)$.
  Public key: $(p, a, b, n, P, Q) = (29, 7, 5, 11, (5, 7), (20, 5))$.
- *Sign:*
  Compute hash of message: $h(m) = 20$.
  Choose ephemeral key: $k = 9$ with $0 < k = 9 < n = 11$.
  Compute: $B = kP = (x_B, y_B) = 9(5, 7) = (3, 16)$.
  Compute: $r = x_B = 3$.
  Compute: $s = 5(20 + 5 \cdot 3) \equiv 10 \bmod 11$.
  Sends to Bob: $(m, (r, s)) = (m, (3, 10))$.

Bob

- *Verify:*
  Verify that: $0 < r = 3 < n = 11$ and $0 < s = 10 < n = 11$.
  Compute: $w = 10^{-1} \equiv 10 \bmod 11$.
  Compute: $u_1 = 10 \cdot 20 \equiv 2 \bmod 11$.
  Compute: $u_2 = 3 \cdot 10 \equiv 8 \bmod 11$.
  $A = u_1 P + u_2 Q = 2(5, 7) + 8(20, 5) = (3, 16)$.
  Verification: $x_A \equiv 3 \bmod 11$.
  $x_A \equiv r \bmod 11 \Longrightarrow$ valid signature.

3.6.4 ECC encryption/decryption

In this section, we will present how to implement elliptic curve based public key encryption/decryption (asymmetric cryptosystem based on ECC).
Since ECC is a asymmetric cryptography, we require a private-public key pair for to encrypt and decrypt a data. Assume Alice and Bob are the two communicating users, they agree upon a some public parameters are elliptic curve equation E and a primitive point P of cyclic group G. Each user selects a private key and generates public key, let K_A and K_B are private keys and $Y_A = K_A P$ and $Y_B = K_B P$ are public keys of Alice and Bob respectively (see [60, 81, 83]).

Encryption:

Process of encryption as follows:

- Let the message be m.
- First encode this message m into a point on elliptic curve, let this point be P_m.
- For encryption and send a message P_m to Bob, Alice choose a random positive integer k.
- Compute the ciphertext C_m that consists of a pair of points and given by:

$$C_m = \{kP, P_m + kY_B\}.$$

Decryption:

Process of decryption as follows:

- For decryption the ciphertext, Bob multiplies the point kP by Bob's secret key K_B and subtracts the result from $P_m + kY_B$, we have:

$$P_m + kY_B - K_B(kP) = P_m + k(K_BP) - K_B(kP) = P_m.$$

Example 3.13. Let's apply an example of the encryption process, taking a prime number $p = 97$, the elliptic curve $E : y^2 = x^3 + 5x + 72$ and a primitive point $P = (11, 87)$ generates a cyclic group G of order 81.
Assume that Alice wants to send a message to Bob that is encoded in the elliptic point $P_m = (35, 32)$ and that Alice chooses the random positive integer $k = 67$.

$$\begin{cases} \text{Public key of Alice: } Y_A = K_AP = 15(11, 87) = (13, 54). \\ \text{Public key of Bob: } Y_B = K_BP = 73(11, 87) = (73, 22). \end{cases}$$

We have

$$\begin{cases} kP = 67(11, 87) = (72, 91), \text{ and} \\ P_m + kY_B = (35, 32) + 67(73, 22) = 75(11, 87) = (14, 48). \end{cases}$$

Thus, Alice sends the ciphertext: $C_m = \{(72, 91), (14, 48)\}$.

What makes ECC hard to crack?

The security of ECC depends on the difficulty of solving the elliptic curve discrete logarithm problem (ECDLP) i.e. finding k, given P and $Q = kP$. The problem is computationally intractable for large values of k. The best fastest technique for solving the elliptic curve logarithm is the Pollard ρ method. With ECC, you can creat faster, smaller, and more efficient cryptographic keys for get the same levels of security of RSA/DSA or D-H as shows follows in the table3.2 (see [59, 60, 81]).

Symmetric scheme (key size in bits)	ECC-based scheme (size of n in bits)	RSA/DSA/D-H (modulus size in bits)
56	112	512
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360

Table 3.2: Comparable key sizes for equivalent security.

Where can we apply ECC?

- ❖ Web browsing on internet.
- ❖ Wireless communication devices.

- ❖ Protect confidential transactions "credit card and debit card transactions".
- ❖ Verification to protect data privacy, digital signing and cryptographic key generation.
- ❖ Constrained environments: Pagers, PDAs, Cellular Phones.

Chapter 4

Cryptographic applications over a non-commutative rings

"Due to the development of quantum computation, which has become a major threat to asymmetric cipher systems, which made many researchers they focus on creating new encryption algorithms that allow public and private keys and be resistant to quantum computers. In this chapter, we are interested in non commutative cryptography where the methods and systems of cryptography are based on algebraic structures such as groups and rings which are non-commutative. We introduce a new encryption schemes using the two special rings R_p and R_m with non commutative structures, where these cryptosystems are fully homomorphic encryption and based on the two hard problems are the discrete logarithm problem (DLP) and the conjugal classical problem (CCP) [68, 69]. "
For more infromation about elliptic curve in cryptography using the rings, see the following articles and thesis: [2, 7]; [13, 20]; [65] and [88, 92].

Contents in Brief

4.1 Fully homomorphic encryption 89
4.2 ECC over a non commutative ring R_p 90
4.2.1 The ring R_p 90
4.2.2 Cryptographic protocols 92
4.2.3 Numerical example of cryptography 95
4.3 FHE scheme over a non commutative ring R_m 97
4.3.1 The ring R_m 97
4.3.2 Encryption scheme using the ring R_m 104
4.3.3 Numerical example of cryptography 107

4.1 Fully homomorphic encryption

Since the advent of D-H protocol the imperative for full privacy of digital data has become stronger. Naturally, strong and secure encryption system have emerged in the past few decades. One way to achieve confidentiality in applications, such as secure your connection to a website, electronic voting, sending encrypted emails and online banking etc., are homomorphic and especially fully homomorphic cryptographic schemes. Originally the notion of fully homomorphic encryption (FHE) scheme is called a privacy homomorphism, were introduced by R. L. Rivest, L. Adleman and M. L. Dertouzos in their article in 1978 (see [61]). Principally, FHE scheme which allows to evaluate arbitrary computations on encrypted data, hence considered as "holy grail" of modern cryptography.

Definition 4.1. A public key cryptosystem is a triplet $(\mathcal{K}, \mathcal{P}, \mathcal{C})$ such that:

- $\mathcal{K}$ is a finite set called space of the keys.
- $\mathcal{P}$ is a finite set of the plaintext space.
- $\mathcal{C}$ is a finite set of the ciphertext space.
- For all outputs $(pk, sk) \in \mathcal{K}$, there is an encryption function $Encpk$ and a decryption function $Decsk$ such that:
  1. For any plaintext $m \in \mathcal{P}$, the ciphertext is: $c = Encpk(m) \in \mathcal{C}$.
  2. For any ciphertext $c \in \mathcal{C}$, the plaintext is: $m = Decsk(c) \in \mathcal{P}$.
  3. For any plaintext m: $Decsk(Encpk(m)) = m$.

Definition 4.2 (See [11,91]). A public-key encryption scheme $(\mathcal{K}, \mathcal{P}, \mathcal{C})$ is homomorphic if for all outputs $(pk, sk) \in \mathcal{K}$, it is possible to define groups $(M, \star)$, $(C, \circledcirc)$ so that:

- The plaintext space M, and all ciphertexts output by $Encpk$ are elements of C.
- For any $\mathfrak{m}_1, \mathfrak{m}_2 \in M$ and $\mathfrak{c}_1, \mathfrak{c}_2 \in C$ with $\mathfrak{m}_1 = Decsk(\mathfrak{c}_1, sk)$ and $\mathfrak{m}_2 = Decsk(\mathfrak{c}_2, sk)$.

holds that:

$$Decsk(\mathfrak{c}_1 \circledcirc \mathfrak{c}_1, sk) = \mathfrak{m}_1 \star \mathfrak{m}_2.$$

A fully homomorphic encryption scheme can be defined as a tuple of three algorithms $(\mathcal{K}, \mathcal{P}, \mathcal{C})$ for which the message space is a ring $(R, \ominus, \circledast)$ and the ciphertext space is also a ring $(R', \oplus, \odot)$ such that for all messages $\mathfrak{m}_1, \mathfrak{m}_2 \in R$, and all outputs $(pk, sk) \in \mathcal{K}$, we have:

$$\begin{aligned} \mathfrak{m}_1 \ominus \mathfrak{m}_2 &= Decsk(Encpk(\mathfrak{m}_1, pk) \oplus Encpk(\mathfrak{m}_2, pk), sk); \\ \mathfrak{m}_1 \circledast \mathfrak{m}_2 &= Decsk(Encpk(\mathfrak{m}_1, pk) \odot Encpk(\mathfrak{m}_2, pk), sk). \end{aligned}$$

If $(\mathcal{K}, \mathcal{P}, \mathcal{C})$ is a symmetric fully homomorphic encryption scheme, we will have a single key for encryption and decryption, so the role of pk will be played by sk.
A scheme is supposed to be somewhat homomorphic if it permits only a limited number of additions and multiplications.

The aim of these totally homomorphic systems is data integrity in communication, non-repudiation, confidentiality and storage processes, such as the ability to perform computations to untrusted persons. If a user could take a problem defined in one algebraic system and encrypting it into a problem in a different algebraic system in a method that decrypting back to the original algebraic system is difficult, then the user could encrypts expensive computations and send them to his sender. This receiver then performs the corresponding computation in the second algebraic system, returning the result to the user. Upon receiving the result, the user can decrypt it into a solution in the original algebraic system, while the untrusted party is always hidden [26].

4.2 ECC over a non commutative ring R_p

In this section, we introduce a novel non commutative cryptography scheme based on the CCP and DLP using the special ring R_p.

4.2.1 The ring R_p

In the section 2.3, we defined the ring $(\mathbb{F}_q[\varepsilon], +, \cdot)$ where $\varepsilon^4 = \varepsilon^3$ of characteristic $\neq 2, 3$, and the elliptic curve over it. Now, we define a new structure of this ring, on which two binary operations are defined, called addition $(+)$ and start $(*)$, and denoted by $(R_p, +, *)$. Let $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3$ and $Y = y_0 + y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3$ are two elements in R_p, we define the binary operations by:

$$+ : \left| \begin{array}{ccc} R_p \times R_p & \longrightarrow & R_p \\ (X, Y) & \longmapsto & X + Y \end{array} \right.$$

$$* : \left| \begin{array}{ccc} R_p \times R_p & \longrightarrow & R_p \\ (X, Y) & \longmapsto & X * Y \end{array} \right.$$

such that:

$$X + Y = (x_0 + y_0) + (x_1 + y_1)\varepsilon + (x_2 + y_2)\varepsilon^2 + (x_3 + y_3)\varepsilon^3, \tag{4.1}$$

$$X * Y = x_0y_0 + (x_0y_1 + x_1y_3)\varepsilon + (x_3y_2 + x_2y_0)\varepsilon^2 + x_3y_3\varepsilon^3. \tag{4.2}$$

Lemma 4.1. *$(R_p, +, *)$ is a ring with unitary $1_{R_p} = 1 + \varepsilon^3$ whose $*$ is not commutative.*

Proof. To show the previous lemma, we check the following properties:

- Associative laws: $\forall X, Y, Z \in R_p$,

$$(X + Y) + Z = X + (Y + Z) \text{ and}$$
$$(X * Y) * Z = X * (Y * Z).$$

- Commutative law: $\forall X, Y \in R_p, X + Y = Y + X$.
- A non commutative law: $\exists X = 1 + \varepsilon + \varepsilon^2, Y = 1 + \varepsilon^2 + \varepsilon^3 \in R_p$, such that:

$$X * Y \neq Y * X.$$

- Distributive laws: $\forall X, Y, Z \in R_p$,

$$(X + Y) * Z = X * Z + Y * Z \text{ and}$$
$$Z * (X + Y) = Z * X + Z * Y.$$

- Additive identity: $\forall X \in R_p, X + 0 = 0 + X = X$.
- Start identity: $\forall X \in R_p, X * 1_{R_p} = 1_{R_p} * X = X$, 1_{R_p} is called the start identity element of R_p.
- Additive inverses: $\forall X \in R_p, X + (-X) = 0$, $-X$ is called the additive inverse of X.

□

Let $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 \in R_p$ and $k \in \mathbb{N}^*$.

Lemma 4.2. *The element X is invertible if and only if $x_0x_3 \neq 0$, in this case we have:*

$$X^{-1*} = \frac{1}{x_0} - \frac{x_1}{x_0x_3}\varepsilon - \frac{x_2}{x_0x_3}\varepsilon^2 + \frac{1}{x_3}\varepsilon^3.$$

Proof. We have:

$$X * Y = x_0y_0 + (x_0y_1 + x_1y_3)\varepsilon + (x_3y_2 + x_2y_0)\varepsilon^2 + x_3y_3\varepsilon^3, \tag{4.3}$$

$$Y * X = x_0y_0 + (y_0x_1 + y_1x_3)\varepsilon + (y_3x_2 + y_2x_0)\varepsilon^2 + x_3y_3\varepsilon^3. \tag{4.4}$$

So,

$$X * Y = 1 + \varepsilon^3 \text{ and } Y * X = 1 + \varepsilon^3, \tag{α}$$

$$(\alpha) \iff \begin{cases} x_0y_0 = 1; \\ x_0y_1 + x_1y_3 = y_0x_1 + y_1x_3 = 0; \\ x_3y_2 + x_2y_0 = y_3x_2 + y_2x_0 = 0; \\ x_3y_3 = 1. \end{cases}$$

$$\iff \begin{cases} y_0 = \dfrac{1}{x_0}, x_0 \neq 0; \\ y_1 = -\dfrac{x_1}{x_0x_3}; \\ y_2 = -\dfrac{x_2}{x_0x_3}; \\ y_3 = \dfrac{1}{x_3}, x_3 \neq 0. \end{cases}$$

Since, $X^{-1*} = \dfrac{1}{x_0} - \dfrac{x_1}{x_0x_3}\varepsilon - \dfrac{x_2}{x_0x_3}\varepsilon^2 + \dfrac{1}{x_3}\varepsilon^3$. □

Lemma 4.3. *The k-power of X can be given by* $X^{*k} = \beta_0 + \beta_1\varepsilon + \beta_2\varepsilon^2 + \beta_3\varepsilon^3$, *where:*

- ❖ $\beta_0 = x_0^k$;
- ❖ $\beta_1 = x_1 \sum_{i+j=k-1} x_0^i x_3^j$;
- ❖ $\beta_2 = x_2 \sum_{i+j=k-1} x_0^i x_3^j$;
- ❖ $\beta_3 = x_3^k$.

Proof. The last relation is true for $k = 1$, since $X^{*1} = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3$ we assume that $X^{*k} = \beta_0 + \beta_1\varepsilon + \beta_2\varepsilon^2 + \beta_3\varepsilon^3$, for certain $k \geqslant 1$, where:

- ❖ $\beta_0 = x_0^k$;
- ❖ $\beta_1 = x_1 \sum_{i+j=k-1} x_0^i x_3^j$;
- ❖ $\beta_2 = x_2 \sum_{i+j=k-1} x_0^i x_3^j$;
- ❖ $\beta_3 = x_3^k$.

We have:

$$X^{*(k+1)} = (\beta_0 + \beta_1\varepsilon + \beta_2\varepsilon^2 + \beta_3\varepsilon^3)(x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3).$$

So, $X^{*(k+1)} = z_0 + z_1\varepsilon + z_2\varepsilon^2 + z_3\varepsilon^3$, where:

- ❖ $z_0 = \beta_0x_0 = x_0^{k+1}$;
- ❖ $z_1 = \beta_0x_1 + \beta_1x_3 = x_1 \sum_{i+j=k} x_0^i x_3^j$;
- ❖ $z_2 = \beta_3x_2 + \beta_2x_0 = x_2 \sum_{i+j=k} x_0^i x_3^j$;
- ❖ $z_3 = \beta_3x_3 = x_3^{k+1}$.

Hence: let k be a positive integer, $X^{*k} = \beta_0 + \beta_1\varepsilon + \beta_2\varepsilon^2 + \beta_3\varepsilon^3$, where:

- ❖ $\beta_0 = x_0^k$;
- ❖ $\beta_1 = x_1 \sum_{i+j=k-1} x_0^i x_3^j$;
- ❖ $\beta_2 = x_2 \sum_{i+j=k-1} x_0^i x_3^j$;
- ❖ $\beta_3 = x_3^k$.

□

4.2.2 Cryptographic protocols

This subsection we describe, exchange of secret key and we provide a construct a new fully homomorphic encryption scheme using the ring R_p.

4.2.2.1 Exchange of secret keys

For a secure encrypted message exchange between two entities Alice and Bob requires an exchange of keys first by using protocol of Diffie and Hellman. This key can be used to encrypt and decrypt messages transmitted between them. The elliptic curve Diffie and Hellman key exchange given as follows:

1. Alice and Bob agree on a prime number p, a point P generating subgroup of known order of the elliptic curve $E_{a,b}(R_p)$, where $(a, b) \in R_p^2$.
2. Alice chooses a private random integer $K_A < ord(P)$, and sends $Y_A = K_A P$ to Bob.
3. Bob chooses a private random integer $K_B < ord(P)$, and sends $Y_B = K_B P$ to Alice.
4. Alice computes $K_A Y_B = K_A K_B P$.
5. Bob computes $K_B Y_A = K_B K_A P$.

If $K_A K_B P = K_B K_A P = [K : t : 1]$ and K is $*$ invertible then the secret key between Alice and Bob is K, else return (2). Both Alice and Bob can use this number as their key. Notice that p and P need not be protected.

4.2.2.2 Encryption and decryption functions

The scheme is constructed using the commutative ring $(\mathbb{F}_q, +, \cdot)$

- $(\alpha_1, \alpha_2, \alpha_3) \in \mathbb{F}_q^3$ is a public.
- The secret key is an invertible element for the operation $*$, $K \in R_p$.
- To encrypt a message $m \in \mathbb{F}_q$, where $m = \sum_{i=0}^{l} m_i$, $(m_i)_{0 \leqslant i \leqslant l} \in \mathbb{F}_q$ and l be a positive integer, we compute the ciphertext $Encpk(m_i) \in \mathbb{F}_q$ such that:
  $c_i = Encpk(m_i) = coeff(K * (\alpha_1 + m_i\varepsilon + \alpha_2\varepsilon^2 + \alpha_3\varepsilon^3) * K^{-1*}, \varepsilon)$, where $0 \leqslant i \leqslant l$, and sends $c = (c_0, c_1, \ldots, c_l)$ to receiver.
- To decrypt a ciphertext $c \in \mathbb{F}_q$, we compute:
  $m = \sum_{i=0}^{l} Decsk(c_i) = \sum_{i=0}^{l} coeff(K^{-1*} * (\alpha_1 + c_i\varepsilon + \alpha_2\varepsilon^2 + \alpha_3\varepsilon^3) * K, \varepsilon)$.

