جامعة سيدي محمد بن عبد الله بفاس
ⵜⴰⵙⴷⴰⵡⵉⵜ ⵙⵉⴷⵉ ⵎⵓⵃⵎⵎⴰⴷ ⴱⵏ ⵄⴱⴷⵍⵍⴰⵀ ⵏ ⴼⴰⵙ
UNIVERSITÉ SIDI MOHAMED BEN ABDELLAH DE FES

كلية العلوم والتقنيات فاس
ⵜⴰⵖⵉⵡⴰⵏⵜ ⵏ ⵜⵎⴰⵙⵙⴰⵏⵉⵏ ⴷ ⵜⵙⵏⵉⴳⵉⵜⵉⵏ
FACULTÉ DES SCIENCES ET TECHNIQUES DE FÈS

Centre d'Études Doctorales : Sciences et Techniques de l'Ingénieur

N° d'ordre : 23 /2020

THÈSE DE DOCTORAT

Présentée par

Mr : Aziz Boulbot

Discipline : Mathématiques.

Spécialité : Mathématiques fondamentales et appliquées.

Sujet de la thèse : Courbes elliptiques sur certains anneaux finis et application en cryptographie.

Formation doctorale : Sciences de l'ingénieur, Sciences physique, Mathématique et Informatique.

Thèse présentée et soutenue le 20 Juillet 2010 à 10h au centre de Conférence devant le jury composé de :

Nom Prénom	Titre	Établissement	
Pr. Lhoussain El Fadil	PES	Faculté des Sciences Dhar El Mehraz de Fès	Président
Pr. Mohamed Abdou Elomary	PES	Faculté des Sciences et Techniques de Settat	Rapporteur
Pr. Ali Kacha	PES	Faculté des Sciences de Kenitra	Rapporteur
Pr. Abdelkarim Boua	PES	Faculté Polydisciplinaire de Taza	Rapporteur
Pr. Ismail Akharraz	PH	Faculté Polydisciplinaire de Taza	Examinateur
Pr. Abdelhakim Chillali	PH	Faculté Polydisciplinaire de Taza	Examinateur
Pr. Ali Mouhib	PES	Faculté Polydisciplinaire de Taza	Directeur de thèse

Laboratoire d'accueil : Laboratoire des sciences de l'ingénieur.

Établissement : Faculté des Sciences et Techniques de Fès.

Université Sidi Mohamed ben Abdellah
Faculté des Sciences et Techniques-Fès

THÈSE

Pour l'obtention du grade de :

DOCTEUR EN SCIENCES

Discipline : Mathématiques

Spécialité : Mathématiques fondamentales et appliquées

Présentée et soutenue par :

Aziz Boulbot

Titre de la thèse :

Courbes elliptiques sur certains anneaux finis et application en cryptographie

Directeur de thèse : **Pr. Ali Mouhib**

Co-directeur de thèse : **Pr. Abdelhakim Chillali**

Thèse présentée et soutenue le lundi 20 Juillet 2020 à 10h
au Centre de Conférence devant le jury composé de :

Prénom Nom	Titre	Établissement	Qualité
Lhoussain EL FADIL	PES	Faculté des Sciences Dhar El Mehraz de Fès	Président
Mohamed Abdou ELOMARY	PES	Faculté des Sciences et Techniques de Settat	Rapporteur
Ali KACHA	PES	Faculté des Sciences de Kenitra	Rapporteur
Abdelkarim BOUA	PH	Faculté Polydisciplinaire de Taza	Rapporteur
Ismail AKHARRAZ	PH	Faculté Polydisciplinaire de Taza	Examinateur
Abdelhakim CHILLALI	PH	Faculté Polydisciplinaire de Taza	Examinateur
Ali MOUHIB	PES	Faculté polydisciplinaire de Taza	Directeur de thèse

Centre des Études Doctorales : Sciences et Techniques de l'Ingénieur
Faculté des Sciences et Techniques Fès, B.P. 2202, Route d'Imouzzer Fès

Dédicace

Au nom D'ALLAH le Tout-Miséricordieux

Paix et Salut sur le Prophète Mohammed.

Je dédie cette thèse à :

L'âme de mon grand-père, que Dieu lui fasse miséricorde.

Mes chers parents, ma femme, mes frères, sœurs et toute ma famille.

Tous mes professeurs sans le soutien desquels ce travail n'aurait pas été fait.

Tous ceux qui m'ont soutenu de près ou de loin, et à tous mes amis et collègues.

Remerciements

Je remercie ALLAH le Tout-Miséricordieux de m'avoir donné la volonté, la patience et le courage pour mener à terme ce travail.

Je tiens à remercier vivement monsieur le professeur *Ali Mouhib* qui a dirigé mes travaux de thèse. Il a su motiver chaque étape de recherche par des remarques pertinentes ; je le remercie très sincèrement pour la confiance qu'il a en mes compétences, puis pour m'avoir guidé, encouragé, conseillé et pour tout ce qu'il a fait pour moi et que je ne saurais entièrement lister ici. Cette thèse lui doit beaucoup.

Mes remerciements vont également à monsieur le professeur *Abdelhakim Chillali* qui m'a donné des idées très convenables pour réaliser cette thèse. Ce travail doit beaucoup à la clarté de ses explications et à sa disponibilité parfaitement complémentaire. Je le remercie de m'avoir apporté toute son aide et tout son soutien.

Je remercie très chaleureusement messieurs les professeurs *Mohamed Abdou Elomary, Ali Kacha* et *Abdelkarim Boua* pour avoir accepté d'être les rapporteurs de ce manuscrit. Leurs conseils m'ont été très précieux pour améliorer cette thèse.

Je suis très reconnaissant envers messieurs les professeurs *Lhoussain El Fadil, Ismail Akharraz* et *Abdelhakim Chillali* qui ont bien voulu faire partie du jury de soutenance et ainsi d'évaluer mes travaux de thèse.

Je présente mes sincères remerciements et respects à mes parents, ma femme et à toute ma famille pour leur soutien et leur encouragement tout au long de ce travail.

Enfin, j'adresse mes vives reconnaissances à mon ami le professeur *Mohammed Fri* pour son aide à la correction des erreurs linguistiques dans ce manuscrit, et à toutes les personnes qui m'ont accompagné de près ou de loin dans ce parcours de recherche et m'ont permis de mener à bien cette thèse.

Fiche représentative de la thèse

Prénom et Nom de l'auteur : Aziz Boulbot.

Titre de la thèse : Courbes elliptiques sur certains anneaux finis et application en cryptographie.

Thème de recherche : Mathématiques fondamentales et appliquées & Informatique.

Formation Doctorale : Sciences de l'ingénieur, Sciences physique, Mathématique et Informatique.

Directeur de recherche : Le professeur Ali Mouhib (PES)- Faculté Polydisciplinaire de Taza.

Co-directeur de recherche : Le professeur Abdelhakim Chillali (PH)- Faculté Polydisciplinaire de Taza.

Laboratoire d'accueil : Laboratoire des sciences de l'ingénieur.

Etablissement domiciliant le laboratoire d'accueil : Faculté Polydisciplinaire de Taza.

Publications :

1. A. Boulbot, A. Chillali et A. Mouhib. Elliptic curves over the ring R. *Boletim da Sociedade Paranaense de Matemática*, 2020, 38, 193–201.
2. A. Boulbot, M. Elhassani, A. Chillali et A. Mouhib. Fully homomorphic encryption scheme on a non-commutative ring R. *International Conference on Intelligent Systems and Advanced Computing Sciences (ISACS)*, 2019, 1–4.
3. A. Boulbot, A. Chillali et A. Mouhib. Elliptic curve over a finite ring generated by 1 and an idempotent element e with coefficients in the finite field $\mathbb{F}_3^d$. *Boletim da Sociedade Paranaense de Matemática*, p. 1–19, 2018.
4. A. Boulbot, A. Chillali et A. Mouhib. Cryptographic protocols on the non-commutative ring R. *International Journal of Mathematical and Computational Methods, International Association of Research and Science*, 2017, 2, 138–141.
5. A. Boulbot, A. Chillali et A. Mouhib. Elliptic curves over the ring $\mathbf{E}_{a,b}\left(\mathbb{F}_{p^d}[e]\right)$, où $e^3 = e^2$. *Gulf Journal of Mathematics*, 2016, 4, 123–129.
6. A. Boulbot, A. Chillali et A. Mouhib. Elliptic curve over a finite ring of characteristic two. Soumis.

Résumé

Le but de cette thèse est d'étudier les applications cryptographiques des courbes elliptiques définies sur des anneaux finis et non-locaux.

Dans le premier chapitre, nous avons donné sous forme d'une introduction aux courbes elliptiques, des préliminaires nécessaires à l'élaboration de cette thèse.

Dans le deuxième chapitre, nous avons étudié des courbes elliptiques définies sur l'anneau $\mathbb{F}_q[e]$, où $e^2 = e$ et $\mathbb{F}_q$ est un corps fini d'ordre $q = p^d$, avec p un nombre premier et d un entier positif. Le résultat essentiel, que nous avons montré, est l'isomorphisme entre la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$ et le groupe $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q) \times E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$. Ce résultat nous a permis de munir la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$ d'une structure de groupe et de donner explicitement sa loi du groupe.

Dans le troisième chapitre, nous avons étudié les courbes elliptiques définies sur l'anneau $\mathbb{F}_q[e]$, où $e^3 = e^2$ et q est une puissance d'un nombre premier supérieur ou égal à 5. Après avoir classifié les points dans ces courbes elliptiques, nous avons donné explicitement leur loi de groupe.

Enfin, dans le quatrième chapitre, nous avons donné deux systèmes de chiffrement entièrement homomorphes sur ces courbes.

Mots clés : Anneau fini, Anneau non-local, Caractéristique, Corps finis, Courbes elliptiques, Cryptographie, Chiffrement entièrement homomorphe, Équation de Weierstrass, Isomorphisme, Logarithme discret.

Abstract

The goal of this thesis is to study the cryptographic applications of elliptic curves defined over finite and non-local rings.

In the first chapter, we have given, in the form of an introduction to elliptic curves, the necessary preliminaries for the elaboration of this thesis.

In the second chapter, we studied the elliptic curves defined over the ring $\mathbb{F}_q[e]$, where $e^2 = e$ and $\mathbb{F}_q$ is a finite field of order $q = p^d$, with p is a prime number and d is a positive integer. The essential result, which we have shown is the isomorphism between the elliptic curve $E_{a,b}(\mathbb{F}_q[e])$ and the group $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q) \times E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$. This result allowed us to provide the elliptic curve $E_{a,b}(\mathbb{F}_q[e])$ with a group structure and to explicitly give its group law.

In the third chapter, we studied the elliptic curves defined over the ring $\mathbb{F}_q[e]$, where $e^3 = e^2$ and q is a power of a prime number greater than or equal to 5. After classifying the points in these elliptic curves, we explicitly gave their group law.

Finally, in the fourth chapter, we have given two fully homomorphic encryption schemes over these curves.

Keywords : Finite ring, Non-local ring, Characteristic, Finite fields, Elliptic curves, Cryptography, Fully homomorphic encryption scheme, Weierstrass equation, Isomorphism, Discrete logarithm.

ملخص

إن هدف هذه الأطروحة هو دراسة تطبيقات التشفير للمنحنيات الإهليجية المعرفة على الحلقات المنتهية وغير المحلية.

في الفصل الأول، أعطينا على شكل مدخل للمنحنيات الإهليجية، الأولويات اللازمة لتطوير هذه الأطروحة.

في الفصل الثاني، درسنا المنحنيات الإهليجية المعرفة على الحلقة $\mathbb{F}_q[e]$، حيث $e^2 = e$ و $\mathbb{F}_q$ الحقل المنتهُ ذو الرتبة $q = p^d$، مع p عدد أولي و d عدد صحيح موجب. النتيجة الأساسية التي أثبتناها، هي التشاكل التقابلي بين المنحنى الإهليجي $E_{a,b}(\mathbb{F}_q[e])$ والزمرة $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q) \times E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$. هذه النتيجة، مكنتنا من تزويد المنحنى الإهليجي $E_{a,b}(\mathbb{F}_q[e])$ ببنية زمرة وإعطاء قانونها صراحة.

في الفصل الثالث، درسنا المنحنيات الإهليجية المعرفة على الحلقة $\mathbb{F}_q[e]$، حيث $e^3 = e^2$ و q هو عدد أولي أكبر من أو يساوي 5. بعد تصنيف نقط هذه المنحنيات الإهليجية، أعطينا صراحة قانون زمرتها.

أخيرا، في الفصل الرابع، أعطينا نظامي تشفير متماثلين تماما على هذه المنحنيات.

الكلمات المفتاح : حلقة منتهية، حلقة غير محلية، مميزة، حقل منتهُ، منحنيات إهليجية، تشفير، تشفير متماثل تماما، معادلة ويرستراس، تشاكل تقابلي، اللوغاريتم المتقطع.

Table des matières

Table des matières viii

Table des figures ix

Liste des tableaux x

Liste des symboles xi

Introduction 1

1 Préliminaires sur les courbes elliptiques 5
- 1.1 Courbes planes . . . 6
  - 1.1.1 Courbes affines planes . . . 6
  - 1.1.2 Courbes projectives planes . . . 7
- 1.2 Courbes elliptiques . . . 9
  - 1.2.1 Courbes elliptiques affines . . . 9
  - 1.2.2 Courbes elliptiques projectives . . . 11
- 1.3 Structure de groupe d'une courbe elliptique . . . 11
  - 1.3.1 Construction géométrique . . . 12
  - 1.3.2 Formules d'addition en coordonnées affines . . . 13
  - 1.3.3 Exemples . . . 16
  - 1.3.4 Formules d'addition en coordonnées projectives . . . 18
- 1.4 Courbes elliptiques sur les anneaux finis . . . 21
  - 1.4.1 Triplet primitif . . . 21
  - 1.4.2 Plan projectif sur un anneau . . . 22
  - 1.4.3 Courbes elliptiques sur un anneau fini . . . 23

2 Courbes elliptiques sur l'anneau $\mathbb{F}_q[e], e^2 = e$ 24
- 2.1 Introduction . . . 25
- 2.2 L'anneau $\mathbb{F}_q[e], e^2 = e$ . . . 25
  - 2.2.1 Opérations arithmétiques de $\mathbb{F}_q[e]$ . . . 26

2.2.2 Coûts des opérations arithmétiques . . . 28
2.3 Courbes elliptiques sur l'anneau $\mathbb{F}_q[e]$, $e^2 = e$. . . . 28
2.3.1 Les courbes elliptiques $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$ et $E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$ . . . 29
2.3.2 Classification des points de la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$ . . . 33
2.3.3 Applications cryptographiques . . . 34
2.4 Loi de groupe pour $E_{a,b}(\mathbb{F}_q[e])$ . . . 35
2.4.1 La structure de groupe pour $E_{a,b}(\mathbb{F}_q[e])$ . . . 35
2.4.2 Formules explicites d'addition pour $E_{a,b}(\mathbb{F}_{3^d}[e])$ . . . 37
2.5 Conclusion . . . 43

3 Courbes elliptiques sur l'anneau $\mathbb{F}_q[e]$, $e^3 = e^2$ 44
3.1 Introduction . . . 45
3.2 L'anneau $\mathbb{F}_q[e]$, $e^3 = e^2$ . . . 45
3.2.1 Propriétés algébriques . . . 45
3.2.2 Coûts des opérations arithmétiques . . . 48
3.3 Courbes elliptiques sur l'anneau $\mathbb{F}_q[e]$, $e^3 = e^2$ . . . 48
3.3.1 Réductions de $\mathbf{E}_{a,b}(\mathbb{F}_q[e])$ sur $\mathbb{F}_q$ . . . 49
3.3.2 Classification des points dans $\mathbf{E}_{a,b}(\mathbb{F}_q[e])$ . . . 51
3.3.3 Loi de groupe pour $\mathbf{E}_{a,b}(\mathbb{F}_q[e])$ . . . 54
3.4 Conclusion . . . 55

4 Applications cryptographiques 56
4.1 Préliminaires . . . 57
4.1.1 Introduction . . . 57
4.1.2 Terminologie . . . 59
4.1.3 Principe d'Auguste Kerckhoffs (1883) . . . 61
4.1.4 Objectifs de la cryptographie . . . 61
4.1.5 Cryptanalyse . . . 62
4.1.6 Sécurité des cryptosystèmes . . . 63
4.1.7 Signature numérique . . . 64
4.2 Algorithmes cryptographiques . . . 64
4.2.1 Algorithmes symétriques . . . 65
4.2.2 Algorithmes asymétriques . . . 67
4.3 Protocoles d'échange de clefs . . . 68
4.3.1 Problème du logarithme discret . . . 68
4.3.2 Protocole de Diffie-Hellman . . . 70
4.3.3 Cryptosystème d'ElGamal . . . 71
4.3.4 Chiffrement RSA . . . 72
4.4 Cryptographie sur les courbes elliptiques . . . 73
4.4.1 Échange de clefs Diffie-Hellman . . . 74
4.4.2 Cryptosystème d'ElGamal . . . 75
4.5 Chiffrement entièrement homomorphe . . . 75
4.5.1 Introduction . . . 75

4.5.2 Premier cryptosystème 78
4.5.2.1 L'anneau R 78
4.5.2.2 Description du cryptosystème basé sur R 79
4.5.3 Deuxième cryptosystème 81
4.5.3.1 L'anneau R 81
4.5.3.2 Description du cryptosystème basé sur R 82
4.5.3.3 Exemple numérique 84
4.5.4 Sécurité de ces cryptosystèmes 85
4.5.5 Conclusion 85

Conclusion générale et perspectives **87**

Références bibliographiques **89**

Index **97**

Table des figures

1.1 La courbe $Y^2 = X^3 + X^2$. 7
1.2 La courbe $Y^2 = X^3 + X$. 7
1.3 Addition des points distincts d'une courbe elliptique. 12
1.4 Doublement des points d'une courbe elliptique. 13

4.1 Schéma de communication entre Alice et Bob. 60
4.2 Schéma d'un cryptosystème. 65
4.3 Chiffrement et déchiffrement symétrique. 66
4.4 Chiffrement et déchiffrement asymétrique. 67
4.5 Echange de clés Diffie-Hellman. 70
4.6 Système de chiffrement à clé publique. 77

Liste des tableaux

1.1 Formes normales d'une courbe elliptique affine. 10
1.2 Formes normales d'une courbe elliptique projective. 11
1.3 Loi de groupe pour $y^2 = x^3 + x^2 + 1$ sur $\mathbb{F}_3$. 16
1.4 Loi de groupe pour $y^2 = x^3 + x + 1$ sur $\mathbb{F}_5$. 17

2.1 Équation de Weierstrass de $E_{a,b}(\mathbb{F}_q[e])$. 28
2.2 Réductions de $E_{a,b}(\mathbb{F}_q[e])$ sur $\mathbb{F}_q$. 29

4.1 Longueur de clefs entre ECC et RSA. 74

Liste des symboles

$\mathrm{card}\,(\mathbf{E}\,(\mathbb{F}_q))$ nombre de points de la courbe elliptique $\mathbf{E}/\mathbb{F}_q$

$\mathrm{char}\,(\mathbf{K})$ caractéristique du corps $\mathbf{K}$

Δ discriminant d'une courbe elliptique définie sur un corps, de la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$

Δ_0 discriminant de la courbe elliptique $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$

Δ_1 discriminant de la courbe elliptique $E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$

$(\mathbb{F}_q[e])^\times$ ensemble des éléments inversibles de l'anneau $\mathbb{F}_q[e]$

$[0:1:0]$ point à l'infini d'une courbe elliptique projective définie sur $\mathbf{K}$

$[\pi_i(X):\pi_i(Y):\pi_i(Z)]$ point de la courbe elliptique $E_{\pi_i(a),\pi_i(b)}\,(\mathbb{F}_q)$

$[X:Y:Z]$ point de la courbe elliptique $E_{a,b}\,(\mathbb{F}_q\,[e])$

$[x:y:z]$ classe d'équivalence du triplet (x,y,z)

$\mathbb{A}^2\,(\mathbf{K})$ plan affine défini sur le corps $\mathbf{K}$

$\mathbb{F}_q$ corps fini à q éléments

$\mathbb{F}_q[e],\ e^2=e$ anneau $\mathbb{F}_q[e]$, où $e^2=e$

$\mathbb{F}_q[X]$ anneau des polynômes à une seule variable et à coefficients dans le corps fini $\mathbb{F}_q$

$\mathbb{F}_q\,[e]\,,\ e^3=e^2$ anneau $\mathbb{F}_q\,[e]$, où $e^3=e^2$

$\mathbb{P}^2\,(\mathbb{F}_q[e])$ plan projectif sur l'anneau $\mathbb{F}_q[e]$

$\mathbb{P}^2\,(\mathbf{K})$ plan projectif défini sur le corps $\mathbf{K}$

$\mathbb{P}^2\,(R)$ plan projectif définie sur l'anneau R

$\mathbb{P}^2\,(\mathbb{F}_q)$ plan projectif sur $\mathbb{F}_q$

$\mathbb{R}$ corps des nombres réels

$\mathbf{E}/\mathbf{K}$ courbe elliptique définie sur $\mathbf{K}$

$\mathbf{E}(\mathbf{K})$ ensemble des points $\mathbf{K}$-rationnels de $\mathbf{E}/\mathbf{K}$

$\mathbf{E}/\mathbb{F}_q$ courbe elliptique définie sur $\mathbb{F}_q$

$\mathbf{K}$ corps algébriquement clos

$\mathbf{K}[X,Y,Z]$ anneau des polynômes à trois variables et à coefficients dans le corps $\mathbf{K}$

$\mathbf{K}[X,Y]$ anneau des polynômes à deux variables et à coefficients dans le corps $\mathbf{K}$

$\mathbf{K}[X,Y,Z]_{\text{hom}}$ ensemble des polynômes homogènes de l'anneau $\mathbf{K}[X,Y,Z]$

$\mathbf{K}^*$ groupe multiplicatif du corps $\mathbf{K}$

$\mathcal{C}$ courbe affine, espace de textes chiffrés

$\mathcal{C}^*$ clôture projective du courbe affine $\mathcal{C}$

$\mathcal{D}$ ensemble des opérations de déchiffrement

$\mathcal{E}$ ensemble des opérations de chiffrement

$\mathcal{K}$ espace de clefs

$\mathcal{M}$ espace de textes en clairs

$\mathcal{O}$ point à l'infini du plan projectif $\mathbb{P}^2(\mathbf{K})$

$\mathcal{P}(R)$ ensemble des triplets primitifs sur l'anneau R

π_0 homomorphisme d'anneaux de $\mathbb{F}_q[e]$ dans $\mathbb{F}_q$

π_1 homomorphisme d'anneaux de $\mathbb{F}_q[e]$ dans $\mathbb{F}_q$

$\widetilde{\pi}_0$ application définie de $\mathbf{E}_{a,b}(\mathbb{F}_q[e])$ et à valeurs dans $\mathbf{E}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$

$\widetilde{\pi}_1$ application définie de $\mathbf{E}_{a,b}(\mathbb{F}_q[e])$ et à valeurs dans $\mathbf{E}_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$

$\widetilde{\pi}$ isomomorphisme de groupes de $E_{a,b}(\mathbb{F}_q[e])$ dans $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q) \times E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$

$a = a_0 + a_1 e$ élément de l'anneau $\mathbb{F}_q[e],\ e^2 = e$

$a = a_0 + a_1 e + a_2 e^2$ élément de l'anneau $\mathbb{F}_q[e], e^3 = e^2$

$b = b_0 + b_1 e$ élément de l'anneau $\mathbb{F}_q[e],\ e^2 = e$

$b = b_0 + b_1 e + b_2 e^2$ élément de l'anneau $\mathbb{F}_q[e], e^3 = e^2$

$E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$ courbe elliptique sur $\mathbb{F}_q$

$E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$ courbe elliptique sur $\mathbb{F}_q$

$E_{a,b}(\mathbb{F}_q[e])$ courbe elliptique sur l'anneau $\mathbb{F}_q[e]$

j j-invariant d'une courbe elliptique

p nombre premier

q puissance d'un nombre premier

R anneau

$R^\times$ ensemble des éléments inversibles de l'anneau R

U ensemble des points finis du plan projectif $\mathbb{P}^2(\mathbf{K})$

Introduction

Les courbes elliptiques sont des objets mathématiques intensivement étudiés en géométrie algébrique et théorie des nombres, où plusieurs problèmes se traduisent naturellement par des questions sur les courbes elliptiques. Les courbes elliptiques ont trouvé des applications dans plusieurs domaines de mathématiques et il existe un volume important de publications à ce sujet :

- ◇ La résolution d'Andrew Wiles du dernier théorème de Fermat [140].
- ◇ Dans des algorithmes de la théorie des nombres [4, 73].
- ◇ Pour le test de la primalité des nombres [3, 49, 104].
- ◇ Dans la conception des algorithmes efficaces pour la factorisation des entiers [74, 76, 90, 91, 123].
- ◇ Dans la cryptologie, pour la génération des bits pseudo-aléatoires [61, 62] et les permutations unidirectionnelles [63].
- ◇ Dans la théorie du codage, où elles sont utilisées pour obtenir de bons codes correcteurs d'erreurs [36, 136].
- ◇ Dans la cryptographie, pour la construction des cryptosystèmes à clef publique [69, 87].

Durant ces trois dernières décennies, la cryptographie a connu un récent regain d'intérêt grâce à l'émergence de la théorie des courbes elliptiques. Tout a commencé en 1985, lorsque N. Koblitz [69] (voir aussi [68, Chap. 6]) et V. Miller [87] ont proposé indépendamment d'adapter les protocoles cryptographiques existant aux courbes elliptiques. Ils n'ont pas inventé un nouvel algorithme cryptographique à clef publique qui utilise les courbes elliptiques, mais ils ont réalisé une variante de la cryptographie à clef publique basée sur le *problème du logarithme discret* (PLD) [1] des algorithmes existant, tels que Diffie-Hellman et ElGamal à l'aide des courbes elliptiques définies sur des corps finis. Ensuite, en 1987, H. Lenstra a publié le document de référence [76] qui introduit et analyse la méthode de courbe elliptique (ECM) [2], qui est un puissant algorithme pour factoriser des entiers en utilisant ces courbes (la méthode de H. Lenstra est également décrite dans [23, Chap. 10, § 3], [31, Chap. 8, § 5] et [122, Chap. 4, § 4]).

1. En anglais, Discrete Logarithm Problem (DLP).
2. Elliptic Curve Method.

Depuis 1985, le développement de la cryptographie sur les courbes elliptiques a donné naissance à des nouveaux résultats ; le plus intéressant a été la démonstration publiée en 1990 par Menezes, Okamoto et Vanstone [84] et qui annonce que le PLD sur une courbe elliptique supersingulière peut être réduit au problème du logarithme discret sur un corps fini. Cette réduction est efficace pour la classe des courbes elliptiques super-singulières, et signifie que la complexité du logarithme discret sur ces courbes est la même que celle du corps fini sous-jacent. Compte tenu de ces résultats et pour éviter le cassage du PLD sur ce type de courbes, il est évident que lors de la conception d'un cryptosystème une certaine prudence doit être exercée dans le choix de la courbe et du corps sous-jacent et donc on devrait éviter l'ensemble (relativement petit) des courbes super-singulières si l'on veut avoir un cryptosystème dont la complexité est au meilleur de nos connaissances actuelles, d'une complexité exponentielle.