The secret key K admits an inverse in R_p. To encrypt a message $m = \sum_{i=0}^{l} m_i \in \mathbb{F}_q$, the ciphertext $Encpk(m_i)$ is an element $c_i \in \mathbb{F}_q$ such that: $c_i = Encpk(m_i)$. To decrypt a ciphertext c_i, we compute: $m_i = Decsk(c_i)$.

Remark 4.1. For all message $m = \sum_{i=0}^{l} m_i \in \mathbb{F}_q$, where l be positive integer. We have:

$$\sum_{i=0}^{l} Decsk \circ Encpk(m_i) = m.$$

Let m', m'' be two messages in $\mathbb{F}_q$, where $m' = \sum_{i=0}^{l} m'_i, m'' = \sum_{j=0}^{r} m''_j$ and l, r are two positive integers.

Proposition 4.1. *The encryption system $(\mathcal{K}, \mathcal{P}, \mathcal{C})$ is homomorphic if and only if $\alpha_1 = \alpha_3$ or $K = k_0 + k_2\varepsilon^2 + k_3\varepsilon^3$.*

Proof. Let $K = k_0 + k_1\varepsilon + k_2\varepsilon^2 + k_3\varepsilon^3 \in R_p$ be an invertible element for the law $*$ and let $pk = (\alpha_1, \alpha_2, \alpha_3) \in \mathbb{F}_q^3$.
By the encryption function, we have:

$$\forall (m', m'') \in \mathbb{F}_q^2 : \begin{cases} Encpk(m'_i + m''_j) = k_0(m'_i + m''_j)k_3^{-1} + k_1k_3^{-1}(\alpha_3 - \alpha_1); \\ Encpk(m'_i) = k_0(m'_i)k_3^{-1} + k_1k_3^{-1}(\alpha_3 - \alpha_1); \\ Encpk(m''_j) = k_0(m''_j)k_3^{-1} + k_1k_3^{-1}(\alpha_3 - \alpha_1). \end{cases}$$

Then:

$$\begin{aligned} Encpk(m'_i + m''_j) = Encpk(m'_i) + Encpk(m''_j) &\iff k_1k_3^{-1}(\alpha_3 - \alpha_1) = 0 \\ &\iff k_1 = 0 \text{ or } \alpha_1 = \alpha_3. \end{aligned}$$

Thus, the proposition is proved. □

Corollary 4.1. *If $K = k_0 + k_2\varepsilon^2 + k_3\varepsilon^3$, then the encryption system $(\mathcal{K}, \mathcal{P}, \mathcal{C})$, verify:*

$$\forall (m', m'') \in \mathbb{F}_q^2 : Encpk(m'_i \cdot m''_j) = k_3k_0^{-1}Encpk(m'_i) \cdot Encpk(m''_j).$$

Proof. Let $K = k_0 + k_2\varepsilon^2 + k_3\varepsilon^3$ be an invertible element in R_p, according to the previous proposition, we have:

$$\forall (m', m'') \in \mathbb{F}_q^2 : \begin{cases} Encpk(m'_i \cdot m''_j) = k_0(m'_i \cdot m''_j)k_3^{-1}; \\ Encpk(m'_i) = k_0(m'_i)k_3^{-1}; \\ Encpk(m''_j) = k_0(m''_j)k_3^{-1}. \end{cases}$$

So, $k_0k_3^{-1}Encpk(m'_i \cdot m''_j) = Encpk(m'_i) \cdot Encpk(m''_j)$. Then:

$$Encpk(m'_i \cdot m''_j) = k_3k_0^{-1}Encpk(m'_i) \cdot Encpk(m''_j).$$

□

Remark 4.2. The previous corollary means that the encryption system $(\mathcal{K}, \mathcal{P}, \mathcal{C})$ is fully homomorphic in the following direction:

$$\forall K = k_0 + k_2\varepsilon^2 + k_3\varepsilon^3 \in R_p^{\times}, \forall (m', m'') \in \mathbb{F}_q^2 : Enc_{K^2}(m'_i \cdot m''_j) = Enc_K(m'_i) \cdot Enc_K(m''_j),$$

where: $K^2 = K * K$.

4.2.2.3 Security of this protocol

The security of our system which uses elliptic curve cryptography on a non commutative ring has a stronger with a short key because to decrypt a message we must solve the elliptic curve discrete logarithm problem and the conjugate problem on a non commutative ring.

4.2.3 Numerical example of cryptography

In this section, we will try to give a numerical example of the cryptosystem thus constructed.

- Alice and Bob have chosen a prime number:
  $q = 68647976601306097149819007990813932172694353001433054093944634591855431833976560521225596406614545549772963113914808580371219879997166438125740282911150594 61.$
- Public key $(\alpha_1, \alpha_2, \alpha_3) \in \mathbb{F}_q$, where:
  $\alpha_1 = 20747222467734852078216952221076085874809964747211172927529925899121966847505496583100844167325500 77.$
  $\alpha_2 = 53713936060247752512565504367735659774067242691529421364157627828105625541315990749074260107375035 01.$
  $\alpha_3 = 72126101472954749095445237850434924099693821481867654600825000853935195565259214555887054230207514 21.$
- Let a message $m \in \mathbb{F}_q$ sucht that $m = \sum_{i=0}^{3} m_i$, where:
  $m_0 = 28275548353370728705475218432112134576686148069744870344385701215326440743976601304240257 1.$
  $m_1 = 66486914377319660846200177277938265031167356854223785254671591313568843461473171784486826 1.$
  $m_2 = 97652263702130640315055193331900613772012404862454417207273505578041183410486266715592284 1.$
  $m_3 = 62516179395462474621167929933162156793136976894420563579135569472777448767770601384205877 9.$

$m = \sum_{i=0}^{3} m_i = 254930905828283504487898518975113170173002886680843636385466$
$367579713916383706641188525245 2.$

❖ The secret key

$$K = K_0 + K_1\varepsilon + K_2\varepsilon^2 + K_3\varepsilon^3,$$

where:
$K_0 = 185323955009471744507093833849366798683834244443114056794632807824057796233163977.$
$K_1 = 466952384993213050887639255471340752131911723963794322498001567615649 1.$
$K_2 = 521064401567922879406069432539095585333589848390805645835218385101837255573570 7.$
$K_3 = 121416805764108066932466369176469931665150427440758720078238275608681517825325532757.$

❖ Inverse of the secret key

$$K^{-1*} = K_a + K_b\varepsilon + K_c\varepsilon^2 + K_d\varepsilon^3,$$

where:
$K_a = 445668460750991954708233276853422478970136571695263624647040589080946458803137790674158077227825452674066760154195309206422707777411480241600342438423751 37.$
$K_b = 362952951322901577826337250452664023646028078467669719969549269324716755427872023620013884349309452412282931827620482643678762012926965540046768939782149433 0.$
$K_c = 606435853982882839372146394661342036315045541762147035663557328676798343929094186106682149136719346381547743637105888656102083250348196028642153866134132042 8.$
$K_d = 389200439551316511852195492976569991941249559370312167982346030269427566566352476915615118590800181034908575236563646674905160835208366704334594559194316392 8.$

❖ We compute an encrypt message c, as follow:

$$c_i = Encpk(m_i) = coeff(K * (\alpha_1 + m_i\varepsilon + \alpha_2\varepsilon^2 + \alpha_3\varepsilon^3) * K^{-1*}, \varepsilon),$$

where $0 \leqslant i \leqslant 3$, we have:
$c = (c_0, c_1, c_2, c_3)$ such that:
$c_0 = 182132916883357075201027446602086185460877645299381039173378505857705376186648778282054444408488811253482684074226847570915589507375959473179044602415632603 4.$
$c_1 = 132060693544847042041861987089551727479196863715879778423520060764 1$

539902113155291536291200425572652531215173005323495701330102449245179889651782681192547 04.

$c_2 = 29505406962316403975824075900766354152211720890303162925241727318959993632300384441862555475465993301563637558139844205985915639095173849957726272241519405 23.$

$c_3 = 34636162686688612812351893518121643198746955075629974868897425892320411181988724310846466374662356467185222274184991307541845326060030978156014587811976922 78.$

Remark 4.3. With this application, we can encrypt and decrypt any message of any length. The motivation of this work is that decryption is very difficult for an interceptor who cannot solve the conjugal classical problem and elliptic curve discrete logarithm problem.

4.3 FHE scheme over a non commutative ring R_m

In this section, we make a new fully homomorphic encryption scheme over the ring R_m based on two difficult problems; problem of conjugal and discrete logarithm problem.

4.3.1 The ring R_m

Based on the study in section 2.3, we have $E_{a,b}(\mathbb{F}_q[\varepsilon])$ is an elliptic curve over the ring $\mathbb{F}_q[\varepsilon]$, P is a point of order l and G is the subgroup generated by P. We consider the set:

$$R_m = \left\{ \begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix} \mid (x_i)_{1\leqslant i\leqslant 3} \in \{0,1,2,...,l-1\} \text{ and } S,L,T \in G \right\}.$$

Let $X = \begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix}$ and $Y = \begin{bmatrix} x'_1 & S' & L' \\ 0 & x'_2 & T' \\ 0 & 0 & x'_3 \end{bmatrix}$ be two elements in R_m, on which two binary operations are defined, called addition $(+)$ and start $(*)$ and denoted by:

$$X+Y = \begin{bmatrix} x_1+x'_1 & S+S' & L+L' \\ 0 & x_2+x'_2 & T+T' \\ 0 & 0 & x_3+x'_3 \end{bmatrix}, X*Y = \begin{bmatrix} x_1x'_1 & x_1S'+x'_2S & x_1L'+x'_3L \\ 0 & x_2x'_2 & x_2T'+x'_3T \\ 0 & 0 & x_3x'_3 \end{bmatrix}.$$

Lemma 4.4. *The ring $(R_m,+,*)$ is not commutative, with identity*

$$1_{R_m} = \begin{bmatrix} 1 & [0:1:0] & [0:1:0] \\ 0 & 1 & [0:1:0] \\ 0 & 0 & 1 \end{bmatrix}.$$

Proof. Let $X = \begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix}, Y = \begin{bmatrix} x_1' & S' & L' \\ 0 & x_2' & T' \\ 0 & 0 & x_3' \end{bmatrix}$ and $Z = \begin{bmatrix} x_1'' & S'' & L'' \\ 0 & x_2'' & T'' \\ 0 & 0 & x_3'' \end{bmatrix}$ be three elements in R_m.

- ❖ Associative laws: $\forall X, Y, Z \in R_m$.
  - For addition law

$$\begin{aligned}(X+Y)+Z &= \begin{bmatrix} x_1+x_1' & S+S' & L+L' \\ 0 & x_2+x_2' & T+T' \\ 0 & 0 & x_3+x_3' \end{bmatrix} + \begin{bmatrix} x_1'' & S'' & L'' \\ 0 & x_2'' & T'' \\ 0 & 0 & x_3'' \end{bmatrix} \\ &= \begin{bmatrix} x_1+x_1'+x_1'' & S+S'+S'' & L+L'+L'' \\ 0 & x_2+x_2'+x_2'' & T+T'+T'' \\ 0 & 0 & x_3+x_3'+x_3'' \end{bmatrix} \\ &= X+(Y+Z).\end{aligned}$$

  - For start law

$$\begin{aligned}(X*Y)*Z &= \begin{bmatrix} x_1x_1' & x_1S'+x_2'S & x_1L'+x_3'L \\ 0 & x_2x_2' & x_2T'+x_3'T \\ 0 & 0 & x_3x_3' \end{bmatrix} * \begin{bmatrix} x_1'' & S'' & L'' \\ 0 & x_2'' & T'' \\ 0 & 0 & x_3'' \end{bmatrix} \\ &= \begin{bmatrix} x_1x_1'x_1'' & x_1x_1'S''+x_2''(x_1S'+x_2'S) & x_1x_1'L''+x_3''(x_1L'+x_3'L) \\ 0 & x_2x_2'x_2'' & x_2x_2'T''+x_3''(x_2T'+x_3'T) \\ 0 & 0 & x_3x_3'x_3'' \end{bmatrix} \\ &= \begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix} * \begin{bmatrix} x_1'x_1'' & x_1'S''+x_2''S' & x_1'L''+x_3''L' \\ 0 & x_2'x_2'' & x_2'T''+x_3''T' \\ 0 & 0 & x_3'x_3'' \end{bmatrix} \\ &= X*(Y*Z).\end{aligned}$$

- ❖ Commutative law: $\forall X, Y \in R_m$,

$$X+Y = \begin{bmatrix} x_1+x_1' & S+S' & L+L' \\ 0 & x_2+x_2' & T+T' \\ 0 & 0 & x_3+x_3' \end{bmatrix} = \begin{bmatrix} x_1'+x_1 & S'+S & L'+L \\ 0 & x_2'+x_2 & T'+T \\ 0 & 0 & x_3'+x_3 \end{bmatrix} = Y+X.$$

  So, $+$ is commutative.

- ❖ A non commutative law: assume that G is the subgroup generated by P of order 30.

  $\exists X = \begin{bmatrix} 2 & 2P & 4P \\ 0 & 4 & 3P \\ 0 & 0 & 1 \end{bmatrix}, Y = \begin{bmatrix} 1 & 4P & 2P \\ 0 & 2 & 5P \\ 0 & 0 & 3 \end{bmatrix} \in R_m$ such that:

$$X*Y = \begin{bmatrix} 2 & 12P & 16P \\ 0 & 8 & 29P \\ 0 & 0 & 3 \end{bmatrix} \neq \begin{bmatrix} 2 & 18P & 6P \\ 0 & 8 & 11P \\ 0 & 0 & 3 \end{bmatrix} = Y*X.$$

  So, $*$ is not commutative.

❖ Distributive laws: $\forall X, Y, Z \in R_m$,

$$
\begin{aligned}
(X+Y)*Z &= \begin{bmatrix} x_1+x_1' & S+S' & L+L' \\ 0 & x_2+x_2' & T+T' \\ 0 & 0 & x_3+x_3' \end{bmatrix} * \begin{bmatrix} x_1'' & S'' & L'' \\ 0 & x_2'' & T'' \\ 0 & 0 & x_3'' \end{bmatrix} \\
&= \begin{bmatrix} (x_1+x_1')x_1'' & (x_1+x_1')S''+x_2''(S+S') & (x_1+x_1')L''+x_3''(L+L') \\ 0 & (x_2+x_2')x_2'' & (x_2+x_2')T''+x_3''(T+T') \\ 0 & 0 & (x_3+x_3')x_3'' \end{bmatrix} \\
&= \begin{bmatrix} x_1x_1'' & x_1S''+x_2''S & x_1L''+x_3''L \\ 0 & x_2x_2'' & x_2T''+x_3''T \\ 0 & 0 & x_3x_3'' \end{bmatrix} \\
&+ \begin{bmatrix} x_1'x_1'' & x_1'S''+x_2''S' & x_1'L''+x_3''L' \\ 0 & x_2'x_2'' & x_2'T''+x_3''T' \\ 0 & 0 & x_3'x_3'' \end{bmatrix} \\
&= X*Z+Y*Z \\
Z*(X+Y) &= \begin{bmatrix} x_1'' & S'' & L'' \\ 0 & x_2'' & T'' \\ 0 & 0 & x_3'' \end{bmatrix} * \begin{bmatrix} x_1+x_1' & S+S' & L+L' \\ 0 & x_2+x_2' & T+T' \\ 0 & 0 & x_3+x_3' \end{bmatrix} \\
&= \begin{bmatrix} x_1''(x_1+x_1') & x_1''(S+S')+(x_2+x_2')S'' & x_1''(L+L')+(x_3+x_3')L'' \\ 0 & x_2''(x_2+x_2') & x_2''(T+T')+(x_3+x_3')T'' \\ 0 & 0 & x_3''(x_3+x_3') \end{bmatrix} \\
&= \begin{bmatrix} x_1''x_1 & x_1''S+x_2S'' & x_1''L+x_3L'' \\ 0 & x_2''x_2 & x_2''T+x_3T'' \\ 0 & 0 & x_3''x_3 \end{bmatrix} \\
&+ \begin{bmatrix} x_1''x_1' & x_1''S'+x_2'S'' & x_1''L'+x_3'L'' \\ 0 & x_2''x_2' & x_2''T'+x_3'T'' \\ 0 & 0 & x_3''x_3' \end{bmatrix} \\
&= Z*X+Z*Y.
\end{aligned}
$$

So, $*$ is distributive with respect to $+$.

❖ Additive identity: $\forall X \in R_m$,

$$
\begin{aligned}
X+0_{R_m} &= \begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix} + \begin{bmatrix} 0 & [0:1:0] & [0:1:0] \\ 0 & 0 & [0:1:0] \\ 0 & 0 & 0 \end{bmatrix} \\
&= \begin{bmatrix} 0 & [0:1:0] & [0:1:0] \\ 0 & 0 & [0:1:0] \\ 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix} \\
&= \begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix} \\
&= 0_{R_m}+X = X.
\end{aligned}
$$

So, $0_{R_m} = \begin{bmatrix} 0 & [0:1:0] & [0:1:0] \\ 0 & 0 & [0:1:0] \\ 0 & 0 & 0 \end{bmatrix}$ is called the additive identity element of R_m.

❖ Start identity: $\forall X \in R_m$,

$$X * 1_{R_m} = \begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix} * \begin{bmatrix} 1 & [0:1:0] & [0:1:0] \\ 0 & 1 & [0:1:0] \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & [0:1:0] & [0:1:0] \\ 0 & 1 & [0:1:0] \\ 0 & 0 & 1 \end{bmatrix} * \begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix} = 1_{R_m} * X = X.$$

So, $1_{R_m} = \begin{bmatrix} 1 & [0:1:0] & [0:1:0] \\ 0 & 1 & [0:1:0] \\ 0 & 0 & 1 \end{bmatrix}$ is called the start identity element of R_m.

❖ Additive inverses: $\forall X \in R_m$,

$$X + (-X) = \begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix} + \begin{bmatrix} -x_1 & -S & -L \\ 0 & -x_2 & -T \\ 0 & 0 & -x_3 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & [0:1:0] & [0:1:0] \\ 0 & 0 & [0:1:0] \\ 0 & 0 & 0 \end{bmatrix} = 0_{R_m}.$$

So, $-X = \begin{bmatrix} -x_1 & -S & -L \\ 0 & -x_2 & -T \\ 0 & 0 & -x_3 \end{bmatrix}$ is called the additive inverse of X.

□

Lemma 4.5. *Let* $X = \begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix} \in R_m$, *the element* X *is invertible if and only if* $\gcd(x_i, l) = 1$, *for* $1 \leqslant i \leqslant 3$, *in this case we have:* $X^{-1*} = \begin{bmatrix} x_1^{-1} & -x_1^{-1}x_2^{-1}S & -x_1^{-1}x_3^{-1}L \\ 0 & x_2^{-1} & -x_2^{-1}x_3^{-1}T \\ 0 & 0 & x_3^{-1} \end{bmatrix}$.

Proof. Let $Y = \begin{bmatrix} x_1' & S' & L' \\ 0 & x_2' & T' \\ 0 & 0 & x_3' \end{bmatrix}$ be the inverse of X, we have: $X * Y = Y * X = 1_{R_m}$.

So,

$$X * Y = \begin{bmatrix} x_1x_1' & x_1S' + x_2'S & x_1L' + x_3'L \\ 0 & x_2x_2' & x_2T' + x_3'T \\ 0 & 0 & x_3x_3' \end{bmatrix} = \begin{bmatrix} 1 & [0:1:0] & [0:1:0] \\ 0 & 1 & [0:1:0] \\ 0 & 0 & 1 \end{bmatrix}$$

and

$$Y * X = \begin{bmatrix} x_1x_1' & x_1'S + x_2S' & x_1'L + x_3L' \\ 0 & x_2x_2' & x_2'T + x_3T' \\ 0 & 0 & x_3x_3' \end{bmatrix} = \begin{bmatrix} 1 & [0:1:0] & [0:1:0] \\ 0 & 1 & [0:1:0] \\ 0 & 0 & 1 \end{bmatrix},$$

$$x_ix_i' \equiv 1[l] \text{ for } 1 \leqslant i \leqslant 3,$$

thus,

$$\begin{cases} x_1S' + x_2'S = [0:1:0] \\ x_1'S + x_2S' = [0:1:0] \end{cases} \Longrightarrow S' = -x_1^{-1}x_2'S = -x_2^{-1}x_1'S = -x_1^{-1}x_2^{-1}S.$$

$$\begin{cases} x_1L' + x_3'L = [0:1:0] \\ x_1'L + x_3L' = [0:1:0] \end{cases} \Longrightarrow L' = -x_1^{-1}x_3'L = -x_3^{-1}x_1'L = -x_1^{-1}x_3^{-1}L.$$

$$\begin{cases} x_2T' + x_3'T = [0:1:0] \\ x_2'T + x_3T' = [0:1:0] \end{cases} \Longrightarrow T' = -x_2^{-1}x_3'T = -x_3^{-1}x_2'T = -x_2^{-1}x_3^{-1}T.$$

Therefore, the element X is invertible if and only if $\gcd(x_i, l) = 1$, for $1 \leqslant i \leqslant 3$, in this case we have:

$$X^{-1*} = \begin{bmatrix} x_1^{-1} & -x_1^{-1}x_2^{-1}S & -x_1^{-1}x_3^{-1}L \\ 0 & x_2^{-1} & -x_2^{-1}x_3^{-1}T \\ 0 & 0 & x_3^{-1} \end{bmatrix}.$$

□

Lemma 4.6. *Let k be a strictly positive integer. Then if $X = \begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix}$ is any element of R_m, the k-power of X can be given by: $X^k = \begin{bmatrix} x_1^k & \alpha_kS & \beta_kL \\ 0 & x_2^k & \gamma_kT \\ 0 & 0 & x_3^k \end{bmatrix}$ where: $\begin{cases} \alpha_k = \sum\limits_{i+j=k-1} x_1^ix_2^j; \\ \beta_k = \sum\limits_{i+j=k-1} x_1^ix_3^j; \\ \gamma_k = \sum\limits_{i+j=k-1} x_2^ix_3^j. \end{cases}$*

Proof. Using a proof is by induction on k, for $k = 1$: we have $\alpha_1 = 1, \beta_1 = 1$ and $\gamma_1 = 1$, for $k \geqslant 1$ assume that, $\begin{cases} \alpha_k = \sum\limits_{i+j=k-1} x_1^ix_2^j; \\ \beta_k = \sum\limits_{i+j=k-1} x_1^ix_3^j; \\ \gamma_k = \sum\limits_{i+j=k-1} x_2^ix_3^j. \end{cases}$ and proof that: $\begin{cases} \alpha_{k+1} = \sum\limits_{i+j=k} x_1^ix_2^j; \\ \beta_{k+1} = \sum\limits_{i+j=k} x_1^ix_3^j; \\ \gamma_{k+1} = \sum\limits_{i+j=k} x_2^ix_3^j. \end{cases}$

We have:

$$X^{k+1} = \begin{bmatrix} x_1^k & \alpha_kS & \beta_kL \\ 0 & x_2^k & \gamma_kT \\ 0 & 0 & x_3^k \end{bmatrix} * \begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix} = \begin{bmatrix} x_1^{k+1} & x_1^kS + x_2\alpha_kS & x_1^kL + x_3\beta_kL \\ 0 & x_2^{k+1} & x_2^kT + x_3\gamma_kT \\ 0 & 0 & x_3^{k+1} \end{bmatrix},$$

thus, $\begin{cases} \alpha_{k+1} = x_1^k + x_2\alpha_k = x_1^k + x_2 \sum\limits_{i+j=k-1} x_1^i x_2^j = \sum\limits_{i+j=k} x_1^i x_2^j; \\ \beta_{k+1} = x_1^k + x_3\beta_k = x_1^k + x_3 \sum\limits_{i+j=k-1} x_1^i x_3^j = \sum\limits_{i+j=k} x_1^i x_3^j; \\ \gamma_{k+1} = x_2^k + x_3\gamma_k = x_2^k + x_3 \sum\limits_{i+j=k-1} x_2^i x_3^j = \sum\limits_{i+j=k} x_2^i x_3^j. \end{cases}$

we conclude that, $\forall k \geqslant 1, \begin{cases} \alpha_k = \sum\limits_{i+j=k-1} x_1^i x_2^j; \\ \beta_k = \sum\limits_{i+j=k-1} x_1^i x_3^j; \\ \gamma_k = \sum\limits_{i+j=k-1} x_2^i x_3^j. \end{cases}$ □

Definition 4.3. Let $X = \begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix}$ be an element in R_m. We define the tilde of an element X; $\widetilde{X}$ which is written as follows: $\widetilde{X} = \begin{bmatrix} x_3 & T & L \\ 0 & x_2 & S \\ 0 & 0 & x_1 \end{bmatrix}$.

Lemma 4.7. *Let X be an element in the ring R_m, then: $\widetilde{\widetilde{X}} = X$.*

Proof. We have: $\widetilde{\widetilde{X}} = \widetilde{\begin{bmatrix} x_3 & T & L \\ 0 & x_2 & S \\ 0 & 0 & x_1 \end{bmatrix}} = \begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix} = X.$ □

Lemma 4.8. *Let $(X, Y) \in R_m^2$, then: $\widetilde{X+Y} = \widetilde{X} + \widetilde{Y}$.*

Proof. Let $X = \begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix}$ and $Y = \begin{bmatrix} x_1' & S' & L' \\ 0 & x_2' & T' \\ 0 & 0 & x_3' \end{bmatrix}$ be two elements in R_m,

$$\widetilde{X+Y} = \widetilde{\begin{bmatrix} x_1+x_1' & S+S' & L+L' \\ 0 & x_2+x_2' & T+T' \\ 0 & 0 & x_3+x_3' \end{bmatrix}} = \begin{bmatrix} x_3+x_3' & T+T' & L+L' \\ 0 & x_2+x_2' & S+S' \\ 0 & 0 & x_1+x_1' \end{bmatrix}$$
$$= \begin{bmatrix} x_3 & T & L \\ 0 & x_2 & S \\ 0 & 0 & x_1 \end{bmatrix} + \begin{bmatrix} x_3' & T' & L' \\ 0 & x_2' & S' \\ 0 & 0 & x_1' \end{bmatrix} = \widetilde{X} + \widetilde{Y}.$$ □

Proposition 4.2. *Let X, Y be two elements in the ring R_m, then: $\widetilde{X * Y} = \widetilde{Y} * \widetilde{X}$.*

Proof. Let $X = \begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix}$ and $Y = \begin{bmatrix} x_1' & S' & L' \\ 0 & x_2' & T' \\ 0 & 0 & x_3' \end{bmatrix}$ be two elements in R_m.

We have $X * Y = \begin{bmatrix} x_1x_1' & x_1S' + x_2'S & x_1L' + x_3'L \\ 0 & x_2x_2' & x_2T' + x_3'T \\ 0 & 0 & x_3x_3' \end{bmatrix}$, then:

$$\widetilde{X * Y} = \begin{bmatrix} x_3x_3' & x_2T' + x_3'T & x_1L' + x_3'L \\ 0 & x_2x_2' & x_1S' + x_2'S \\ 0 & 0 & x_1x_1' \end{bmatrix} = \begin{bmatrix} x_3' & T' & L' \\ 0 & x_2' & S' \\ 0 & 0 & x_1' \end{bmatrix} * \begin{bmatrix} x_3 & T & L \\ 0 & x_2 & S \\ 0 & 0 & x_1 \end{bmatrix}$$
$$= \widetilde{Y} * \widetilde{X}.$$

□

Lemma 4.9. *If the element X is invertible in the ring R_m, then $\widetilde{X}$ is invertible and we have:*

$$(\widetilde{X})^{-1*} = \widetilde{X^{-1*}}.$$

Proof. Let $X = \begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix} \in R_m$. We have the tilde of X is $\widetilde{X} = \begin{bmatrix} x_3 & T & L \\ 0 & x_2 & S \\ 0 & 0 & x_1 \end{bmatrix}$, then:

$$(\widetilde{X})^{-1*} = \begin{bmatrix} x_3^{-1} & -x_3^{-1}x_2^{-1}T & -x_3^{-1}x_1^{-1}L \\ 0 & x_2^{-1} & -x_2^{-1}x_1^{-1}S \\ 0 & 0 & x_1^{-1} \end{bmatrix} = \overbrace{\begin{bmatrix} x_1^{-1} & -x_1^{-1}x_2^{-1}S & -x_1^{-1}x_3^{-1}L \\ 0 & x_2^{-1} & -x_2^{-1}x_3^{-1}T \\ 0 & 0 & x_3^{-1} \end{bmatrix}}$$
$$= \widetilde{X^{-1*}}.$$

□

Using the Lemma 4.6, we deduce the following corollary.

Corollary 4.2. *Let $k \in \mathbb{N}^*$. Then if $\widetilde{X} = \begin{bmatrix} x_3 & T & L \\ 0 & x_2 & S \\ 0 & 0 & x_1 \end{bmatrix}$ is any element of R_m, the k-power of $\widetilde{X}$ can be given by: $(\widetilde{X})^k = \begin{bmatrix} x_3^k & \gamma_k T & \beta_k L \\ 0 & x_2^k & \alpha_k S \\ 0 & 0 & x_1^k \end{bmatrix}$, where: $\begin{cases} \alpha_k = \sum\limits_{i+j=k-1} x_1^i x_2^j; \\ \beta_k = \sum\limits_{i+j=k-1} x_1^i x_3^j; \\ \gamma_k = \sum\limits_{i+j=k-1} x_2^i x_3^j. \end{cases}$*

Corollary 4.3. *Let $k \in \mathbb{N}^*$, the k-power of $\widetilde{X} = \begin{bmatrix} x_3 & T & L \\ 0 & x_2 & S \\ 0 & 0 & x_1 \end{bmatrix}$ given by: $(\widetilde{X})^k = \widetilde{X^k}$.*

The center of a ring R_m, denoted as $Z(R_m)$ is the subring consisting of the elements X such that $X * Y = Y * X$ for all element Y in R_m.

Proposition 4.3. *The mapping φ given by:*

$$\varphi : \left| \begin{array}{ccc} Z(R_m) & \longrightarrow & Z(R_m) \\ X & \longmapsto & \widetilde{X} \end{array} \right.$$

is an isomorphism.

Proof. For all $X, Y \in Z(R_m)$

1. φ is a ring morphism:
   - ❖ $\varphi(X+Y) = \widetilde{X+Y} = \widetilde{X} + \widetilde{Y} = \varphi(X) + \varphi(Y)$.
   - ❖ $\varphi(X*Y) = \widetilde{X*Y} = \widetilde{Y} * \widetilde{X} = \widetilde{X} * \widetilde{Y} = \varphi(X) * \varphi(Y)$.
   - ❖ $\varphi(1_{Z(R_m)}) = \widetilde{1}_{Z(R_m)} = 1_{Z(R_m)}$.
2. φ is a injective:
   $\varphi(X) = \varphi(Y) \Longleftrightarrow \widetilde{X} = \widetilde{Y} \Longleftrightarrow \widetilde{\widetilde{X}} = \widetilde{\widetilde{Y}} \Longleftrightarrow X = Y$.
3. φ is a surjective:
   $\forall\, Y \in Z(R_m), \exists X = \widetilde{Y} \in Z(R_m)$ such that $\varphi(X) = \varphi(\widetilde{Y}) = \widetilde{\widetilde{Y}} = Y$.

Finally, by (1),(2) and (3) the mapping φ is an isomorphism. □

4.3.2 Encryption scheme using the ring R_m

In this subsection we describes, exchange of secret key and we provide a construct a new cryptosystem for encryption and decryption using the non commutative ring R_m based on the conjugal problem whose intractability is necessary for the security of R_m cryptographic schemes.

4.3.2.1 Key exchange protocol

For a secure encrypted message exchange between two entities Alice and Bob requires an exchange of keys first by using protocol Diffie-Hellman. This key can be used to encrypt and decrypt messages transmitted between them.
The Diffie-Hellman protocol given by the following diagram:

1. Alice and Bob agree on a prime number p, a point P generating subgroup G of order l of the elliptic curve $E_{a,b}(\mathbb{F}_q[\varepsilon])$, where $(a,b) \in (\mathbb{F}_q[\varepsilon])^2$.
2. (x_1, x_2, x_3) in $\{0, 1, 2, ..., l-1\}^3$ is a public and $\gcd(x_i, l) = 1$, for $1 \leq i \leq 3$.

3. Alice chooses three private random integers are all different $a_i < ord(P)$, and sends a_iP to Bob, for $1 \leq i \leq 3$.

4. Bob chooses three private random integers are all different $b_i < ord(P)$, and sends by the order b_iP to Alice, for $1 \leq i \leq 3$.

5. Alice build the following table:

Private keys / Message sent by Bob	a_1	a_2	a_3	Sum
b_1P	a_1b_1P	a_2b_1P	a_3b_1P	K_1
b_2P	a_1b_2P	a_2b_2P	a_3b_2P	K_2
b_3P	a_1b_3P	a_2b_3P	a_3b_3P	K_3

6. Bob build the following table:

Private keys / Message sent by Alice	b_1	b_2	b_3
a_1P	b_1a_1P	b_2a_1P	b_3a_1P
a_2P	b_1a_2P	b_2a_2P	b_3a_2P
a_3P	b_1a_3P	b_2a_3P	b_3a_3P
Sum	K_1	K_2	K_3

7. The secret key between Alice and Bob is $K = \begin{bmatrix} x_1 & K_1 & K_2 \\ 0 & x_2 & K_3 \\ 0 & 0 & x_3 \end{bmatrix}$, K is $*$ invertible in R_m.

4.3.2.2 Encryption and decryption functions

The scheme is constructed using the non commutative ring $(R_m, +, *)$. To encrypt a message $m \in R_m$, we compute the ciphertext $E_{nc}(m)$ such that:

$$c = E_{nc}(m) = \widetilde{K * m * K^{-1*}}.$$

To decrypt a ciphertext $c \in R_m$, we compute:

$$m = D_{ec}(c) = K^{-1*} * \tilde{c} * K.$$

❖ Encryption function: $\forall K \in R_m^{\times}$,

$$E_{nc} : \left| \begin{array}{ccc} R_m & \longrightarrow & R_m \\ m & \longmapsto & \widetilde{K * m * K^{-1*}} \end{array} \right.$$

❖ Decryption function: $\forall K \in R_m^{\times}$,

$$D_{ec} : \left| \begin{array}{ccc} R_m & \longrightarrow & R_m \\ c & \longmapsto & K^{-1*} * \widetilde{c} * K \end{array} \right.$$

Remark 4.4. For all message m in R_m, we have:

$$D_{ec} \circ E_{nc}(m) = m.$$

Lemma 4.10. *Let m_1, m_2 are two messages in R_m, then:*

$$E_{nc}(m_1 + m_2) = E_{nc}(m_1) + E_{nc}(m_2).$$

Proof. By the encryption function we have:

$$\begin{aligned} E_{nc}(m_1 + m_2) &= \widetilde{K * (m_1 + m_2) * K^{-1*}} \\ &= \widetilde{K * m_1 * K^{-1*} + K * m_2 * K^{-1*}} \\ &= \widetilde{K * m_1 * K^{-1*}} + \widetilde{K * m_2 * K^{-1*}} \\ &= E_{nc}(m_1) + E_{nc}(m_2). \end{aligned}$$

□

Lemma 4.11. *For all $m_1, m_2 \in R_m$. If $m_1 * m_2 = m_2 * m_1$ then:*

$$E_{nc}(m_1 * m_2) = E_{nc}(m_1) * E_{nc}(m_2).$$

Proof. By the encryption function we have:

$$E_{nc}(m_1 * m_2) = \widetilde{K * (m_1 * m_2) * K^{-1*}}.$$

Using the Proposition 4.2, if $m_1 * m_2 = m_2 * m_1$ then:

$$\begin{aligned} E_{nc}(m_1 * m_2) &= \widetilde{K * (m_2 * m_1) * K^{-1*}} \\ &= \widetilde{K * m_2 * K^{-1*} * K * m_1 * K^{-1*}} \\ &= \widetilde{K * m_1 * K^{-1*}} * \widetilde{K * m_2 * K^{-1*}} \\ &= E_{nc}(m_1) * E_{nc}(m_2). \end{aligned}$$

Thus, the lemma is proved. □

Remark 4.5. Fully homomorphic cryptosystem based on the ring R_m:

❖ Space of lights: $E = Z(R_m)$.

❖ Space of quantified: $F = Z(R_m)$.