Le problème du logarithme discret, évoqué initialement par W. Diffie et M. Hellman en 1976 [33], va prendre la relève et faire preuve d'une résistance étonnante face aux attaques menées par les cryptanalystes. Quoique ces attaques aient réussi à le casser dans des cas particuliers [47, 56, 59], sa réputation n'a pas été touchée, et il demeure plus résistant dans le groupe de points d'une courbe elliptique. En effet, la structure du groupe dans chaque courbe elliptique a suffisamment de propriétés pour construire des algorithmes cryptographiques plus sûrs vu l'absence de certaines propriétés dans ce groupe qui faciliterait la cryptanalyse, par exemple les algorithmes de calcul d'indice [87]. À l'heure actuelle, on ne connaît pas d'algorithmes sous-exponentiels permettant de résoudre ce problème, et il semble que pour un nombre premier p, le PLD dans le groupe des points d'une courbe elliptique définie sur $\mathbb{F}_p$ est beaucoup plus difficile que celui dans le groupe multiplicatif du corps fini $\mathbb{F}_p$.

Dans la plupart des systèmes cryptographiques, la longueur des clés est un paramètre sécuritaire important. La cryptographie sur les courbes elliptiques présente deux intérêts majeurs pour la taille des clés par rapport aux autres cryptosystèmes [3] :

- ◇ La taille des clés est bien moindre (160 bits contre 1024 bits pour une sécurité équivalente à 2^{80}).
- ◇ La taille des clés évolue beaucoup plus lentement (224 bits contre 2048 pour une sécurité équivalente à 2^{112}).

Cela suggère qu'en utilisant un système cryptographique basé sur les courbes elliptiques, on obtient une sécurité équivalente avec des longueurs de clés beaucoup plus petites, ce qui est une raison pour laquelle la construction de cryptosystèmes en utilisant des courbes elliptiques est attrayante pour certains cryptologues. Les systèmes cryptographiques à clés de petites tailles sur les courbes elliptiques [53] sont très pratiques, et sont adaptés aux logiciels et à la mise en œuvre du matériel. Par exemple, *Certicom* [4], une entreprise qui soutient fortement la cryptographie sur les courbes elliptiques, prétend [127, p. 139] : « Les appareils nécessitent moins de stockage, moins de puissance, moins de mémoire et moins de bandes passantes que les autres systèmes. Cela vous permet de mettre en œuvre la cryptographie dans les plates-formes qui sont limitées, telles que les appareils sans fil, les ordinateurs portables, les applications mobiles et les cartes intelligentes, etc. ».

3. `https://www.keylength.com/fr/`
4. `https://blackberry.certicom.com/`

Le sujet d'étude de ma thèse s'inscrit dans le cadre des applications cryptographiques des courbes elliptiques définies sur certains anneaux finis et non-locaux. Les courbes elliptiques définies sur un anneau ont été étudiées sous différents aspects :

- ◇ En géométrie algébrique : l'étude de ces courbes dans le cas d'un anneau local est exposée dans le livre de Silverman [121].
- ◇ En théorie des nombres : H. Lenstra a donné une méthode de factorisation des grands entiers en utilisant des courbes elliptiques sur l'anneau $\mathbb{Z}_{pq}$, où p et q sont deux nombres premiers distincts [75].
- ◇ En cryptographie :
  - ○ S. M. Molleví a construit un cryptosystème de type ElGamal utilisant ces courbes sur un anneau $\mathbb{Z}_{pq}$, où p et q sont deux nombres premiers distincts [89].
  - ○ M. Virat a construit un cryptosystème semblable à celui d'ElGamal avec des performances supplémentaires, en utilisant des courbes elliptiques définies sur l'anneau local $\mathbb{F}_p[\epsilon], \epsilon^2 = 0$, où p est un nombre premier supérieur ou égal à 5 [138].
  - ○ A. Chillali a généralisé les travaux de M. Virat sur l'anneau local $\mathbb{F}_q[\epsilon], \epsilon^n = 0$, où q est une puissance d'un nombre premier p supérieur ou égal à 5 et n un entier strictement positif [21].
  - ○ Les cas particuliers des anneaux $\mathbb{F}_{2^d}[\epsilon], \epsilon^n = 0$ et $\mathbb{F}_{3^d}[\epsilon], \epsilon^n = 0$, où d et n des entiers strictement positifs, sont étudiés respectivement par A. Tadmori [131] et M. H. Hassib [54] dans leurs travaux de thèses.

De notre côté, nous nous intéressons aux applications cryptographiques des courbes elliptiques définies sur les anneaux $\mathbb{F}_q[e]$, où $e^2 = e$ et $e^3 = e^2$. Dans un premier temps, nous avons étudié les structures algébriques de ces anneaux, sur lesquels nous avons par la suite développé l'étude théorique de ces courbes elliptiques, et puis dans un second temps, nous avons pu construire un système de chiffrement entièrement homomorphe sur chacun d'eux.

Le présent mémoire est composé de quatre chapitres organisés de la façon suivante :

Chapitre 1 : contient des préliminaires nécessaires à l'élaboration de cette thèse. Particulièrement, il est destiné aux prérequis de base sur les courbes elliptiques définies sur un corps. Nous rappelons dans ce chapitre les définitions et les propriétés des courbes elliptiques affines et projectives, puis nous donnons les formules explicites d'addition permettant de calculer la somme des points d'une courbe elliptique dans les deux cas affine et projective ; et nous terminons par quelques résultats concernant les courbes elliptiques définies sur un anneau.

Chapitre 2 : pour pouvoir réaliser des applications cryptographiques sur les courbes elliptiques définies sur l'anneau non-local $\mathbb{F}_q[e]$, où $e^2 = e$, nous commençons par étudier ces objets mathématiques. Ainsi, notre intérêt final dans ce chapitre est d'aboutir aux formules explicites des calculs à effectuer pour obtenir la somme des points dans la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$. Le résultat essentiel porté par ce chapitre a beaucoup d'intérêt cryptographique et se résume dans l'isomorphisme entre la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$ et le produit des courbes elliptiques $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$ et $E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$. Il s'agit de notre première contribution dans cette thèse.

Chapitre 3 : dans ce chapitre nous avons étudié en caractéristique supérieure ou égale à 5 des courbes elliptiques définies sur l'anneau non-local $\mathbb{F}_q[e]$, où $e^3 = e^2$, dans le but d'avoir des idées suffisantes pour aboutir à une généralisation des courbes elliptiques définies sur les anneaux de type $\mathbb{F}_q[e]$, où $e^{n+1} = e^n$, avec n un entier supérieur ou égal à 2. Les résultats essentiels portés par cette deuxième contribution sont la classification des points de la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$, ainsi que les formules explicites permettant de calculer sa loi de groupe. Dans la partie perspective de recherche (voir page 87), nous posons une question de grand intérêt sur cette courbe elliptique.

Chapitre 4 : dans ce chapitre, nous allons donner deux applications cryptographiques des résultats théoriques trouvés précédemment. Ainsi, nous avons commencé ce chapitre par des préliminaires sur la cryptographie, puis nous avons parlé des algorithmes symétriques et asymétriques, ensuite nous avons introduit le célèbre problème du logarithme discret dans le cadre des protocoles asymétriques d'échange de clés, afin de présenter l'article de base de la cryptographie à clé publique due à W. Diffie et M. Hellman [33] et le cryptosystème d'ElGamal [40] ; ainsi que le chiffrement RSA [111] qui est basé sur le problème de factorisation de grands entiers. La cryptographie sur les courbes elliptiques est aussi introduite dans ce chapitre, où nous examinons brièvement les versions Diffie-Hellman et ElGamal pour les courbes elliptiques. Dans la dernière section de ce chapitre, nous avons proposé deux systèmes de chiffrement entièrement homomorphes basés sur les courbes elliptiques $E_{a,b}(\mathbb{F}_q[e])$, dans les deux cas $e^2 = e$ et $e^3 = e^2$; il s'agit de notre troisième contribution dans cette thèse.

1

Préliminaires sur les courbes elliptiques

Sommaire

1.1 Courbes planes 6
1.1.1 Courbes affines planes 6
1.1.2 Courbes projectives planes 7
1.2 Courbes elliptiques 9
1.2.1 Courbes elliptiques affines 9
1.2.2 Courbes elliptiques projectives 11
1.3 Structure de groupe d'une courbe elliptique 11
1.3.1 Construction géométrique 12
1.3.2 Formules d'addition en coordonnées affines 13
1.3.3 Exemples 16
1.3.4 Formules d'addition en coordonnées projectives 18
1.4 Courbes elliptiques sur les anneaux finis 21
1.4.1 Triplet primitif 21
1.4.2 Plan projectif sur un anneau 22
1.4.3 Courbes elliptiques sur un anneau fini 23

Ce chapitre est une brève introduction aux courbes elliptiques. Essentiellement, nous ne cherchons pas l'exhaustivité dans la présentation de la théorie des courbes elliptiques, mais nous souhaitons plutôt développer une introduction aux courbes elliptiques dont nous aurons besoin dans le reste de cette thèse. Précisément, on va s'intéresser aux formes normales d'une courbe elliptique définie sur un corps fini, puis nous établirons les formules explicites pour la loi du groupe selon les différents cas particuliers et nous finirons par des préliminaires sur les courbes elliptiques définies sur des anneaux finis.

Pour une vision détaillée et précise sur les courbes elliptiques, le lecteur pourra se référer aux livres suivants :

◇ Silverman. *The arithmetic of elliptic curves* [120].

- ◇ Silverman et Tate. *Rational points on elliptic curves* [122].
- ◇ Charlap et Robbins. *An elementary introduction to elliptic curves* [18].
- ◇ Koblitz. *A course in number theory and cryptography* [68].
- ◇ Enge. *Elliptic curves and their applications to cryptography : an introduction* [41].
- ◇ Fulton. *Algebraic curves : an introduction to algebraic geometry* [45].

Le long de ce chapitre, $\mathbf{K}$ désigne un corps algébriquement clos, et $\mathbf{K}[X,Y]$ est l'anneau des polynômes à deux variables et à coefficients dans $\mathbf{K}$.

1.1 Courbes planes

Dans cette section, nous présentons quelques principes de base des courbes planes.

1.1.1 Courbes affines planes

Les courbes affines planes sur $\mathbf{K}$ sont des courbes définies dans le plan affine noté $\mathbb{A}^2(\mathbf{K})$ et défini par : $\mathbb{A}^2(\mathbf{K}) := \mathbf{K} \times \mathbf{K} = \{(x,y) \mid x \in \mathbf{K} \text{ et } y \in \mathbf{K}\}$.

Définitions 1.1.1 *Soit C un polynôme de $\mathbf{K}[X,Y]$.*

1. *On dit qu'un point $(x,y) \in \mathbb{A}^2(\mathbf{K})$ est un zéro de C si $C(x,y) = 0$.*
2. *On dit que C est irréductible si C ne peut pas s'écrire comme produit de deux polynômes non-triviaux de $\mathbf{K}[X,Y]$.*

Définitions 1.1.2 *(voir [41, Définition 2.2 & 2.3, p. 13]).*
Soit C un polynôme irréductible de $\mathbf{K}[X,Y]$.

1. *L'ensemble des zéros de C dans $\mathbb{A}^2(\mathbf{K})$ est dit courbe affine plane définie sur $\mathbf{K}$. On note cette courbe par $\mathcal{C}$ et on a : $\mathcal{C} = \left\{(x,y) \in \mathbb{A}^2(\mathbf{K}) \mid C(x,y) = 0\right\}$.*
2. *Un point $P = (x,y) \in \mathcal{C}$ est dit singulier, si $\dfrac{\partial C}{\partial X}(P) = \dfrac{\partial C}{\partial Y}(P) = 0$.*
3. *On dit que $\mathcal{C}$ est une courbe singulière, si elle possède au moins un point singulier.*

Définition 1.1.1 *(voir [41, Définition 2.41, p. 36]).*
Soit $P = (x,y)$ un point non-singulier d'une courbe affine plane $\mathcal{C}$. La droite tangente à $\mathcal{C}$ en P est la droite de $\mathbb{A}^2(\mathbf{K})$ définie par : $\dfrac{\partial C}{\partial X}(P)(X-x) + \dfrac{\partial C}{\partial Y}(P)(Y-y) = 0$.

Exemple 1.1.1 *Considérons les deux courbes affines $\mathcal{C}_1$ et $\mathcal{C}_2$ définies sur $\mathbb{R}$ respectivement par : $C_1(X,Y) = Y^2 - X^3 - X^2$ et $C_2(X,Y) = Y^2 - X^3 - X$.*

1. *On a : $\dfrac{\partial C_1}{\partial X}(X,Y) = -\left(3X^2 + 2X\right)$ et $\dfrac{\partial C_1}{\partial Y}(X,Y) = 2Y$, donc $\dfrac{\partial C_1}{\partial X}(0,0) = \dfrac{\partial C_1}{\partial Y}(0,0) = 0$; et alors $(0,0)$ est un point singulier dans la courbe $\mathcal{C}_1$.*
2. *On a : $\dfrac{\partial C_2}{\partial X}(X,Y) = -\left(3X^2 + 1\right)$, donc $\dfrac{\partial C_2}{\partial X}(0,0) = -1$; et alors $(0,0)$ est un point non-singulier dans la courbe $\mathcal{C}_2$. La tangente à $\mathcal{C}_2$ en $(0,0)$ est donnée par $X = 0$.*

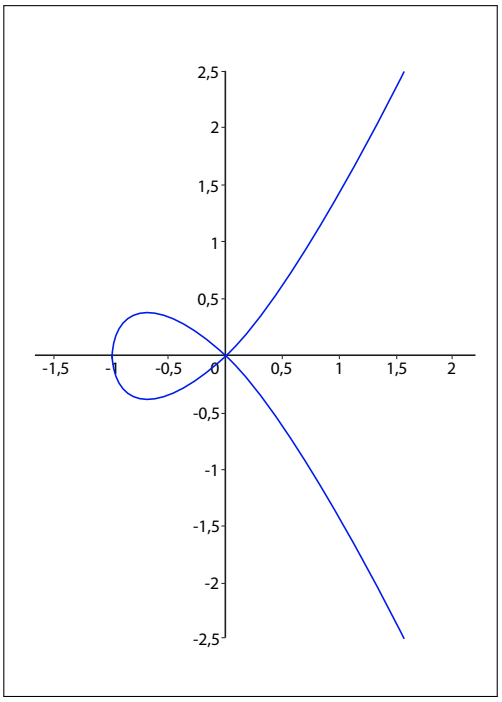

FIGURE 1.1: La courbe $Y^2 = X^3 + X^2$.

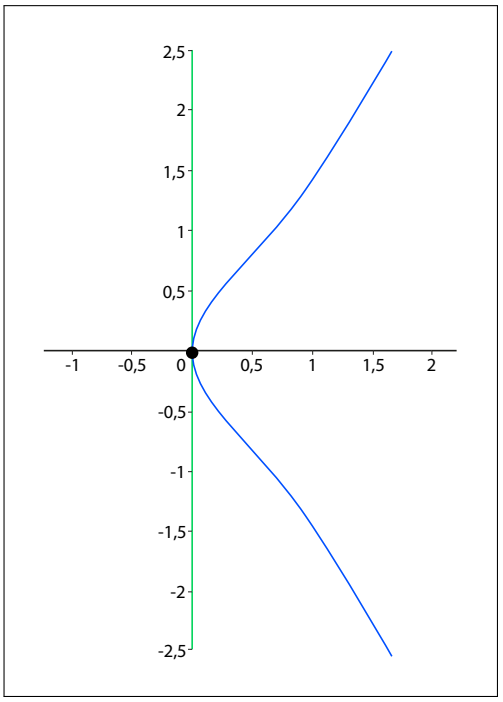

FIGURE 1.2: La courbe $Y^2 = X^3 + X$.

1.1.2 Courbes projectives planes

Une courbe projective plane est une courbe affine plane dans laquelle on ajoute un point particulier noté $\mathcal{O}$ et dit le point à l'infini. Lorsque ce nouveau point est ajouté à un plan affine, on parlera dans ce cas d'un plan projectif.

Définition 1.1.2 *(voir [120, Chap. 1, § 2, p. 10]).*
Le plan projectif sur $\mathbf{K}$ *est l'ensemble des classes d'équivalences de* $\mathbf{K}^3 \setminus \{(0,0,0)\}$ *modulo la relation d'équivalence* $\sim$ *définie par :*

$$(x_1, y_1, z_1) \sim (x_2, y_2, z_2) \Leftrightarrow \exists \lambda \in \mathbf{K} \setminus \{0\} : \ (x_2, y_2, z_2) = \lambda (x_1, y_1, z_1) .$$

L'ensemble quotient $\dfrac{\mathbf{K}^3 \setminus \{(0,0,0)\}}{\sim}$ *est noté* $\mathbb{P}^2(\mathbf{K})$ *et la classe d'équivalence d'un élément* $(x, y, z) \in \mathbf{K}^3 \setminus \{(0,0,0)\}$ *est noté* $[x : y : z]$. *Ainsi, on a :*

$$[x_1 : y_1 : z_1] = [x_2 : y_2 : z_2] \Leftrightarrow \exists \lambda \in \mathbf{K} \setminus \{0\} : \ x_2 = \lambda x_1 \ , \ y_2 = \lambda y_1 \ \text{et} \ z_2 = \lambda z_1.$$

Définition 1.1.3 *(voir [41, Définition 2.17, pp. 26–27]).*
Soit U *le sous-ensemble du plan projectif* $\mathbb{P}^2(\mathbf{K})$ *constitué des points dont la troisième coordonnée est non nulle. Les applications* $(.,.)^*$ *et* $[.,.,.]_*$ *définies par :*

$$\begin{aligned} (.,.)^* : \ \mathbb{A}^2(\mathbf{K}) &\longrightarrow U \\ P = (x, y) &\longmapsto P^* = (x, y)^* = [x : y : 1] \end{aligned}$$

et

$$\begin{array}{rcl} [.,.,.]_* : U & \longrightarrow & \mathbb{A}^2(\mathbf{K}) \\ P=[x:y:z] & \longmapsto & P_*=[x:y:z]_*=\left[\frac{x}{z}:\frac{y}{z}:1\right]_*=\left(\frac{x}{z},\frac{y}{z}\right) \end{array}$$

sont dites respectivement homogénéisation et déshomogénéisation des points suivant z.

Remarques 1.1.1 :

1. *Les applications $(.,.)^*$ et $[.,.,.]_*$ sont réciproques l'une de l'autre et donc on peut identifier l'ensemble U avec le plan affine $\mathbb{A}^2(\mathbf{K})$.*
2. *Les points de l'ensemble U sont dits points finis du plan projectif $\mathbb{P}^2(\mathbf{K})$; alors que les autres points sont dits points à l'infini et ce sont les nouveaux points du plan projectif.*
3. *Le plan projectif $\mathbb{P}^2(\mathbf{K})$ s'identifie à l'ensemble $\mathbb{A}^2(\mathbf{K}) \cup \{\mathcal{O}\}$ où $\mathcal{O}$ est le point à l'infini.*

Corollaire 1.1.1 *Deux droites distinctes dans $\mathbb{P}^2(\mathbf{K})$ se coupent toujours en un unique point.*

Définition 1.1.4 *Soit $C \in \mathbf{K}[X,Y,Z]$ et soit d un entier positif. On dit que C est un polynôme homogène de degré d, si tous les monômes de C ont le même degré d ; où le degré d'un monôme $aX^iY^jZ^k$ de C, avec $a \in \mathbf{K}^*$ et i,j et k sont des entiers positifs est défini par $\deg\left(aX^iY^jZ^k\right) = i+j+k$. L'ensemble des polynômes homogènes de $\mathbf{K}[X,Y,Z]$ est noté $\mathbf{K}[X,Y,Z]_{\text{hom}}$.*

Définition 1.1.5 *(voir [41, Définition 2.16, p. 26]).*
L'ensemble des zéros dans le plan projectif $\mathbb{P}^2(\mathbf{K})$ d'un polynôme irréductible et homogène $C \in \mathbf{K}[X,Y,Z]_{\text{hom}}$ est dit courbe projective plane.
Un point $P=[x:y:z]$ d'une courbe projective plane donnée par un polynôme irréductible et homogène $C \in \mathbf{K}[X,Y,Z]_{\text{hom}}$ est dit point singulier si : $\frac{\partial C}{\partial X}(P) = \frac{\partial C}{\partial Y}(P) = \frac{\partial C}{\partial Z}(P) = 0$.

Remarque 1.1.1 *Soit $C \in \mathbf{K}[X,Y,Z]_{\text{hom}}$ de degré d. Pour tout $(x,y,z) \in \mathbf{K}^3 \setminus \{(0,0,0)\}$ et pour tout $t \in \mathbf{K}^*$, on a : $C(tx,ty,tz) = t^dC(x,y,z)$; et donc si C s'annule en (x,y,z), il sera nul sur toute la classe de (x,y,z).*

Définition 1.1.6 *(voir [41, Définition 2.18, p. 27]).*
Soient $f \in \mathbf{K}[X,Y]$ et $F \in \mathbf{K}[X,Y,Z]_{\text{hom}}$. On définit les polynômes $f^* \in \mathbf{K}[X,Y,Z]_{\text{hom}}$ et $F_* \in \mathbf{K}[X,Y]$ par : $f^*(X,Y,Z) = Z^{\deg(f)}f\left(\frac{X}{Z},\frac{Y}{Z}\right)$ et $F_*(X,Y) = F(X,Y,1)$.
f^* est dite homogénéisation de f et F_* est dite déshomogénéisation de F.

Proposition 1.1.1 *(voir [41, Proposition 2.19, p. 27]).*
Soient $f,g \in \mathbf{K}[X,Y]$ et $F,G \in \mathbf{K}[X,Y,Z]_{\text{hom}}$. Alors :

1. $(fg)^* = f^*g^*$
2. $(FG)_* = F_*G_*$
3. $(f^*)_* = f$
4. *Si Z ne divise pas F, alors $(F_*)^* = F$.*

Corollaire 1.1.2 *(voir [41, Corollaire 2.20, p. 27]).*
Un polynôme $f \in \mathbf{K}[X,Y]$ définit une courbe affine si, et seulement si f^* définit une courbe projective.

Définition 1.1.7 *([41, Définition 2.21, p. 27]).*
Si $\mathcal{C}$ est une courbe affine, alors $\mathcal{C}^*$ est dite sa clôture projective.

1.2 Courbes elliptiques

Une courbe elliptique est un cas particulier de courbes algébriques, donnée par une cubique irréductible et non-singulière. Dans cette section, nous présenterons les courbes elliptiques par leurs équations de Weierstrass affines et projectives.

1.2.1 Courbes elliptiques affines

Définition 1.2.1 *(voir [41, Définition 2.7, p. 15] & [120, Chap. 3, § 1, pp. 46–48]).*
Une équation de Weierstrass affine sur $\mathbf{K}$ est une équation de la forme :

$$\mathbf{E}:\ Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6\ , \tag{1.1}$$

avec $(a_1, a_2, a_3, a_4, a_6) \in \mathbf{K}^5$.
Une équation de Weierstrass affine et non-singulière définit une courbe elliptique affine sur $\mathbf{K}$, qu'on note par $\mathbf{E}/\mathbf{K}$; et l'ensemble des solutions dans $\mathbb{A}^2(\mathbf{K})$ de cet équation est noté $\mathbf{E}(\mathbf{K})$ et est dit ensemble des points $\mathbf{K}$-rationnels de $\mathbf{E}/\mathbf{K}$.
À toute équation de Weierstrass (1.1)*, on définit les quantités suivantes :*

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2\ ;\\
b_4 &= 2a_4 + a_1a_3\ ;\\
b_6 &= a_3^2 + 4a_6\ ;\\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2\ ;\\
c_4 &= b_2^2 - 24b_4\ ;\\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6\ ;\\
j &= \frac{c_4^3}{\Delta}\ \textit{si}\ \Delta \neq 0.
\end{aligned}$$

Δ est appelé le discriminant de $\mathbf{E}$ et j son j-invariant ; et si l'équation (1.1) *définit une courbe elliptique $\mathbf{E}$ sur $\mathbf{K}$, alors dans ce cas Δ est appelé le discriminant de $\mathbf{E}/\mathbf{K}$ et j son j-invariant.*

Proposition 1.2.1 *(voir [41, pp. 15–16]).*
Toute équation de Weierstrass (1.1) *est irréductible dans $\mathbf{K}[X,Y]$.*

Proposition 1.2.2 *(voir [120, Proposition 1.4(a), p. 50]).*
Une courbe donnée par une équation de Weierstrass est singulière si, et seulement si son discriminant est nul.

Corollaire 1.2.1 *Une courbe elliptique affine* $\mathbf{E}/\mathbf{K}$ *est une courbe donnée par une équation de Weierstrass* (1.1) *dont le discriminant* Δ *est non nul. Dans ce cas, la tangente à* $\mathbf{E}/\mathbf{K}$ *en un point* $P = (x, y) \in \mathbf{E}(\mathbf{K})$ *est donnée par :*

$$\left(a_1 y - \left(3x^2 + 2a_2 x + a_4\right)\right)(X - x) + (2y + a_1 x + a_3)(Y - y) = 0.$$

Remarques 1.2.1 :

1. *On écrit l'équation de Weierstrass* (1.1) *sous la forme* $f(X, Y) = 0$, *avec :*

$$f(X, Y) = Y^2 + a_1 XY + a_3 Y - \left(X^3 + a_2 X^2 + a_4 X + a_6\right).$$

2. *Si deux courbes elliptiques sur* $\mathbf{K}$ *ont le même* j*-invariant, alors elles sont isomorphes (voir [120, Proposition 1.4(b), p. 50]).*

3. *L'utilisation des courbes elliptiques super-singulières*[1] *en cryptographie est risquée et n'est pas sécurisée ; en effet Menezes, Okamoto et Vanstone ont lancé une attaque sur ce type de courbes [84].*

4. *Si* $\Delta \neq 0$, *alors selon la caractéristique du corps* $\mathbf{K}$, *une courbe elliptique* $\mathbf{E}/\mathbf{K}$ *a l'une des formes normales suivantes (voir [120, Appendix A, Proposition 1.1, pp. 324–325]) :*

<table>
<tr><td colspan="2" rowspan="2"></td><td colspan="2">Forme affine de l'équation de Weierstrass</td></tr>
<tr><td colspan="2">$Y^2 = X^3 + a_4X + a_6$</td></tr>
<tr><td colspan="2" rowspan="2">$\mathrm{char}(\mathbf{K}) \neq 2, 3$</td><td>$\Delta = -16\left(4a_4^3 + 27a_6^2\right)$</td><td>$j = 1728\dfrac{4a_4^3}{4a_4^3 + 27a_6^2}$</td></tr>
<tr><td rowspan="2">$\mathrm{char}(\mathbf{K}) = 3$</td><td rowspan="2">$j = 0$</td><td colspan="2">$Y^2 = X^3 + a_4X + a_6$</td></tr>
<tr><td colspan="2">$\Delta = -a_4^3$</td></tr>
<tr><td rowspan="2"></td><td rowspan="2">$j \neq 0$</td><td colspan="2">$Y^2 = X^3 + a_2X^2 + a_6$</td></tr>
<tr><td>$\Delta = -a_2^3a_6$</td><td>$j = -a_2^3/a_6$</td></tr>
<tr><td rowspan="4">$\mathrm{char}(\mathbf{K}) = 2$</td><td rowspan="2">$j = 0$</td><td colspan="2">$Y^2 + a_3Y = X^3 + a_4X + a_6$</td></tr>
<tr><td colspan="2">$\Delta = a_3^4$</td></tr>
<tr><td rowspan="2">$j \neq 0$</td><td colspan="2">$Y^2 + XY = X^3 + a_2X^2 + a_6$</td></tr>
<tr><td>$\Delta = a_6$</td><td>$j = 1/a_6$</td></tr>
</table>

TABLE 1.1: Formes normales d'une courbe elliptique affine.