- Space of keys: $R_m^{\times} - \{Z(R_m)\}$.
- Encryption function: $\forall K \in R_m^{\times} - \{Z(R_m)\}$,

$$E_{nc} : \left| \begin{array}{ccc} E & \longrightarrow & F \\ m & \longmapsto & \overbrace{K * m * K^{-1*}} \end{array} \right.$$

- Decryption function: $\forall K \in R_m^{\times} - \{Z(R_m)\}$,

$$D_{ec} : \left| \begin{array}{ccc} F & \longrightarrow & E \\ c & \longmapsto & K^{-1*} * \widetilde{c} * K \end{array} \right.$$

4.3.2.3 Security of this protocol

We designed a encryption scheme that is one the alternatives to resist quantum attacks, it depends on two difficult problems are problem of discerte logarithm and problem of conjugal on a non commutative ring . The security of our cryptosystem over the non commutative ring R_m is very strong and secure because it based on two problems DLP and CCP which are very difficult to solve.
If another person wants to compute the secret key K, it must solve the following problem $K_i = \sum_{j=1}^{3} b_i a_j P = \sum_{j=1}^{3} a_j b_i P$ for $1 \leq i \leq 3$, this problem is very difficult to solve, and if he wants to compute message m, it must solve the conjugal problem.

4.3.3 Numerical example of cryptography

Alice and Bob agree on a prime number $p = 7$ and a point $P = [3\varepsilon^2 + 5\varepsilon + 6 : 1 : 3\varepsilon^3 + 5\varepsilon^2 + 3\varepsilon + 3]$ generating the subgroup G of order $l = 35$ of elliptic curve $E_{a,b}(\mathbb{F}_7[\varepsilon])$, where $a = 2\varepsilon^3 + 1, b = 2\varepsilon^3 + 3\varepsilon^2 + \varepsilon + 1$ in $\mathbb{F}_7[\varepsilon]$. The subgroup of $G =< P >$ is shown as follows:

n	nP	n	nP
1	$[3\varepsilon^2 + 5\varepsilon + 6 : 1 : 3\varepsilon^3 + 5\varepsilon^2 + 3\varepsilon + 3]$	19	$[4\varepsilon^3+6\varepsilon^2+3\varepsilon+1 : 1 : 4\varepsilon^3+4\varepsilon^2+2\varepsilon+4]$
2	$[5\varepsilon^3 + 3\varepsilon^2 + 6\varepsilon : 1 : \varepsilon^3 + 6\varepsilon^2 + \varepsilon + 6]$	20	$[5\varepsilon^3 + \varepsilon^2 + \varepsilon : 1 : 0]$
3	$[5\varepsilon^3 + 5\varepsilon^2 + 4\varepsilon : 1 : 2\varepsilon^3 + 3\varepsilon^2 + \varepsilon + 1]$	21	$[6\varepsilon^3 + 3\varepsilon^2 + 6\varepsilon + 6 : 1 : 3\varepsilon^2 + \varepsilon + 3]$
4	$[6\varepsilon^3 + 3\varepsilon^2 + 4\varepsilon + 1 : 1 : 3\varepsilon^2 + 4]$	22	$[3\varepsilon^2 + 4\varepsilon : 1 : 2\varepsilon^3 + 4\varepsilon^2 + 2\varepsilon + 6]$
5	$[3\varepsilon^3 + 2\varepsilon^2 + 2\varepsilon : 1 : 0]$	23	$[6\varepsilon^3 + 6\varepsilon^2 + 2\varepsilon : 1 : 4\varepsilon^3 + 2\varepsilon + 1]$
6	$[\varepsilon^2 + 6 : 1 : \varepsilon^3 + 4\varepsilon^2 + 6\varepsilon + 3]$	24	$[6\varepsilon^3+2\varepsilon^2+5\varepsilon+1 : 1 : 6\varepsilon^3+6\varepsilon^2+5\varepsilon+4]$
7	$[5\varepsilon^2 + 2\varepsilon : 1 : 5\varepsilon^3 + 3\varepsilon + 6]$	25	$[\varepsilon^3 + 3\varepsilon^2 + 3\varepsilon : 1 : 0]$

8	$[2\varepsilon^3+5\varepsilon^2:1:4\varepsilon^3+6\varepsilon^2+3\varepsilon+1]$	26	$[3\varepsilon^3+4\varepsilon^2+\varepsilon+6:1:6\varepsilon^3+\varepsilon^2+4\varepsilon+3]$
9	$[4\varepsilon^3+3\varepsilon^2+6\varepsilon+1:1:\varepsilon^3+6\varepsilon^2+3\varepsilon+4]$	27	$[5\varepsilon^3+2\varepsilon^2:1:3\varepsilon^3+\varepsilon^2+4\varepsilon+6]$
10	$[6\varepsilon^3+4\varepsilon^2+4\varepsilon:1:0]$	28	$[2\varepsilon^2+5\varepsilon:1:2\varepsilon^3+4\varepsilon+1]$
11	$[\varepsilon^3+5\varepsilon^2+2\varepsilon+6:1:\varepsilon^3+\varepsilon^2+2\varepsilon+3]$	29	$[6\varepsilon^2+1:1:6\varepsilon^3+3\varepsilon^2+\varepsilon+4]$
12	$[\varepsilon^3+\varepsilon^2+5\varepsilon:1:3\varepsilon^3+5\varepsilon+6]$	30	$[4\varepsilon^3+5\varepsilon^2+5\varepsilon:1:0]$
13	$[4\varepsilon^2+3\varepsilon:1:5\varepsilon^3+3\varepsilon^2+5\varepsilon+1]$	31	$[\varepsilon^3+4\varepsilon^2+3\varepsilon+6:1:4\varepsilon^2+3]$
14	$[\varepsilon^3+4\varepsilon^2+\varepsilon+1:1:4\varepsilon^2+6\varepsilon+4]$	32	$[2\varepsilon^3+2\varepsilon^2+3\varepsilon:1:5\varepsilon^3+4\varepsilon^2+6\varepsilon+6]$
15	$[2\varepsilon^3+6\varepsilon^2+6\varepsilon:1:0]$	33	$[2\varepsilon^3+4\varepsilon^2+\varepsilon,1,6\varepsilon^3+\varepsilon^2+6\varepsilon+1]$
16	$[3\varepsilon^3+\varepsilon^2+4\varepsilon+6:1:3\varepsilon^3+3\varepsilon^2+5\varepsilon+3]$	34	$[4\varepsilon^2+2\varepsilon+1:1:4\varepsilon^3+2\varepsilon^2+4\varepsilon+4]$
17	$[\varepsilon^3+5\varepsilon^2+\varepsilon:1:2\varepsilon^3+6\varepsilon^2+6]$	35	$[0:1:0]=\infty$
18	$[6\varepsilon^3+2\varepsilon^2+6\varepsilon:1:5\varepsilon^3+\varepsilon^2+1]$		

- $(x_1,x_2,x_3)=(2,6,3)\in\{0,1,...,34\}^3$ is a public and $\gcd(x_i,35)=1$, for $1\leqslant i\leqslant 3$.
- Alice chooses three private random integers are all different less than $ord(P)$:
$$\begin{cases} a_1=5 \\ a_2=7 \\ a_3=10 \end{cases} \xrightarrow{\text{and sends}} \begin{cases} 5P \\ 7P \\ 10P \end{cases} \text{ to Bob.}$$
- Bob chooses three private random integers are all different less than $ord(P)$:
$$\begin{cases} b_1=4 \\ b_2=9 \\ b_3=13 \end{cases} \xrightarrow{\text{and sends by the order}} \begin{cases} 4P \\ 9P \\ 13P \end{cases} \text{ to Alice.}$$
- Alice calculates:
$K_1=5\times 4P+7\times 4P+10\times 4P=18P=[6\varepsilon^3+2\varepsilon^2+6\varepsilon:1:5\varepsilon^3+\varepsilon^2+1]$;
$K_2=5\times 9P+7\times 9P+10\times 9P=23P=[6\varepsilon^3+6\varepsilon^2+2\varepsilon:1:4\varepsilon^3+2\varepsilon+1]$;
$K_3=5\times 13P+7\times 13P+10\times 13P=6P=[\varepsilon^2+6:1:\varepsilon^3+4\varepsilon^2+6\varepsilon+3]$.
- Bob calculates:
$K_1=4\times 5P+4\times 7P+4\times 10P=18P=[6\varepsilon^3+2\varepsilon^2+6\varepsilon:1:5\varepsilon^3+\varepsilon^2+1]$;
$K_2=9\times 5P+9\times 7P+9\times 10P=23P=[6\varepsilon^3+6\varepsilon^2+2\varepsilon:1:4\varepsilon^3+2\varepsilon+1]$;
$K_3=13\times 5P+13\times 7P+13\times 10P=6P=[\varepsilon^2+6:1:\varepsilon^3+4\varepsilon^2+6\varepsilon+3]$.
- The secret key between Alice and Bob is $K=\begin{bmatrix}2 & K_1 & K_2\\ 0 & 6 & K_3\\ 0 & 0 & 3\end{bmatrix}$. The inverse of K is:
$$K^{-1*}=\begin{bmatrix}2^{-1} & -2^{-1}6^{-1}K_1 & -2^{-1}3^{-1}K_2\\ 0 & 6^{-1} & -6^{-1}3^{-1}K_3\\ 0 & 0 & 3^{-1}\end{bmatrix}=\begin{bmatrix}18 & 32K_1 & 29K_2\\ 0 & 6 & 33K_3\\ 0 & 0 & 12\end{bmatrix}=\begin{bmatrix}18 & S_1 & S_2\\ 0 & 6 & S_3\\ 0 & 0 & 12\end{bmatrix},$$
where:

$S_1 = 32K_1 = 32 \times 18P = 16P = [3\varepsilon^3 + \varepsilon^2 + 4\varepsilon + 6 : 1 : 3\varepsilon^3 + 3\varepsilon^2 + 5\varepsilon + 3]$,
$S_2 = 29K_2 = 29 \times 23P = 2P = [5\varepsilon^3 + 3\varepsilon^2 + 6\varepsilon : 1 : \varepsilon^3 + 6\varepsilon^2 + \varepsilon + 6]$,
$S_3 = 33K_3 = 33 \times 6P = 23P = [6\varepsilon^3 + 6\varepsilon^2 + 2\varepsilon : 1 : 4\varepsilon^3 + 2\varepsilon + 1]$.

❖ To encrypt a message $m = \begin{bmatrix} 20 & 19P & 14P \\ 0 & 31 & 27P \\ 0 & 0 & 26 \end{bmatrix} \in R_m$, we compute:

$c = E_{nc}(m) = \widetilde{K * m * K^{-1*}}$, we have:

$$K * m * K^{-1*} = \begin{bmatrix} 2 & K_1 & K_2 \\ 0 & 6 & K_3 \\ 0 & 0 & 3 \end{bmatrix} * \begin{bmatrix} 20 & 19P & 14P \\ 0 & 31 & 27P \\ 0 & 0 & 26 \end{bmatrix} * \begin{bmatrix} 18 & S_1 & S_2 \\ 0 & 6 & S_3 \\ 0 & 0 & 12 \end{bmatrix}$$
$$= \begin{bmatrix} 5 & P & 31P \\ 0 & 11 & 3P \\ 0 & 0 & 8 \end{bmatrix} * \begin{bmatrix} 18 & S_1 & S_2 \\ 0 & 6 & S_3 \\ 0 & 0 & 12 \end{bmatrix}$$
$$= \begin{bmatrix} 5 & P & 31P \\ 0 & 11 & 3P \\ 0 & 0 & 8 \end{bmatrix} * \begin{bmatrix} 18 & 16P & 2P \\ 0 & 6 & 23P \\ 0 & 0 & 12 \end{bmatrix} = \begin{bmatrix} 20 & 16P & 32P \\ 0 & 31 & 9P \\ 0 & 0 & 26 \end{bmatrix}.$$

Then the ciphertext is: $c = \widetilde{\begin{bmatrix} 20 & 16P & 32P \\ 0 & 31 & 9P \\ 0 & 0 & 26 \end{bmatrix}} = \begin{bmatrix} 26 & 9P & 32P \\ 0 & 31 & 16P \\ 0 & 0 & 20 \end{bmatrix}$.

❖ To decrypt a ciphertext $c = \begin{bmatrix} 26 & 9P & 32P \\ 0 & 31 & 16P \\ 0 & 0 & 20 \end{bmatrix} \in R_m$, we compute:

$$m = K^{-1*} * \tilde{c} * K = \begin{bmatrix} 18 & S_1 & S_2 \\ 0 & 6 & S_3 \\ 0 & 0 & 12 \end{bmatrix} * \begin{bmatrix} 20 & 16P & 32P \\ 0 & 31 & 9P \\ 0 & 0 & 26 \end{bmatrix} * \begin{bmatrix} 2 & K_1 & K_2 \\ 0 & 6 & K_3 \\ 0 & 0 & 3 \end{bmatrix}$$
$$= \begin{bmatrix} 10 & 14P & 33P \\ 0 & 11 & 22P \\ 0 & 0 & 32 \end{bmatrix} * \begin{bmatrix} 2 & 18P & 23P \\ 0 & 6 & 6P \\ 0 & 0 & 3 \end{bmatrix} = \begin{bmatrix} 20 & 19P & 14P \\ 0 & 31 & 27P \\ 0 & 0 & 26 \end{bmatrix}.$$

Then the plaintext is: $m = \begin{bmatrix} 20 & 19P & 14P \\ 0 & 31 & 27P \\ 0 & 0 & 26 \end{bmatrix}$.

Chapter 5

Encryption scheme based on a local ring

"We consider $A_4 := \mathbb{F}_{3^d}[X]/(X^4)$ is a finite local ring, where $\varepsilon^4 = 0$. In this chapter, we show (in the sections 5.1 and 5.2) the fundamental results of the article [32] about an elliptic curve over this ring and classification of their elements, then the group law. We focus on giving a numerical cryptographic application (encryption and decryption) by two methods with using an encoding of the elements of a cyclic subgroup G generated by a point P of known order [70]."
For more information about ECC based on the finite rings, see the following articles: [1] [15–17]; [30, 31] and [84].

Contents in Brief

5.1 The finite ring A_4 111
5.2 Elliptic curve over the ring A_4 111
5.2.1 Classification of elements in $E^4_{a,b}$ 111
5.2.2 The group law over $E^4_{a,b}$ 112
5.3 Cryptographic protocols 112
5.3.1 Exchange of secret key 113
5.3.2 Encryption and decryption functions 113
5.4 Cryptographic application 114
5.4.1 Coding of elements of G 114
5.4.2 Example for cryptography 115

5.1 The finite ring A_4

Let d be a positive integer. We consider the quotient ring $A_4 = \mathbb{F}_{3^d}[X]/(X^4)$ where $\mathbb{F}_{3^d}$ is the finite field of order 3^d. Then the ring A_4 is identified to the ring $\mathbb{F}_{3^d}[\varepsilon]$, $\varepsilon^4 = 0$. So we have:

$$A_4 = \{\sum_{i=0}^{3} x_i\varepsilon^i \mid (x_i)_{0\leqslant i\leqslant 3} \in \mathbb{F}_{3^d}\}.$$

Lemma 5.1. *We have the following lemmas:*

1. *Let $X = \sum_{i=0}^{3} x_i\varepsilon^i$. The element X is invertible in A_4 if and only if $x_0 \neq 0$.*
2. *A_4 is a local ring, it's maximal ideal is $I_4 = (\varepsilon)$.*
3. *A_4 is a vector space over $\mathbb{F}_{3^d}$ and have $(1, \varepsilon, \varepsilon^2, \varepsilon^3)$ as basis.*

Definition 5.1. Let π the canonical projection of elements in the ring A_4 defined by:

$$\pi : \left| \begin{array}{ccc} A_4 & \longrightarrow & \mathbb{F}_{3^d} \\ \sum_{i=0}^{3} x_i\varepsilon^i & \longmapsto & x_0 \end{array} \right.$$

5.2 Elliptic curve over the ring A_4

Definition 5.2. We consider the elliptic curve over the ring A_4 which is given by the equation $Y^2Z = X^3 + aX^2Z + bZ^3$, where $a, b \in A_4$ and the discriminant $\triangle = -a^3b$ is invertible in A_4, and denoted by $E^4_{a,b}$. So we have:

$$E^4_{a,b} = \{[X : Y : Z] \in \mathbb{P}^2(A_4) \mid Y^2Z = X^3 + aX^2Z + bZ^3\}.$$

5.2.1 Classification of elements in $E^4_{a,b}$

Proposition 5.1. *Every element in $E^4_{a,b}$ is of the form $[X : Y : 1]$ (where X or $Y \in A_4 \setminus I_4$), or $[X : 1 : Z]$ where $X, Z \in I_4$ and we write:*

$$\begin{aligned} E^4_{a,b} = &\{[X : Y : 1] \mid Y^2 = X^3 + aX^2 + b, \text{and } X \text{or} Y \notin I_4\} \\ &\cup \{[X : 1 : Z] \mid Z = X^3 + aX^2Z + bZ^3, \text{and } X, Z \in I_4\}. \end{aligned}$$

Proof. See [32]. □

Lemma 5.2. *Let* $[X : 1 : Z] \in E^4_{a,b}$ *where* $X, Z \in (\varepsilon)$. *If* $X = x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3$, *then* $[X : 1 : Z] = [X : 1 : x_1^3\varepsilon^3]$.

5.2.2 The group law over $E^4_{a,b}$

After classifying the elements of $E^4_{a,b}$, we will define the group law over the ring A_4. We consider firstly the mapping $\widetilde{\pi}$:

$$\widetilde{\pi} : \left| \begin{array}{ccc} E^4_{a,b} & \longrightarrow & E^1_{\pi(a),\pi(b)} \\ [X : Y : Z] & \longmapsto & [\pi(X) : \pi(Y) : \pi(Z)] \end{array} \right.$$

Theorem 5.1. *Let* $P = [X_1 : Y_1 : Z_1]$ *and* $Q = [X_2 : Y_2 : Z_2]$ *be two points in* $E^4_{a,b}$, *and* $P + Q = [X_3 : Y_3 : Z_3]$.