1. Courbes elliptiques ayant un j-invariant nul.

1.2.2 Courbes elliptiques projectives

Les courbes elliptiques projectives se définissent comme étant la clôture projective des courbes elliptiques affines. Ainsi, plusieurs résultats de la section précédente se généralisent facilement dans le cas projectif.

Définition 1.2.2 *(voir [41, Définition 2.24, p. 29] & [120, Chap. 3, § 1, p. 46]).*
Une équation de Weierstrass projective sur $\mathbf{K}$ *est une équation de la forme :*

$$\mathbf{E}: \ Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{1.2}$$

avec $(a_1, a_2, a_3, a_4, a_6) \in \mathbf{K}^5$. *Le discriminant* Δ *et le* j*-invariant de l'équation* (1.2) *sont comme dans la Définition 1.2.1.*
Une équation de Weierstrass projective et non-singulière sur $\mathbf{K}$ *définit une courbe elliptique projective dans* $\mathbb{P}^2(\mathbf{K})$.

Proposition 1.2.3 *(voir [41, Proposition 2.25, p. 29]).*
Toute équation de Weierstrass projective est irréductible. Elle contient un unique point à l'infini noté $[0:1:0]$, *et elle est singulière si, et seulement si son discriminant est nul.*

Remarque 1.2.1 *D'après la Table 1.1, une courbe elliptique projective a l'une des formes normales suivantes :*

	Forme projective de l'équation de Weierstrass
$\text{char}(\mathbf{K}) \neq 2, 3$	$Y^2Z = X^3 + a_4XZ^2 + a_6Z^3$
$\text{char}(\mathbf{K}) = 3$ et $j = 0$	$Y^2Z = X^3 + a_4XZ^2 + a_6Z^3$
$\text{char}(\mathbf{K}) = 3$ et $j \neq 0$	$Y^2Z = X^3 + a_2X^2Z + a_6Z^3$
$\text{char}(\mathbf{K}) = 2$ et $j = 0$	$Y^2Z + a_3YZ^2 = X^3 + a_4XZ^2 + a_6Z^3$
$\text{char}(\mathbf{K}) = 2$ et $j \neq 0$	$Y^2Z + XYZ = X^3 + a_2X^2Z + a_6Z^3$

TABLE 1.2: Formes normales d'une courbe elliptique projective.

1.3 Structure de groupe d'une courbe elliptique

Les courbes elliptiques définies sur un corps peuvent être munies d'une structure de groupe abélien noté additivement. La construction géométrique de l'addition des points d'une courbe elliptique se fait par la méthode de la sécante-tangente, où la somme de deux points est plus ou moins le point d'intersection de la droite passant par ces deux points avec la courbe. Cette loi de groupe est basée sur la proposition suivante :

Proposition 1.3.1 *(voir [120, Chap. 3, § 2, p. 55]).*
Soit $\mathbf{E}$ *une courbe elliptique définie sur* $\mathbf{K}$ *et soit* L *une droite projective sur* $\mathbf{K}$*. Si la droite* L *coupe la courbe* $\mathbf{E}$ *en deux points (comptés avec leur multiplicité), alors* L *coupe* $\mathbf{E}$ *en un unique troisième point.*

L'objectif de cette section est de définir géométriquement l'addition des points d'une courbe elliptique ; ainsi que de donner explicitement les formules permettant de calculer cette loi de groupe.

1.3.1 Construction géométrique

Soit $\mathbf{E}$ une courbe elliptique définie sur $\mathbf{K}$, et soient P et Q deux points de $\mathbf{E}(\mathbf{K})$ et soit L la droite passant par P et Q. La droite L coupe la courbe $\mathbf{E}$ en un unique troisième point noté R. Soit S le point d'intersection de la droite passant par le point à l'infini $\mathcal{O} = [0 : 1 : 0]$ et le point R avec la courbe $\mathbf{E}$. L'opération $P + Q = S$ munit l'ensemble $\mathbf{E}(\mathbf{K})$ d'une structure de groupe abélien ayant le point à l'infini $\mathcal{O}$ comme élément neutre et nous avons :

Théorème 1.3.1 *(voir [41, Théorème 2.46, p. 40] & [82, Théorème 2.3, p. 18]).*
$(\mathbf{E}, +)$ *est un groupe abélien ayant le point à l'infini* $\mathcal{O} = [0 : 1 : 0]$ *comme élément neutre.*

La construction géométrique de cette loi de groupe est illustrée par les figures suivantes (voir [82, Chap. 2, § 2, pp. 17–18]) :

1. Si $P \neq Q$, alors :
   (a) Si la droite L coupe la courbe en un troisième point R, alors $P + Q = S$.
   (b) Si la droite L est verticale, alors $Q = -P$ et dans ce cas $P + Q = \mathcal{O}$.

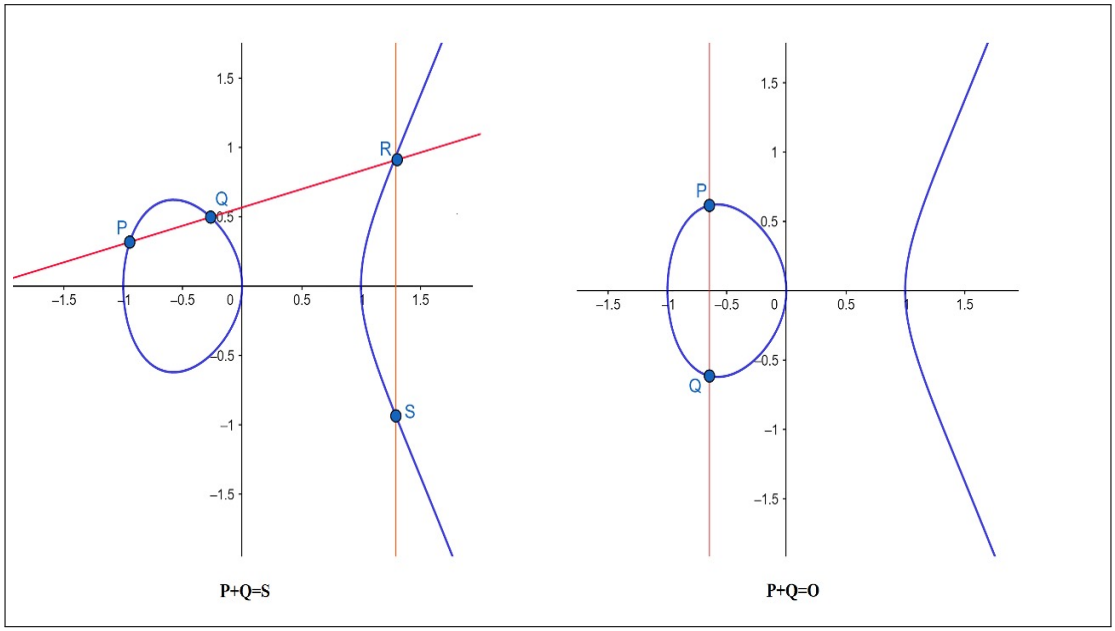

FIGURE 1.3: Addition des points distincts d'une courbe elliptique.

2. Si $P = Q$, alors :
   (a) Si la tangente à $\mathbf{E}$ en P coupe la courbe en un autre point R, alors $2P = S$.
   (b) Si la tangente à $\mathbf{E}$ en P est verticale, alors $2P = \mathcal{O}$.

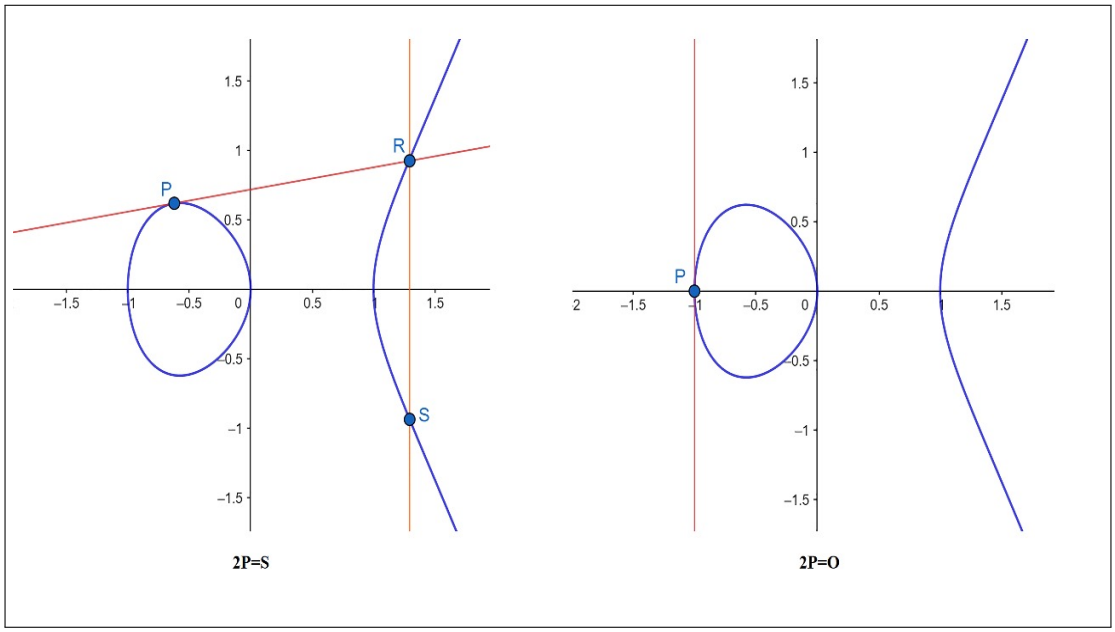

FIGURE 1.4: Doublement des points d'une courbe elliptique.

1.3.2 Formules d'addition en coordonnées affines

Proposition 1.3.2 *(voir [41, p. 41] & [120, Group Law Algorithm 2.3, pp. 58–59]).*
Soient P et Q deux points d'une courbe elliptique $\mathbf{E}/\mathbf{K}$ donnée par l'équation de Weierstrass :

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

1. *Si $P = [0 : 1 : 0]$ ou $Q = [0 : 1 : 0]$, alors $P + Q = P$ (ou bien $P + Q = Q$).*
2. *Si $P = [x_1 : y_1 : 1]$ et $Q = [x_2 : y_2 : 1]$, alors :*
   (a) L'opposé du point P est le point $-P = [x_1 : -(y_1 + a_1x_1 + a_3) : 1]$.
   (b) Si $x_1 = x_2$ et $y_2 = -y_1 - a_1x_1 - a_3$, alors $P + Q = [0 : 1 : 0]$.
   (c) Si $x_1 \neq x_2$ ou $y_2 \neq -y_1 - a_1x_1 - a_3$, alors $P + Q = [x_3 : y_3 : 1]$, où x_3 et y_3 sont données par :

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \text{ et } y_3 = -(\lambda + a_1)\, x_3 - a_3 - \mu,$$

$$\text{avec } \lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{si } P \neq Q \\ \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, & \text{si } P = Q \end{cases} \quad \text{et } \mu = y_1 - \lambda x_1.$$

En substituant λ et μ par leurs valeurs, on obtient les formules suivantes pour x_3 et y_3 :

Corollaire 1.3.1 *(voir [41, Table 2.3, p. 42]).*

$$x_3 = \begin{cases} \left(\dfrac{y_2 - y_1}{x_2 - x_1}\right)^2 + a_1\left(\dfrac{y_2 - y_1}{x_2 - x_1}\right) - a_2 - x_1 - x_2 \ , \ si\ P \neq Q \\ \\ \left(\dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}\right)^2 + a_1\left(\dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}\right) - a_2 - 2x_1 \ , \ si\ P = Q \end{cases} \tag{1.3}$$

$$y_3 = \begin{cases} \left(\dfrac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1 - (a_1x_3 + a_3) \ , \ si\ P \neq Q \\ \\ \left(\dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}\right)(x_1 - x_3) - y_1 - (a_1x_3 + a_3) \ , \ si\ P = Q \end{cases} \tag{1.4}$$

Selon les formes normales de l'équation de Weierstrass d'une courbe elliptique (voir Table 1.2), les valeurs de x_3 et y_3 sont données à nouveau par les corollaires suivants :

Corollaire 1.3.2 *(formules d'addition pour* $\mathrm{char}\,(\mathbf{K}) = 2$*)(voir [41, pp. 42–43] & [82, pp. 21–23]).*

1. *Si* $j \neq 0, Y^2Z + XYZ = X^3 + a_2X^2Z + a_6Z^3$*, alors :*

$$x_3 = \begin{cases} \left(\dfrac{y_1 + y_2}{x_1 + x_2}\right)^2 + \left(\dfrac{y_1 + y_2}{x_1 + x_2}\right) + a_2 + x_1 + x_2 \ , \ si\ P \neq Q \\ \\ x_1^2 + \dfrac{a_6}{x_1^2} \ , \ si\ P = Q \end{cases} \tag{1.5}$$

$$y_3 = \begin{cases} \left(\dfrac{y_1 + y_2}{x_1 + x_2}\right)(x_1 + x_3) + y_1 + x_3 \ , \ si\ P \neq Q \\ \\ \left(\dfrac{x_1^2 + y_1}{x_1}\right)x_3 + x_1^2 + x_3 \ , \ si\ P = Q \end{cases} \tag{1.6}$$

2. *Si* $j = 0, Y^2Z + a_3YZ^2 = X^3 + a_4XZ^2 + a_6Z^3$*, alors :*

$$x_3 = \begin{cases} \left(\dfrac{y_1 + y_2}{x_1 + x_2}\right)^2 + x_1 + x_2 \ , \ si\ P \neq Q \\ \\ \left(\dfrac{x_1^2 + a_4}{a_3}\right)^2 \ , \ si\ P = Q \end{cases} \tag{1.7}$$

$$y_3 = \begin{cases} \left(\dfrac{y_1+y_2}{x_1+x_2}\right)(x_1+x_3)+y_1+a_3\ ,\ si\ P\neq Q \\ \\ \left(\dfrac{x_1^2+a_4}{a_3}\right)(x_1+x_3)+y_1+a_3\ ,\ si\ P=Q \end{cases} \tag{1.8}$$

Corollaire 1.3.3 *(formules d'addition pour* $\mathrm{char}\,(\mathbf{K})=3$*)(voir [41, pp. 41–42]).*

1. *Si* $j\neq 0, Y^2Z=X^3+a_2X^2Z+a_6Z^3$*, alors :*

$$x_3 = \begin{cases} \left(\dfrac{y_2+2y_1}{x_2+2x_1}\right)^2+2\left(a_2+x_1+x_2\right)\ ,\ si\ P\neq Q \\ \\ \left(\dfrac{a_2x_1}{y_1}\right)^2+2a_2+x_1\ ,\ si\ P=Q \end{cases} \tag{1.9}$$

$$y_3 = \begin{cases} \left(\dfrac{y_2+2y_1}{x_2+2x_1}\right)(x_1+2x_3)+2y_1\ ,\ si\ P\neq Q \\ \\ \left(\dfrac{a_2x_1}{y_1}\right)(x_1+2x_3)+2y_1\ ,\ si\ P=Q \end{cases} \tag{1.10}$$

2. *Si* $j=0, Y^2Z=X^3+a_4XZ^2+a_6Z^3$*, alors :*

$$x_3 = \begin{cases} \left(\dfrac{y_2+2y_1}{x_2+2x_1}\right)^2+2x_1+2x_2\ ,\ si\ P\neq Q \\ \\ \left(\dfrac{a_4}{2y_1}\right)^2+x_1\ ,\ si\ P=Q \end{cases} \tag{1.11}$$

$$y_3 = \begin{cases} \left(\dfrac{y_2+2y_1}{x_2+2x_1}\right)(x_1+2x_3)+2y_1\ ,\ si\ P\neq Q \\ \\ \left(\dfrac{a_4}{2y_1}\right)(x_1+2x_3)+2y_1\ ,\ si\ P=Q \end{cases} \tag{1.12}$$

Corollaire 1.3.4 *(formules d'addition pour* $\mathrm{char}\,(\mathbf{K})\neq 2,3$*) (voir [82, p. 21]).*
Si $Y^2Z=X^3+a_4XZ^2+a_6Z^3$*, alors :*

$$x_3 = \begin{cases} \left(\dfrac{y_2-y_1}{x_2-x_1}\right)^2-x_1-x_2\ ,\ si\ P\neq Q \\ \\ \left(\dfrac{3x_1^2+a_4}{2y_1}\right)^2-2x_1\ ,\ si\ P=Q \end{cases} \tag{1.13}$$

$$y_3 = \begin{cases} \left(\dfrac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1 \ , \ si\ P \neq Q \\ \\ \left(\dfrac{3x_1^2 + a_4}{2y_1}\right)(x_1 - x_3) - y_1 \ , \ si\ P = Q \end{cases} \tag{1.14}$$

Remarque 1.3.1 *Soit $-P$ l'opposé d'un point $P = [x : y : 1] \in \mathbf{E}(\mathbf{K})$.*

1. *Si* $\mathrm{char}(\mathbf{K}) \neq 2$, *alors* $-P = [x : -y : 1]$.
2. *Si* $\mathrm{char}(\mathbf{K}) = 2$, *alors :*
   (a) *Si* $j = 0$, *alors* $-P = [x : y + a_3 : 1]$.
   (b) *Si* $j \neq 0$, *alors* $-P = [x : x + y : 1]$.

Corollaire 1.3.5 *(voir [41, Corollaire 2.48, p. 44]).*
Soit $\mathbf{E}$ *une courbe elliptique définie sur un corps K qui n'est pas nécessairement algébriquement clos. Alors* $(\mathbf{E}, +)$ *est un groupe abélien, où la loi d'addition « + » est définie par la Proposition 1.3.2.*

Le théorème de Hasse ci-dessous permet d'estimer le nombre de points d'une courbe elliptique définie sur un corps fini.

Théorème 1.3.2 (Théorème de Hasse) *(voir [120, Théorème 1.1, p. 131]).*
Soit $\mathbf{E}/\mathbb{F}_q$ *une courbe elliptique définie sur le corps fini* $\mathbb{F}_q$, *où q est une puissance d'un nombre premier p. Alors :* $|\mathrm{card}(\mathbf{E}(\mathbb{F}_q)) - q - 1| \leqslant 2\sqrt{q}$.

1.3.3 Exemples

Exemple 1.3.1 *Soit* $\mathbf{E}/\mathbb{F}_3$ *la courbe elliptique définie par* $y^2 = x^3 + x^2 + 1$. *L'ensemble des points* $\mathbb{F}_3$*-rationnels de* $\mathbf{E}$ *est :* $\mathbf{E}(\mathbb{F}_3) = \{(0,1), (0,2), (1,0), (2,1), (2,2)\} \cup \{\mathcal{O}\}$.
D'après la Proposition 1.3.2 et les formules d'addition (1.9) *et* (1.10), *la somme des points dans* $\mathbf{E}(\mathbb{F}_3)$ *est donnée par la table suivante :*

« + »	$(0,1)$	$(0,2)$	$(1,0)$	$(2,1)$	$(2,2)$
$(0,1)$	$(2,2)$	$\mathcal{O}$	$(2,2)$	$(0,2)$	$\mathcal{O}$
$(0,2)$	$\mathcal{O}$	$(2,1)$	$(2,2)$	$\mathcal{O}$	$(0,1)$
$(1,0)$	$(2,2)$	$(2,2)$	$\mathcal{O}$	$(0,2)$	$(0,2)$
$(2,1)$	$(0,2)$	$\mathcal{O}$	$(0,2)$	$(2,2)$	$\mathcal{O}$
$(2,2)$	$\mathcal{O}$	$(0,1)$	$(0,2)$	$\mathcal{O}$	$(2,1)$

TABLE 1.3: Loi de groupe pour $y^2 = x^3 + x^2 + 1$ sur $\mathbb{F}_3$.

Exemple 1.3.2 *Soit la courbe elliptique* $\mathbf{E}: y^2 = x^3 + x + 1$ *définie sur* $\mathbf{k} = \mathbb{F}_5$. *L'ensemble des points* $\mathbb{F}_5$*-rationnels de* $\mathbf{E}$ *est :*

$$\mathbf{E}(\mathbb{F}_5) = \{(0,1), (0,4), (2,1), (2,4), (3,1), (3,4), (4,2), (4,3)\} \cup \{\mathcal{O}\}.$$

D'après la Proposition 1.3.2 et les formules d'addition (1.13) *et* (1.14), *la somme des points de cette courbe elliptique est donnée par la table suivante :*

« + »	$(0,1)$	$(0,4)$	$(2,1)$	$(2,4)$	$(3,1)$	$(3,4)$	$(4,2)$	$(4,3)$
$(0,1)$	$(4,2)$	$\mathcal{O}$	$(3,4)$	$(4,3)$	$(2,4)$	$(3,1)$	$(2,1)$	$(0,4)$
$(0,4)$	$\mathcal{O}$	$(4,3)$	$(4,2)$	$(3,1)$	$(3,4)$	$(2,1)$	$(0,1)$	$(2,4)$
$(2,1)$	$(3,4)$	$(4,2)$	$(2,4)$	$\mathcal{O}$	$(0,4)$	$(4,3)$	$(3,1)$	$(0,1)$
$(2,4)$	$(4,3)$	$(3,1)$	$\mathcal{O}$	$(2,1)$	$(4,2)$	$(0,1)$	$(0,4)$	$(3,4)$
$(3,1)$	$(2,4)$	$(3,4)$	$(0,4)$	$(4,2)$	$(0,1)$	$\mathcal{O}$	$(4,3)$	$(2,1)$
$(3,4)$	$(3,1)$	$(2,1)$	$(4,3)$	$(0,1)$	$\mathcal{O}$	$(3,1)$	$(2,4)$	$(4,2)$
$(4,2)$	$(2,1)$	$(0,1)$	$(3,1)$	$(0,4)$	$(4,3)$	$(2,4)$	$(3,4)$	$\mathcal{O}$
$(4,3)$	$(0,4)$	$(2,4)$	$(0,1)$	$(3,4)$	$(2,1)$	$(4,2)$	$\mathcal{O}$	$(3,1)$

TABLE 1.4: Loi de groupe pour $y^2 = x^3 + x + 1$ sur $\mathbb{F}_5$.

Exemple 1.3.3 *Soit la courbe elliptique* $\mathbf{E}: y^2 = x^3 + x + 1$ *définie sur* $\mathbf{k} = \mathbb{F}_{23}$. *L'ensemble des points* $\mathbf{k}$*-rationnels de* $\mathbf{E}$ *est :*

$$\begin{aligned}\mathbf{E}(\mathbf{k}) = \{&(0,1)\,;\,(0,22)\,;\,(1,7)\,;\,(1,16)\,;\,(3,10)\,;\,(3,13)\,;\,(4,0)\,;\,(5,4)\,;\,(5,19)\,;\,(6,4)\,;\,(6,19)\,;\\ &(7,11)\,;\,(7,12)\,;\,(9,7)\,;\,(9,16)\,;\,(11,3)\,;\,(11,20)\,;\,(12,4)\,;\,(12,19)\,;\,(13,7)\,;\,(13,16)\,;\\ &(17,3)\,;\,(17,20)\,;\,(18,3)\,;\,(18,20)\,;\,(19,5)\,;\,(19,18)\} \cup \{\mathcal{O}\}.\end{aligned}$$

D'après la Proposition 1.3.2 et les formules d'addition (1.13) *et* (1.14), *nous avons :*

1. *Si* $x_1 = x_2$ *et* $y_2 = -y_1$, *alors* $(x_1, y_1) + (x_2, y_2) = \mathcal{O}$.
2. *Si* $x_1 \neq x_2$ *ou* $y_2 \neq -y_1$, *alors* $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$, *où :*

$$x_3 = \begin{cases} \left(\dfrac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2\ ,\ si\ (x_1, y_1) \neq (x_2, y_2) \\ \\ \left(\dfrac{3x_1^2 + 1}{2y_1}\right)^2 - 2x_1\ ,\ si\ (x_1, y_1) = (x_2, y_2) \end{cases};$$

$$y_3 = \begin{cases} \left(\dfrac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1\ ,\ si\ (x_1, y_1) \neq (x_2, y_2) \\ \\ \left(\dfrac{3x_1^2 + 1}{2y_1}\right)(x_1 - x_3) - y_1\ ,\ si\ (x_1, y_1) = (x_2, y_2) \end{cases}.$$

Par exemple, on a : $(3,10)+(9,7)=(17,20)$; $2(3,10)=(7,12)$ *et* $2(9,7)=(6,19)$.

1.3.4 Formules d'addition en coordonnées projectives

Soit $\mathbf{E}/\mathbf{k}$ une courbe elliptique donnée par une équation de Weierstrass sous sa forme normale (voir Table 1.2) et soient $P=[X_1:Y_1:Z_1]$ et $Q=[X_2:Y_2:Z_2]$ deux points finis de $\mathbf{E}(\mathbf{k})$ tels que $Q\neq -P$. Pour $i\in\{1,2\}$, on pose $x_i=\dfrac{X_i}{Z_i}$ et $y_i=\dfrac{Y_i}{Z_i}$. Alors :

$$P+Q=[X_1:Y_1:Z_1]+[X_2:Y_2:Z_2]=[x_1:y_1:1]+[x_2:y_2:1]=[x_3:y_3:1],$$

où x_3 et y_3 sont données par les Corollaires 1.3.2, 1.3.3 et 1.3.4.
Posons $X_3=x_3Z_3$ et $Y_3=y_3Z_3$, où Z_3 est un dénominateur commun à x_3 et y_3 . Alors :

$$P+Q=[x_3:y_3:1]=[x_3Z_3:y_3Z_3:Z_3]=[X_3:Y_3:Z_3];$$

où les formules algébriques de X_3, Y_3 et Z_3 sont données par les propositions suivantes :

Proposition 1.3.3 *(formules projectives d'addition pour* $\mathrm{char}(\mathbf{k})\neq 2,3$*).*
Si $Y^2Z=X^3+a_4XZ^2+a_6Z^3$*, alors :*

1. *Si* $P\neq Q$*, alors :*

$$\begin{aligned}
X_3&=(X_2Z_1-X_1Z_2)\left(Z_1Z_2(Y_2Z_1-Y_1Z_2)^2-(X_2Z_1+X_1Z_2)(X_2Z_1-X_1Z_2)^2\right);\\
Y_3&=\left(2Z_1Z_2(X_1Y_2-X_2Y_1)+X_2Y_2Z_1^2-X_1Y_1Z_2^2\right)(X_2Z_1-X_1Z_2)^2-Z_1Z_2(Y_2Z_1-Y_1Z_2)^3;\\
Z_3&=Z_1Z_2(X_2Z_1-X_1Z_2)^3.
\end{aligned}$$

2. *Si* $P=Q$*, alors :*

$$\begin{aligned}
X_3&=2Y_1Z_1\left(\left(3X_1^2+a_4Z_1^2\right)^2-8X_1Y_1^2Z_1\right);\\
Y_3&=\left(3X_1^2+a_4Z_1^2\right)\left(12X_1Y_1^2Z_1-\left(3X_1^2+a_4Z_1^2\right)^2\right)-8Y_1^4Z_1^2;\\
Z_3&=8Y_1^3Z_1^3.
\end{aligned}$$

Preuve. D'après le Corollaire 1.3.4, on a :

1. Si $P\neq Q$, alors :

$$\begin{aligned}
x_3&=\left(\frac{y_2-y_1}{x_2-x_1}\right)^2-x_1-x_2=\left(\frac{Y_2Z_1-Y_1Z_2}{X_2Z_1-X_1Z_2}\right)^2-\frac{X_1Z_2+X_2Z_1}{Z_1Z_2};\\
y_3&=\left(\frac{y_2-y_1}{x_2-x_1}\right)(x_1-x_3)-y_1=\frac{Y_2Z_1-Y_1Z_2}{X_2Z_1-X_1Z_2}\left(\frac{X_1}{Z_1}-x_3\right)-\frac{Y_1}{Z_1}.
\end{aligned}$$

Posons $Z_3 = Z_1Z_2\left(X_2Z_1 - X_1Z_2\right)^3$. Alors :

$$\begin{aligned}
X_3 = x_3Z_3 &= \left(X_2Z_1 - X_1Z_2\right)\Big(Z_1Z_2\left(Y_2Z_1 - Y_1Z_2\right)^2 - \left(X_2Z_1 + X_1Z_2\right)\left(X_2Z_1 - X_1Z_2\right)^2\Big);\\
Y_3 = y_3Z_3 &= \left(Y_2Z_1 - Y_1Z_2\right)\Big(X_1Z_2\left(X_2Z_1 - X_1Z_2\right)^2 - Z_1Z_2\left(Y_2Z_1 - Y_1Z_2\right)^2 + \left(X_2Z_1 + X_1Z_2\right)\\
&\quad \left(X_2Z_1 - X_1Z_2\right)^2\Big) - Y_1Z_2\left(X_2Z_1 - X_1Z_2\right)^3\\
&= \left(X_2Z_1 - X_1Z_2\right)^2\left(\left(Y_2Z_1 - Y_1Z_2\right)\left(2X_1Z_2 + X_2Z_1\right) - Y_1Z_2\left(X_2Z_1 - X_1Z_2\right)\right)\\
&\quad - Z_1Z_2\left(Y_2Z_1 - Y_1Z_2\right)^3\\
&= \left(2Z_1Z_2\left(X_1Y_2 - X_2Y_1\right) + X_2Y_2Z_1^2 - X_1Y_1Z_2^2\right)\left(X_2Z_1 - X_1Z_2\right)^2\\
&\quad - Z_1Z_2\left(Y_2Z_1 - Y_1Z_2\right)^3.
\end{aligned}$$

2. Si $P = Q$, alors :

$$\begin{aligned}
x_3 &= \left(\frac{3x_1^2 + a_4}{2y_1}\right)^2 - 2x_1 = \left(\frac{3X_1^2 + a_4Z_1^2}{2Y_1Z_1}\right)^2 - \frac{2X_1}{Z_1} = \frac{\left(3X_1^2 + a_4Z_1^2\right)^2 - 8X_1Y_1^2Z_1}{4Y_1^2Z_1^2};\\
y_3 &= \frac{3x_1^2 + a_4}{2y_1}\left(x_1 - x_3\right) - y_1 = \frac{3X_1^2 + a_4Z_1^2}{2Y_1Z_1}\left(\frac{X_1}{Z_1} - x_3\right) - \frac{Y_1}{Z_1}.
\end{aligned}$$

Posons $Z_3 = 8Y_1^3Z_1^3$. Alors :

$$\begin{aligned}
X_3 = x_3Z_3 &= 2Y_1Z_1\left(\left(3X_1^2 + a_4Z_1^2\right)^2 - 8X_1Y_1^2Z_1\right);\\
Y_3 = y_3Z_3 &= \left(3X_1^2 + a_4Z_1^2\right)\left(12X_1Y_1^2Z_1 - \left(3X_1^2 + a_4Z_1^2\right)^2\right) - 8Y_1^4Z_1^2.
\end{aligned}$$

□

Par la même démarche précédente, nous obtiendrons pour les cas particuliers, où $\mathrm{char}\,(\mathbf{k}) = 3$ et $\mathrm{char}\,(\mathbf{k}) = 2$, les formules algébriques suivantes de X_3, Y_3 et Z_3 :

Proposition 1.3.4 *(formules projectives d'addition pour* $\mathrm{char}\,(\mathbf{k}) = 3$*).*

1. *Si* $j \neq 0, Y^2Z = X^3 + a_2X^2Z + a_6Z^3$*, alors :*

   (a) *Si* $P \neq Q$*, alors :*

$$\begin{aligned}
X_3 &= Z_1Z_2\left(X_2Z_1 - X_1Z_2\right)\Big(\left(Y_2Z_1 - Y_1Z_2\right)^2 - a_2\left(X_2Z_1 - X_1Z_2\right)^2\Big)\\
&\quad - \left(X_1Z_2 + X_2Z_1\right)\left(X_2Z_1 - X_1Z_2\right)^3;\\
Y_3 &= Z_1Z_2\left(Y_2Z_1 - Y_1Z_2\right)\Big(a_2\left(X_2Z_1 - X_1Z_2\right)^2 - \left(Y_2Z_1 - Y_1Z_2\right)^2\Big)\\
&\quad + \left(Y_2Z_1 + Y_1Z_2\right)\left(X_2Z_1 - X_1Z_2\right)^3;\\
Z_3 &= Z_1Z_2\left(X_2Z_1 - X_1Z_2\right)^3.
\end{aligned}$$

(b) Si $P = Q$, alors :

$$\begin{aligned} X_3 &= a_2 Y_1 Z_1 \left(a_2 X_1^2 - Y_1^2\right) + X_1 Y_1^3; \\ Y_3 &= a_2^2 X_1 Z_1 \left(Y_1^2 - a_2 X_1^2\right) - Y_1^4; \\ Z_3 &= Y_1^3 Z_1. \end{aligned}$$

2. Si $j = 0, Y^2Z = X^3 + a_4XZ^2 + a_6Z^3$, alors :

(a) Si $P \neq Q$, alors :

$$\begin{aligned} X_3 &= Z_1 Z_2 \left(X_2 Z_1 - X_1 Z_2\right) \left(Y_2 Z_1 - Y_1 Z_2\right)^2 - \left(X_1 Z_2 + X_2 Z_1\right) \left(X_2 Z_1 - X_1 Z_2\right)^3; \\ Y_3 &= \left(Y_2 Z_1 + Y_1 Z_2\right) \left(X_2 Z_1 - X_1 Z_2\right)^3 - Z_1 Z_2 \left(Y_2 Z_1 - Y_1 Z_2\right)^3; \\ Z_3 &= Z_1 Z_2 \left(X_2 Z_1 - X_1 Z_2\right)^3. \end{aligned}$$

(b) Si $P = Q$, alors :

$$\begin{aligned} X_3 &= 2Y_1 \left(a_4^2 Z_1^3 + X_1 Y_1^2\right); \\ Y_3 &= Y_1^4 - a_4^3 Z_1^4; \\ Z_3 &= 2Y_1^3 Z_1. \end{aligned}$$

Proposition 1.3.5 *(formules projectives d'addition pour* $\mathrm{char}\,(\mathbf{K}) = 2$*).*

1. Si $j \neq 0, Y^2Z + XYZ = X^3 + a_2X^2Z + a_6Z^3$, alors :

(a) Si $P \neq Q$, alors :

$$\begin{aligned} X_3 &= \left(a_2 Z_1 Z_2 + X_1 Z_2 + X_2 Z_1\right) \left(X_1 Z_2 + X_2 Z_1\right)^3 \\ &\quad + Z_1 Z_2 \left(X_1 Z_2 + X_2 Z_1\right) \left(Y_1 Z_2 + Y_2 Z_1\right) \left(\left(X_1 + Y_1\right) Z_2 + \left(X_2 + Y_2\right) Z_1\right); \\ Y_3 &= \left(X_1 Z_2 + X_2 Z_1\right)^4 + a_2 Z_1 Z_2 \left(X_1 Z_2 + X_2 Z_1\right)^3 + Z_1 Z_2 \left(Y_1 Z_2 + Y_2 Z_1\right)^3 \\ &\quad + \left(\left(1 + a_2\right) Z_1 Z_2 \left(Y_1 Z_2 + Y_2 Z_1\right) + X_1 Y_1 Z_2^2 + X_2 Y_2 Z_1^2\right) \left(X_1 Z_2 + X_2 Z_1\right)^2; \\ Z_3 &= Z_1 Z_2 \left(X_1 Z_2 + X_2 Z_1\right)^3. \end{aligned}$$

(b) Si $P = Q$, alors :

$$\begin{aligned} X_3 &= X_1 Z_1 \left(X_1^4 + a_6 Z_1^4\right); \\ Y_3 &= X_1^6 + a_6 Z_1^4 \left(X_1^2 + \left(X_1 + Y_1\right) Z_1\right) + X_1^4 Y_1 Z_1; \\ Z_3 &= X_1^3 Z_1^3. \end{aligned}$$

2. *Si $j = 0, Y^2Z + a_3YZ^2 = X^3 + a_4XZ^2 + a_6Z^3$, alors :*

(a) Si $P \neq Q$, alors :

$$\begin{aligned} X_3 &= Z_1 Z_2 \left(X_1 Z_2 + X_2 Z_1\right) \left(Y_1 Z_2 + Y_2 Z_1\right)^2 + \left(X_1 Z_2 + X_2 Z_1\right)^4 ; \\ Y_3 &= a_3 Z_1 Z_2 \left(X_1 Z_2 + X_2 Z_1\right)^3 + \left(X_1 Y_1 Z_2^2 + X_2 Y_2 Z_1^2\right) \left(X_1 Z_2 + X_2 Z_1\right)^2 \\ &\quad + Z_1 Z_2 \left(Y_1 Z_2 + Y_2 Z_1\right)^3 ; \\ Z_3 &= Z_1 Z_2 \left(X_1 Z_2 + X_2 Z_1\right)^3 . \end{aligned}$$

(b) Si $P = Q$, alors :

$$\begin{aligned} X_3 &= a_3 Z_1^2 \left(X_1^4 + a_4^2 Z_1^4\right) ; \\ Y_3 &= X_1^6 + \left(a_3^4 + a_4^3\right) Z_1^6 + a_3^2 \left(a_4 X_1 + a_3 Y_1\right) Z_1^5 + \left(a_3^2 X_1 Z_1 + a_4^2 Z_1^2 + a_4 X_1^2\right) X_1^2 Z_1^2 ; \\ Z_3 &= a_3^3 Z_1^6 . \end{aligned}$$

1.4 Courbes elliptiques sur les anneaux finis

La définition des courbes elliptiques sur les anneaux diffère de celle des corps ; en particulier la loi de groupe définie géométriquement par la méthode de la sécante et la tangente sur un corps est assurée sous certaines conditions [75, Conditions (i) et (ii), p. 104] et qui sont vérifiées pour le cas des anneaux finis. Dans cette section, on va introduire les notions de triplets primitifs et de plan projectif sur un anneau ; ainsi que la définition et les propriétés des courbes elliptiques définies sur des anneaux finis.

1.4.1 Triplet primitif

Définition 1.4.1 *(voir [75, p. 104]).*
Soit R un anneau. On dit qu'un triplet $(x, y, z) \in R^3$ est primitif si $xR + yR + zR = R$. L'ensemble des triplets primitifs sur R sera noté $\mathcal{P}(R)$.

Remarque 1.4.1 *L'égalité $xR + yR + zR = R$ veut dire qu'il existe $(\alpha, \beta, \lambda) \in R^3$ tels que $1_R = \alpha x + \beta y + \lambda z$.*

Proposition 1.4.1 *Soit R un anneau local. Un triplet $(x, y, z) \in R^3$ est primitif si, et seulement si au moins un des éléments x, y et z est inversible dans R.*

Preuve. Supposons que x, y et z ne sont pas inversibles dans R, alors $(x, y, z) \in \mathcal{M}^3$ où $\mathcal{M}$ est l'unique idéal maximal de R, d'où $xR + yR + zR \subset \mathcal{M} \subsetneq R$, ce qui contredit que (x, y, z) est un triplet primitif.

Réciproquement, supposons par exemple que x est inversible dans R, alors $xR = R$ et donc $xR \subset xR + yR + zR \subset R$; ce qui montre que $xR + yR + zR = R$. □

Corollaire 1.4.1 *Si R est un corps, alors un triplet $(x, y, z) \in R^3$ est primitif si, et seulement si $(x, y, z) \neq (0, 0, 0)$.*

1.4.2 Plan projectif sur un anneau

Définition 1.4.2 *(voir [75, p. 105]).*
Soit R un anneau. Le plan projectif sur R est l'ensemble des classes d'équivalences de $\mathcal{P}(R)$ modulo la relation d'équivalence $\sim_R$ définie par :

$$(x_1, y_1, z_1) \sim_R (x_2, y_2, z_2) \Leftrightarrow \exists \lambda \in R^\times : \ (x_2, y_2, z_2) = \lambda (x_1, y_1, z_1).$$

L'ensemble quotient $\dfrac{\mathcal{P}(R)}{\sim_R}$ est noté $\mathbb{P}^2(R)$, et la classe d'équivalence d'un triplet primitif (x, y, z) est noté $[x : y : z]$, et on a :

$$[x_1 : y_1 : z_1] = [x_2 : y_2 : z_2] \Leftrightarrow \exists \lambda \in R^\times : \ x_2 = \lambda x_1 \, , \, y_2 = \lambda y_1 \ \text{et} \ z_2 = \lambda z_1.$$

Exemple 1.4.1 *(voir [131, p. 19]).*
Considérons l'anneau fini $\mathbb{F}_2[e] = \left\{\alpha + \beta e \mid (\alpha, \beta) \in \mathbb{F}_2 \times \mathbb{F}_2 \ \text{et} \ e^2 = 0\right\}$ dont le groupe des unités est $(\mathbb{F}_2[e])^\times = \{1, 1 + e\}$. Comme cet anneau est local d'idéal maximal $e\mathbb{F}_2[e]$, alors un triplet (x, y, z) est non-primitif si, et seulement si $(x, y, z) \in \{0, e\}^3$. Donc il y a 8 triplets au total qui ne sont pas primitifs, et alors l'ensemble $\mathcal{P}(\mathbb{F}_2[e])$ contient 56 triplets primitifs ; et pour tous éléments (x, y, z) et (x', y', z') dans $\mathcal{P}(\mathbb{F}_2[e])$, on a :

$$\left[x' : y' : z'\right] = [x : y : z] \Leftrightarrow \left(x', y', z'\right) = (x, y, z) \ \ ou \ \ \left(x', y', z'\right) = (x + xe, y + ye, z + ze).$$

Ainsi, chaque classe d'équivalence dans $\mathbb{P}^2(\mathbb{F}_2[e])$ a exactement deux représentants, et donc le plan projectif $\mathbb{P}^2(\mathbb{F}_2[e])$ contient exactement les 28 points suivants :

$$\begin{aligned}\mathbb{P}^2(\mathbb{F}_2[e]) = \{&[0:1:0]\,;[0:0:1]\,;[1:0:0]\,;[0:1:1]\,;[1:1:0]\,;[1:0:1]\,;[1:1:1]\,;[0:1:e]\,;\\ &[0:e:1]\,;[1:0:e]\,;[e:0:1]\,;[1:e:0]\,;[e:1:0]\,;[1:e:e]\,;[e:1:e]\,;[e:e:1]\,;[1:e:1]\,;\\ &[1:1:e]\,;[e:1:1]\,;[0:1:1+e]\,;[1:0:1+e]\,;[1:1+e:0]\,;[1:1:1+e]\,;[1:1+e:1]\,;\\ &[1:e:1+e]\,;[1:1+e:e]\,;[e:1:1+e]\,;[1:1+e:1+e]\}.\end{aligned}$$

Exemple 1.4.2 *Si l'élément e de l'exemple précédent est un idempotent, alors l'anneau fini $\mathbb{F}_2[e] = \left\{\alpha + \beta e \mid (\alpha, \beta) \in \mathbb{F}_2^2 \ \text{et} \ e^2 = e\right\}$ n'est pas local et son groupe des unités est réduit. Comme $\mathbb{F}_2[e] = e\mathbb{F}_2[e] + (1 + e)\mathbb{F}_2[e]$, alors un triplet (x, y, z) est n'est pas primitif si, et seulement si $(x, y, z) \in \{0, e\}^3 \cup \{0, 1 + e\}^3$; et donc il y a 15 triplets qui ne sont pas primitifs, et l'ensemble $\mathcal{P}(\mathbb{F}_2[e])$ contient 49 triplets primitifs. Comme l'anneau $\mathbb{F}_2[e]$ est réduit, alors chaque classe d'équivalence dans $\mathbb{P}^2(\mathbb{F}_2[e])$ contient un seul représentant, et donc le plan projectif $\mathbb{P}^2(\mathbb{F}_2[e])$ contient les 49 points suivants :*

$$\begin{aligned}\mathbb{P}^2(\mathbb{F}_2[e]) = \{&[0:1:0]\,;[0:0:1]\,;[1:0:0]\,;[1:0:1]\,;[0:1:1]\,;[1:1:0]\,;[1:1:1]\,;[0:1:e]\,;\\ &[0:e:1]\,;[1:0:e]\,;[e:0:1]\,;[1:e:0]\,;[e:1:0]\,;[1:e:1]\,;[1:1:e]\,;[e:1:1]\,;[1:e:e]\,;\\ &[e:1:e]\,;[e:e:1]\,;[0:1:1+e]\,;[1:0:1+e]\,;[0:e:1+e]\,;[e:0:1+e]\,;[e:1:1+e]\,;\end{aligned}$$

$[1:e:1+e]\,;[1:1:1+e]\,;[e:e:1+e]\,;[0:1+e:1]\,;[1:1+e:0]\,;[0:1+e:e]\,;[e:1+e:0]\,;$
$[e:1+e:1]\,;[e:1+e:e]\,;[1+e:0:1]\,;[1+e:1:0]\,;[1+e:0:e]\,;[1+e:e:0]\,;[1+e:1:1]\,;$
$[1:1+e:1]\,;[1:1+e:e]\,;[1+e:1:e]\,;[1+e:e:1]\,;[1+e:e:e]\,;[1:1+e:1+e]\,;[1+e:1:$
$1+e]\,;[1+e:1+e:1]\,;[e:1+e:1+e]\,;[1+e:e:1+e]\,;[1+e:1+e:e]\}\,.$

1.4.3 Courbes elliptiques sur un anneau fini

Définition 1.4.3 *(voir [44, Définition 4.3.1, p. 174]).*
Soit R un anneau et soit $a=(a_1,a_2,a_3,a_4,a_6)\in R^5$. Une courbe elliptique sur R qu'on note $E_a(R)$ est l'ensemble des zéros dans le plan projectif $\mathbb{P}^2(R)$ de l'équation de Weierstrass :

$$\mathbf{E}:\ Y^2Z+a_1XYZ+a_3YZ^2=X^3+a_2X^2Z+a_4XZ^2+a_6Z^3 \tag{1.15}$$

et tel que le discriminant $\Delta_a:=\Delta(a_1,a_2,a_3,a_4,a_6)$ (voir Définition 1.2.1) est inversible dans R.

Remarque 1.4.2 *Soit $\mathbb{F}_q$ le corps fini d'ordre $q=p^d$, avec p un nombre premier et d un entier strictement positif. Dans toute la suite de cette thèse, nous nous intéresserons à des courbes elliptiques définies sur l'anneau $\mathbb{F}_q[e]$ [2] par les équations de Weierstrass suivantes :*

1. *Si $p=2$, alors :*

$$E_{a,b}(R):=\left\{[X:Y:Z]\in\mathbb{P}^2(R)\mid Y^2Z+XYZ=X^3+aX^2Z+bZ^3\right\}, \tag{1.16}$$

   avec $(a,b)\in R^2$ tel que $\Delta_{a,b}:=b\in R^\times$ (voir [131, p. 28]).

2. *Si $p=3$, alors :*

$$E_{a,b}(R):=\left\{[X:Y:Z]\in\mathbb{P}^2(R)\mid Y^2Z=X^3+aX^2Z+bZ^3\right\}, \tag{1.17}$$

   avec $(a,b)\in R^2$ tel que $\Delta_{a,b}:=-a^3b\in R^\times$ (voir [54, p. 35]).

3. *Si $p\geq 5$, alors :*

$$E_{a,b}(R):=\left\{[X:Y:Z]\in\mathbb{P}^2(R)\mid Y^2Z=X^3+aXZ^2+bZ^3\right\}, \tag{1.18}$$

   avec $(a,b)\in R^2$ tel que $\Delta_{a,b}:=-16\left(4a^3+27b^2\right)\in R^\times$ (voir [75, pp. 104–105]).

2. e est tel que $e^2=e$ ou bien $e^3=e^2$.

2

Courbes elliptiques sur l'anneau $\mathbb{F}_q[e], e^2 = e$

Sommaire

2.1 Introduction **25**
2.2 L'anneau $\mathbb{F}_q[e], e^2 = e$ **25**
2.2.1 Opérations arithmétiques de $\mathbb{F}_q[e]$ 26
2.2.2 Coûts des opérations arithmétiques 28
2.3 Courbes elliptiques sur l'anneau $\mathbb{F}_q[e]$, $e^2 = e$. **28**
2.3.1 Les courbes elliptiques $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$ et $E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$ 29
2.3.2 Classification des points de la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$ 33
2.3.3 Applications cryptographiques 34
2.4 Loi de groupe pour $E_{a,b}(\mathbb{F}_q[e])$ **35**
2.4.1 La structure de groupe pour $E_{a,b}(\mathbb{F}_q[e])$ 35
2.4.2 Formules explicites d'addition pour $E_{a,b}(\mathbb{F}_{3^d}[e])$ 37
2.5 Conclusion **43**

Dans ce chapitre, nous allons étudier des courbes elliptiques définies sur l'anneau $\mathbb{F}_q[e]$, où e est tel que $e^2 = e$ et $\mathbb{F}_q$ est le corps fini d'ordre $q = p^d$, avec p un nombre premier et d un entier naturel strictement positif. Dans un premier temps, on va étudier l'arithmétique de l'anneau $\mathbb{F}_q[e]$, et dans un deuxième temps on va étudier la courbe elliptique notée $E_{a,b}(\mathbb{F}_q[e])$. Les résultats de ce chapitre font l'objet d'étude des travaux [10, 11, 12].

2.1 Introduction

Soit $\mathbb{F}_q[X]$ l'anneau des polynômes à une indéterminée et à coefficients dans le corps finis $\mathbb{F}_q$. Le quotient de l'anneau $\mathbb{F}_q[X]$ par l'idéal engendré par le polynôme $X^2 - X$ est un anneau commutatif, unitaire et finis qui s'identifie à l'anneau fini noté $\mathbb{F}_q[e]$ des éléments de la forme $\alpha + \beta e$, où $(\alpha, \beta) \in \mathbb{F}_q \times \mathbb{F}_q$ et $e^2 = e$. Pour $(a, b) \in (\mathbb{F}_q[e])^2$, on désigne par $E_{a,b}(\mathbb{F}_q[e])$ la courbe elliptique définie sur l'anneau $\mathbb{F}_q[e]$ par l'équation de Weierstrass (1.16) ou (1.17) ou (1.18) (voir Remarque 1.4.2).

Nous allons commencer ce chapitre par étudier l'arithmétique de l'anneau $\mathbb{F}_q[e]$, puis nous allons caractériser et classifier les points de la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$ et nous finirons par des formules explicites permettant de calculer la loi du groupe de cette courbe elliptique. Les sections de ce chapitre sont organisées comme suit :

- ◇ Dans la deuxième section, nous allons étudier les opérations arithmétiques de l'anneau $\mathbb{F}_q[e]$. En particulier, nous donnerons une nouvelle formule pour la multiplication des éléments de $\mathbb{F}_q[e]$; ce qui nous permettra de caractériser l'ensemble $(\mathbb{F}_q[e])^\times$ de ses éléments inversibles et de déduire la non-localité de l'anneau $\mathbb{F}_q[e]$. Ensuite, nous allons définir deux morphismes d'anneaux que nous noterons π_0 et π_1, et qui seront essentiels pour étudier la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$. Nous terminerons cette section par la donnée des coûts des opérations arithmétiques de l'anneau $\mathbb{F}_q[e]$; où nous remarquons que la nouvelle formule du produit des éléments permet de réduire le coût de la multiplication.

- ◇ Nous commencerons la troisième section par la donnée de deux réductions de la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$ sur le corps fini $\mathbb{F}_q$. Ces deux réductions nous permettront d'établir une condition nécessaire et suffisante pour qu'un point P du plan projectif $\mathbb{P}^2(\mathbb{F}_q[e])$ soit dans la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$. Le résultat essentiel qu'on va montrer dans cette section est la bijection entre la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$ et le produit cartésien des courbes elliptiques $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$ et $E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$. À la fin de cette section, nous donnerons une classification de tous les points de la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$; ainsi que quelques applications cryptographiques de cette courbe elliptique.

- ◇ Dans la quatrième section, nous utiliserons la bijection établie dans la section précédente pour donner les formules explicites permettant de calculer la loi du groupe de la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$.

- ◇ Dans la dernière section, nous donnerons une courte conclusion de ce travail.

2.2 L'anneau $\mathbb{F}_q[e], e^2 = e$

L'anneau $\mathbb{F}_q[e]$ où $e^2 = e$ est construit comme une extension de l'anneau $(\mathbb{F}_q, +, .)$ par le quotient de l'anneau des polynômes $(\mathbb{F}_q[X], +, .)$ par l'idéal engendré le polynôme $X^2 - X$. Un élément de $\mathbb{F}_q[e]$ s'écrit d'une manière unique sous la forme $\alpha + \beta e$, où $(\alpha, \beta) \in \mathbb{F}_q^2$ et $e^2 = e$.

2.2.1 Opérations arithmétiques de $\mathbb{F}_q[e]$

Soient $X = x_0 + x_1 e$ et $Y = y_0 + y_1 e$ deux éléments de $\mathbb{F}_q[e]$. On définit les opérations arithmétiques « X+Y » et « X.Y » par :

$$X + Y = (x_0 + y_0) + (x_1 + y_1)e \text{ et } X.Y = (x_0 y_0) + (x_0 y_1 + x_1 y_0 + x_1 y_1)e.$$

Alors :

Proposition 2.2.1 :

1. $(\mathbb{F}_q[e], +, .)$ *est un anneau commutatif, unitaire et fini.*
2. $\mathbb{F}_q[e]$ *est un* $\mathbb{F}_q$*-espace vectoriel de dimension* 2 *et de base* $\{1, e\}$.
3. $\mathbb{F}_q[e]$ *est isomorphe à l'anneau quotient* $\mathbb{F}_q[X]/\langle X^2 - X\rangle$.

Preuve. Évidente. □

Dans la suite de ce chapitre, la formule (2.1) suivante, sera adaptée pour le calcul du produit des éléments de l'anneau $\mathbb{F}_q[e]$, pour la caractérisation de ses éléments inversibles et ainsi pour établir la loi du groupe de la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$.

Proposition 2.2.2 *Soient* $X = x_0 + x_1 e$ *et* $Y = y_0 + y_1 e$ *deux éléments de* $\mathbb{F}_q[e]$. *Alors :*

$$X.Y = x_0 y_0 + ((x_0 + x_1)(y_0 + y_1) - x_0 y_0)e. \tag{2.1}$$

Preuve. Évidente. □

Par un raisonnement par récurrence, nous en déduisons immédiatement que :

Corollaire 2.2.1 *Pour tout* $X = x_0 + x_1 e \in \mathbb{F}_q[e]$ *et pour tout entier positif* n, *on a :*

$$X^n = x_0^n + ((x_0 + x_1)^n - x_0^n)e.$$

En particulier, si $p = 2$, *alors* $X^2 = x_0^2 + x_1^2 e$ *et si* $p = 3$, *alors* $X^3 = x_0^3 + x_1^3 e$.