- *If* $\widetilde{\pi}(P) = \widetilde{\pi}(Q)$, *then:*
  $X_3 = Y_1Y_2^2X_1 + Y_1^2Y_2X_2 + 2aX_1^2X_2Y_2 + 2aX_1X_2^2Y_1 + 2abZ_1Z_2^2Y_1 + 2abZ_1^2Z_2Y_2.$
  $Y_3 = Y_1^2Y_2^2 + 2a^2X_1^2X_2^2 + a^2bX_1Z_1Z_2^2 + a^2bX_2Z_1^2Z_2.$
  $Z_3 = aX_1X_2(Y_1Z_2 + Y_2Z_1) + a(X_1Y_2 + X_2Y_1)(X_1Z_2 + X_2Z_1) + Y_1Y_2(Y_1Z_2 + Y_2Z_1).$

- *If* $\widetilde{\pi}(P) \neq \widetilde{\pi}(Q)$, *then:*
  $X_3 = 2X_1Y_2Y_1Z_2 + X_1Y_2^2Z_1 + 2X_2Y_1^2Z_2 + X_2Y_1Y_2Z_1 + 2aX_1^2X_2Z_2 + aX_1X_2^2Z_1.$
  $Y_3 = 2Y_1^2Y_2Z_2 + Y_1Y_2^2Z_1 + 2aX_1X_2Y_1Z_2 + aX_1X_2Y_2Z_1 + 2aX_1^2Y_2Z_2 + aX_2^2Y_1Z_1.$
  $Z_3 = 2Y_1^2Z_2^2 + Y_2^2Z_1^2 + aX_1^2Z_2^2 + 2aX_2^2Z_1^2.$

Proof. By using the explicit formulas in W. Bosma and H. Lenstra article see [8][p.236-238], we prove the theorem. □

Lemma 5.3. *The mapping* $\widetilde{\pi}$ *is a surjective homomorphism of groups.*

5.3 Cryptographic protocols

In this section we describe, key generation and we provide a construct an encryption and decryption schemes using the ring A_4.

5.3.1 Exchange of secret key

Using the Diffie-Hellman key exchange mentioned in the subsection 3.6.2. We have the following protocol for exchange of secret key based on $E^4_{a,b}$:

- Alice and Bob agree on a prime number p, a point P generating subgroup of known order of the elliptic curve $E_{a,b}(A_4)$ and $(a, b) \in A_4 \times A_4$.
- Alice chooses a private random integer $K_A < ord(P)$ and sends $Y_A = K_A P$ to Bob.
- Bob chooses a private random integer $K_B < ord(P)$ and sends $Y_B = K_B P$ to Alice.
- Alice calculates: $K_A Y_B$.
- Bob calculates: $K_B Y_A$.
- The common secret key: $K = K_A K_B P = K_B K_A P$.

5.3.2 Encryption and decryption functions

We will consider two-party key agreement protocols derived from the basic Diffie-Hellman protocol. Alice and Bob chooses an elliptic curve over the ring A_4 and a secret key K in $E^4_{a,b}$.
To encrypt a message m in $E^4_{a,b}$, Alice calculate: $C = Enc(m) = m + K$.
To decrypt a ciphertext c in $E^4_{a,b}$, Bob calculate: $M = Dec(c) = c - K$.
Cryptosystem based on A_4:

- Space of lights: $L = E^4_{a,b}$.
- Space of quantified: $F = E^4_{a,b}$.
- Space of keys: $E^4_{a,b}$.
- Function of encryption: $\forall K \in E^4_{a,b}$,

$$Enc : \left| \begin{array}{ccc} L & \longrightarrow & F \\ m & \longmapsto & m + K \end{array} \right.$$

- Function of decryption: $\forall K \in E^4_{a,b}$,

$$Dec : \left| \begin{array}{ccc} F & \longrightarrow & L \\ c & \longmapsto & c - K \end{array} \right.$$

We have:

$$Dec \circ Enc(m) = m, \quad \forall m \in E^4_{a,b}.$$

Remark 5.1. The proposed diagram is very safe because it guarantees the authentication thanks to the key K calculated by the method of D-H which is based on the problem of the discrete logarithm on the elliptic curves in question.

5.4 Cryptographic application

Let $E^4_{a,b}$ be an elliptic curve over the ring A_4 and an irreducible polynomial $H(X) = X^3 + 2X^2 + 1$ in $\mathbb{F}_3[X]$. The polynomial $H(X)$ has no roots in the $\mathbb{F}_3$ because $H(0) = H(1) = 1, H(2) = 2$ but there exists an α where $H(\alpha) = 0$ in $\mathbb{F}_{27} = \dfrac{\mathbb{F}_3[X]}{(H(X))}$ so $(1, \alpha, \alpha^2)$ is a basis of the vector space $\mathbb{F}_{27}$ over $\mathbb{F}_3$.
Let a and b in $\mathbb{F}_{27}[\varepsilon]$, so we have:

$$E_{a,b}(\mathbb{F}_{27}[\varepsilon]) = \{[X : Y : Z] \in \mathbb{P}^2(\mathbb{F}_{27}[\varepsilon]) \mid Y^2Z = X^3 + aX^2Z + bZ^3\}.$$

Let $P = [X : Y : Z] \in E_{a,b}(\mathbb{F}_{27}[\varepsilon])$ of order n, we will use the subgroup $\langle P \rangle$ of $E_{a,b}(\mathbb{F}_{27}[\varepsilon])$ to encrypt messages, and we denote $G = \langle P \rangle$.

5.4.1 Coding of elements of G

We will give a code to each element $Q = tP$ where $t \in \{1, 2, ..., n\}$ defined as following:
Assume $Q = [x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 : y_0 + y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3 : Z]$ where $x_i, y_i \in \mathbb{F}_{27}$ for $i \in \{0, 1, 2, 3\}$ and $Z = 0$ or $Z = 1$, we set:

$$\begin{aligned} x_i &= e_{0i} + e_{1i}\alpha + e_{2i}\alpha^2, \\ y_i &= r_{0i} + r_{1i}\alpha + r_{2i}\alpha^2, \end{aligned}$$

where α is a primitive root of an irreducible polynomial of degree 3 over $\mathbb{F}_3$ and $e_{ij}, r_{ij} \in \mathbb{F}_3$, then we code Q as it follows:

- If $Z = 1$,then:
  $Q = e_{00}e_{10}e_{20}e_{01}e_{11}e_{21}e_{02}e_{12}e_{22}e_{03}e_{13}e_{23}r_{00}r_{10}r_{20}r_{01}r_{11}r_{21}r_{02}r_{12}r_{22}r_{03}r_{13}r_{23}1.$
- If $Z = 0$, then:
  $Q = e_{00}e_{10}e_{20}e_{01}e_{11}e_{21}e_{02}e_{12}e_{22}e_{03}e_{13}e_{23}r_{00}r_{10}r_{20}r_{01}r_{11}r_{21}r_{02}r_{12}r_{22}r_{03}r_{13}r_{23}0.$

5.4.2 Example for cryptography

Let $a = 1+\alpha+\alpha\varepsilon+\varepsilon^2+2\varepsilon^3$ and $b = 1+\alpha^2+\alpha^2\varepsilon+\varepsilon^2+(1+\alpha+\alpha^2)\varepsilon^3$ are two elements in $\mathbb{F}_{27}[\varepsilon]$. One will not explicitly write all the points of the curve, but only the points of the subgroup $G = \langle P\rangle$ which one will use to encrypt and decipher the messages. We consider the point $P = [2+\varepsilon+\varepsilon^2+2\varepsilon^3 : 1+2\alpha+(2\alpha^2+\alpha)\varepsilon+(2\alpha^2+1)\varepsilon^2+(2\alpha^2+1)\varepsilon^3 : 1]$, we have $G = \langle P\rangle$ is the subgroup of order 63. So, for $Q \in G$, $\exists t \in \{1, 2, \ldots, 63\}$: $Q = tP$. The points of G are:

n	nP
1	$[2+\varepsilon+\varepsilon^2+2\varepsilon^3 : 1+2\alpha+(2\alpha^2+\alpha)\varepsilon+(2\alpha^2+1)\varepsilon^2+(2\alpha^2+1)\varepsilon^3 : 1]$
2	$[\alpha+1+2\varepsilon+(\alpha+2)\varepsilon^2+\alpha^2\varepsilon^3 : 1+\alpha^2\varepsilon+\alpha^2\varepsilon^2+(\alpha+1)\varepsilon^3 : 1]$
3	$[2+2\alpha^2+(2\alpha^2+2)\varepsilon+(\alpha+1)\varepsilon^2 : 2\alpha+(\alpha+1)\varepsilon+(2\alpha+2\alpha^2)\varepsilon^2+\varepsilon^3 : 1]$
4	$[2+2\alpha^2+(\alpha^2+1)\varepsilon+(2\alpha+2)\varepsilon^2+(\alpha^2+\alpha+1)\varepsilon^3 : \alpha+(\alpha+1)\varepsilon+(2\alpha^2+2)\varepsilon^2+(2\alpha+1)\varepsilon^3 : 1]$
5	$[\alpha+1+(2\alpha^2+2\alpha+2)\varepsilon+(\alpha^2+2)\varepsilon^2+(2\alpha^2+1)\varepsilon^3 : 2+2\varepsilon+(\alpha^2+\alpha)\varepsilon^2+(\alpha^2+2\alpha+2)\varepsilon^3 : 1]$
6	$[2+(\alpha^2+2\alpha)\varepsilon+(2\alpha^2+\alpha+2)\varepsilon^2 : \alpha+2+(\alpha^2+\alpha+1)\varepsilon+(\alpha^2+2\alpha)\varepsilon^2+\varepsilon^3 : 1]$
7	$[(\alpha^2+\alpha)\varepsilon+(2\alpha^2+\alpha+1)\varepsilon^2+2\alpha^2\varepsilon^3 : 1 : 0]$
8	$[2+(2\alpha^2+\alpha+2)\varepsilon+\varepsilon^2+(\alpha^2+2\alpha+2)\varepsilon^3 : 2\alpha+1+(2\alpha^2+1)\varepsilon+(2\alpha+2)\varepsilon^2+(\alpha^2+2)\varepsilon^3 : 1]$
9	$[1+\alpha+(\alpha^2+\alpha+2)\varepsilon+(2\alpha+1)\varepsilon^3 : 1+(2\alpha^2+2)\varepsilon+(\alpha^2+2)\varepsilon^2+\alpha\varepsilon^3 : 1]$
10	$[2\alpha^2+2+(2\alpha+1)\varepsilon^2+(2\alpha^2+2)\varepsilon^3 : 2\alpha+2\alpha\varepsilon^2+(2\alpha^2+\alpha)\varepsilon^3 : 1]$
11	$[2+2\alpha^2+(2\alpha+1)\varepsilon^2+(\alpha+2)\varepsilon^3 : \alpha+\alpha\varepsilon^2+(2\alpha^2+\alpha+2)\varepsilon^3 : 1]$
12	$[\alpha+1+(\alpha^2+\alpha+2)\varepsilon+\alpha\varepsilon^3 : 2+(\alpha^2+1)\varepsilon+(2\alpha^2+1)\varepsilon^2+(\alpha^2+2\alpha)\varepsilon^3 : 1]$
13	$[2+(2\alpha^2+\alpha+2)\varepsilon+\varepsilon^2+\varepsilon^3 : 2+\alpha+(\alpha^2+2)\varepsilon+(\alpha+1)\varepsilon^2+(\alpha^2+2\alpha+2)\varepsilon^3 : 1]$
14	$[(2\alpha^2+2\alpha)\varepsilon+(\alpha^2+2\alpha+2)\varepsilon^2+(2\alpha^2+\alpha+2)\varepsilon^3 : 1 : 0]$
15	$[2+(\alpha^2+2\alpha)\varepsilon+(2\alpha^2+\alpha+2)\varepsilon^2+(2\alpha+2)\varepsilon^3 : 1+2\alpha+(2\alpha^2+2\alpha+2)\varepsilon+(2\alpha^2+\alpha)\varepsilon^2+(\alpha^2+\alpha+2)\varepsilon^3 : 1]$
16	$[1+\alpha+(2\alpha^2+2\alpha+2)\varepsilon+(\alpha^2+2)\varepsilon^2+(2\alpha+2)\varepsilon^3 : 1+\varepsilon+(2\alpha^2+2\alpha)\varepsilon^2+(\alpha^2+\alpha+2)\varepsilon^3 : 1]$
17	$[2+2\alpha^2+(\alpha^2+1)\varepsilon+(2\alpha+2)\varepsilon^2+(2\alpha^2+2\alpha)\varepsilon^3 : 2\alpha+(2\alpha+2)\varepsilon+(\alpha^2+1)\varepsilon^2+(2\alpha^2+\alpha+1)\varepsilon^3 : 1]$
18	$[2+2\alpha^2+(2\alpha^2+2)\varepsilon+(\alpha+1)\varepsilon^2+(\alpha^2+1)\varepsilon^3 : \alpha+(2\alpha+2)\varepsilon+(\alpha^2+\alpha)\varepsilon^2+\varepsilon^3 : 1]$
19	$[\alpha+1+2\varepsilon+(\alpha+2)\varepsilon^2+(\alpha^2+2)\varepsilon^3 : 2+2\alpha^2\varepsilon+2\alpha^2\varepsilon^2+(\alpha^2+\alpha+1)\varepsilon^3 : 1]$
20	$[2+\varepsilon+\varepsilon^2+(\alpha^2+\alpha+1)\varepsilon^3 : \alpha+2+(\alpha^2+2\alpha)\varepsilon+(\alpha^2+2)\varepsilon^2+(2\alpha^2+2)\varepsilon^3 : 1]$
21	$[(2\alpha^2+\alpha+2)\varepsilon^3 : 1 : 0]$
22	$[2+\varepsilon+\varepsilon^2+(2\alpha^2+2\alpha)\varepsilon^3 : 1+2\alpha+(2\alpha^2+\alpha)\varepsilon+(2\alpha^2+1)\varepsilon^2+\varepsilon^3 : 1]$
23	$[1+\alpha+2\varepsilon+(\alpha+2)\varepsilon^2+(\alpha+2)\varepsilon^3 : 1+\alpha^2\varepsilon+\alpha^2\varepsilon^2+(\alpha^2+\alpha+2)\varepsilon^3 : 1]$

24	$[2\alpha^2+2+(2\alpha^2+2)\varepsilon+(\alpha+1)\varepsilon^2+(\alpha+2)\varepsilon^3 : 2\alpha+(\alpha+1)\varepsilon+(2\alpha^2+2\alpha)\varepsilon^2+(2\alpha^2+2\alpha)\varepsilon^3 : 1]$
25	$[2\alpha^2+2+(\alpha^2+1)\varepsilon+(2\alpha+2)\varepsilon^2+(\alpha^2+2)\varepsilon^3 : \alpha+(\alpha+1)\varepsilon+(2\alpha^2+2)\varepsilon^2+(2\alpha^2+\alpha)\varepsilon^3 : 1]$
26	$[1+\alpha+(2\alpha^2+2\alpha+2)\varepsilon+(\alpha^2+2)\varepsilon^2+(2\alpha+2)\varepsilon^3 : 2+2\varepsilon+(\alpha^2+\alpha)\varepsilon^2+(2\alpha^2+2\alpha)\varepsilon^3 : 1]$
27	$[2+(\alpha^2+2\alpha)\varepsilon+(2\alpha^2+\alpha+2)\varepsilon^2+(\alpha^2+\alpha+2)\varepsilon^3 : \alpha+2+(\alpha^2+\alpha+1)\varepsilon+(\alpha^2+2\alpha)\varepsilon^2+(\alpha^2+1)\varepsilon^3 : 1]$
28	$[(\alpha^2+\alpha)\varepsilon+(2\alpha^2+\alpha+1)\varepsilon^2+(\alpha^2+\alpha+2)\varepsilon^3 : 1 : 0]$
29	$[2+(2\alpha^2+\alpha+2)\varepsilon+\varepsilon^2+\alpha\varepsilon^3 : 2\alpha+1+(2\alpha^2+1)\varepsilon+(2\alpha+2)\varepsilon^2+(2\alpha^2+2)\varepsilon^3 : 1]$
30	$[\alpha+1+(\alpha^2+\alpha+2)\varepsilon+2\alpha^2\varepsilon^3 : 1+(2\alpha^2+2)\varepsilon+(\alpha^2+2)\varepsilon^2+(\alpha^2+\alpha+1)\varepsilon^3 : 1]$
31	$[2\alpha^2+2+(2\alpha+1)\varepsilon^2+(2\alpha^2+\alpha+1)\varepsilon^3 : 2\alpha+2\alpha\varepsilon^2+(\alpha^2+2)\varepsilon^3 : 1]$
32	$[2\alpha^2+2+(2\alpha+1)\varepsilon^2 : \alpha+\alpha\varepsilon^2+(\alpha^2+1)\varepsilon^3 : 1]$
33	$[\alpha+1+(\alpha^2+\alpha+2)\varepsilon+(\alpha^2+1)\varepsilon^3 : 2+(\alpha^2+1)\varepsilon+(2\alpha^2+1)\varepsilon^2+(2\alpha^2+2\alpha+1)\varepsilon^3 : 1]$
34	$[2+(2\alpha^2+\alpha+2)\varepsilon+\varepsilon^2+(\alpha^2+\alpha)\varepsilon^3 : 2+\alpha+(\alpha^2+2)\varepsilon+(\alpha+1)\varepsilon^2+(2\alpha^2+2\alpha+2)\varepsilon^3 : 1]$
35	$[(2\alpha^2+2\alpha)\varepsilon+(\alpha^2+2\alpha+2)\varepsilon^2+(\alpha^2+2\alpha+1)\varepsilon^3 : 1 : 0]$
36	$[2+(\alpha^2+2\alpha)\varepsilon+(2\alpha^2+\alpha+2)\varepsilon^2+(2\alpha^2+\alpha)\varepsilon^3 : 2\alpha+1+(2\alpha^2+2\alpha+2)\varepsilon+(2\alpha^2+\alpha)\varepsilon^2+(2\alpha^2+\alpha+2)\varepsilon^3 : 1]$
37	$[\alpha+1+(2\alpha^2+2\alpha+2)\varepsilon+(\alpha^2+2)\varepsilon^2+(2\alpha+1)\varepsilon^3 : 1+\varepsilon+(2\alpha^2+2\alpha)\varepsilon^2+(2\alpha^2+\alpha)\varepsilon^3 : 1]$
38	$[2\alpha^2+2+(\alpha^2+1)\varepsilon+(2\alpha+2)\varepsilon^2+(2\alpha^2+2)\varepsilon^3 : 2\alpha+(2\alpha+2)\varepsilon+(\alpha^2+1)\varepsilon^2+\alpha^2\varepsilon^3 : 1]$
39	$[2\alpha^2+2+(2\alpha^2+2)\varepsilon+(\alpha+1)\varepsilon^2+(\alpha^2+2\alpha+2)\varepsilon^3 : \alpha+(2\alpha+2)\varepsilon+(\alpha^2+\alpha)\varepsilon^2+(2\alpha^2+2\alpha)\varepsilon^3 : 1]$
40	$[\alpha+1+2\varepsilon+(\alpha+2)\varepsilon^2+(2\alpha^2+2\alpha)\varepsilon^3 : 2+2\alpha^2\varepsilon+2\alpha^2\varepsilon^2+(2\alpha^2+\alpha+2)\varepsilon^3 : 1]$
41	$[2+\varepsilon+\varepsilon^2+(2\alpha^2+2\alpha)\varepsilon^3 : \alpha+2+(\alpha^2+2\alpha)\varepsilon+(\alpha^2+2)\varepsilon^2+2\varepsilon^3 : 1]$
42	$[(\alpha^2+2\alpha+1)\varepsilon^3 : 1 : 0]$
43	$[2+\varepsilon+\varepsilon^2+(\alpha^2+\alpha+1)\varepsilon^3 : 1+2\alpha+(2\alpha^2+\alpha)\varepsilon+(2\alpha^2+1)\varepsilon^2+(\alpha^2+1)\varepsilon^3 : 1]$
44	$[\alpha+1+2\varepsilon+(\alpha+2)\varepsilon^2+(2\alpha^2+2\alpha+1)\varepsilon^3 : 1+\alpha^2\varepsilon+\alpha^2\varepsilon^2+(2\alpha^2+\alpha)\varepsilon^3 : 1]$
45	$[2\alpha^2+2+(2\alpha^2+2)\varepsilon+(\alpha+1)\varepsilon^2+(2\alpha+1)\varepsilon^3 : 2\alpha+(\alpha+1)\varepsilon+(2\alpha^2+2\alpha)\varepsilon^2+(\alpha^2+\alpha+2)\varepsilon^3 : 1]$
46	$[2\alpha^2+2+(\alpha^2+1)\varepsilon+(2\alpha+2)\varepsilon^2+(\alpha^2+2\alpha)\varepsilon^3 : \alpha+(\alpha+1)\varepsilon+(2\alpha^2+2)\varepsilon^2+(\alpha^2+2)\varepsilon^3 : 1]$
47	$[1+\alpha+(2\alpha^2+2\alpha+2)\varepsilon+(\alpha^2+2)\varepsilon^2+(\alpha^2+\alpha)\varepsilon^3 : 2+2\varepsilon+(\alpha^2+\alpha)\varepsilon^2+(2\alpha+1)\varepsilon^3 : 1]$
48	$[2+(\alpha^2+2\alpha)\varepsilon+(2\alpha^2+\alpha+2)\varepsilon^2+(2\alpha^2+2\alpha+1)\varepsilon^3 : \alpha+2+(\alpha^2+\alpha+1)\varepsilon+(\alpha^2+2\alpha)\varepsilon^2+(2\alpha^2+1)\varepsilon^3 : 1]$
49	$[(\alpha^2+\alpha)\varepsilon+(2\alpha^2+\alpha+1)\varepsilon^2+(2\alpha+1)\varepsilon^3 : 1 : 0]$
50	$[2+(2\alpha^2+\alpha+2)\varepsilon+\varepsilon^2+(2\alpha^2+1)\varepsilon^3 : 2\alpha+1+(2\alpha^2+1)\varepsilon+(2\alpha+2)\varepsilon^2+2\varepsilon^3 : 1]$
51	$[1+\alpha+(\alpha^2+\alpha+2)\varepsilon+(\alpha^2+\alpha+2)\varepsilon^3 : 1+(2\alpha^2+2)\varepsilon+(\alpha^2+2)\varepsilon^2+(2\alpha^2+\alpha+2)\varepsilon^3 : 1]$
52	$[2\alpha^2+2+(2\alpha+1)\varepsilon^2+(2\alpha^2+2\alpha)\varepsilon^3 : 2\alpha+2\alpha\varepsilon^2+(2\alpha+1)\varepsilon^3 : 1]$
53	$[2+2\alpha^2+(2\alpha+1)\varepsilon^2+(2\alpha+1)\varepsilon^3 : \alpha+\alpha\varepsilon^2+2\alpha\varepsilon^3 : 1]$
54	$[1+\alpha+(\alpha^2+\alpha+2)\varepsilon+(2\alpha^2+2\alpha+2)\varepsilon^3 : 2+(\alpha^2+1)\varepsilon+(2\alpha^2+1)\varepsilon^2+(2\alpha+2)\varepsilon^3 : 1]$
55	$[2+(2\alpha^2+\alpha+2)\varepsilon+\varepsilon^2+(2\alpha^2+2\alpha+2)\varepsilon^3 : 2+\alpha+(\alpha^2+2)\varepsilon+(\alpha+1)\varepsilon^2+(2\alpha+2)\varepsilon^3 : 1]$
56	$[(2\alpha^2+2\alpha)\varepsilon+(\alpha^2+2\alpha+2)\varepsilon^2 : 1 : 0]$