La proposition suivante, caractérise l'ensemble $(\mathbb{F}_q[e])^\times$ des éléments inversibles de l'anneau $\mathbb{F}_q[e]$.

Proposition 2.2.3 *Soit* $X = x_0 + x_1 e \in \mathbb{F}_q[e]$. *Alors* X *est inversible si, et seulement si* x_0 *et* $x_0 + x_1$ *ne sont pas nuls dans le corps fini* $\mathbb{F}_q$. *Dans ce cas, l'inverse de* X *est donné par :*

$$X^{-1} = x_0^{-1} + \left((x_0 + x_1)^{-1} + x_0^{-1}\right) e.$$

Preuve. Soit $X = x_0 + x_1 e \in \mathbb{F}_q[e]$. On a $X \in (\mathbb{F}_q[e])^\times \Leftrightarrow \exists Y = y_0 + y_1 e \in \mathbb{F}_q[e] : X.Y = 1$.

D'après la formule (2.1), nous avons :

$$X.Y = 1 \Leftrightarrow \begin{cases} x_0y_0 = 1 \\ (x_0 + x_1)(y_0 + y_1) - x_0y_0 = 0 \end{cases} \Leftrightarrow \begin{cases} x_0y_0 = 1 \\ (x_0 + x_1)(y_0 + y_1) = 1 \end{cases}$$
$$\Leftrightarrow \begin{cases} y_0 = x_0^{-1} \\ y_0 + y_1 = (x_0 + x_1)^{-1} \end{cases} \Leftrightarrow \begin{cases} y_0 = x_0^{-1} \\ y_1 = (x_0 + x_1)^{-1} - x_0^{-1} \end{cases}.$$

Ainsi, la proposition est montrée, et l'inverse de X est donné par $X^{-1} = x_0^{-1} + \left((x_0 + x_1)^{-1} - x_0^{-1}\right) e$. □

Remarque 2.2.1 *Si x_0 et $x_0 + x_1$ ne sont pas nuls dans $\mathbb{F}_q$, alors par la formule (2.1), nous vérifions immédiatement que :*

$$(x_0 + x_1e)\left(x_0^{-1} + \left((x_0 + x_1)^{-1} - x_0^{-1}\right) e\right) = 1,$$

ce qui montre que $x_0^{-1} + \left((x_0 + x_1)^{-1} - x_0^{-1}\right) e$ est l'inverse de $X = x_0 + x_1e$.

Corollaire 2.2.2 *L'ensemble des éléments non-inversibles de l'anneau $\mathbb{F}_q[e]$ est formé de la réunion des idéaux engendrés par e et $1 - e$.*

Corollaire 2.2.3 *L'anneau $(\mathbb{F}_q[e], +, .)$ est non-local.*

Preuve. Comme $\langle e \rangle$ et $\langle 1 - e \rangle$ sont deux idéaux distincts de $\mathbb{F}_q[e]$, alors $\langle e \rangle \cup \langle 1 - e \rangle$ n'est pas un idéal de $\mathbb{F}_q[e]$, et donc $(\mathbb{F}_q[e], +, .)$ n'est pas un anneau local. □

Nous finirons cette sous-section par la donnée de deux applications que nous utiliserons dans la suite pour l'étude de la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$.

Proposition 2.2.4 *Soient π_0 et π_1 les applications définies par :*

$$\begin{array}{ccc} \pi_0 : \mathbb{F}_q[e] & \longrightarrow & \mathbb{F}_q \\ x_0 + x_1e & \longmapsto & x_0 \end{array} \quad et \quad \begin{array}{ccc} \pi_1 : \mathbb{F}_q[e] & \longrightarrow & \mathbb{F}_q \\ x_0 + x_1e & \longmapsto & x_0 + x_1 \end{array}.$$

Pour tout $X \in \mathbb{F}_q[e]$, on a :

1. $X = \pi_0(X) + (\pi_1(X) - \pi_0(X))\, e$.
2. $Xe = \pi_1(X)e$.
3. $X(1 - e) = \pi_0(X)(1 - e)$.
4. $X = 0$ *si, et seulement si* $\pi_0(X) = 0$ *et* $\pi_1(X) = 0$.
5. X *est inversible dans* $\mathbb{F}_q[e]$ *si, et seulement si* $\pi_0(X)$ *et* $\pi_1(X)$ *ne sont pas nuls dans* $\mathbb{F}_q$.

Preuve. Évidente. □

Corollaire 2.2.4 *Les applications π_0 et π_1 sont deux homomorphismes surjectifs d'anneaux.*

Preuve. Soient X et Y deux éléments de $\mathbb{F}_q[e]$. D'après la première propriété de la Proposition 2.2.4, et la formule du produit (2.1), on a :

$$X + Y = \pi_0(X) + \pi_0(Y) + (\pi_1(X) - \pi_0(X) + \pi_1(Y) - \pi_0(Y))\, e\,;$$
$$X.Y = \pi_0(X)\,\pi_0(Y)\, e + (\pi_1(X)\,\pi_1(Y) - \pi_0(X)\,\pi_0(Y))\, e\,.$$

D'où, l'on déduit facilement que :

(i) $\pi_0(X+Y) = \pi_0(X) + \pi_0(Y)$ et $\pi_0(X.Y) = \pi_0(X).\pi_0(Y)$;

(ii) $\pi_1(X+Y) = \pi_1(X) + \pi_1(Y)$ et $\pi_1(X.Y) = \pi_1(X).\pi_1(Y)$;

et donc π_0 et π_1 sont deux homomorphismes d'anneaux. La surjectivité de π_0 et π_1 provient du fait que, pour tout $x \in \mathbb{F}_q$, on a $\pi_0(x) = \pi_1(x) = x$. □

2.2.2 Coûts des opérations arithmétiques

Soient s, m et i (resp. S, M et I) respectivement les coûts d'addition, de multiplication et d'inversion dans $\mathbb{F}_q$ (resp. $\mathbb{F}_q[e]$). Par définition des opérations arithmétiques d'addition, de multiplication et d'inversion dans $\mathbb{F}_q[e]$, nous avons $S = 2s, M = 2s + 4m$ et $I = s + 2i$; alors que par la formule du produit (2.1), nous réduisons la valeur de M à $3s + 2m$; ce qui montre que la formule (2.1) est plus efficace pour le calcul du produit des éléments de l'anneau $\mathbb{F}_q[e]$.

2.3 Courbes elliptiques sur l'anneau $\mathbb{F}_q[e],\ e^2 = e$.

Dans le reste de ce chapitre a et b sont deux éléments de l'anneau $\mathbb{F}_q[e]$ fixés par $a = a_0 + a_1 e$ et $b = b_0 + b_1 e$, où $(a_0, a_1, b_0, b_1) \in \mathbb{F}_q^4$. Dans cette section, nous prouvons une bijection entre la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$ et le produit cartésien des courbes elliptiques $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$ et $E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$. La courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$ est donnée par la définition suivante (voir Remarque 1.4.2) :

Définition 2.3.1 *La courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$ est l'ensemble des zéros dans le plan projectif $\mathbb{P}^2(\mathbb{F}_q[e])$ de l'équation $F(X,Y,Z) = 0$, où F est définie par l'une des formes normales de Weierstrass suivantes :*

$p \neq 2, 3$	$F(X,Y,Z) = Y^2Z - X^3 - aXZ^2 - bZ^3$	$\Delta = -16\left(4a^3 + 27b^2\right)$
$p = 3$	$F(X,Y,Z) = Y^2Z - X^3 - aX^2Z - bZ^3$	$\Delta = -a^3b$
$p = 2$	$F(X,Y,Z) = Y^2Z + XYZ - X^3 - aX^2Z - bZ^3$	$\Delta = b$

TABLE 2.1: Équation de Weierstrass de $E_{a,b}(\mathbb{F}_q[e])$.

et tel que le discriminant Δ de F est inversible dans l'anneau $\mathbb{F}_q[e]$. On écrit :

$$E_{a,b}(\mathbb{F}_q[e]) = \left\{[X:Y:Z] \in \mathbb{P}^2(\mathbb{F}_q[e]) \mid F(X,Y,Z) = 0\right\}.$$

2.3.1 Les courbes elliptiques $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$ et $E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$

Soit $i \in \{0,1\}$ et soit Δ_i le discriminant du polynôme f_i défini par l'une des formes de Weierstrass suivantes :

$p \neq 2,3$	$f_i(x,y,z) = y^2z - \left(x^3 + \pi_i(a)xz^2 + \pi_i(b)z^3\right)$
	$\Delta_i = -16\left(4\pi_i(a)^3 + 27\pi_i(b)^2\right)$
$p = 3$	$f_i(x,y,z) = y^2z - \left(x^3 + \pi_i(a)x^2z + \pi_i(b)z^3\right)$
	$\Delta_i = -\pi_i(a)^3\pi_i(b)$
$p = 2$	$f_i(x,y,z) = y^2z + xyz - \left(x^3 + \pi_i(a)x^2z + \pi_i(b)z^3\right)$
	$\Delta_i = \pi_i(b)$

TABLE 2.2: Réductions de $E_{a,b}(\mathbb{F}_q[e])$ sur $\mathbb{F}_q$.

Pour $i \in \{0,1\}$, on définit l'ensemble $E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q)$ par :

$$E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q) = \left\{[x:y:z] \in \mathbb{P}^2(\mathbb{F}_q) \mid f_i(x,y,z) = 0\right\}.$$

Alors :

Proposition 2.3.1 *Pour tout $i \in \{0,1\}$, l'ensemble $E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q)$ est une courbe elliptique sur le corps fini $\mathbb{F}_q$.*

Preuve. Soit $i \in \{0,1\}$. Comme Δ est inversible dans $\mathbb{F}_q[e]$ et $\Delta_i := \pi_i(\Delta)$, alors le résultat découle de la Proposition 2.2.4(5). □

Proposition 2.3.2 *Soit $(X,Y,Z) \in (\mathbb{F}_q[e])^3$. Alors $[X:Y:Z] \in \mathbb{P}^2(\mathbb{F}_q[e])$ si, et seulement si pour tout $i \in \{0,1\}$, $[\pi_i(X):\pi_i(Y):\pi_i(Z)] \in \mathbb{P}^2(\mathbb{F}_q)$.*

Preuve. Soit $(X,Y,Z) \in (\mathbb{F}_q[e])^3$. Si $[X:Y:Z] \in \mathbb{P}^2(\mathbb{F}_q[e])$, alors il existe un triplet (X',Y',Z') de $\mathbb{F}_q[e]$ tel que $XX' + YY' + ZZ' = 1$. Ainsi, pour tout $i \in \{0,1\}$, on aura :

$$\pi_i(X)\pi_i(X') + \pi_i(Y)\pi_i(Y') + \pi_i(Z)\pi_i(Z') = 1;$$

et donc $(\pi_i(X),\pi_i(Y),\pi_i(Z)) \neq (0,0,0)$, i.e. $[\pi_i(X):\pi_i(Y):\pi_i(Z)] \in \mathbb{P}^2(\mathbb{F}_q)$.

Réciproquement, supposons que pour tout $i \in \{0,1\}$, on a $[\pi_i(X):\pi_i(Y):\pi_i(Z)] \in \mathbb{P}^2(\mathbb{F}_q)$. Alors, nous aurions deux cas pour $\pi_0(Z)$:

1. Si $\pi_0(Z) = 0$, alors $\pi_0(X) = 0$ et $\pi_0(Y) = 1$; et donc :

$$\begin{cases} X = \pi_1(X)e \\ Y = 1 + (\pi_1(Y) - 1)\,e \\ Z = \pi_1(Z)e \end{cases};$$

et nous aurions deux cas pour $\pi_1(Z)$:

(a) Si $\pi_1(Z) = 0$, alors $\pi_1(X) = 0$ et $\pi_1(Y) = 1$; et donc $[X : Y : Z] = [0 : 1 : 0]$.

(b) Si $\pi_1(Z) \neq 0$, alors :

i. Si $\pi_1(Y) \neq 0$, alors Y sera inversible ; et donc $[X : Y : Z] \in \mathbb{P}^2(\mathbb{F}_q[e])$.

ii. Si $\pi_1(Y) = 0$, alors $Y = 1 - e$; et donc $Y + Z = 1 + (\pi_1(Z) - 1)\, e$ est inversible dans $\mathbb{F}_q[e]$. Ainsi, il existe $U \in (\mathbb{F}_q[e])^\times$ tel que $UY + UZ = 1$, et donc $[X : Y : Z]$ est un point du plan projectif $\mathbb{P}^2(\mathbb{F}_q[e])$.

2. Si $\pi_0(Z) \neq 0$, alors :

(a) Si $\pi_1(Z) \neq 0$, alors Z sera inversible ; et donc $[X : Y : Z] \in \mathbb{P}^2(\mathbb{F}_q[e])$.

(b) Si $\pi_1(Z) = 0$, alors $\pi_1(X) = 0$ et $\pi_1(Y) = 1$; et donc :

$$\begin{cases} X = \pi_0(X)\,(1 - e) \\ Y = \pi_0(Y) + (1 - \pi_0(Y))\, e \\ Z = \pi_0(Z)\,(1 - e) \end{cases} ;$$

et nous aurions deux cas pour $\pi_0(Y)$:

i. Si $\pi_0(Y) \neq 0$, alors Y sera inversible ; et donc $[X : Y : Z] \in \mathbb{P}^2(\mathbb{F}_q[e])$.

ii. Si $\pi_0(Y) = 0$, alors $Y = e$; et donc $Y + Z = \pi_0(Z) + (1 - \pi_0(Z))\, e$ est inversible dans $\mathbb{F}_q[e]$. Ainsi, il existe $V \in (\mathbb{F}_q[e])^\times$ tel que $VY + VZ = 1$; et donc $[X : Y : Z] \in \mathbb{P}^2(\mathbb{F}_q[e])$.

□

Proposition 2.3.3 *Un point $[X : Y : Z] \in \mathbb{P}^2(\mathbb{F}_q[e])$ est un zéro de F si, et seulement si pour tout $i \in \{0, 1\}$, le point $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)]$ est un zéro de f_i.*

Preuve. Soit $[X : Y : Z] \in \mathbb{P}^2(\mathbb{F}_q[e])$. Alors, d'après la Proposition 2.2.4(5), on a :

$$\begin{aligned} F(X, Y, Z) = 0 &\Leftrightarrow \pi_0(F(X, Y, Z)) = 0 \text{ et } \pi_1(F(X, Y, Z)) = 0 \\ &\Leftrightarrow f_0(\pi_0(X), \pi_0(Y), \pi_0(Z)) = 0 \text{ et } f_1(\pi_1(X), \pi_1(Y), \pi_1(Z)) = 0. \end{aligned}$$

□

Théorème 2.3.1 *Soit $(X, Y, Z) \in (\mathbb{F}_q[e])^3$. Alors $[X : Y : Z] \in E_{a,b}(\mathbb{F}_q[e])$ si, et seulement si $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \in E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q)$ pour tout $i \in \{0, 1\}$.*

Preuve. Cela découle directement des Propositions 2.3.2 et 2.3.3. □

Corollaire 2.3.1 *Pour tout $i \in \{0, 1\}$, l'application $\widetilde{\pi}_i$ donnée par :*

$$\begin{array}{rccc} \widetilde{\pi}_i & : & E_{a,b}(\mathbb{F}_q[e]) & \longrightarrow & E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q) \\ & & [X : Y : Z] & \longmapsto & [\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \end{array}$$

est bien définie et surjective.

Preuve.

1. Soient $[X : Y : Z]$ et $[X' : Y' : Z']$ deux points de $E_{a,b}(\mathbb{F}_q[e])$. Si $[X : Y : Z] = [X' : Y' : Z']$, alors il existe un élément inversible $U \in \mathbb{F}_q[e]$ tel que $X' = UX$, $Y' = UY$ et $Z' = UZ$. Ainsi, pour tout $i \in \{0, 1\}$, on a :

$$\widetilde{\pi_i}\left([X' : Y' : Z']\right) = [\pi_i(X') : \pi_i(Y') : \pi_i(Z')] = \underbrace{[\pi_i(U)\pi_i(X) : \pi_i(U)\pi_i(Y) : \pi_i(U)\pi_i(Z)]}_{\pi_i(U)\in\mathbb{F}_q^*}$$
$$= [\pi_i(X) : \pi_i(Y) : \pi_i(Z)] = \widetilde{\pi_i}\left([X : Y : Z]\right);$$

   et donc $\widetilde{\pi_i}$ est bien définie.

2. Soit $[x : y : z] \in E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$. Le point $P := [x - xe : y + (1 - y)\, e : z - ze]$ de $E_{a,b}\left(\mathbb{F}_q[e]\right)$ vérifie $\widetilde{\pi_0}\ (P) = [x : y : z]$; et donc $\widetilde{\pi_0}$ est une application surjective.

3. Soit $[x : y : z] \in E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$. Le point $P := [xe : 1 + (y - 1)\, e : ze]$ de $E_{a,b}\left(\mathbb{F}_q[e]\right)$ vérifie $\widetilde{\pi_1}\ (P) = [x : y : z]$; et donc $\widetilde{\pi_1}$ est une application surjective.

□

Le théorème suivant donne une bijection entre la courbe elliptique $E_{a,b}\left(\mathbb{F}_q[e]\right)$ et le produit cartésien des courbes elliptiques $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$ et $E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$.

Théorème 2.3.2 *L'application $\widetilde{\pi}$ donnée par :*

$$\begin{array}{rcl} \widetilde{\pi}\ :\ E_{a,b}(\mathbb{F}_q[e]) & \longrightarrow & E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q) \times E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q) \\ P & \longmapsto & \left(\widetilde{\pi_0}\ (P), \widetilde{\pi_1}\ (P)\right) \end{array}$$

est bien définie, bijective et son inverse est donné par :

$$\widetilde{\pi}^{-1}\ ([x_0 : y_0 : z_0], [x_1 : y_1 : z_1]) = [x_0 + (x_1 - x_0)e : y_0 + (y_1 - y_0)e : z_0 + (z_1 - z_0)e]\,.$$

Preuve.

1. Montrons que $\widetilde{\pi}$ est bien définie.
   Soient P et Q deux points de $E_{a,b}\left(\mathbb{F}_q[e]\right)$ tels que $P = Q$. Comme $\widetilde{\pi_0}$ et $\widetilde{\pi_1}$ sont bien définies, alors $\widetilde{\pi}\ (P) = \left(\widetilde{\pi_0}\ (P), \widetilde{\pi_1}\ (P)\right) = \left(\widetilde{\pi_0}\ (Q), \widetilde{\pi_1}\ (Q)\right) = \widetilde{\pi}\ (Q)$; et donc $\widetilde{\pi}$ est bien définie.

2. Montrons que $\widetilde{\pi}$ est surjective.
   Soit $([x_0 : y_0 : z_0], [x_1 : y_1 : z_1]) \in E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q) \times E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$. Le point :

$$P = [x_0 + (x_1 - x_0)\, e : y_0 + (y_1 - y_0)\, e : z_0 + (z_1 - z_0)\, e],$$

   vérifie $\widetilde{\pi}\ (P) = ([x_0 : y_0 : z_0], [x_1 : y_1 : z_1])$; et donc $\widetilde{\pi}$ est une application surjective.

3. Montrons que $\widetilde{\pi}$ est injective.
   Soient $P = [x_0 + x_1 e : y_0 + y_1 e : z_0 + z_1 e]$ et $Q = [x'_0 + x'_1 e : y'_0 + y'_1 e : z'_0 + z'_1 e]$ deux points

de $E_{a,b}(\mathbb{F}_q[e])$ tels que $\widetilde{\pi}(P) = \widetilde{\pi}(Q)$. Alors :

$$[x_0 : y_0 : z_0] = [x'_0 : y'_0 : z'_0] \text{ et } [x_0 + x_1 : y_0 + y_1 : z_0 + z_1] = [x'_0 + x'_1 : y'_0 + y'_1 : z'_0 + z'_1];$$

et donc il existe deux éléments non nuls α et β de $\mathbb{F}_q$ tels que :

$$\begin{cases} x'_0 = \alpha x_0 \\ y'_0 = \alpha y_0 \\ z'_0 = \alpha z_0 \end{cases} \text{ et } \begin{cases} x'_0 + x'_1 = \beta(x_0 + x_1) \\ y'_0 + y'_1 = \beta(y_0 + y_1) \\ z'_0 + z'_1 = \beta(z_0 + z_1) \end{cases}.$$

Ainsi :

$$\begin{cases} x'_1 = \beta(x_0 + x_1) - \alpha x_0 = (\beta - \alpha) x_0 + \beta x_1 \\ y'_1 = \beta(y_0 + y_1) - \alpha y_0 = (\beta - \alpha) y_0 + \beta y_1 \\ z'_1 = \beta(z_0 + z_1) - \alpha z_0 = (\beta - \alpha) z_0 + \beta z_1 \end{cases};$$

et alors :

$$\begin{cases} x'_0 + x'_1 e = \alpha x_0 + ((\beta - \alpha) x_0 + \beta x_1) e = (\alpha + (\beta - \alpha) e)(x_0 + x_1 e) \\ y'_0 + y'_1 e = \alpha y_0 + ((\beta - \alpha) y_0 + \beta y_1) e = (\alpha + (\beta - \alpha) e)(y_0 + y_1 e) \\ z'_0 + z'_1 e = \alpha z_0 + ((\beta - \alpha) z_0 + \beta z_1) e = (\alpha + (\beta - \alpha) e)(z_0 + z_1 e) \end{cases}.$$

Comme $\alpha + (\beta - \alpha) e$ est inversible dans $\mathbb{F}_q[e]$, alors :

$$P = [x_0 + x_1 e : y_0 + y_1 e : z_0 + z_1 e] = [x'_0 + x'_1 e : y'_0 + y'_1 e : z'_0 + z'_1 e] = Q;$$

et donc $\widetilde{\pi}$ est une application injective.

4. Pour la formule de $\widetilde{\pi}^{-1}$ nous vérifions facilement que :
   (a) Pour tout $[x_0 + x_1 e : y_0 + y_1 e : z_0 + z_1 e] \in E_{a,b}(\mathbb{F}_q[e])$, on a :

$$\begin{aligned} \widetilde{\pi}^{-1} \circ \widetilde{\pi}([x_0 + x_1 e : y_0 + y_1 e : z_0 + z_1 e]) &= \widetilde{\pi}^{-1}([x_0 : y_0 : z_0], [x_0 + x_1 : y_0 + y_1 : z_0 + z_1]) \\ &= [x_0 + x_1 e : y_0 + y_1 e : z_0 + z_1 e]; \end{aligned}$$

   et alors $\widetilde{\pi}^{-1} \circ \widetilde{\pi} = id_{E_{a,b}(\mathbb{F}_q[e])}$.

   (b) Pour tout $([x_0 : y_0 : z_0], [x_1 : y_1 : z_1]) \in E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q) \times E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$, on a :

$$\begin{aligned} \widetilde{\pi} \circ \widetilde{\pi}^{-1}([x_0 : y_0 : z_0], [x_1 : y_1 : z_1]) &= \widetilde{\pi}([x_0 + (x_1 - x_0) e : y_0 + (y_1 - y_0) e : z_0 + (z_1 - z_0) e]) \\ &= ([x_0 : y_0 : z_0], [x_1 : y_1 : z_1]); \end{aligned}$$

   et alors $\widetilde{\pi} \circ \widetilde{\pi}^{-1} = id_{E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q) \times E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)}$.

Donc $\widetilde{\pi}$ est bijective et son inverse est $\widetilde{\pi}^{-1}$. □

Corollaire 2.3.2 *La courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$ a le même nombre de points que l'ensemble $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q) \times E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$; et pour tous points P et Q de $E_{a,b}(\mathbb{F}_q[e])$, nous avons :*

$$P = Q \Leftrightarrow \widetilde{\pi}(P) = \widetilde{\pi}(Q) \Leftrightarrow \widetilde{\pi_0}(P) = \widetilde{\pi_0}(Q) \text{ et } \widetilde{\pi_1}(P) = \widetilde{\pi_1}(Q).$$

2.3.2 Classification des points de la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$

Dans cette sous-section, nous classifions les points de la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$ selon l'inversibilité de la troisième coordonnée projective Z. Plus précisément, nous avons :

Théorème 2.3.3 *Chaque point de la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$ a l'une des formes suivantes :*

1. $[X : Y : 1]$ *avec* $(X, Y) \in \mathbb{F}_q[e] \times \mathbb{F}_q[e]$.
2. $[\alpha e : 1 : \beta e]$ *avec* $(\alpha, \beta) \in \mathbb{F}_q \times \mathbb{F}_q$.
3. $[\alpha e : 1 - e : \beta e]$ *avec* $(\alpha, \beta) \in \mathbb{F}_q \times \mathbb{F}_q^*$.
4. $[\alpha(1-e) : 1 : \beta(1-e)]$ *avec* $(\alpha, \beta) \in \mathbb{F}_q \times \mathbb{F}_q$.
5. $[\alpha(1-e) : e : \beta(1-e)]$ *avec* $(\alpha, \beta) \in \mathbb{F}_q \times \mathbb{F}_q^*$.

Preuve. Soit $P = [X : Y : Z]$ un point de la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$.

1. Si Z est inversible, alors $[X : Y : Z] \sim [X : Y : 1]$.
2. Si Z n'est pas inversible, alors $\pi_0(Z) = 0$ ou $\pi_1(Z) = 0$.
   (a) Si $\pi_0(Z) = 0$, alors $\widetilde{\pi_0}([X : Y : Z]) = [\pi_0(X) : \pi_0(Y) : 0] = [0 : 1 : 0]$; ainsi $[X : Y : Z] = [\pi_1(X)\, e : 1 + (\pi_1(Y) - 1)\, e : \pi_1(Z)\, e]$ et on aura deux cas pour $\pi_1(Y)$.
      i. Si $\pi_1(Y) \neq 0$, alors Y sera inversible ; et donc $[X : Y : Z] = [\alpha e : 1 : \beta e]$, où $\alpha = Y^{-1}\pi_1(X) \in \mathbb{F}_q$ et $\beta = Y^{-1}\pi_1(Z) \in \mathbb{F}_q$.
      ii. Si $\pi_1(Y) = 0$, alors $[X : Y : Z] = [\pi_1(X)\, e : 1 - e : \pi_1(Z)\, e]$; et comme $\widetilde{\pi_1}([X : Y : Z]) = [\pi_1(X) : 0 : \pi_1(Z)]$, alors nécessairement $\pi_1(Z) \neq 0$; et donc $[X : Y : Z] = [\alpha e : 1 - e : \beta e]$, où $\alpha = \pi_1(X) \in \mathbb{F}_q$ et $\beta = \pi_1(Z) \in \mathbb{F}_q^*$.
   (b) Si $\pi_1(Z) = 0$, alors $\widetilde{\pi_1}([X : Y : Z]) = [\pi_1(X) : \pi_1(Y) : 0] = [0 : 1 : 0]$; ainsi $[X : Y : Z] = [\pi_0(X)(1-e) : \pi_0(Y) + (1 - \pi_0(Y))\, e : \pi_0(Z)(1-e)]$ et on aura deux cas pour $\pi_0(Y)$.
      i. Si $\pi_0(Y) \neq 0$, alors Y sera inversible ; et donc $[X : Y : Z] = [\alpha(1-e) : 1 : \beta(1-e)]$, où $\alpha = Y^{-1}\pi_0(X) \in \mathbb{F}_q$ et $\beta = Y^{-1}\pi_0(Z) \in \mathbb{F}_q$.
      ii. Si $\pi_0(Y) = 0$, alors $[X : Y : Z] = [\pi_0(X)(1-e) : e : \pi_0(Z)(1-e)]$; et comme $\widetilde{\pi_0}([X : Y : Z]) = [\pi_0(X) : 0 : \pi_0(Z)]$, alors nécessairement $\pi_0(Z) \neq 0$; et donc $[X : Y : Z] = [\alpha(1-e) : e : \beta(1-e)]$, où $\alpha = \pi_0(X) \in \mathbb{F}_q$ et $\beta = \pi_0(Z) \in \mathbb{F}_q^*$.

Ainsi, le théorème est montré. □

Exemple 2.3.1 *Soient $a = 1 + e$ et $b = 1$ deux éléments de $\mathbb{F}_2[e]$. Alors :*

$$E_{a,b}(\mathbb{F}_2[e]) = \{[0 : 1 : 0] ; [0 : 1 : 1] ; [0 : 1 : e] ; [0 : 1 : 1 + e] ; [e : 1 : 1] ; [e : 1 : e] ; [e : 1 + e : 1]; [e : 1 + e : e]\} ;$$

$$E_{1,1}(\mathbb{F}_2) = \{[0:1:0]\,;\,[0:1:1]\}\,;$$
$$E_{0,1}(\mathbb{F}_2) = \{[0:1:0]\,;\,[0:1:1]\,;\,[1:0:1]\,;\,[1:1:1]\}\,.$$

Ainsi, $\mathrm{card}(E_{a,b}(\mathbb{F}_2[e])) = 8, \mathrm{card}(E_{1,1}(\mathbb{F}_2)) = 2$ *et* $\mathrm{card}(E_{0,1}(\mathbb{F}_2)) = 4$.

Exemple 2.3.2 *Soient* $a = 1 + e$ *et* $b = 2 + 2e$ *deux éléments de* $\mathbb{F}_3[e]$. *Alors :*

$$\begin{aligned}
E_{a,b}(\mathbb{F}_3[e]) =& \{[0:1:0]\,;\,[0:1:e]\,;\,[0:1:2e]\,;\,[1:1:1]\,;\,[1:2:1]\,;\,[1:1+e:1]\,;\,[1:2+2e:1];\\
&[e:1:e]\,;\,[2e:1:2e]\,;\,[e:1+e:e]\,;\,[e:2+2e:e]\,;\,[1+2e:1:1]\,;\,[1+2e:2:1];\\
&[1+2e:1+e:1]\,;\,[1+2e:2+2e:1]\};\\
E_{1,2}(\mathbb{F}_3) =& \{[0:1:0]\,;\,[1:1:1]\,;\,[1:2:1]\};\\
E_{2,1}(\mathbb{F}_3) =& \{[0:1:0]\,;\,[0:1:1]\,;\,[0:2:1]\,;\,[1:1:1]\,;\,[1:2:1]\}.
\end{aligned}$$

Ainsi, $\mathrm{card}(E_{a,b}(\mathbb{F}_3[e])) = 15, \mathrm{card}(E_{1,2}(\mathbb{F}_3)) = 3$ *et* $\mathrm{card}(E_{2,1}(\mathbb{F}_5)) = 5$.

Exemple 2.3.3 *Soient* $a = 1 + 3e$ *et* $b = 1 + 2e$ *deux éléments de* $\mathbb{F}_5[e]$. *Alors :*

$$\begin{aligned}
E_{a,b}\,(\mathbb{F}_5[e]) =& \{[0:1:0]\,;\,[2:1+e:1]\,;\,[2:1+2e:1]\,;\,[2:4+3e:1]\,;\,[2:4+4e:1]\,;\,[2e:1+e:1];\\
&[2e:1+2e:1]\,;\,[2e:4+3e:1]\,;\,[2e:4+4e:1]\,;\,[3+4e:1+e:1]\,;\,[3+4e:1+2e:1];\\
&[3+4e:4+3e:1]\,;\,[3+4e:4+4e:1]\,;\,[4+3e:2+e:1]\,;\,[4+3e:2:1]\,;\,[4+3e:3:1];\\
&[4+3e:3+4e:1]\,;\,[0:1:1-e]\,;\,[0:1:4-4e]\,;\,[2-2e:1:1-e]\,;\,[2-2e:1:3-3e];\\
&[e:1:3e]\,;\,[4e:1:2e]\,;\,[2-2e:1:4-4e]\,;\,[3-3e:1:1-e]\,;\,[3-3e:1:2-2e];\\
&[3-3e:1:4-4e]\};\\
E_{1,1}(\mathbb{F}_5) =& \{[0:1:0]\,;\,[0:1:1]\,;\,[0:4:1]\,;\,[2:1:1]\,;\,[2:4:1]\,;\,[3:1:1]\,;\,[3:4:1]\,;\,[4:2:1];\\
&[4:3:1]\};\\
E_{4,3}(\mathbb{F}_5) =& \{[0:1:0]\,;\,[2:2:1]\,;\,[2:3:1]\}.
\end{aligned}$$

Ainsi, $\mathrm{card}(E_{a,b}(\mathbb{F}_5[e])) = 27, \mathrm{card}(E_{1,1}(\mathbb{F}_5)) = 9$ *et* $\mathrm{card}(E_{4,3}(\mathbb{F}_5)) = 3$.

2.3.3 Applications cryptographiques

Comme applications cryptographiques du Théorème 2.3.2, nous avons :

1. Si $\mathrm{card}(E_{a,b}(\mathbb{F}_q[e])) = n$, alors $n = s \times t$ est une factorisation de n, où $s = \mathrm{card}(E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q))$ et $t = \mathrm{card}(E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q))$.
2. Le cardinal de $E_{a,b}(\mathbb{F}_q[e])$ n'est pas un nombre premier.
3. Le problème du logarithme discret dans la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$ est équivalent à celui de l'ensemble $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q) \times E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$.

2.4 Loi de groupe pour $E_{a,b}(\mathbb{F}_q[e])$

Dans cette section, nous allons montrer qu'on peut munir la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$ d'une structure de groupe abélien.

2.4.1 La structure de groupe pour $E_{a,b}(\mathbb{F}_q[e])$

Soient P et Q deux points de la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$. Posons :

$$P+Q = \widetilde{\pi}^{-1}\left(\widetilde{\pi}(P)+\widetilde{\pi}(Q)\right) = \widetilde{\pi}^{-1}\left(\widetilde{\pi}_0(P)+\widetilde{\pi}_0(Q), \widetilde{\pi}_1(P)+\widetilde{\pi}_1(Q)\right) \tag{2.2}$$

où pour tout $i \in \{0,1\}$, $\widetilde{\pi}_i(P)+\widetilde{\pi}_i(Q)$ est donné par la loi du groupe de la courbe elliptique $E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q)$ (voir les formules explicites d'addition données au chapitre 1).

Théorème 2.4.1 *L'ensemble $(E_{a,b}(\mathbb{F}_q[e]),+)$, où la loi « + » est définie par la formule (2.2), est un groupe abélien d'élément neutre le point $[0:1:0]$; et pour tout point $P=[X:Y:Z]$ de $E_{a,b}(\mathbb{F}_q[e])$, l'inverse de P est le point $-P$ donné par :*

1. *Si $p \neq 2$, alors $-P=[X:-Y:Z]$.*
2. *Si $p=2$, alors $-P=[X:X+Y:Z]$.*

Preuve. Soient P,Q et R des points de la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$. Alors :

1. **Commutativité.**

$$\begin{aligned} P+Q &= \widetilde{\pi}^{-1}\left(\widetilde{\pi}(P)+\widetilde{\pi}(Q)\right) = \widetilde{\pi}^{-1}\left(\widetilde{\pi}_0(P)+\widetilde{\pi}_0(Q), \widetilde{\pi}_1(P)+\widetilde{\pi}_1(Q)\right) \\ &= \widetilde{\pi}^{-1}\left(\widetilde{\pi}_0(Q)+\widetilde{\pi}_0(P), \widetilde{\pi}_1(Q)+\widetilde{\pi}_1(P)\right) = \widetilde{\pi}^{-1}\left(\widetilde{\pi}(Q)+\widetilde{\pi}(P)\right) \\ &= Q+P; \end{aligned}$$

   d'où la loi « + » est commutative.

2. **Associativité.**

$$\begin{aligned} P+(Q+R) &= P+\widetilde{\pi}^{-1}\left(\widetilde{\pi}(Q)+\widetilde{\pi}(R)\right) \\ &= \widetilde{\pi}^{-1}\left(\widetilde{\pi}(P)+\widetilde{\pi}\left(\widetilde{\pi}^{-1}\left(\widetilde{\pi}(Q)+\widetilde{\pi}(R)\right)\right)\right) \\ &= \widetilde{\pi}^{-1}\left(\widetilde{\pi}(P)+\left(\widetilde{\pi}(Q)+\widetilde{\pi}(R)\right)\right) \\ &= \widetilde{\pi}^{-1}\left(\widetilde{\pi}_0(P)+\left(\widetilde{\pi}_0(Q)+\widetilde{\pi}_0(R)\right), \widetilde{\pi}_1(P)+\left(\widetilde{\pi}_1(Q)+\widetilde{\pi}_1(R)\right)\right) \\ &= \widetilde{\pi}^{-1}\left(\left(\widetilde{\pi}_0(P)+\widetilde{\pi}_0(Q)\right)+\widetilde{\pi}_0(R), \left(\widetilde{\pi}_1(P)+\widetilde{\pi}_1(Q)\right)+\widetilde{\pi}_1(R)\right) \\ &= \widetilde{\pi}^{-1}\left(\left(\widetilde{\pi}(P)+\widetilde{\pi}(Q)\right)+\widetilde{\pi}(R)\right) \\ &= \widetilde{\pi}^{-1}\left(\widetilde{\pi}\left(\widetilde{\pi}^{-1}\left(\widetilde{\pi}(P)+\widetilde{\pi}(Q)\right)\right)+\widetilde{\pi}(R)\right) \end{aligned}$$

$$= \widetilde{\pi}^{-1}\left(\widetilde{\pi}(P) + \widetilde{\pi}(Q)\right) + R = (P+Q) + R;$$

d'où la loi « + » est associative.

3. **Élément neutre.**

$$\begin{aligned} P + [0:1:0] &= \widetilde{\pi}^{-1}\left(\widetilde{\pi}(P) + \widetilde{\pi}([0:1:0])\right) \\ &= \widetilde{\pi}^{-1}\left(\widetilde{\pi_0}(P) + \widetilde{\pi_0}([0:1:0]), \widetilde{\pi_1}(P) + \widetilde{\pi_1}([0:1:0])\right) \\ &= \widetilde{\pi}^{-1}\left(\widetilde{\pi_0}(P) + [0:1:0], \widetilde{\pi_1}(P) + [0:1:0]\right) \\ &= \widetilde{\pi}^{-1}\left(\widetilde{\pi_0}(P), \widetilde{\pi_1}(P)\right) \\ &= \widetilde{\pi}^{-1}\left(\widetilde{\pi}(P)\right) \\ &= P; \end{aligned}$$

d'où $[0:1:0]$ est l'élément neutre pour la loi « + ».

4. **Élément opposé.** Soit $P = [X:Y:Z]$. Alors :
   (a) Si $p \neq 2$, alors :

$$\begin{aligned} P + (-P) &= \widetilde{\pi}^{-1}\left(\widetilde{\pi}(P) + \widetilde{\pi}(-P)\right) \\ &= \widetilde{\pi}^{-1}([\pi_0(X):\pi_0(Y):\pi_0(Z)] + [\pi_0(X):\pi_0(-Y):\pi_0(Z)], \\ &\quad [\pi_1(X):\pi_1(Y):\pi_1(Z)] + [\pi_1(X):\pi_1(-Y):\pi_1(Z)]) \\ &= \widetilde{\pi}^{-1}([\pi_0(X):\pi_0(Y):\pi_0(Z)] + [\pi_0(X):-\pi_0(Y):\pi_0(Z)], \\ &\quad [\pi_1(X):\pi_1(Y):\pi_1(Z)] + [\pi_1(X):-\pi_1(Y):\pi_1(Z)]) \\ &= \widetilde{\pi}^{-1}([0:1:0],[0:1:0]) \\ &= [0:1:0]; \end{aligned}$$

   d'où $-P = [X:-Y:Z]$ est l'opposé du point $P = [X:Y:Z]$.
   (b) Si $p = 2$, alors :

$$\begin{aligned} P + (-P) &= \widetilde{\pi}^{-1}\left(\widetilde{\pi}(P) + \widetilde{\pi}(-P)\right) \\ &= \widetilde{\pi}^{-1}([\pi_0(X):\pi_0(Y):\pi_0(Z)] + [\pi_0(X):\pi_0(X+Y):\pi_0(Z)], \\ &\quad [\pi_1(X):\pi_1(Y):\pi_1(Z)] + [\pi_1(X):\pi_1(X+Y):\pi_1(Z)]) \\ &= \widetilde{\pi}^{-1}([\pi_0(X):\pi_0(Y):\pi_0(Z)] + [\pi_0(X):\pi_0(X)+\pi_0(Y):\pi_0(Z)], \\ &\quad [\pi_1(X):\pi_1(Y):\pi_1(Z)] + [\pi_1(X):\pi_1(X)+\pi_1(Y):\pi_1(Z)]) \\ &= \widetilde{\pi}^{-1}([0:1:0],[0:1:0]) \\ &= [0:1:0]; \end{aligned}$$

   d'où $-P = [X:X+Y:Z]$ est l'opposé du point $P = [X:Y:Z]$.

Ce qui prouve le théorème. □

Corollaire 2.4.1 *Soient P et Q deux points de $E_{a,b}(\mathbb{F}_q[e])$. Alors :*

$$P+Q=\left[x_0+(x_1-x_0)\,e : y_0+(y_1-y_0)\,e : z_0+(z_1-z_0)\,e\right],$$

où $[x_0 : y_0 : z_0] = \widetilde{\pi}_0(P)+\widetilde{\pi}_0(Q)$ *et* $[x_1 : y_1 : z_1] = \widetilde{\pi}_1(P)+\widetilde{\pi}_1(Q)$.

Corollaire 2.4.2 *L'application $\widetilde{\pi}$ donnée par le Théorème 2.3.2 est un isomorphisme de groupes.*

Preuve. Découle directement de la formule (2.2). □

Corollaire 2.4.3 *Les applications $\widetilde{\pi}_0$ et $\widetilde{\pi}_1$ données par le Corollaire 2.3.1 sont des homomorphismes de groupes.*

Preuve. Soient P et Q deux points de $E_{a,b}(\mathbb{F}_q[e])$. Alors :

$$\begin{aligned}\widetilde{\pi}(P+Q) &= \left(\widetilde{\pi}_0(P+Q), \widetilde{\pi}_1(P+Q)\right);\\ \widetilde{\pi}(P)+\widetilde{\pi}(Q) &= \left(\widetilde{\pi}_0(P)+\widetilde{\pi}_0(Q), \widetilde{\pi}_1(P)+\widetilde{\pi}_1(Q)\right).\end{aligned}$$

Comme $\widetilde{\pi}(P+Q) = \widetilde{\pi}(P)+\widetilde{\pi}(Q)$, alors pour tout $i\in\{0,1\}$, $\widetilde{\pi}_i(P+Q) = \widetilde{\pi}_i(P)+\widetilde{\pi}_i(Q)$; et donc $\widetilde{\pi}_0$ et $\widetilde{\pi}_1$ sont des homomorphismes de groupes. □

2.4.2 Formules explicites d'addition pour $E_{a,b}(\mathbb{F}_{3^d}[e])$

Dans cette sous-section, nous allons donner les formules explicites d'addition des points de la courbe elliptique $E_{a,b}(\mathbb{F}_{3^d}[e])$. Pour ceci, nous avons utilisé les formules explicites d'addition des points d'une courbe elliptique définie sur le corps fini $\mathbb{F}_{3^d}$ par l'équation (1.17). Ces formules sont données par la Proposition 1.3.4 ; mais dans l'article [10], nous avons travaillé par les formules données par W. Bosma et H. W. Lenstra dans [7, pp. 236–238]. Le résultat est donné par le théorème suivant :

Théorème 2.4.2 *Pour tout $i\in\{0,1\}$, l'ensemble $E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_{3^d})$ est un groupe abélien noté additivement, d'élément neutre le point $[0:1:0]$; et pour tous points $P=[x_1:y_1:z_1]$ et $Q=[x_2:y_2:z_2]$ de $E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_{3^d})$, on a $P+Q=[x_3:y_3:z_3]$, où :*

(i) Si $P=Q$, alors :

$$\begin{aligned}x_3 &= (2\pi_i(a)x_1x_2+y_1y_2)(x_1y_2+x_2y_1)+2\pi_i(ab)z_1z_2(y_1z_2+y_2z_1);\\ y_3 &= y_1^2y_2^2+2(\pi_i(a))^2x_1^2x_2^2+(\pi_i(a))^2\pi_i(b)z_1z_2(x_1z_2+x_2z_1);\\ z_3 &= (\pi_i(a)x_1x_2+y_1y_2)(y_1z_2+y_2z_1)+\pi_i(a)(x_1y_2+x_2y_1)(x_1z_2+x_2z_1).\end{aligned}$$

(ii) Si $P\neq Q$, alors :

$$\begin{aligned}x_3 &= (2\pi_i(a)x_1x_2+y_1y_2)(x_1z_2+2x_2z_1)+(x_1y_2+2x_2y_1)(y_1z_2+y_2z_1);\\ y_3 &= y_1y_2(2y_1z_2+y_2z_1)+\pi_i(a)(x_1y_2+x_2y_1)(2x_1z_2+x_2z_1);\\ z_3 &= 2y_1^2z_2^2+y_2^2z_1^2+\pi_i(a)x_1^2z_2^2+2\pi_i(a)x_2^2z_1^2.\end{aligned}$$

Soient P et Q deux points de la courbe elliptique $E_{a,b}(\mathbb{F}_{3^d}[e])$. D'après le Corollaire 2.4.1, on a $P+Q = [x_0 + (x_1 - x_0)\, e : y_0 + (y_1 - y_0)\, e : z_0 + (z_1 - z_0)\, e]$, où $[x_0 : y_0 : z_0] = \widetilde{\pi_0}\ (P) + \widetilde{\pi_0}\ (Q)$ et $[x_1 : y_1 : z_1] = \widetilde{\pi_1}\ (P) + \widetilde{\pi_1}\ (Q)$ sont donnés par le Théorème 2.4.2. En se servant du Théorème 3.3.3, nous obtiendrons les formules suivantes d'addition des points de la courbe elliptique $E_{a,b}(\mathbb{F}_{3^d}[e])$:

Lemme 2.4.1 $[xe : 1 : ze] + [x'e : 1 : z'e] = [x_1e : 1 + (y_1 - 1)\, e : z_1e]$, *où* x_1, y_1 *et* z_1 *sont donnés par :*

(i) Si $x' = x$ *et* $z' = z$, *alors :*

$$\begin{aligned} x_1 =& 2x + \pi_1(a)\left(x^3 + \pi_1(b)z^3\right)\ ; \\ y_1 =& 1 + 2\left(\pi_1(a)\right)^2 x\left(x^3 + \pi_1(b)z^3\right)\ ; \\ z_1 =& 2z\ . \end{aligned}$$

(ii) Si $x' \neq x$ *ou* $z' \neq z$, *alors :*

$$\begin{aligned} x_1 =& \left(2\pi_1(a)xx' + 1\right)\left(xz' + 2x'z\right) + \left(x + 2x'\right)\left(z' + z\right)\ ; \\ y_1 =& 2\left(z' + 2z\right) + 2\pi_1(a)\left(x + x'\right)\left(xz' + 2x'z\right)\ ; \\ z_1 =& 2z'^2 + z^2 + \pi_1(a)\left(x^2z'^2 + 2x'^2z^2\right)\ . \end{aligned}$$

Preuve. Posons $P = [xe : 1 : ze]$ et $Q = [x'e : 1 : z'e]$. Alors :

$$\begin{aligned} [x_0 : y_0 : z_0] =& \widetilde{\pi_0}\ (P) + \widetilde{\pi_0}\ (Q) = [0 : 1 : 0] + [0 : 1 : 0] = [0 : 1 : 0]\ ; \\ [x_1 : y_1 : z_1] =& \widetilde{\pi_1}\ (P) + \widetilde{\pi_1}\ (Q) = [x : 1 : z] + [x' : 1 : z']\ ; \end{aligned}$$

et le Théorème 2.4.2 pour $i = 1$, permet de déduire les valeurs de x_1, y_1 et z_1. □

Lemme 2.4.2 $[xe : 1 : ze] + [x'e : 1 - e : z'e] = [x_1e : 1 + (y_1 - 1)\, e : z_1e]$, *où* x_1, y_1 *et* z_1 *sont donnés par :*

$$\begin{aligned} x_1 =& 2\pi_1(a)xx'\left(x + 2x'z\right) + 2x'\ ; \\ y_1 =& 2\pi_1(a)x'\left(x + 2x'z\right)\ ; \\ z_1 =& 2 + \pi_1(a)\left(x^2 + 2x'^2z^2\right)\ . \end{aligned}$$

Preuve. Posons $P = [xe : 1 : ze]$ et $Q = [x'e : 1 - e : z'e]$. Alors :

$$\begin{aligned} [x_0 : y_0 : z_0] =& \widetilde{\pi_0}\ (P) + \widetilde{\pi_0}\ (Q) = [0 : 1 : 0]\ ; \\ [x_1 : y_1 : z_1] =& \widetilde{\pi_1}\ (P) + \widetilde{\pi_1}\ (Q) = [x : 1 : z] + [x' : 0 : z']\ ; \end{aligned}$$

et le Théorème 2.4.2 pour $i = 1$, permet de trouver les valeurs de x_1, y_1 et z_1. □

Lemme 2.4.3 $[xe : 1 : ze] + [x' - x'e : 1 : z' - z'e] = [x' + (x - x')\, e : 1 : z' + (z - z')\, e]$.

Preuve. Posons $P = [xe : 1 : ze]$ et $Q = [x' - x'e : 1 : z' - z'e]$. Alors :

$$\begin{aligned}[x_0 : y_0 : z_0] =& \widetilde{\pi_0}(P) + \widetilde{\pi_0}(Q) = [0 : 1 : 0] + [x' : 1 : z'] = [x' : 1 : z'] ;\\ [x_1 : y_1 : z_1] =& \widetilde{\pi_1}(P) + \widetilde{\pi_1}(Q) = [x : 1 : z] + [0 : 1 : 0] = [x : 1 : z] .\end{aligned}$$

□

Lemme 2.4.4 $[xe : 1 : ze] + [x' - x'e : e : z' - z'e] = [x' + (x - x')\, e : e : z' + (z - z')\, e]$.

Preuve. Posons $P = [xe : 1 : ze]$ et $Q = [x' - x'e : e : z' - z'e]$. Alors :

$$\begin{aligned}[x_0 : y_0 : z_0] =& \widetilde{\pi_0}(P) + \widetilde{\pi_0}(Q) = [0 : 1 : 0] + [x' : 0 : z'] = [x' : 0 : z'] ;\\ [x_1 : y_1 : z_1] =& \widetilde{\pi_1}(P) + \widetilde{\pi_1}(Q) = [x : 1 : z] + [0 : 1 : 0] = [x : 1 : z] .\end{aligned}$$

□

Lemme 2.4.5 $[xe : 1 : ze] + [X : Y : 1] = [\pi_0(X) + (x_1 - \pi_0(X))\, e : \pi_0(Y) + (y_1 - \pi_0(Y))\, e : 1 + (z_1 - 1)\, e]$, *où* x_1, y_1 *et* z_1 *sont donnés par :*

(*i*) *Si* $z \neq 0$, $\pi_1(Y) = z^{-1}$ *et* $\pi_1(X) = z^{-1}x$, *alors :*

$$\begin{aligned}x_1 =& 2x + \pi_1(a)\left(x^3 + \pi_1(b)z^3\right) ;\\ y_1 =& 1 + 2\left(\pi_1(a)\right)^2 x\left(x^3 + \pi_1(b)z^3\right) ;\\ z_1 =& 2z .\end{aligned}$$

(*ii*) *Si* $z = 0$ *ou* $\pi_1(Y) \neq z^{-1}$ *ou* $\pi_1(X) \neq z^{-1}x$, *alors :*

$$\begin{aligned}x_1 =& (2\pi_1(a)x\pi_1(X) + \pi_1(Y))\,(x + 2\pi_1(X)z) + (x\pi_1(Y) + 2\pi_1(X))\,(1 + \pi_1(Y)z) ;\\ y_1 =& 2\pi_1(Y)\,(1 + 2\pi_1(Y)z) + 2\pi_1(a)\,(x\pi_1(Y) + \pi_1(X))\,(x + 2\pi_1(X)z) ;\\ z_1 =& 2 + \left(\pi_1(Y)\right)^2 z^2 + \pi_1(a)\left(x^2 + 2\left(\pi_1(X)\right)^2 z^2\right) .\end{aligned}$$

Preuve. Posons $P = [xe : 1 : ze]$ et $Q = [X : Y : 1]$. Alors :

$$\begin{aligned}[x_0 : y_0 : z_0] =& \widetilde{\pi_0}(P) + \widetilde{\pi_0}(Q) = [0 : 1 : 0] + [\pi_0(X) : \pi_0(Y) : 1] = [\pi_0(X) : \pi_0(Y) : 1] ;\\ [x_1 : y_1 : z_1] =& \widetilde{\pi_1}(P) + \widetilde{\pi_1}(Q) = [x : 1 : z] + [\pi_1(X) : \pi_1(Y) : 1] ;\end{aligned}$$

et le Théorème 2.4.2 pour $i = 1$, permet de trouver les valeurs de x_1, y_1 et z_1. □

Lemme 2.4.6 $[x - xe : 1 : z - ze] + [x' - x'e : 1 : z' - z'e] = [x_0 - x_0e : y_0 + (1 - y_0)\, e : z_0 - z_0e]$, *où* x_0, y_0 *et* z_0 *sont donnés par :*

(*i*) *Si* $x' = x$ *et* $z' = z$, *alors :*

$$\begin{aligned}x_0 =& 2x + \pi_0(a)\left(x^3 + \pi_0(b)z^3\right) ;\\ y_0 =& 1 + 2\left(\pi_0(a)\right)^2 x\left(x^3 + \pi_0(b)z^3\right) ;\\ z_0 =& 2z .\end{aligned}$$

(ii) Si $x' \neq x$ ou $z' \neq z$, alors :

$$\begin{aligned} x_0 =& \left(2\pi_0(a)xx' + 1\right)\left(xz' + 2x'z\right) + \left(x + 2x'\right)\left(z' + z\right) \ ; \\ y_0 =& 2\left(z' + 2z\right) + 2\pi_0(a)\left(x + x'\right)\left(xz' + 2x'z\right) \ ; \\ z_0 =& 2z'^2 + z^2 + \pi_0(a)\left(x^2z'^2 + 2x'^2z^2\right) \ . \end{aligned}$$

Preuve. Posons $P = [x - xe : 1 : z - ze]$ et $Q = [x' - x'e : 1 : z' - z'e]$. Alors :

$$\begin{aligned} [x_0 : y_0 : z_0] =& \widetilde{\pi_0}\,(P) + \widetilde{\pi_0}\,(Q) = [x : 1 : z] + [x' : 1 : z'] \ ; \\ [x_1 : y_1 : z_1] =& \widetilde{\pi_1}\,(P) + \widetilde{\pi_1}\,(Q) = [0 : 1 : 0] + [0 : 1 : 0] = [0 : 1 : 0] \ ; \end{aligned}$$

et le Théorème 2.4.2 pour $i = 0$, permet de déduire les valeurs de x_0, y_0 et z_0. □

Lemme 2.4.7 $[x - xe : 1 : z - ze] + [x'e : 1 - e : z'e] = [x + (x' - x)\,e : 1 - e : z + (z' - z)\,e]$.