57	$[2+(\alpha^2+2\alpha)\varepsilon+(2\alpha^2+\alpha+2)\varepsilon^2+(\alpha^2+1)\varepsilon^3 : 2\alpha+1+(2\alpha^2+2\alpha+2)\varepsilon+(2\alpha^2+\alpha)\varepsilon^2+(\alpha+2)\varepsilon^3 : 1]$
58	$[1+\alpha+(2\alpha^2+2\alpha+2)\varepsilon+(\alpha^2+2)\varepsilon^2+(\alpha^2+\alpha)\varepsilon^3 : 1+\varepsilon+(2\alpha^2+2\alpha)\varepsilon^2+(\alpha+1)\varepsilon^3 : 1]$
59	$[2+2\alpha^2+(\alpha^2+1)\varepsilon+(2\alpha+2)\varepsilon^2+(2\alpha^2+\alpha+1)\varepsilon^3 : 2\alpha+(2\alpha+2)\varepsilon+(\alpha^2+1)\varepsilon^2+(2\alpha+2)\varepsilon^3 : 1]$
60	$[2+2\alpha^2+(2\alpha^2+2)\varepsilon+(\alpha+1)\varepsilon^2+(\alpha^2+\alpha)\varepsilon^3 : \alpha+(2\alpha+2)\varepsilon+(\alpha^2+\alpha)\varepsilon^2+(\alpha^2+\alpha+2)\varepsilon^3 : 1]$
61	$[\alpha+1+2\varepsilon+(\alpha+2)\varepsilon^2+(\alpha+1)\varepsilon^3 : 2+2\alpha^2\varepsilon+2\alpha^2\varepsilon^2+\alpha\varepsilon^3 : 1]$
62	$[2+\varepsilon+\varepsilon^2+2\varepsilon^3 : 2+\alpha+(\alpha^2+2\alpha)\varepsilon+(\alpha^2+2)\varepsilon^2+(\alpha^2+2)\varepsilon^3 : 1]$
63	$[0:1:0]=\infty$

Table 5.1: Elements of the subgroup G of order 63.

Using the subsection 5.4.1, we code the elements of G and use english letters and symbols for this application.
The coding are as follows:

n	Code of nP	n	Code of nP
1	$200100100200120012102102 1 = A$	2	$110200210001100001001110 1 = B$
3	$202202110000020110022100 1 = C$	4	$202101220111010110202120 1 = D$
5	$110222201102200200011221 1 = E$	6	$200021212000210111021100 1 = F$
7	$000011112002100000000000 = G$	8	$200212100221120102220201 1 = H$
9	$110211000120100202201010 1 = I$	10	$202000120202020000020012 1 = J$
11	$202000120210010000010212 1 = K$	12	$110211000010200101102021 1 = L$
13	$200212100100210201110221 1 = M$	14	$000022221212100000000000 = N$
15	$200021212220120222012211 1 = O$	16	$110222201220100100022211 1 = P$
17	$202101220022020220101112 1 = Q$	18	$202202110101010220011100 1 = R$
19	$110200210201200002002111 1 = S$	20	$200100100111210021201202 1 = T$
21	$000000000212100000000000 = U$	22	$200100100022120012102100 1 = V$
23	$110200210210100001001211 1 = W$	24	$202202110210020110022022 1 = X$
25	$202101220201010110202012 1 = Y$	26	$110222201220200200011022 1 = Z$
27	$200021212211210111021101 1 = a$	28	$000011112211100000000000 = b$
29	$200212100010120102220202 1 = c$	30	$110211000002100202201111 1 = d$
31	$202000120112020000020201 1 = e$	32	$202000120000010000010101 1 = f$
33	$110211000101200101102122 1 = g$	34	$200212100011210201110222 1 = h$
35	$000022221121100000000000 = i$	36	$200021212012120222012212 1 = j$
37	$110222201102100100022012 1 = k$	38	$202101220202020220101001 1 = l$
39	$202202110221010220011022 1 = m$	40	$110200210022200002002212 1 = n$
41	$200100100022210021201200 1 = o$	42	$000000000121100000000000 = p$
43	$200100100111120012102101 1 = q$	44	$110200210122100001001012 1 = r$
45	$202202110120020110022211 1 = s$	46	$202101220021010110202201 1 = t$

47	$11022220101120020001112 01 = u$	48	$20002121212221011102110 21 = v$
49	$00001111212010000000000 00 = w$	50	$20021210010212010222020 01 = x$
51	$11021100021110020220121 21 = y$	52	$20200012002202000002012 01 = z$
53	$20200012012001000001002 01 = -$	54	$11021100022220010110222 01 = .$
55	$20021210022221020111022 01 = [$	56	$00002222100010000000000 00 =]$
57	$20002121210112022201221 01 = /$	58	$11022220101110010002211 01 = ($
59	$20210122011202022010122 01 =)$	60	$20220211001101022001121 11 = !$
61	$11020021011020000200201 01 = ?$	62	$20010010020021002120120 11 = :$
63	$00000000000010000000000 00 = @$		

Table 5.2: Code elements of the subgroup G.

5.4.2.1 The first method of cryptography

Exchange of secret key

- Alice chooses a random number integer $K_A = 7 < ord(P) = 63$ and computes $Y_A = 7P$.
- Alice sends Y_A to Bob, but keep K_A.
- Bob chooses a random number $K_B = 5 < ord(P) = 63$ and computes $Y_B = 5P$.
- Bob sends Y_B to Alice, but keep K_B.
- Alice calculates: $K_A Y_B = 35P$.
- Bob calculates: $K_B Y_A = 35P$.
- The secret key between Alice and Bob is $K = 35P$.

1. To encrypt the following message "Meet Me In The Garden". We follow these steps:
   (a) Remove the white space, the message becomes "MeetMeInTheGarden".
   (b) Transmutation every letter in the message into a point of the subgroup $G = \langle P \rangle$.
   (c) To encrypt every point tP by using the secret key and computes $tP + 35P$.
   (d) By the elements of G we get "vCCRvCrL[FCp:PBCL".
   (e) Build their codes according to elements of G.

➥ **Its encryption is:**
200021212122210111021102120220211000002011002210012022021100000201100221001202202110000020110022100120220211010101022001110012000212121222101110211021202202110000020110022100111020021012210000100101211102110000102001011020211000201100221001100000000012110000000000002001001002002100212012011110222201220100100022211111020021000110000100111012022021100000201100221001110211000010200101102021

2. To decrypt the following message:
202202110011010220011211120220211000002011002210012021012200220202201011121200212100102120102222020012021012201110101102021201202000120112020000020201120021210010021020111022111102002102012000020021111110222201220100100022211120210122002202202010111212022021100000201100221001

We follow these steps:

(a) Gather the bits in the blocks of 25 bits.

(b) Replace the blocks code with points of $G = \langle P \rangle$ and Computes $tP - 35P$.

(c) Transmutation the points on symbol letters.

(d) We get the result after completing the space.

➥ **Its decryption is:** Yes Of Course.

5.4.2.2 The second method of cryptography

1. To encrypt the following message "Nice To Meet You Here". We follow these steps:

(a) Remove the white space, the message becomes: "NiceToMeetYouHere"

(b) Choose a password for example "strong".

(c) Share the message in blocks of six letters, and w add x at the end of the message to balance: "NiceTo/MeetYo/uHerex".

(d) Substitute the letters in each block with a cycle (1,2,3,4,5,6), we get: "oNiceT/oMeetY/xuHere".

(e) Build their codes according to elements of G.

➥ **Its encryption is:**
200100100022210021201200100002222121210000000000000000222211211000
000000000200212100010120102220202120200012011202000002020112001001
001112100212012021200100100022210021201200120021210010021020111022
112020001201120200000202011202000120112020000020201120210122002101
011020220112021012202010101102020121200212100102120102220200111022
220101120020001112012002121002211201022202011202000120112020000020
201111020021012210000100101212020001201120200000202011

2. To decrypt the following message:
202101220201010110202012120010010011121002120120212002121000112102011 1
022212000212122112101110211011110200210022200002002212111022220110210 0
100022012120021210010212010222020012001001000222100212012001110222201 0
112002000111201200212100102120102222020012002121001021201022202001200 21
210010212010222020 01

We follow these steps:

(a) Gather the bits in the blocks of 150 bits.

(b) Replace the blocks code on symbol letters.

(c) Substitute the letters in each block with the reverse cycle.

(d) We get the result after completing the space and removing the x's wich are added.

➥ **Its decryption is:** Thank You.

Remark 5.2.

❖ With this application, we can encrypt and decrypt any message of any length.

❖ The motivation of this work is that decryption is difficult for an interceptor who cannot solve the discret logarithm problem.

❖ The diagram proposed shows the interest of these curves which offers safer methods to encrypt and decrypt messages and transform alphabets into points of an elliptical curve.

General conclusion and perspectives

The object of this thesis was to study the elliptic curves defined over a finite rings, as well as their cryptography applications.

- In the first part, we have given an overview of elliptic curves on the field $\mathbb{K}$, then we have studied the elliptic curve over the non local ring $\mathbb{F}_q[\varepsilon]$, where $\varepsilon^4 = \varepsilon^3$ of the characteristic $p \neq 2, 3$. And we have given a classification of the elements in $E_{a,b}(\mathbb{F}_q[\varepsilon])$ using two elliptic curves over the finite field $\mathbb{F}_q$ which they are $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$ and $E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$. Also, we followed the same approach of this study for the non local ring $\mathbb{F}_{3^d}[\varepsilon]$, $\varepsilon^4 = \varepsilon^3$ of the characteristic $p = 3$.

- In the second part, we discussed on the elliptic curve cryptography and the famous protocols; DLP; Diffie-Hellman algorithm and DSA algorithm, and we showed the security level of these protocols. In addition, we have defined the non commutative rings R_m and R_p, and have introduced the two new encryption schemes based on these rings, where we have shown that these cryptosystems are difficult to decipher because they have a strong security level, where are based on two hard problems are the DLP and conjugacy search problem for a non commutative ring and are also a totally homomorphic encryption schemes which will be widely used in practice especially in cloud computing, e-commerce, e-voting etc.

  In the rest of this part, we have given an example of cryptography (encryption-decryption) with a secret key based on the study of the elliptic curve over a special ring $A_4 = \mathbb{F}_{3^d}[\varepsilon]$, where $\varepsilon^4 = 0$ in M.H. Hassib article [32]. We have calculated these cryptographic applications with the help of Maple software 18.

There is still much to study on this topic and it opens up other areas of study.

1. The attack of the discrete logarithm.
2. Other cryptographic systems, in particular signature systems, can be built from these curves and their study could make it possible to obtain more solid ones.
3. Study the group law of the elliptic curve over the ring $\mathbb{F}_q[\varepsilon]$ where $\varepsilon^4 = \varepsilon^3$.
4. In particular, study of the elliptic curve defined on the ring $\mathbb{F}_q[\varepsilon]$ where $\varepsilon^n = \varepsilon^{n-1}$ with n an integer greater than 4 of characteristic different 2 and 3.

Appendix A

Groups, rings and fields

"This appendix contains a concise overeview of the basic notions of groups, rings, fields and finite fields. It describes some, order of group, polynomial rings, homomorphism rings and extension of fields."
For more information on abstract algebra, see the following book [24]

Contents in Brief

A.1 Basic definitions of the groups 123
A.2 Introduction to rings 124
A.3 Field extensions and finite fields 126

A.1 Basic definitions of the groups

Let G be a set. A binary operation on G is a function that assigns each ordered pair of elements of G an element of G.

Group

Let G be a set together with a binary operation (usually called multiplication) that assigns to each ordered pair (a, b) of elements of G an element in G denoted by ab. We say G is a group under this operation if the following three properties are satisfied.

1. (Associativity). The operation is associative; that is, $(ab)c = a(bc)$ for all $a, b, c \in G$.
2. (Identity). There is an element e (called the identity) in G such that $ae = ea = a$ for all $a \in G$.
3. (Inverses). For each element $a \in G$, there is an element $b \in G$ (called an inverse of a) such that $ab = ba = e$.

Order of a Group and an element

- The number of elements of a group (finite or infinite) is called its order. We will use $|G|$ or $\#G$ to denote the order of G.
- The order of an element g in a group G is the smallest positive integer n such that $g^n = e$ (in additive notation, this would be $ng = 0$). If no such integer exists, we say that g has infinite order. The order of an element g is denoted by $O(g)$.

Subgroup

If a subset H of a group G is itself a group under the operation of G, we say that H is a subgroup of G.

Theorem A.1. *Let G be a group, and let a be any element of G. Then, $\langle a \rangle$ is a subgroup of G. The subgroup $\langle a \rangle$ is called the cyclic subgroup of G generated by a. In the case that $G = \langle a \rangle$, we say that G is cyclic and a is a generator of G.*

Theorem A.2. *If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$. Moreover, the number of distinct left (right) cosets of H in G is $|G|/|H|$ and denoted by $|G : H|$.*

Group Isomorphism

An isomorphism f from a group G to a group G' is a one-to-one mapping from G onto G' that preserves the group operation.
That is $f(ab) = f(a)f(b)$ for all $a, b \in G$. If there is an isomorphism from G onto G', we say that G and G' are isomorphic and write $G \cong G'$.

A.2 Introduction to rings

Ring

A ring R is a set with two binary operations, addition (denoted by $a + b$) and multiplication (denoted by ab), such that for all $a, b, c \in R$:

1. $a + b = b + a$.
2. $(a + b) + c = a + (b + c)$.
3. There is an additive identity 0. That is, there is an element 0 in R such that $a+0 = a$ for all $a \in R$.
4. There is an element $-a$ in R such that $a + (-a) = 0$.
5. $a(bc) = (ab)c$.
6. $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.

So, a ring is an Abelian group under addition, also having an associative multiplication that is left and right distributive over addition.

Remark A.1. Note that multiplication need not be commutative. When it is, we say that the ring is commutative. Also, a ring need not have an identity under multiplication. A unity (or identity) in a ring is a nonzero element that is an identity under multiplication. A nonzero element of a commutative ring with unity need not have a multiplicative inverse. When it does, we say that it is a unit of the ring. Thus, a is a unit if a^{-1} exists.

Subring

A subset S of a ring R is a subring of R if S is itself a ring with the operations of R.

Theorem A.3. *A nonempty subset S of a ring R is a subring if S is closed under subtraction and multiplication that is, if $a - b$ and ab are in S whenever $a, b \in S$.*

Characteristic of a ring

The characteristic of a ring R is the least positive integer n such that $nx = 0$ for all x in R. If no such integer exists, we say that R has characteristic 0. The characteristic of R is denoted by $char(R)$.