Preuve. Posons $P = [x - xe : 1 : z - ze]$ et $Q = [x'e : 1 - e : z'e]$. Alors :

$$\begin{aligned} [x_0 : y_0 : z_0] =& \widetilde{\pi_0}\,(P) + \widetilde{\pi_0}\,(Q) = [x : 1 : z] + [0 : 1 : 0] = [x : 1 : z] \ ; \\ [x_1 : y_1 : z_1] =& \widetilde{\pi_1}\,(P) + \widetilde{\pi_1}\,(Q) = [0 : 1 : 0] + [x' : 0 : z'] = [x' : 0 : z'] \ . \end{aligned}$$

□

Lemme 2.4.8 $[x - xe : 1 : z - ze] + [x' - x'e : e : z' - z'e] = [x_0 - x_0e : y_0 + (1 - y_0)\,e : z_0 - z_0e]$, *où x_0, y_0 et z_0 sont donnés par :*

$$\begin{aligned} x_0 =& 2\pi_0(a)xx'\left(x + 2x'z\right) + 2x' \ ; \\ y_0 =& 2\pi_0(a)x'\left(x + 2x'z\right) \ ; \\ z_0 =& 2 + \pi_0(a)\left(x^2 + 2x'^2z^2\right) \ . \end{aligned}$$

Preuve. Posons $P = [x - xe : 1 : z - ze]$ et $Q = [x' - x'e : e : z' - z'e]$. Alors :

$$\begin{aligned} [x_0 : y_0 : z_0] =& \widetilde{\pi_0}\,(P) + \widetilde{\pi_0}\,(Q) = [x : 1 : z] + [x' : 0 : z'] \ ; \\ [x_1 : y_1 : z_1] =& \widetilde{\pi_1}\,(P) + \widetilde{\pi_1}\,(Q) = [0 : 1 : 0] + [0 : 1 : 0] = [0 : 1 : 0] \ ; \end{aligned}$$

et le Théorème 2.4.2 pour $i = 0$, permet de déduire les valeurs de x_0, y_0 et z_0. □

Lemme 2.4.9 $[x - xe : 1 : z - ze] + [X : Y : 1] = [x_0 + (\pi_1(X) - x_0)\,e : y_0 + (\pi_1(Y) - y_0)\,e : z_0 + (1 - z_0)\,e]$, *où x_0, y_0 et z_0 sont donnés par :*

(i) Si $z \neq 0$, $\pi_0(Y) = z^{-1}$ et $\pi_0(X) = z^{-1}x$, alors :

$$\begin{aligned} x_0 =& 2x + \pi_0(a)\left(x^3 + \pi_0(b)z^3\right) \ ; \\ y_0 =& 1 + 2\left(\pi_0(a)\right)^2 x\left(x^3 + 2\pi_0(b)z^3\right) \ ; \\ z_0 =& 2z \ . \end{aligned}$$

(ii) Si $z = 0$ *ou* $\pi_0(Y) \neq z^{-1}$ *ou* $\pi_0(X) \neq z^{-1}x$, *alors :*

$$\begin{aligned} x_0 =& (2\pi_0(a)x\pi_1(X) + \pi_1(Y))\,(x + 2\pi_1(X)z) + (x\pi_1(Y) + 2\pi_1(X))\,(1 + \pi_1(Y)z)\ ; \\ y_0 =& 2\pi_1(Y)\,(1 + 2\pi_1(Y)z) + 2\pi_0(a)\,(x\pi_1(Y) + \pi_1(X))\,(x + 2\pi_1(X)z)\ ; \\ z_0 =& 2 + (\pi_1(Y)z)^2 + \pi_0(a)\left(x^2 + 2\,(\pi_1(X)z)^2\right)\ . \end{aligned}$$

Preuve. Posons $P = [x - xe : 1 : z - ze]$ et $Q = [X : Y : 1]$. Alors :

$$\begin{aligned} [x_0 : y_0 : z_0] =& \widetilde{\pi_0}\,(P) + \widetilde{\pi_0}\,(Q) = [x : 1 : z] + [\pi_0(X) : \pi_0(Y) : 1]\ ; \\ [x_1 : y_1 : z_1] =& \widetilde{\pi_1}\,(P) + \widetilde{\pi_1}\,(Q) = [0 : 1 : 0] + [\pi_1(X) : \pi_1(Y) : 1] = [\pi_1(X) : \pi_1(Y) : 1]\ ; \end{aligned}$$

et le Théorème 2.4.2 pour $i = 0$, permet de déduire les valeurs de x_0, y_0 et z_0. □

En suivant la même démarche précédente, nous obtiendrons la suite des lemmes suivants :

Lemme 2.4.10 $[xe : 1 - e : ze] + [x'e : 1 - e : z'e] = [x_1e : 1 + (y_1 - 1)\,e : z_1e]$, *où* x_1, y_1 *et* z_1 *sont donnés par :*

(i) Si $x' = x$ *et* $z' = z$, *alors* $x_1 = z_1 = 0$ *et* $y_1 = 2\,(\pi_1(a))^2\,x\left(x^3 + \pi_1(b)\right)$.

(ii) Si $x' \neq x$ *ou* $z' \neq z$, *alors* $x_1 = 2\pi_1(a)\,(x + 2x')\,xx'$; $y_1 = 0$ *et* $z_1 = \pi_1(a)\left(x^2 + 2x'^2\right)$.

Lemme 2.4.11 $[xe : 1 - e : ze] + [x' - x'e : e : z' - z'e] = [x' + (x - x')\,e : 0 : z' + (z - z')\,e]$.

Lemme 2.4.12 $[xe : 1 - e : ze] + [X : Y : 1] = [\pi_0(X) + (x_1 - \pi_0(X))\,e : \pi_0(Y) + (y_1 - \pi_0(Y))\,e : 1 + (z_1 - 1)\,e]$, *où* x_1, y_1 *et* z_1 *sont donnés par :*

(i) Si $\pi_1(Y) = 0$ *et* $\pi_1(X) = z^{-1}x$, *alors* $x_1 = z_1 = 0$ *et* $y_1 = 2\,(\pi_1(a))^2\,x\left(x^3 + \pi_1(b)\right)$.

(ii) Si $\pi_1(Y) \neq 0$ *ou* $\pi_1(X) \neq z^{-1}x$, *alors :*

$$\begin{aligned} x_1 =& 2\pi_1(a)x\pi_1(X)\,(x + 2\pi_1(X)) + x\,(\pi_1(Y))^2\ ; \\ y_1 =& 2\pi_1(a)\pi_1(Y)\,(x + 2\pi_1(X))\,x\ ; \\ z_1 =& (\pi_1(Y)z)^2 + \pi_1(a)\left(x^2 + 2\,(\pi_1(X))^2\right)\ . \end{aligned}$$

Lemme 2.4.13 $[x - xe : e : z - ze] + [x' - x'e : e : z' - z'e] = [x_0 - x_0e : y_0 + (1 - y_0)\,e : z_0 - z_0e]$, *où* x_0, y_0 *et* z_0 *sont donnés par :*

(i) Si $xz' = x'z$, *alors* $x_0 = z_0 = 0$ *et* $y_0 = 2\,(\pi_0(a))^2\,x\left(x^3 + \pi_0(b)\right)$.

(ii) Si $xz' \neq x'z$, *alors* $x_0 = 2\pi_0(a)\,(x + 2x')\,xx'$; $y_0 = 0$ *et* $z_0 = \pi_0(a)\left(x^2 + 2x'^2\right)$.

Lemme 2.4.14 $[x - xe : e : z - ze] + [X : Y : 1] = [x_0 + (\pi_1(X) - x_0)\,e : y_0 + (\pi_1(Y) - y_0)\,e : z_0 + (1 - z_0)\,e]$, *où* x_0, y_0 *et* z_0 *sont donnés par :*

(i) Si $\pi_0(Y) = 0$ *et* $\pi_0(X) = z^{-1}x$, *alors* $x_0 = z_0 = 0$ *et* $y_0 = 2\,(\pi_0(a))^2\,x\left(x^3 + \pi_0(b)\right)$.

(ii) Si $\pi_0(Y) \neq 0$ *ou* $\pi_0(X) \neq z^{-1}x$, *alors :*

$$\begin{aligned} x_0 =& 2\pi_0(a)x\pi_0(X)\,(x + 2\pi_0(X)) + x\pi_0(Y)\pi_1(Y)\ ; \\ y_0 =& 2\pi_0(a)\pi_0(Y)\,(x + 2\pi_0(X))\,x\ ; \\ z_0 =& (\pi_0(Y))^2 + \pi_0(a)\left(x^2 + 2\,(\pi_0(X))^2\right)\ . \end{aligned}$$

Lemme 2.4.15 $[X : Y : 1] + [X' : Y' : 1] = [x_0 + (x_1 - x_0)\, e : y_0 + (y_1 - y_0)\, e : z_0 + (z_1 - z_0)\, e]$, *où pour tout* $i \in \{0, 1\}$, x_i, y_i *et* z_i *sont donnés par :*

(*i*) *Si* $\pi_i(X') = \pi_i(X)$ *et* $\pi_i(Y') = \pi_i(Y)$, *alors :*

$$\begin{aligned} x_i =& \left(\pi_i(a)\left(\pi_i(X)\right)^2 + 2\left(\pi_i(Y)\right)^2\right)\pi_i(XY) + \pi_i(ab)\pi_i(Y) ; \\ y_i =& \left(\pi_i(Y)\right)^4 + 2\left(\pi_i(a)\right)^2\left(\pi_i(X)\right)^4 + 2\left(\pi_i(a)\right)^2\pi_i(b)\pi_i(X) ; \\ z_i =& 2\left(\left(\pi_i(Y)\right)^2 + \pi_i(a)\left(\pi_i(X)\right)^2\right)\pi_i(Y) + \pi_i(a)\pi_i(X^2Y) . \end{aligned}$$

(*ii*) *Si* $\pi_i(X') \neq \pi_i(X)$ *ou* $\pi_i(Y') \neq \pi_i(Y)$, *alors :*

$$\begin{aligned} x_i =& \left(2\pi_i(a)\pi_i(XX') + \pi_i(YY')\right)\left(\pi_i(X) + 2\pi_i(X')\right) + \left(\pi_i(XY') + 2\pi_i(X'Y)\right)\left(\pi_i(Y) + \pi_i(Y')\right) ; \\ y_i =& \pi_i(YY')\left(2\pi_i(Y) + \pi_i(Y')\right) + 2\pi_i(a)\left(\pi_i(XY') + \pi_i(X'Y)\right)\left(\pi_i(X) + 2\pi_i(X')\right) ; \\ z_i =& 2\left(\pi_i(Y)\right)^2 + \left(\pi_i(Y')\right)^2 + \pi_i(a)\left(\pi_i(X)\right)^2 + 2\pi_i(a)\left(\pi_i(X')\right)^2 . \end{aligned}$$

Nous regroupons les Lemmes 2.4.1 à 2.4.15 au théorème suivant, qui donne explicitement la loi du groupe de la courbe elliptique $E_{a,b}(\mathbb{F}_{3^d}[e])$ donnée par le Corollaire 2.4.1.

Théorème 2.4.3 *Soient* $P = [X_0 : Y_0 : Z_0]$ *et* $Q = [X_1 : Y_1 : Z_1]$ *deux points de la courbe elliptique* $E_{a,b}(\mathbb{F}_{3^d}[e])$ *et soient* $[x_0 : y_0 : z_0] = \widetilde{\pi_0}(P) + \widetilde{\pi_0}(Q)$ *et* $[x_1 : y_1 : z_1] = \widetilde{\pi_1}(P) + \widetilde{\pi_1}(Q)$. *Alors* $P + Q = [X_2 : Y_2 : Z_2]$, *où* X_2, Y_2 *et* Z_2 *sont donnés par :*

(*i*) *Si* $\widetilde{\pi_0}(P) = [0 : 1 : 0]$, *alors :*

$$\begin{aligned} X_2 =& \pi_0(X_1) + (x_1 - \pi_0(X_1))\, e ; \\ Y_2 =& \pi_0(Y_1) + (y_1 - \pi_0(Y_1))\, e ; \\ Z_2 =& \pi_0(Z_1) + (z_1 - \pi_0(Z_1))\, e . \end{aligned}$$

(*ii*) *Si* $\widetilde{\pi_1}(P) = [0 : 1 : 0]$, *alors :*

$$\begin{aligned} X_2 =& x_0 + (\pi_1(X_1) - x_0)\, e ; \\ Y_2 =& y_0 + (\pi_1(Y_1) - y_0)\, e ; \\ Z_2 =& z_0 + (\pi_1(Z_1) - z_0)\, e . \end{aligned}$$

(*iii*) *Si* $\widetilde{\pi_0}(P) \neq [0 : 1 : 0]$ *et* $\widetilde{\pi_1}(P) \neq [0 : 1 : 0]$, *alors :*

$$\begin{aligned} X_2 =& x_0 + (x_1 - x_0)\, e ; \\ Y_2 =& y_0 + (y_1 - y_0)\, e ; \\ Z_2 =& z_0 + (z_1 - z_0)\, e . \end{aligned}$$

Preuve. D'après le Corollaire 2.4.1, nous avons :

(*i*) Si $\widetilde{\pi_0}(P) = [0:1:0]$, alors $[x_0 : y_0 : z_0] = \widetilde{\pi_0}(Q) = [\pi_0(X_1) : \pi_0(Y_1) : \pi_0(Z_1)]$; et donc :

$$\begin{aligned} X_2 &= \pi_0(X_1) + (x_1 - \pi_0(X_1))\, e \ ; \\ Y_2 &= \pi_0(Y_1) + (y_1 - \pi_0(Y_1))\, e \ ; \\ Z_2 &= \pi_0(Z_1) + (z_1 - \pi_0(Z_1))\, e \ . \end{aligned}$$

(*ii*) Si $\widetilde{\pi_1}(P) = [0:1:0]$, alors $[x_1 : y_1 : z_1] = \widetilde{\pi_1}(Q) = [\pi_1(X_1) : \pi_1(Y_1) : \pi_1(Z_1)]$; et donc :

$$\begin{aligned} X_2 &= x_0 + (\pi_1(X_1) - x_0)\, e \ ; \\ Y_2 &= y_0 + (\pi_1(Y_1) - y_0)\, e \ ; \\ Z_2 &= z_0 + (\pi_1(Z_1) - z_0)\, e \ . \end{aligned}$$

(*iii*) Si $\widetilde{\pi_0}(P) \neq [0:1:0]$ et $\widetilde{\pi_1}(P) \neq [0:1:0]$, alors :

$$\begin{aligned} X_2 &= x_0 + (x_1 - x_0)\, e \ ; \\ Y_2 &= y_0 + (y_1 - y_0)\, e \ ; \\ Z_2 &= z_0 + (z_1 - z_0)\, e \ . \end{aligned}$$

□

Remarque 2.4.1 *Nous remarquons que les Lemmes 2.4.1, 2.4.2, 2.4.3, 2.4.4, 2.4.5, 2.4.10, 2.4.11 et 2.4.12 vérifient le premier cas du Théorème 2.4.3 et les Lemmes 2.4.6, 2.4.7, 2.4.8, 2.4.9, 2.4.13 et 2.4.14 vérifient le deuxième cas ; alors que le Lemme 2.4.15 vérifie le dernier cas.*

2.5 Conclusion

Dans ce chapitre, nous avons déterminé une bijection entre la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$ et le produit cartésien des courbes elliptiques $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$ et $E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$. Cette bijection, nous a permis de munir la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$ d'une structure de groupe abélien, où nous avons donné explicitement les formules d'addition de ses points pour le cas particulier où $q = 3^d$, avec d un entier strictement positif. Pour les courbes elliptiques $E_{a,b}(\mathbb{F}_{2^d}[e])$ et $E_{a,b}(\mathbb{F}_{p^d}[e])$ où p est un nombre premier supérieur ou égal à 5, nous obtiendrons des théorèmes analogues au Théorème 2.4.3.

3

Courbes elliptiques sur l'anneau $\mathbb{F}_q[e],\ e^3 = e^2$

Sommaire

3.1 Introduction **45**

3.2 L'anneau $\mathbb{F}_q[e],\ e^3 = e^2$ **45**

3.2.1 Propriétés algébriques 45

3.2.2 Coûts des opérations arithmétiques 48

3.3 Courbes elliptiques sur l'anneau $\mathbb{F}_q[e],\ e^3 = e^2$ **48**

3.3.1 Réductions de $\mathbf{E}_{a,b}(\mathbb{F}_q[e])$ sur $\mathbb{F}_q$ 49

3.3.2 Classification des points dans $\mathbf{E}_{a,b}(\mathbb{F}_q[e])$ 51

3.3.3 Loi de groupe pour $\mathbf{E}_{a,b}(\mathbb{F}_q[e])$ 54

3.4 Conclusion **55**

Soit $\mathbb{F}_q$ un corps fini d'ordre $q = p^d$, avec p un nombre premier supérieur ou égal à 5 et d un entier strictement positif. Dans ce chapitre, nous allons présenter les résultats publiés dans l'article [8] concernant l'étude de la courbe elliptique définie sur l'anneau $\mathbb{F}_q[e]$, où $e^3 = e^2$, par l'équation de Weierstrass :

$$Y^2Z = X^3 + aXZ^2 + bZ^3 \tag{3.1}$$

où a et b sont deux éléments de l'anneau $\mathbb{F}_q[e]$, tels que $4a^3 + 27b^2$ est inversible.

3.1 Introduction

Soit $\mathbb{F}_q[X]$ l'anneau des polynômes à une indéterminée et à coefficients dans le corps fini $\mathbb{F}_q$ et soit P le polynôme de $\mathbb{F}_q[X]$ défini par $P(X) = X^3 - X^2$. Le quotient de l'anneau $\mathbb{F}_q[X]$ par l'idéal engendré par le polynôme P est un anneau commutatif, unitaire et fini. Posons e l'image de X par la surjection canonique [1]. Alors :

- $\mathbb{F}_q[X]/(P)$ est un $\mathbb{F}_q$-espace vectoriel de dimension 3 et de base $\left\{1, e, e^2\right\}$;
- e vérifie $e^3 - e^2 = 0$.

Donc, on peut identifier l'anneau quotient $\mathbb{F}_q[X]/(P)$ à l'anneau $\mathbb{F}_q\left[e\right]$ des éléments de la forme $x_0 + x_1e + x_2e^2$, où $(x_0, x_1, x_2) \in \mathbb{F}_q^3$ et $e^3 = e^2$.

Dans un premier temps, nous allons donner quelques propriétés algébriques de l'anneau $\left(\mathbb{F}_q\left[e\right], +, .\right)$, où pour tous éléments $X = x_0 + x_1e + x_2e^2$ et $Y = y_0 + y_1e + y_2e^2$ de $\mathbb{F}_q\left[e\right]$, les opérations arithmétiques d'addition « $X + Y$ » et de multiplication « $X.Y$ » sont définies par :

$$\begin{aligned} X + Y &= (x_0 + y_0) + (x_1 + y_1)\, e + (x_2 + y_2)\, e^2; \\ X.Y &= (x_0y_0) + (x_0y_1 + x_1y_0)\, e + (x_2y_0 + (x_1 + x_2)y_1 + (x_0 + x_1 + x_2)y_2)\, e^2. \end{aligned} \tag{3.2}$$

En se servant des propriétés algébriques de l'anneau $\mathbb{F}_q\left[e\right]$, nous étudions dans un deuxième temps la courbe elliptique définie sur cet anneau par l'équation (3.1).

Nous Terminerons ce chapitre par une courte conclusion de ce travail.

3.2 L'anneau $\mathbb{F}_q\left[e\right],\ e^3 = e^2$

Nous commençons cette section par une étude algébrique des propriétés de l'anneau $\mathbb{F}_q\left[e\right]$.

3.2.1 Propriétés algébriques

Nous adapterons la formule (3.3) suivante pour calculer le produit $X.Y$ donné par la formule (3.2).

Lemme 3.2.1 *Soient $X = x_0 + x_1e + x_2e^2$ et $Y = y_0 + y_1e + y_2e^2$ deux éléments de $\mathbb{F}_q\left[e\right]$. Le produit $X.Y$ dans l'anneau $\mathbb{F}_q\left[e\right]$ peut être écrit sous la forme :*

$$X.Y = x_0y_0 + \delta_{XY}e + ((x_0 + x_1 + x_2)(y_0 + y_1 + y_2) - x_0y_0 - \delta_{XY})\, e^2, \tag{3.3}$$

où $\delta_{XY} = x_0y_1 + x_1y_0$.

Preuve. Évidente. □

Corollaire 3.2.1 *Les puissances X^2 et X^3 d'un élément $X = x_0 + x_1e + x_2e^2$ de $\mathbb{F}_q\left[e\right]$ sont*

1. $e = X + (P)$ dans $\mathbb{F}_q[X]/(P)$.

données par :

$$X^2 = x_0^2 + \delta_{X^2} e + \left((x_0 + x_1 + x_2)^2 - x_0^2 - \delta_{X^2}\right) e^2 ;$$
$$X^3 = x_0^3 + \delta_{X^3} e + \left((x_0 + x_1 + x_2)^3 - x_0^3 - \delta_{X^3}\right) e^2 ;$$

où $\delta_{X^2} = 2x_0x_1$ *et* $\delta_{X^3} = 3x_0^2x_1$.

Preuve. Découle directement du Lemme 3.2.1. □

Corollaire 3.2.2 *Les applications* π_0 *et* π_1 *définies par :*

$$\begin{array}{rcl} \pi_0 : \mathbb{F}_q[e] & \longrightarrow & \mathbb{F}_q \\ x_0 + x_1 e + x_2 e^2 & \longmapsto & x_0 \end{array} \quad et \quad \begin{array}{rcl} \pi_1 : \mathbb{F}_q[e] & \longrightarrow & \mathbb{F}_q \\ x_0 + x_1 e + x_2 e^2 & \longmapsto & x_0 + x_1 + x_2 \end{array}$$

sont deux homomorphismes surjectives d'anneaux.

Preuve. Soient $X = x_0 + x_1 e + x_2 e^2$ et $Y = y_0 + y_1 e + y_2 e^2$. On a :

$$X + Y = (x_0 + y_0) + (x_1 + y_1) e + (x_2 + y_2) e^2 ;$$
$$X.Y = x_0y_0 + \delta_{XY} e + ((x_0 + x_1 + x_2)(y_0 + y_1 + y_2) - x_0y_0 - \delta_{XY}) e^2 ;$$

où $\delta_{XY} = x_0y_1 + x_1y_0$. Alors :

(i)

$$\pi_0(X + Y) = x_0 + y_0 = \pi_0(X) + \pi_0(Y) \text{ et } \pi_0(X.Y) = x_0.y_0 = \pi_0(X).\pi_0(Y) ;$$

et donc π_0 est un homomorphisme d'anneaux.

(ii)

$$\pi_1(X + Y) = x_0 + y_0 + x_1 + y_1 + x_2 + y_2 = (x_0 + x_1 + x_2) + (y_0 + y_1 + y_2) = \pi_1(X) + \pi_1(Y) ;$$
$$\pi_1(X.Y) = (x_0 + x_1 + x_2).(y_0 + y_1 + y_2) = \pi_1(X).\pi_1(Y) ;$$

et donc π_1 est un homomorphisme d'anneaux.

De plus, pour tout $x \in \mathbb{F}_q$, nous avons $\pi_0(x) = \pi_1(x) = x$; et alors π_0 et π_1 sont deux homomorphismes surjectifs d'anneaux. □

Corollaire 3.2.3 *Soient* X *et* Y *deux éléments de* $\mathbb{F}_q[e]$. *Alors :*

$$X.Y = \pi_0(XY) + \delta_{XY} e + (\pi_1(XY) - \pi_0(XY) - \delta_{XY}) e^2. \tag{3.4}$$

Preuve. Cela découle directement du Lemme 3.2.1 et du Corollaire 3.2.2. □

La proposition suivante caractérise l'ensemble $(\mathbb{F}_q[e])^\times$ des éléments inversibles dans l'anneau $\mathbb{F}_q[e]$.

Proposition 3.2.1 *Soient $X = x_0 + x_1 e + x_2 e^2 \in \mathbb{F}_q[e]$. Alors X est inversible si, et seulement si $\pi_0(X)$ et $\pi_1(X)$ ne sont pas nuls dans le corps fini $\mathbb{F}_q$. Dans ce cas, l'inverse de X est donné par : $X^{-1} = x_0^{-1} - x_1 x_0^{-2} e + \left((x_0 + x_1 + x_2)^{-1} + x_1 x_0^{-2} - x_0^{-1}\right) e^2$.*

Preuve. Soient $X = x_0 + x_1 e + x_2 e^2$ et $Y = y_0 + y_1 e + y_2 e^2$. Comme l'anneau $\mathbb{F}_q[e]$ est un $\mathbb{F}_q$-espace vectoriel de dimension 3 et de base $\left\{1, e, e^2\right\}$, alors d'après le Lemme 3.2.1, nous avons :

$$
\begin{aligned}
X.Y = 1 \Leftrightarrow & \begin{cases} x_0 y_0 = 1 \\ \delta_{XY} = 0 \\ (x_0 + x_1 + x_2)(y_0 + y_1 + y_2) - x_0 y_0 - \delta_{XY} = 0 \end{cases} \\
\Leftrightarrow & \begin{cases} x_0 \neq 0 \text{ et } y_0 = x_0^{-1} \\ x_0 y_1 = -x_1 y_0 = -x_1 x_0^{-1} \\ (x_0 + x_1 + x_2)(y_0 + y_1 + y_2) = 1 \end{cases} \\
\Leftrightarrow & \begin{cases} x_0 \neq 0 \text{ et } y_0 = x_0^{-1} \\ y_1 = -x_1 x_0^{-2} \\ (x_0 + x_1 + x_2) \neq 0 \text{ et } y_0 + y_1 + y_2 = (x_0 + x_1 + x_2)^{-1} \end{cases} \\
\Leftrightarrow & \begin{cases} x_0 \neq 0 \text{ et } y_0 = x_0^{-1} \\ y_1 = -x_1 x_0^{-2} \\ (x_0 + x_1 + x_2) \neq 0 \text{ et } y_2 = (x_0 + x_1 + x_2)^{-1} + x_1 x_0^{-2} - x_0^{-1} \end{cases} .
\end{aligned}
$$

Ainsi X est inversible si, et seulement si $x_0 \neq 0$ et $x_0 + x_1 + x_2 \neq 0$; et l'inverse de X est donné par : $X^{-1} = Y = x_0^{-1} - x_1 x_0^{-2} e + \left((x_0 + x_1 + x_2)^{-1} + x_1 x_0^{-2} - x_0^{-1}\right) e^2$. □

Corollaire 3.2.4 *L'ensemble des éléments non inversibles dans l'anneau $\mathbb{F}_q[e]$ est formé de la réunion des idéaux I et J définis par :*

$$
I = \left\{xe + ye^2 \mid (x, y) \in \mathbb{F}_q^2\right\} \text{ et } J = \left\{x + ye - (x + y)e^2 \mid (x, y) \in \mathbb{F}_q^2\right\}.
$$

Preuve. Soit $w = x + ye + ze^2 \in \mathbb{F}_q[e]$. Alors :

$w \notin (\mathbb{F}_q[e])^\times \Leftrightarrow x = 0$ ou $x + y + z = 0 \Leftrightarrow w = ye + ze^2$ ou $w = x + ye - (x + y)e^2 \Leftrightarrow w \in I \cup J$.