Ideal

A subring I of a ring R is called a ideal of R if for every $r \in R$ and every $a \in I$ both ra and ar are in I.

Theorem A.4. *A nonempty subset I of a ring R is an ideal of R if*

1. $a - b \in I$ *whenever* $a, b \in I$.

2. ra *and* ar *are in* I *whenever* $a \in I$ *and* $r \in R$.

Theorem A.5. *Let I be an ideal of a ring R, and let R/I denote the set of all right cosets of I considered as a subgroup of the additive group of R. For $I + a \in R/I$ and $I + b \in R/I$, let*

$$(I + a) + (I + b) = I + (a + b)$$

and

$$(I + a)(I + b) = I + (ab).$$

With these operations R/I is a ring, called the quotient ring of R by I.

Prime ideal, maximal ideal
An ideal I of R,

- I is prime if: $I \neq R$ and for all $a, b \in R$, $ab \in I \Longrightarrow a \in I$ or $b \in I$.
- I is maximal if: $I \neq R$ and if J is an ideal such that $I \subset J$, then $J = I$ or $J = R$.

Ring homomorphism, ring isomorphism
A ring homomorphism f from a ring $(R, +, \cdot)$ to a ring $(S, \oplus, \odot)$ is a mapping from R to S that preserves the two ring operations; that is, for all $a, b \in R$,

$$f(a + b) = f(a) \oplus f(b) \text{ and } f(a \cdot b) = f(a) \odot f(b).$$

A ring homomorphism that is both one-to-one and onto is called a ring isomorphism.

First isomorphism theorem for rings
Let f be a ring homomorphism from R to S. Then the mapping from $R/\ker(f)$ to $f(R)$, given by $r + \ker(f) \longrightarrow f(r)$, is an isomorphism. In symbols, $R/\ker(f) \cong f(R)$.

Ring of polynomials over R
Let R be a commutative ring. The set of formal symbols

$$R[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 | a_i \in R, n \in \mathbb{N}\},$$

is called the ring of polynomials over R in the indeterminate x. If $a_n \neq 0$, then the integer n is the degree of the polynomial, and all is its leading coefficient. Two polynomials in $R[x]$ are equal if and only if the coefficients of like powers of x are equal.

Remark A.2. The set $R[x_1][x_2]$ is the ring of polynomials in the indeterminates x_1 and x_2 over the ring R and we can write $R[x_1][x_2] = R[x_1, x_2]$. Similarly, $R[x_1, x_2, ..., x_n]$, where $n \in \mathbb{N}^*$, is the ring of polynomials with indeterminates $x_1, x_2, ..., x_n$.

A.3 Field extensions and finite fields

Field
A field is a commutative ring with unity in which every nonzero element is a unit.

Field extension
A field L is an extension of a field F if $F \subseteq L$ and the operations of F are those of L restricted to F.

Algebraic and transcendental element
Let L be an extension of F and $\alpha \in L$. We say that α is an algebraic over F if there is a non-zero polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$ if not (if the only one is the zero polynomial) we say that α is transcendental over F.

Finite extension
Let L be an extension field of a field F. We say that L has degree n over F and write $[L : F] = n$ if L has dimension n as a vector space over F. If $[L : F]$ is finite, L is called a finite extension of F; otherwise, we say that L is an infinite extension of F.

Algebraic extension
Let L be an extension of F. The field L is an algebraic extension of F if every element of L is algebraic over F.

Proposition A.1. *If L is a finite extension of F, then L is an algebraic extension of F.*

Theorem A.6. *Let K be a finite extension field of the field L and let L be a finite extension field of the field F. Then K is a finite extension field of F and $[K : F] = [K : L][L : F]$.*

Algebraically closed
Let L be an extention field of F. The field L is called algebraically closed if any nonconstant polynomial in $L[x]$ has at least one root in L.

Algebraic closure
A field $\overline{F}$ is called an algebraic closure of a field F, if F is algebraically closed and is an algebraic extension of F.

Finite field
A finite field is a field has a finite number of elements, this number is called the order of the field, and denoted by $\mathbb{F}_q$ of q elements with $q = p^n$, where p is a prime number, and n a positive integer. Every finite field $\mathbb{F}_q$ of a prime characteristic p is an extension of the field $\mathbb{F}_p \cong \mathbb{Z}_p$.

Proposition A.2. *Any field of cardinal p^k is unique up to isomorphism, and it is denoted by $\mathbb{F}_{p^k}$.*

Lemma A.1. *There exists a polynomial P of degree k, irreducible on $\mathbb{F}_p$ such that $\mathbb{F}_{p^k} \cong \mathbb{F}_p[X]/(P)$.*

Proposition A.3. *The characteristic of a field is either 0 or a prime number p.*

Theorem A.7. *Every finite field is commutative.*

Lemma A.2. *Let $\alpha \in \mathbb{F}_q^*$. Then $ord(\alpha)$ divides $q-1$.*

Theorem A.8. *Let $\mathbb{F}_q$ be a finite field with q elements $(q = p^n)$.*

- *The multiplicative group $\left(\mathbb{F}_q^*, \cdot\right)$ of the nonzero elements of $\mathbb{F}_q$ is cyclic of order $q-1$.*
- *All elements α of $\mathbb{F}_q$ satisfy $\alpha^q - \alpha = 0$.*

Primitive element

A generator of the cyclic group of a finite field $\mathbb{F}_q$ is called a primitive element.

Theorem A.9. *Let α be a primitive element for the finite field $\mathbb{F}_q$. then*

$$\mathbb{F}_q = \left\{0, 1, \alpha, \alpha_2, \ldots, \alpha^{q-2}\right\},$$

where $\alpha^{q-1} = 1$. Moreover, α^k is also primitive if and only if $\gcd(k, q-1) = 1$.

Theorem A.10. *Let K be a subfield of a finite field $\mathbb{F}_{p^n}$. Then $K = \mathbb{F}_{p^m}$ with m divides n.*

Theorem A.11. *Let $\mathbb{F}_{p^m}$ a subfield of a finite field $\mathbb{F}_{p^n}$. Then an element x of $\mathbb{F}_{p^n}$ belongs to $\mathbb{F}_{p^m}$ if and only if $x^{p^m} = x$.*

Appendix B

Algorithms

"In this appendix, we show the fundamental algorithms over the ring $\mathbb{F}_q[\varepsilon]$ and the group $E_{a,b}(\mathbb{F}_q[\varepsilon])$."
For more information about these algorithms, see the following thesis [13, 88]

Contents in Brief

B.1 Representation the elements of $\mathbb{F}_q[\varepsilon]$ **129**
B.2 Representation of group $E_{a,b}(\mathbb{F}_q[\varepsilon])$ **131**

B.1 Representation the elements of $\mathbb{F}_q[\varepsilon]$

Let X be an element in $\mathbb{F}_q[\varepsilon]$, then we will choose to represent X by $[x_0, x_1, x_2, x_3]$. The algorithms 1 and 2 are an algorithms that calculates the sum and product of two elements in $\mathbb{F}_q[\varepsilon]$ respectively.

Algorithm 1: sum(p)

Input: $(X = [x_0, x_1, x_2, x_3], Y = [y_0, y_1, y_2, y_3])$
Output: $X + Y$

for i=0 to 3 do:
$z_i = x_i + y_i \bmod p$
end for
return $\underline{[z_0, z_1, z_2, z_3]}$
end

Algorithm 2: product(p)

Input: $(X = [x_0, x_1, x_2, x_3]$,$Y = [y_0, y_1, y_2, y_3])$
Output: $X \cdot Y$

for j=0 to 2 do:
for i=0 to j do:
$z_j = \sum_{i=0}^{j} x_i y_{j-i} \bmod p$
end for
end for
for i=0 to 3 do:
$a = \sum_{i=0}^{3} x_i y_3 \bmod p$
end for
for i=1 to 3 do:
$b = \sum_{i=1}^{3} x_i y_2 \bmod p$
end for
for i=2 to 3 do:
$c = \sum_{i=2}^{3} x_i y_1 \bmod p$
end for
$z_3 = a + b + c + x_3 y_0 \bmod p$
return $\underline{[z_0, z_1, z_2, z_3]}$
end

The algorithm 3 is an algorithm that calculate the inverse element of $\mathbb{F}_q[\varepsilon]$.

Algorithm 3: inverse(p)

Input: $(X = [x_0, x_1, x_2, x_3])$
Output: inversep

if $(x_0 + x_1 + x_2 + x_3 = 0)$ or $(x_0 = 0)$ then
return("X is not invertible")
else
$y_0 = x_0^{-1} \mod p$
for i=0 to 2 do:
for j=1 to i do:
$y_j = -y_0 \cdot \sum_{i=0}^{j-1} y_i x_{j-i} \bmod p$
end for
end for
for i=0 to 3 do:
$y_3 = ((\sum_{i=0}^{3} x_i)^{-1} - (\sum_{j=0}^{2} y_j)) \bmod p$
end for
end if
return $\underline{[y_0, y_1, y_2, y_3]}$
end

The algorithms 4 and 5 are an algorithms which gives the projection of an element from $\mathbb{F}_q[\varepsilon]$ to $\mathbb{F}_q$.

Algorithm 4: projection(0)

Input: $(X = [x_0, x_1, x_2, x_3])$
Output: x_0

return $\underline{(x_0) \bmod p}$
end

Algorithm 5: projection(1)

Input: $(X = [x_0, x_1, x_2, x_3])$
Output: $x_0 + x_1 + x_2 + x_3$

for i=0 to 3 do:
$Z = \sum_{i=0}^{3} x_i \bmod p$
end for
return $\underline{(x_0 + x_1 + x_2 + x_3) \bmod p}$
end

B.2 Representation of group $E_{a,b}(\mathbb{F}_q[\varepsilon])$

Let $[X, Y, Z]$ be an element in $E_{a,b}(\mathbb{F}_q[\varepsilon])$, then we will choose to represent $[X, Y, Z]$ by $[x_0, x_1, x_2, x_3, y_0, y_1, y_2, y_3, z_0, z_1, z_2, z_3]$.
The algorithms 6 and 7 are an algorithms which represents projection φ_0 and φ_1 respectively.

Algorithm 6: proj(0)

Input: $[x_0, .., x_3, y_0, ..y_3, z_0, .., z_3]$
Output: $[x_0, y_0, z_0]$
1 **return** $[x_0, y_0, z_0]$
2 end

Algorithm 7: proj(1)

Input: $[x_0, .., x_3, y_0, ..y_3, z_0, .., z_3]$
Output: $[x_0 + \cdot\cdot + x_3, y_0 + \cdot\cdot + y_3, z_0 + \cdot\cdot + z_3]$
1 **return** $[x_0 + \cdot\cdot + x_3, y_0 + \cdot\cdot + y_3, z_0 + \cdot\cdot + z_3]$
2 end

The algorithm 8 is an algorithm that checks whether a point belongs or not to $E_{a,b}(\mathbb{F}_q[\varepsilon])$.

Algorithm 8: belong

Input: $[x_0, .., x_3, y_0, .., y_3, z_0, .., z_3]$
Output: true or false
1 $X = [x_0, .., x_3]$
2 $Y = [y_0, .., y_3]$
3 $Z = [z_0, .., z_3]$
4 r := productp(productp$(Y, Y, p), Z, p$)
5 s := productp(productp$(X, X, p), X, p$)
6 t := productp(productp(a, X, p), productp$(Z, Z, p), p$)
7 l := productp(productp(b, Z, p), productp$(Z, Z, p), p$)
8 if (r = sump(s, sump(t, l, p), p))then
9 **return** "true"
10 else
11 **return** "false"
12 end

The algorithm 9 is an algorithm which checks the equality of two elements of $E_{a,b}(\mathbb{F}_q[\varepsilon])$.

Algorithm 9: equal

Input: $([x_0, .., x_3, y_0, .., y_3, z_0, .., z_3]$, $[x'_0, .., x'_3, y'_0, .., y'_3, z'_0, .., z'_3])$
Output: 0 or 1

Output:=0;
if $(z_0 * (z_0 + z_1 + z_2 + z_3) = 0)$ and $(z'_0 * (z'_0 + z'_1 + z'_2 + z'_3) = 0)$ then
r=productp($[x_0, .., x_3]$, inversep($[y_0, .., y_3], p), p$)
s=productp($[x'_0, .., x'_3]$, inversep($[y'_0, .., y'_3], p), p$)
l=productp($[z_0, .., z_3]$, inversep($[y_0, .., y_3], p), p$)
t=productp($[z'_0, .., z'_3]$, inversep($[y'_0, .., y'_3], p), p$)
if r=s and l=t then
return (Output:=1)
end if
else
r=productp($[x_0, .., x_3]$, inversep($[z_0, .., z_3], p), p$)
s=productp($[x'_0, .., x'_3]$, inversep($[z'_0, .., z'_3], p), p$)
l=productp($[y_0, .., y_3]$, inversep($[z_0, .., z_3], p), p$)
t=productp($[y'_0, .., y'_3]$, inversep($[z'_0, .., z'_3], p), p$)
if r=s and l=t then
return (Output:=1)
end if
end if
return Output
end

Customized Index

A

Affine space 3
  Affine plane 3
Algorithms 128
  belong 131
  equal 132
  index(p) 130
  product(p) 129
  proj(0) 131
  proj(1) 131
  projection(0) 130
  sum(p) 129
Authenticity 63

B

Block ciphers 65

C

Chosen cipertext attack 70
Chosen plaintext attack 70
Cipher 62
Ciphertext 62
Ciphertext only attack 69
Coding of elements 114
Communication 61
Communication channel 62
Complexity 57
  Asymptotic notations 58
  Time complexity 58
Confidentiality 63
Cryptanalysis 69
  Attacks 69
Cryptography 62
  Asymmetric key cryptography 68
  Hash functions 66
  Symmetric key cryptography 64
Cryptography using key 118
Cryptography using password 119
Cryptology 61
Cryptosystem 63
Curve ordinary 15
Curve supersingular 15

D

Decoding 62
Decryption 62
Diffie-Hellman protocol 72
Digital signature algorithm 74
Discrete logarithm problem 70
Discriminant 3, 35, 48

E

ECC 78
  ECDH 80
  ECDLP 79
  ECDSA 82
Elliptic curve 3, 30, 44
  Over a finite field $\mathbb{K}$ 15
  Over a finite ring $\mathbb{F}_q[\varepsilon]$ 30
  Over a finite ring $\mathbb{F}_{3^d}[\varepsilon]$ 44
  Isomorphism of EC over field $\mathbb{K}$ 13
  Over the ring A_4 111
Encoding 61
Encryption 62
Encryption scheme 92, 104
Equations of Weierstrass 3

F

Feedback 62
fields 126
  Algebraic closure 126
  Field extension 126
  Finite extension 126
  Finite field 126
  Primitive element 127
  Subfield 127
Frobenius endomorphism 17
Fully homomorphic encryption 89

G

Group law 8
Algebraic addition of points 10
Geometric addition of points 8
Groups 123
Isomorphism of group 123
Order of group 123
Subgroup 123

H

Homogeneous polynomial 18
Homogeneous Weierstrass equation . 19

I

Ideal 124
Maximal ideal 125
Prime ideal 125
Integrity 63
Isogenies 16

J

j-invariant 3, 35, 48

K

Key 62
Key exchange 93, 113
Key exchange 104
Key generation algorithm 76, 83
Known plaintext attack 70

N

Non commutative cryptography . 90, 97
Non-repudiation 63
Number of points 15

O

One way function 66
One way trapdoor 66

P

Plaintext 62
Point at infinity 19
Primitive triplet 29
Projective space 18
Projective plane 18

R

Ring $\mathbb{F}_q[\varepsilon]$ 30
Ring $\mathbb{F}_{3^d}[\varepsilon]$ 44
Ring A_4 111
Ring R_m 97
Ring R_p 90
Rings 124
Ring isomorphism 125
Characteristic of a ring 124
Polynomial of ring 125
Quotient ring 28
Subring 124

S

Security for ECDH 82
Security of ECDLP 80
Security of the D-H protocol 74
Signature generation algorithm ...77, 83
Signature verification algorithm 77, 83
Singular curve 3
Singular elliptic curve 4
Smooth curve 3
Smooth elliptic curve 4
Stream ciphers 65

Bibliography

[1] F. Amounas, E.H. El Kinani and A. Chillali, An Application of Discrete Algorithms in Asymmetric Cryptography, *International Mathematical Forum*, **vol 6(49)**, 2409-2418, (2011).

[2] S. Abdelalim , A. Chaichaa and M. Souhail, Group law and the Security of elliptic curves on $\mathbb{F}_p[e_1, .., e_n]$, *Advances in Science, Technology and Engineering Systems Journal*, **vol 2(5)**, 104-108, (2017).

[3] J.P. Aumasson, Serious Cryptography A Practical Introduction to Modern Encryption, *No Starch Press, Inc., San francisco*, (2018).

[4] A. Boulbot, A. Chillali and A. Mouhib, Elliptic curve over a finite ring generated by 1 and an idempotent element ε with coefficients in the finite field $\mathbb{F}_{3^d}$, *Boletim da Sociedade Paranaense de Matematica* , 1-19, (2018).

[5] A. Boulbot, A. Chillali and A. Mouhib, Elliptic curves over the ring $\mathbb{F}_q[e]$, $e^3 = e^2$, *Gulf Journal of Mathematics*, **vol 4** , 123-129, (2016).

[6] A. Boulbot, A. Chillali and A. Mouhib, Elliptic curves over the ring R, *Boletim da Sociedade Paranaense de Matematica* , **vol 38**, 193-201, (2017).

[7] A. Boulbot, A. Chillali and A. Mouhib, Cryptographic Protocols on the non commutative Ring R, *International Journal of Mathematical and Computational Methods*, **vol 2**, 138-141, (2017).

[8] W. Bosma and H.W. Lenstra, Complete System of Two Addition Laws for Elliptic Curves, *Journal of Number Theory*, **vol 53**, 229-240, 1995.

[9] I.F. Blake, G. Seroussi, and N.P. Smart, Advances in Elliptic Curves in Cryptography, *Number 317 in London Mathematic Society Lecture Notes Series, Cambridge University Press*, (2005).

[10] I.F. Blake, G. Seroussi, and N.P. Smart, Elliptic Curves in Cryptography, *Number 265 in London Mathematic Society Lecture Notes Series. Cambridge University Press*, (1999).

[11] A. Chatterjee and K. M. M. Aung, Fully Homomorphic Encryption in Real World Applications, *Computer Architecture and Design Methodologies, Springer Nature, Singapore*, (2019).

[12] A. Chillali and S. Abdelalim , The elliptic curve $E_{a,b}(\mathbb{F}_p[e_1, e_2, e_3])$, *Gulf Journal of Mathematics* **vol 3(2)**, 49-53, (2015).

[13] A. Chillali, Cryptosystème à clef publique et courbes elliptique sur l'anneau $\mathbb{F}_q[\varepsilon], \varepsilon^n = 0$, *Thése Docteur en Sciences, Université Sidi Mohamed Ben Abdellah, Faculté des Sciences et Techniques, Fes, Maroc*, (2013).

[14] A. Chillali, Elliptic Curves of the Ring $\mathbb{F}_q[\varepsilon]$, $\varepsilon^n = 0$, *International Mathematical*, **vol 6**, 1501-1505, (2011).

[15] A. Chillali, Identification Methods Over $E^n_{a,b}$, *Recent Advances in Computers, Communications, Applied Social Science and Mathematics*, 133-137, (2011).

[16] A. Chillali, Matrix Encryption Scheme, *Advances in Science, Technology and Engineering Systems Journal*, **vol 2(4)**, 56-58, (2016).

[17] A. Chillali, A. Tadmori and M. Ziane, Improved of Elliptic Curves Cryptography over a Ring, *World Academy of Science, Engineering and Technology International Journal of Computer and Information Engineering*, **vol 9(4)**, 235-239, (2015).

[18] W. Diffie and M. E. Hellman, New Directions in Cryptography, *In IEEE Transactions on Information Theory*, **vol 22 (6)**, 644–654, (1976).

[19] Y. Driencourt and J. Michon, Elliptic codes over a field of characteristic 2, *Journal of Pure and Applied Algebra*, **vol 45**, 15-39, (1987).

[20] M. Elhassani, A. Boulbot, A. Chillali and A. Mouhib, Fully homomorphic encryption scheme on a non-Commutative ring R, *International Conference on Intelligent Systems and Advanced Computing Sciences*, (2019).

[21] T. El Gamal, A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, *In IEEE Transactions on Information Theory*, **vol 31(4)**, 469–472, (1985).

[22] A. Enge, Elliptic Curves and Their Applications to Cryptography an Introduction, *Kluwer Academic Publishers, Boston, Dordrecht, London, second printing*, (2001).

[23] S.D. Galbraith, Mathematics of Public-Key Cryptography, *Cambridge University Press*, (2018).

[24] J.A. Gallian, Contemporary Abstract Algebra, *Cengage Learning; Brooks Cole; Cengage*, (2017).

[25] G. van der Geer, Codes and elliptic curves, *Effective Methods in Algebraic Geometry*, 159-168, (1991).

[26] C. Gentry, A fully homomorphic encryption scheme, *PhD thesis, Stanford University*, (2009).

[27] S. Goldwasser and J. Kilian, Almost all primes can be quickly certified, *in Proceedings of the Eighteenth Annual ACM Symposium on Theory of Computing, STOC'86, New York, NY, USA*, (1986).

[28] M. I. González Vasco and R. Steinwandt, Group Theoretic Cryptography, *CRC Press Taylor & Francis Group*, (2015).

[29] R. Granger and F. Vercauteren, On the Discrete Logarithm Problem on Algebraic Tori, *Advances in Cryptology-CRYPTO ,LNCS 3621, Springer*, 66–85, (2005).

[30] M. H. Hassib, Courbes elliptiques sur un anneau de caractéristique 3 et cryptographie, *Thése Docteur en Sciences et Techniques, Université Moulay Ismail, Errachidia, Maroc*, (2015).

[31] M. H. Hassib and A. Chillali, Example of cryptography over the ring $\mathbb{F}_{3^d}[\varepsilon]$, $\varepsilon^2 = 0$, *Latest trends in Applied Informatics and Computing*, 71-73, (2012).

[32] M. H. Hassib, A. Chillali and M. A. Elomary, Elliptic Curves over the Ring $\mathbb{F}_{3^d}[\varepsilon]$, $\varepsilon^4 = 0$, *International Mathematical Forum*, **vol 9(24)**, 1191-1196, (2014).

[33] R. Harkanson and Y. Kim, Applications of Elliptic Curve Cryptography, *In The 12th Annual Cyber and Information Security Research Conference, Oak Ridge, TN, USA (CISRC)*, (2017).

[34] D. Hankerson, A. Menezes and S. Vanstone, Guide to Elliptic Curve Cryptography, *Springer*, (2004).

[35] J. Hoffstein, J. Pipher and J.H. Silverman, An Introduction to Mathematical Cryptography, *Graduate Texts in Mathematics, Springer-verlag*, (2008).

[36] B. Hutz, An Experimental Introduction to Number Theory, *AMS, Pure and applied undergraduate texts*, **vol 31**, (2018).

[37] K. Ireland and M. Rosen , A Classical Introduction to Modern Number Theory, *Bogden and Quigley, Inc., Springer-Verlag, Second Edition*, (1972).

[38] B. S. Kaliski Jr., A pseudo-random bit generator based on elliptic logarithms, *in Proceedings on Advances in cryptology|CRYPTO '86, London, UK, Springer-Verlag*, 84-103, (1987).

[39] A. Kerckhoffs, La cryptologie militaire, *Journal des sciences militaires*, **vol 9**, janvier 5-83, et février 161-191, (1883).

[40] J. Katz and Y. Lindell, Introduction to Modern Cryptography, *Chapman and Hall/CRC*, (2008).

[41] N. Koblitz, Algebraic Aspects of Cryptography, *Algorithms and Computation in Mathematics, Springer*, **vol 3**, (1997).

[42] N. Koblitz, Elliptic curve cryptosystems, *Mathematics of computation*, **vol 48**, 203-209, (1987).

[43] N. Koblitz, Introduction to elliptic curves and modular forms, *Graduate texts in mathematics; 97, Springer-Verlag* , (1984).

[44] A. Kuzmiakova, Computer Science, Algorithms and Complexity, *Arcler Press*, (2021).

[45] H. Lange and W. Ruppert, Complete systems of addition laws on abelian varieties, *In Springer-Verlag, editor, Inventiones mathematicae*, **vol 79**, 603–610, (1985).

[46] H. W. Lenstra Jr., Elliptic curves and number-theoretic algorithms, *Proceedings of the International Congress of Mathematicians, Berkely, California, USA*, **vol 1**, (1986).

[47] W. H. Lenstra Jr., Factoring integers with elliptic curves, *Annals of Math*, **vol 126**, 649-673, (1987).

[48] R. Lercier, Algorithmique de courbes elliptiques dans les corps finis, *PhD thesis, Ecole polytechnique*, (1997).

[49] A. K. Lenstra and E. R. Verheul, Selecting cryptographic key size, *Public Key Cryptography*, 446-465, (2000).

[50] A. K. Lenstra and E. R. Verheul, The XTR Public Key System, *Advances in Cryptology- CRYPTO (Mihir Bellare) Lecture Notes in Computer Science*, **vol 1880**, 1-19, (2000).

[51] S. Martin, Corbes El.liptiques modul N i Applicacions Criptografiques. *PhD thesis, Departament de Matemàtica Aplicada i Telemàtica, Universitat Politècnica de Catalunya*, (1998).

[52] V. Miller, Use of elliptic curves in cryptography, *in crypto 85 LNCS 218, Springer*, 417-426, (1986).

[53] M.I. Mihailescu and S.L. Nita, Pro Cryptography and Cryptanalysis: Creating Advanced Algorithms with C# and .NET, *Apress*, (2021).

[54] R.A. Mollin, An Introduction to Cryptography, *Chapman and Hall/CRC, Taylor and Francis Group, Second Edition*, (2007).

[55] A. Menezes, T. Okamoto and S. A. Vanstone, Reducing elliptic curves logarithms to logarithms in a finite field, *In ACM Press, editor, 23rd Annual ACM Symposium on Theory of Computing*, 80–89, (1991).

[56] U. M. Maurer and S. Wolf, The Relationship Between Breaking the Diffie-Hellman Protocol and Computing Discrete Logarithms, *Society for Industrial and Applied Mathematics Journal on Computing*, **vol 28**, 1698–1721, (1999).

[57] S. C. Pohlig and M.E. Hellman, An Improved Algorithm for Computing Logarithms over $GF(p)$ and its Cryptographic Significance, *IEEE Transactions on Information Theory*, **vol 24(1)**, 106–110, (1978).

[58] S. Pote, J. Katti, Attacks on Elliptic Curve Cryptography Discrete Logarithm Problem (EC-DLP), *International journal of innovative research in electrical, electronics, instrumentation and control engineering*, **vol 3(4)**, 127-131, (2015).

[59] C. Paar and J. Pelzl, Understanding Cryptography, *Springer-Verlag Berlin Heidelberg*, (2010).

[60] K. Rabah, Theory and Implementation of Elliptic Curve Cryptography, *Journal of Applied Sciences*, **vol 5(4)**, 604-633, (2005).

[61] R.L. Rivest , L. Adleman and M. L. Dertouzos, On data banks and privacy homomorphisms, *Foundations of Secure Computation*, **vol 11(4)**, 169-180, (1978).

[62] B. Ryabko and A. Fionov, Basics of Contemporary Cryptography for IT Practitioners, *World Scientific Publishing Co. Re. Ltd*, (2005).

[63] J. Rothe, Complexity Theory and Cryptology: An Introduction to Cryptocomplexity , *Springer*, (2004).

[64] R. Rivest, A. Shamir and L. Adleman, A Method for Obtaining Digital Signatures and Public Key Cryptosystems, *Communications of the ACM*, **vol 21(2)**, 120–126, (1978).

[65] M. Sahmoudi and A. Chillali, Key exchange over particular algebraic closure ring, *Tatra Mountains Mathematical Publications*, **vol 70**, 151-162, (2017).

[66] R. Schoof, Elliptic curves over finite fields and computation of square roots $\mathrm{mod} p$, *Mathematics of Computation*, **vol 44(170)**, 483–494, April (1985).

[67] R. Schoof, Counting points on elliptic curves over finite fields, *Journal de Théorie des Nombres de Bordeaux*, **vol 7**, 219–254, (1995).

[68] B. Selikh, A. Chillali, D. Mihoubi and N. Ghadbane, A new public key cryptosystem based on the non-commutative ring R, *Journal of Discrete Mathematical Sciences & Cryptography*, in press.

[69] B. Selikh, A. Chillali, D. Mihoubi and N. Ghadbane, A novel non-commutative cryptography scheme using a special ring $\mathbb{F}_q[\varepsilon], \varepsilon^4 = \varepsilon^3$, *manuscript submitted for publication*.

[70] B. Selikh, A. Chillali, D. Mihoubi and N. Ghadbane, ECC over the ring $\mathbb{F}_{3^d}[\varepsilon]; \varepsilon^4 = 0$ by using two methods, *Tbilisi Mathematical Journal*, **vol 14(3)**, 213-223, (2021).

[71] B. Selikh, Study of elliptic curve over a finite ring $\mathbb{F}_{3^d}[\varepsilon], \varepsilon^4 = \varepsilon^3$, *Gulf Journal of Mathematics*, in press.

[72] I.A. Semaev, Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p, *In American Mathematical Society, editor, Mathematics of computation*, **vol 67**, 353–356,(1998).

[73] C.E. Shannon, A Mathematical Theory of Communication, *Bell system technical journal*, **vol 27(4)**, 379–423, 623–656, (1948).

[74] C.E. Shannon, Communication Theory of Secrecy Systems, *Bell system technical journal*, **vol 28(4)**, 656–715, (1949).

[75] T.R. Shemanske, Modern cryptography and elliptic curves: a beginner's guide, *AMS, Student mathematical library*, **vol 83**, (2017).

[76] J.H. Silverman, Advanced topics in the arithmetic of elliptic curves, *Graduate Texts in Mathematics, Springer-verlag*, **vol 151**, (1994).

[77] J.H. Silverman, The Arithmetic of Elliptic Curves, *Graduate Texts in Mathematics, Springer*, **vol 106**, (1985).

[78] N.P. Smart, Cryptography Made Simple, *Springer International Publishing Switzerland* , (2016).

[79] N.P. Smart, The discrete logarithm problem on elliptic curves of trace one, *Journal of Cryptology*, **vol 12**, 193–196, (1999).

[80] B. Selikh, D. Mihoubi and N. Ghadbane, Classification of elements in elliptic curve over the ring $\mathbb{F}_q[\varepsilon]$, *Discussiones Mathematicae General Algebra and Applications*, **vol 41(2)**, 283–298, (2021).

[81] L.D. Singh and K.M. Singh, Implementation of Text Encryption using Elliptic Curve Cryptography, *Procedia Computer Science* **vol 54**, 73-82, (2015).

[82] J.H. Silverman and J. Tate, Rational Points on Elliptic Curves, *Springer-Verlag* , (1992).

[83] W. Stallings, Cryptography and Network Security Principles and Practice, *Prentice Hall, Fifth edition* , (2011).

[84] A. Tadmori, A. Chillali and M. Ziane, ECC over the ring $\mathbb{F}_{2^d}[X]/(X^2)$ by using a password, *Gulf Journal of Mathematics*, **vol 6 (4)**, 72-78, (2018).

[85] A. Tadmori, A. Chillali and M. Ziane, Elliptic curves over ring $\mathbb{F}_{2^d}[\varepsilon]; \varepsilon^4 = 0$, *Applied Mathematical Sciences*, **vol 9(35)** , 1721-1733, (2015).

[86] A. Tadmori, A. Chillali and M. Ziane, The Binary Operations Calculus in $E_{a,b,c}$, *International Journal Of Mathematical Models And Methods In Applied Sciences*, **vol 9**, 171-175, (2015).

[87] W. Trappe and L.C. Washington , Introduction to Cryptography with Coding Theory , *Prentice Hall*, (2002).

[88] M. Virat, Courbe elliptique sur un anneau et applications cryptographiques, *Thése Docteur en Sciences, Université Nice-Sophia Antipolis, Nice, France*, (2009).

[89] L.C. Washington, Elliptic Curves Number Theory and Cryptography, *2nd edition*, (2008).

[90] A. J. Wiles, Modular elliptic curves and fermat's last theorem, *Annals of Math*, **vol 141**, 443-551, (1995).

[91] X. Yi, R. Paulet and E. Bertino, Homomorphic encryption and applications, *Springer* , (2014).

[92] M. Zeriouh, A. Chillali and A. Boua, Cryptography Based on the Matrices, *Boletim da Sociedade Paranaense de Matematica*, **vol 37(3)** , (2019).

This thesis deals with the study of the elliptic curves over finite rings and their cryptographic applications. Firstly, we defined the elliptic curves $E_{a,b}(\mathbb{F}_q[\varepsilon])$ and $E_{a,b}(\mathbb{F}_{3^d}[\varepsilon])$ over the rings $\mathbb{F}_q[\varepsilon]$ and $\mathbb{F}_{3^d}[\varepsilon]$ respectively, with $\varepsilon^4 = \varepsilon^3$ by its projective equations, then we studied the classification of elements in these elliptic curves. Moreover, using the elliptic curve $E_{a,b}(\mathbb{F}_q[\varepsilon])$, we introduced new non-commutative cryptography schemes on a special rings so that these cryptosystems are based on the two hard problems, the conjugal classical problem and the discrete logarithm problem, and they have strong security and very difficult to solve for decryption. At the end of the thesis we have given a numerical example of cryptography (encryption and decryption) on the elliptic curve $E^4_{a,b}$ over the ring $\mathbb{F}_{3^d}[\varepsilon]$ where $\varepsilon^4 = 0$ by using two methods (with a secret key and a password).
Keywords: Elliptic curve; Finite ring; Local ring; Elliptic curve cryptography; Non-commutative cryptography; Fully homomorphic encryption.

English Abstract

تتناول هذه الأطروحة دراسة المنحنيات الإهليليجية على الحلقات المنتهية و تطبيقاتها في التشفير. أولا، قمنا بتعريف المنحنيات الإهليليجية $E_{a,b}(\mathbb{F}_q[\varepsilon])$ و $E_{a,b}(\mathbb{F}_{3^d}[\varepsilon])$ على الحلقات $\mathbb{F}_q[\varepsilon]$ و $\mathbb{F}_{3^d}[\varepsilon]$ على التوالي، مع $\varepsilon^4 = \varepsilon^3$ بواسطة معادلاتها الإسقاطية، ثم قمنا بدراسة تصنيف العناصر في هذه المنحنيات الإهليليجية. علاوة على ذلك، باستخدام المنحنى الإهليليجي $E_{a,b}(\mathbb{F}_q[\varepsilon])$ قدمنا مخططات تشفير جديدة غير تبادلية على حلقات خاصة بحيث أن هذه المخططات تعتمد على مشكلتين صعبتين هما المشكلة الكلاسيكية الزوجية و مشكلة اللوغاريتم المنفصل ولديهم أمان قوي يصعب فك تشفيره. في نهاية الأطروحة قدمنا مثالا عدديا للتشفير (التشفير و فك التشفير) فوق المنحنى الإهليليجي $E^4_{a,b}$ على الحلقة $\mathbb{F}_{3^d}[\varepsilon]$ حيث $\varepsilon^4 = 0$ باستخدام طريقتين (المفتاح السري و كلمة المرور).
الكلمات المفتاحية: المنحنى الإهليليجي؛ حلقة منتهية؛ حلقة محلية؛ تشفير منحنى إهليليجي؛ تشفير غير تبادلي؛ تشفير متماثل تماما.

Arabic Abstract

Cette thèse traite de l'étude des courbes elliptiques sur des anneaux finis et de leurs applications cryptographiques. Dans un premier temps, nous avons défini les courbes elliptiques $E_{a,b}(\mathbb{F}_q[\varepsilon])$ et $E_{a,b}(\mathbb{F}_{3^d}[\varepsilon])$ sur les anneaux $\mathbb{F}_q[\varepsilon]$ et $\mathbb{F}_{3^d}[\varepsilon]$ respectivement, avec $\varepsilon^4 = \varepsilon^3$ par ses équations projectives, puis nous avons étudié la classification des éléments dans ces courbes elliptiques. De plus, en utilisant la courbe elliptique $E_{a,b}(\mathbb{F}_q[\varepsilon])$, nous avons introduit de nouveaux schémas de cryptographie non commutative sur des anneaux spéciaux de sorte que ces cryptosystèmes sont basés sur deux problèmes difficiles, le problème conjugal classique et le problème du logarithme discret, et ils ont une sécurité forte et très difficile à résoudre pour le déchiffrement. A la fin de la thèse nous avons donné un exemple numérique de cryptographie (cryptage et décryptage) sur la courbe elliptique $E^4_{a,b}$ sur l'anneau $\mathbb{F}_{3^d}[\varepsilon]$ où $\varepsilon^4 = 0$ en utilisant deux méthodes (avec une clé secrète et un mot de passe).
Mots clés: Courbe elliptique; Anneau fini; Anneau local; Cryptographie à courbe elliptique; Cryptographie non commutative; Cryptage entièrement homomorphe.

French Abstract