Il reste à montrer que I et J sont deux idéaux de $\mathbb{F}_q[e]$.

- On a I est l'idéal de $\mathbb{F}_q[e]$ engendré par les éléments e et e^2.
- Montrons que J est un idéal de $\mathbb{F}_q[e]$.
  (*i*) Comme $0 \in J$ et $X - Y \in J$ pour tous $X, Y \in J$, alors $(J, +)$ est un sous groupe de $(\mathbb{F}_q[e], +)$.

(*ii*) Soient $u = x + ye - (x+y)e^2 \in J$ et $v = \alpha + \delta e + \lambda e^2 \in \mathbb{F}_q[e]$. Alors :

$$\begin{aligned} u.v &= \left(\alpha + \delta e + \lambda e^2\right).\left(x + ye - (x+y)e^2\right) \\ &= \alpha x + (\alpha y + \delta x)e + ((\alpha + \delta + \lambda)(x + y - x - y) - \alpha x - \alpha y - \delta x)e^2 \\ &= \alpha x + (\alpha y + \delta x)e - (\alpha x + \alpha y + \delta x)e^2 \in J . \end{aligned}$$

et donc J est un idéal de $\mathbb{F}_q[e]$.

□

Corollaire 3.2.5 *L'anneau $\mathbb{F}_q[e]$ est non-local.*

Preuve. Comme $I \not\subset J$ et $J \not\subset I$, alors $I \cup J$ n'est pas un idéal de $\mathbb{F}_q[e]$; ce qui entraîne que $\mathbb{F}_q[e]$ n'est pas un anneau local. □

3.2.2 Coûts des opérations arithmétiques

Soient s, m et i (resp. S, M et I) respectivement, les coûts d'addition, de multiplication et d'inversion dans $\mathbb{F}_q$ (resp. $\mathbb{F}_q[e]$). Alors $S = 3s, M = 7s + 4m$ et $I = 4s + m + 3i$, où M est calculé par la formule (3.3).

3.3 Courbes elliptiques sur l'anneau $\mathbb{F}_q[e]$, $e^3 = e^2$

Soient a et b deux éléments de l'anneau $\mathbb{F}_q[e]$ tels que $4a^3 + 27b^2$ est inversible. L'ensemble de solutions dans le plan projectif sur l'anneau $\mathbb{F}_q[e]$ de l'équation (3.1) est une courbe elliptique (voir Remarque 1.4.2 pour $p \geq 5$) qu'on note par $\mathbf{E}_{a,b}(\mathbb{F}_q[e])$ et on écrit :

$$\mathbf{E}_{a,b}(\mathbb{F}_q[e]) = \left\{[X:Y:Z] \in \mathbb{P}^2(\mathbb{F}_q[e]) \mid Y^2Z = X^3 + aXZ^2 + bZ^3\right\}.$$

Dans le reste de ce chapitre a, b, X, Y et Z sont des éléments de l'anneau $\mathbb{F}_q[e]$, fixés par :

$$\begin{aligned} a &= a_0 + a_1e + a_2e^2 ; \\ b &= b_0 + b_1e + b_2e^2 ; \\ X &= x_0 + x_1e + x_2e^2 ; \\ Y &= y_0 + y_1e + y_2e^2 ; \\ Z &= z_0 + z_1e + z_2e^2 ; \end{aligned}$$

et pour $i \in \{0, 1\}$, nous désignons par Δ_i l'image de Δ par l'application π_i, où $\Delta = 4a^3 + 27b^2$ est le discriminant de la courbe elliptique $\mathbf{E}_{a,b}(\mathbb{F}_q[e])$.

3.3.1 Réductions de $\mathbf{E}_{a,b}(\mathbb{F}_q[e])$ sur $\mathbb{F}_q$

Dans le plan projectif défini sur le corps fini $\mathbb{F}_q$, nous définissons les ensembles $\mathbf{E}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$ et $\mathbf{E}_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$ par :

$$\mathbf{E}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q) = \left\{[x:y:z] \in \mathbb{P}^2(\mathbb{F}_q) \mid y^2z = x^3 + \pi_0(a)xz^2 + \pi_0(b)z^3\right\}\ ; \tag{3.5}$$

$$\mathbf{E}_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q) = \left\{[x:y:z] \in \mathbb{P}^2(\mathbb{F}_q) \mid y^2z = x^3 + \pi_1(a)xz^2 + \pi_1(b)z^3\right\}. \tag{3.6}$$

Les discriminants des courbes qui définissent les ensembles (3.5) et (3.6) sont respectivement Δ_0 et Δ_1. Comme Δ est inversible dans l'anneau $\mathbb{F}_q[e]$, alors d'après la Proposition 3.2.1, Δ_0 et Δ_1 ne sont pas nuls dans $\mathbb{F}_q$. Ainsi, nous avons :

Lemme 3.3.1 *Les ensembles $\mathbf{E}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$ et $\mathbf{E}_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$ sont des courbes elliptiques sur le corps fini $\mathbb{F}_q$.*

Lemme 3.3.2 *Les propriétés suivantes sont équivalentes :*

(i) $[X:Y:Z] \in \mathbb{P}^2(\mathbb{F}_q[e])$.

(ii) $\forall i \in \{0,1\} : [\pi_i(X):\pi_i(Y):\pi_i(Z)] \in \mathbb{P}^2(\mathbb{F}_q)$.

Preuve.

- Montrons que $(i) \Rightarrow (ii)$. On a :

$$\begin{aligned}
[X:Y:Z] \in \mathbb{P}^2(\mathbb{F}_q[e]) &\Rightarrow \exists\left(X',Y',Z'\right) \in (\mathbb{F}_q[e])^3 :\ XX'+YY'+ZZ' = 1 \\
&\Rightarrow \forall i \in \{0,1\} :\ \pi_i(X)\pi_i(X') + \pi_i(Y)\pi_i(Y') + \pi_i(Z)\pi_i(Z') = 1 \\
&\Rightarrow \forall i \in \{0,1\} :\ (\pi_i(X),\pi_i(Y),\pi_i(Z)) \neq (0,0,0) \\
&\Rightarrow \forall i \in \{0,1\} :\ [\pi_i(X):\pi_i(Y):\pi_i(Z)] \in \mathbb{P}^2(\mathbb{F}_q).
\end{aligned}$$

- Montrons que $(ii) \Rightarrow (i)$. Supposons que $[\pi_i(X):\pi_i(Y):\pi_i(Z)] \in \mathbb{P}^2(\mathbb{F}_q)$ pour tout $i \in \{0,1\}$. Alors :
  1. Si $\pi_0(Z) \neq 0$, alors :
     (a) Si $\pi_1(Z) \neq 0$, alors Z est inversible dans $\mathbb{F}_q[e]$; et donc $[X:Y:Z] \in \mathbb{P}^2(\mathbb{F}_q[e])$.
     (b) Si $\pi_1(Z) = 0$, alors $\pi_1(Y) \neq 0$, et nous aurions $\pi_0\left(Z+e^2Y\right) = \pi_0(Z) \neq 0$ et $\pi_1\left(Z+e^2Y\right) = \pi_1(Y) \neq 0$; et donc $Z+e^2Y$ est inversible dans $\mathbb{F}_q[e]$. Ainsi, il existe $U \in (\mathbb{F}_q[e])^\times$ tel que $UZ+e^2UY = 1$; et alors $[X:Y:Z] \in \mathbb{P}^2(\mathbb{F}_q[e])$.
  2. Si $\pi_0(Z) = 0$, alors $\pi_0(Y) \neq 0$, et nous aurions deux cas pour $\pi_1(Y)$:
     (a) Si $\pi_1(Y) \neq 0$, alors Y est inversible dans $\mathbb{F}_q[e]$; et donc $[X:Y:Z] \in \mathbb{P}^2(\mathbb{F}_q[e])$.
     (b) Si $\pi_1(Y) = 0$, alors $\pi_1(Z) \neq 0$, et nous aurions $\pi_0\left(Y+e^2Z\right) = \pi_0(Y) \neq 0$ et $\pi_1\left(Y+e^2Z\right) = \pi_1(Z) \neq 0$; et donc $Y+e^2Z$ est inversible dans $\mathbb{F}_q[e]$. Ainsi, il existe $U \in (\mathbb{F}_q[e])^\times$ tel que $UY+e^2UZ = 1$; et alors $[X:Y:Z] \in \mathbb{P}^2(\mathbb{F}_q[e])$.

□

Lemme 3.3.3 *Si $Y^2Z = X^3 + aXZ^2 + bZ^3$, alors :*

$$\forall i \in \{0,1\} : (\pi_i(Y))^2 \pi_i(X) = (\pi_i(X))^3 + \pi_i(a)\pi_i(X)(\pi_i(Z))^2 + \pi_i(b)(\pi_i(Z))^3 .$$

Preuve. Le résultat découle directement du fait que π_i est un homomorphisme d'anneaux pour tout $i \in \{0,1\}$. □

D'après les Lemmes 3.3.1, 3.3.2 et 3.3.3, nous aurions le résultat suivant :

Proposition 3.3.1 *Si $[X : Y : Z] \in \mathbf{E}_{a,b}(\mathbb{F}_q[e])$, alors $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \in E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q)$ pour tout $i \in \{0,1\}$.*

Corollaire 3.3.1 *Pour tout $i \in \{0,1\}$, l'application $\widetilde{\pi_i}$ donnée par :*

$$\begin{array}{ccc} \mathbf{E}_{a,b}(\mathbb{F}_q[e]) & \xrightarrow{\widetilde{\pi_i}} & \mathbf{E}_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q) \\ [X : Y : Z] & \longmapsto & [\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \end{array}$$

est bien définie.

Preuve. Soit $([X : Y : Z], [X' : Y' : Z']) \in (\mathbf{E}_{a,b}(\mathbb{F}_q[e]))^2$. Si $[X : Y : Z] = [X' : Y' : Z']$, alors il existe $U \in (\mathbb{F}_q[e])^\times$ tel que $X' = UX$, $Y' = UY$ et $Z' = UZ$. D'où pour tout $i \in \{0,1\}$, on a :

$$\begin{aligned} \widetilde{\pi_i}\left([X' : Y' : Z']\right) = [\pi_i(X') : \pi_i(Y') : \pi_i(Z')] &= \underbrace{[\pi_i(U)\pi_i(X) : \pi_i(U)\pi_i(Y) : \pi_i(U)\pi_i(Z)]}_{\pi_i(U)\neq 0 \text{ dans } \mathbb{F}_q} \\ &= [\pi_i(X) : \pi_i(Y) : \pi_i(Z)] = \widetilde{\pi_i}([X : Y : Z]) ; \end{aligned}$$

et alors l'application $\widetilde{\pi_i}$ est bien définie. □

Proposition 3.3.2 *Si $\delta_{Y^2Z} = \delta_{X^3} + \delta_{aXZ^2} + \delta_{bZ^3}$, alors la réciproque dans la Proposition 3.3.1 est vraie.*

Preuve. Supposons que $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \in \mathbf{E}_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q)$ pour tout $i \in \{0,1\}$. D'après le Lemme 3.3.2, on aura $[X : Y : Z] \in \mathbb{P}^2(\mathbb{F}_q[e])$; et donc, si $Y^2Z = X^3 + aXZ^2 + bZ^3$, alors $[X : Y : Z] \in \mathbf{E}_{a,b}(\mathbb{F}_q[e])$.
D'après le Corollaire 3.2.3, nous avons :

$$\begin{aligned} Y^2Z &= \pi_0\left(Y^2Z\right) + \delta_{Y^2Z}e + \left(\left(\pi_1\left(Y^2Z\right)\right) - \pi_0\left(Y^2Z\right) - \delta_{Y^2Z}\right)e^2 ; \\ X^3 &= \pi_0\left(X^3\right) + \delta_{X^3}e + \left(\pi_1\left(X^3\right) - \pi_0\left(X^3\right) - \delta_{X^3}\right)e^2 ; \\ aXZ^2 &= \pi_0\left(aXZ^2\right) + \delta_{aXZ^2}e + \left(\pi_1\left(aXZ^2\right) - \pi_0\left(aXZ^2\right) - \delta_{aXZ^2}\right)e^2 ; \\ bZ^3 &= \pi_0\left(bZ^3\right) + \delta_{bZ^3}e + \left(\pi_1\left(bZ^3\right) - \pi_0\left(bZ^3\right) - \delta_{bZ^3}\right)e^2 ; \end{aligned}$$

et alors :

$$Y^2Z = X^3 + aXZ^2 + bZ^3 \Leftrightarrow \begin{cases} \pi_0\left(Y^2Z\right) = \pi_0\left(X^3\right) + \pi_0\left(aXZ^2\right) + \pi_0\left(bZ^3\right) \\ \delta_{Y^2Z} = \delta_{X^3} + \delta_{aXZ^2} + \delta_{bZ^3} \\ \pi_1\left(Y^2Z\right) = \pi_1\left(X^3\right) + \pi_1\left(aXZ^2\right) + \pi_1\left(bZ^3\right) \end{cases} ;$$

ce qui montre que l'équivalence dans la Proposition 3.3.1 est sous l'hypothèse $\delta_{Y^2Z} = \delta_{X^3} + \delta_{aXZ^2} + \delta_{bZ^3}$. □

Remarque 3.3.1 *En utilisant le Lemme 3.2.1, nous vérifions facilement que :*

$$\begin{aligned} \delta_{Y^2Z} &= y_0^2 z_1 + 2y_0 y_1 z_0 \ ; \\ \delta_{X^3} &= 3x_0^2 x_1 \ ; \\ \delta_{aXZ^2} &= 2a_0 x_0 z_0 z_1 + a_0 x_1 z_0^2 + a_1 x_0 z_0^2 \ ; \\ \delta_{bZ^3} &= 3b_0 z_0^2 z_1 + b_1 z_0^3 \ . \end{aligned}$$

Corollaire 3.3.2 *L'application $\widetilde{\pi_1}$ est surjective.*

Preuve. Soit $[x : y : z] \in E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$. Posons $X = xe^2$, $Y = 1 + (y-1)e^2$ et $Z = ze^2$. Alors :

$$\begin{aligned} \delta_{Y^2Z} = \delta_{X^3} = \delta_{aXZ^2} = \delta_{bZ^3} = 0 \ ; \\ \widetilde{\pi_0}\left([X : Y : Z]\right) = [0 : 1 : 0] \in \mathbf{E}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_{p^d}) \ ; \\ \widetilde{\pi_1}\left([X : Y : Z]\right) = [x : y : z] \in \mathbf{E}_{\pi_1(a),\pi_1(b)}(\mathbb{F}_{p^d}) \ . \end{aligned}$$

Ainsi, $[X : Y : Z] \in \mathbf{E}_{a,b}(\mathbb{F}_q[e])$ et l'application $\widetilde{\pi_1}$ est surjective. □

Remarque 3.3.2 *La surjection de l'application $\widetilde{\pi_0}$ sera traitée dans la sous-section suivante.*

3.3.2 Classification des points dans $\mathbf{E}_{a,b}(\mathbb{F}_q[e])$

Dans cette sous-section, nous classifions les points de la courbe elliptique $\mathbf{E}_{a,b}(\mathbb{F}_q[e])$.

Proposition 3.3.3 *Chaque point de la courbe elliptique $\mathbf{E}_{a,b}(\mathbb{F}_q[e])$ a l'une des formes suivantes :*

1. $[X : Y : 1]$, *avec* $Y^2 = X^3 + aX + b$.
2. $[xe + x'e^2 : 1 : ze^2]$, *avec* $[x + x' : 1 : z] \in \mathbf{E}_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$.
3. $[xe + x'e^2 : 1 + ye - (1+y)e^2 : ze^2]$, *avec* $[x + x' : 0 : z] \in \mathbf{E}_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$.
4. $[x + x'e - (x + x')e^2 : 1 : z + z'e - (z + z')e^2]$, *avec x, x', z et z' sont tels que :*

$$[x : 1 : z] \in \mathbf{E}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q) \ \text{ et } z' = 3x^2x' + 2a_0xzz' + \left(a_0x' + a_1x\right)z^2 + 3b_0z^2z' + b_1z^3 \ .$$

5. $[x + x'e - (x + x')e^2 : ye + (1 - y)e^2 : 1 + ze - (1 + z)e^2]$, *avec* x, x', y *et* z *sont tels que :*

$$[x : 0 : 1] \in \mathbf{E}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q) \text{ et } 3x^2x' + 2a_0xz + \left(a_0x' + a_1x\right) + 3b_0z + b_1 = 0\,.$$

Preuve. La preuve de cette proposition est basée sur la Proposition 3.3.2, qui affirme que :

$$[X : Y : Z] \in \mathbf{E}_{a,b}(\mathbb{F}_q[e]) \Leftrightarrow \begin{cases} \widetilde{\pi_0}([X : Y : Z]) \in \mathbf{E}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q) \\ \widetilde{\pi_1}([X : Y : Z]) \in \mathbf{E}_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q) \\ \delta_{Y^2Z} = \delta_{X^3} + \delta_{aXZ^2} + \delta_{bZ^3} \end{cases}.$$

Soit $P = [X : Y : Z] \in \mathbf{E}_{a,b}(\mathbb{F}_q[e])$. Selon l'inversibilité du troisième coordonnée projective Z, nous avons les cas suivants :

1. Si Z est inversible dans $\mathbb{F}_q[e]$, alors $[X : Y : Z] \sim [X : Y : 1]$.
2. Si $z_0 = 0$, alors $P = [x_0 + x_1e + x_2e^2 : y_0 + y_1e + y_2e^2 : z_1e + z_2e^2]$; et on a :
   (a) $\widetilde{\pi_0}([X : Y : Z]) = [x_0 : y_0 : 0] = [0 : 1 : 0]$; et donc :
   $$[X : Y : Z] = [x_1e + x_2e^2 : 1 + y_1e + y_2e^2 : z_1e + z_2e^2].$$
   (b) $\widetilde{\pi_1}([X : Y : Z]) = [x_1 + x_2 : 1 + y_1 + y_2 : z_1 + z_2]$; et nous aurions deux cas pour $1 + y_1 + y_2$:
      i. Si $1 + y_1 + y_2 \neq 0$, alors Y sera inversible dans $\mathbb{F}_q[e]$, et donc :
      $$[X : Y : Z] = [x_1e + x_2e^2 : 1 : z_1e + z_2e^2].$$
      Comme dans ce cas, on a : $\delta_{Y^2Z} = z_1$, $\delta_{X^3} = \delta_{aXZ^2} = 0$ et $\delta_{bZ^3} = 0$; alors l'égalité $\delta_{Y^2Z} = \delta_{X^3} + \delta_{aXZ^2} + \delta_{bZ^3}$ entraîne que $z_1 = 0$. Ainsi :
      $$[X : Y : Z] = [x_1e + x_2e^2 : 1 : z_2e^2], \text{ avec } [x_1 + x_2 : 1 : z_2] \in \mathbf{E}_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)\,.$$
      ii. Si $1 + y_1 + y_2 = 0$, alors :
      $$[X : Y : Z] = [x_1e + x_2e^2 : 1 + y_1e - (1 + y_1)e^2 : z_1e + z_2e^2].$$
      Comme dans ce cas, on a : $\delta_{Y^2Z} = z_1$, $\delta_{X^3} = \delta_{aXZ^2} = \delta_{bZ^3} = 0$; alors l'égalité $\delta_{Y^2Z} = \delta_{X^3} + \delta_{aXZ^2} + \delta_{bZ^3}$ entraîne que $z_1 = 0$. Ainsi :
      $$[X : Y : Z] = [x_1e + x_2e^2 : 1 + y_1e - (1 + y_1)e^2 : z_2e^2],$$
      avec $[x_1 + x_2 : 0 : z_2] \in \mathbf{E}_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)\,.$
3. Si $z_0 + z_1 + z_2 = 0$, alors $P = [x_0 + x_1e + x_2e^2 : y_0 + y_1e + y_2e^2 : z_0 + z_1e - (z_0 + z_1)e^2]$; et on a :

(a) $\widetilde{\pi_1}([X:Y:Z]) = [x_0 + x_1 + x_2 : y_0 + y_1 + y_2 : 0] = [0:1:0]$; et donc :

$$[X:Y:Z] = [x_0 + x_1 e - (x_0 + x_1)\, e^2 : y_0 + y_1 e + y_2 e^2 : z_0 + z_1 e - (z_0 + z_1)\, e^2].$$

(b) $\widetilde{\pi_0}([X:Y:Z]) = [x_0 : y_0 : z_0]$; et nous aurions deux cas pour y_0 :

i. Si $y_0 \neq 0$, alors Y sera inversible dans $\mathbb{F}_q[e]$; et donc :

$$[X:Y:Z] = [x_0 + x_1 e - (x_0 + x_1)\, e^2 : 1 : z_0 + z_1 e - (z_0 + z_1)\, e^2],$$

avec x_0, x_1, z_0 et z_1 sont tels que :

$$[x_0 : 1 : z_0] \in \mathbf{E}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q) \text{ et } \delta_{Y^2Z} = \delta_{X^3} + \delta_{aXZ^2} + \delta_{bZ^3},$$

où :

$$\begin{aligned}
&\delta_{Y^2Z} = z_1 \ ; \\
&\delta_{X^3} = 3x_0^2 x_1 \ ; \\
&\delta_{aXZ^2} = 2a_0 x_0 z_0 z_1 + (a_0 x_1 + a_1 x_0)\, z_0^2 \ ; \\
&\delta_{bZ^3} = 3b_0 z_0^2 z_1 + b_1 z_0^3 \ .
\end{aligned}$$

ii. Si $y_0 = 0$, alors :

$$[X:Y:Z] = [x_0 + x_1 e - (x_0 + x_1)\, e^2 : y_1 e + y_2 e^2 : z_0 + z_1 e - (z_0 + z_1)\, e^2].$$

Comme $[x_0 : 0 : z_0] \in \mathbf{E}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$ et $[0 : y_1 + y_2 : 0] \in \mathbf{E}_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$, alors $z_0 = 1$ et $y_2 = 1 - y_1$. Ainsi :

$$[X:Y:Z] = [x_0 + x_1 e - (x_0 + x_1)\, e^2 : y_1 e + (1 - y_1)\, e^2 : 1 + z_1 e - (1 + z_1)\, e^2],$$

avec x_0, x_1, y_1 et z_1 sont tels que $\delta_{Y^2Z} = \delta_{X^3} + \delta_{aXZ^2} + \delta_{bZ^3}$, où :

$$\begin{aligned}
&\delta_{Y^2Z} = 0 \ ; \\
&\delta_{X^3} = 3x_0^2 x_1 \ ; \\
&\delta_{aXZ^2} = 2a_0 x_0 z_1 + (a_0 x_1 + a_1 x_0) \ ; \\
&\delta_{bZ^3} = 3b_0 z_1 + b_1 \ .
\end{aligned}$$

.

□

Corollaire 3.3.3 *L'application $\widetilde{\pi_1}$ n'est pas injective.*

Preuve. Soit $[x:y:z] \in \mathbf{E}_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$. D'après le deuxième et le troisième cas de la Proposition 3.3.3, on a :

1. Si $y = 1$, alors $\widetilde{\pi_1}\left([xe : 1 : ze^2]\right) = \widetilde{\pi_1}\left([xe^2 : 1 : ze^2]\right)$ et $[xe : 1 : ze^2] \neq [xe^2 : 1 : ze^2]$.

2. Si $y = 0$, alors $\widetilde{\pi_1}\left([xe : 1 - e^2 : ze^2]\right) = \widetilde{\pi_1}\left([xe^2 : 1 - e^2 : ze^2]\right)$ et $[xe : 1 - e^2 : ze^2] \neq [xe^2 : 1 - e^2 : ze^2]$.

Ces deux cas, montre que l'application $\widetilde{\pi_1}$ n'est pas injective. □

Corollaire 3.3.4 *L'application $\widetilde{\pi_0}$ est surjective.*

Preuve. Soit $[x : y : z] \in E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$ et soit $f(x, y, z) = y^2z - x^3 - a_0xz^2 - b_0z^3$. Selon les deux derniers cas de la Proposition 3.3.3, on a :

1. Si $y = 1$, alors le point $P = [x + x'e - (x + x')e^2 : 1 : z + z'e - (z + z')e^2]$ est un antécédent de $[x : 1 : z]$ si x' et z' vérifient $z' = 3x^2x' + 2a_0xzz' + (a_0x' + a_1x)z^2 + 3b_0z^2z' + b_1z^3$. Fixons [2] $z' = 0$. Le problème revient à trouver x' tel que $x'\left(3x^2 + a_0z^2\right) = -\left(a_1xz^2 + b_1z^3\right)$. Comme $[x : 1 : z] \in E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$, alors $\dfrac{\partial f}{\partial x}(x, 1, z) = -3x^2 - a_0z^2 \neq 0$; et donc $x' = -\left(3x^2 + a_0z^2\right)^{-1}\left(a_1xz^2 + b_1z^3\right)$. Ainsi, le point $P = [x + x'e - (x + x')e^2 : 1 : z - ze^2]$ est un antécédent de $[x : 1 : z]$.
2. Si $y = 0$, alors le point $P = [x + x'e - (x + x')e^2 : ye + (1 - y)e^2 : 1 + ze - (1 + z)e^2]$ est un antécédent de $[x : 0 : 1]$ si x' et z vérifient $0 = 3x^2x' + 2a_0xz + (a_0x' + a_1x) + 3b_0z + b_1$. Fixons [3] $x' = 0$. Le problème revient à trouver z tel que $z(2a_0x + 3b_0) = -(a_1x + b_1)$. Comme $[x : 0 : 1] \in E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$, alors $\dfrac{\partial f}{\partial z}(x, 0, 1) = -2a_0x - 3b_0 \neq 0$; et donc $z = -(2a_0x + 3b_0)^{-1}(a_1x + b_1)$. Ainsi, le point $P = [x - xe^2 : e^2 : 1 + ze - (1 + z)e^2]$ est un antécédent de $[x : 0 : 1]$.

Ce qui montre que l'application $\widetilde{\pi_0}$ est surjective. □

Remarque 3.3.3 *Si $a_1 = b_1 = 0$, alors on peut voir facilement que l'application $\widetilde{\pi_0}$ est surjective. En effet, soit $[x : y : z] \in E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$. D'après, la Proposition 3.3.3, on a :*

1. *Si $y = 1$, alors le point $P = [x - xe^2 : 1 : z - ze^2]$ vérifie $\delta_{Y^2Z} = \delta_{X^3} = \delta_{aXZ^2} = \delta_{bZ^3} = 0$; et donc P est un antécédent de $[x : 1 : z]$.*
2. *Si $y = 0$, alors le point $P = [x - xe^2 : e : 1 - e^2]$ vérifie $\delta_{Y^2Z} = \delta_{X^3} = \delta_{aXZ^2} = \delta_{bZ^3} = 0$; et donc P est un antécédent de $[x : 0 : 1]$.*

D'où $\widetilde{\pi_0}$ est une application surjective.

Corollaire 3.3.5 *L'application $\widetilde{\pi_0}$ n'est pas injective.*

Preuve. La preuve du corollaire 3.3.4 montre que l'application $\widetilde{\pi_0}$ est surjective et que chaque point $[x : y : z] \in E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$ a au moins deux antécédents distincts; et donc $\widetilde{\pi_0}$ n'est pas injective. □

3.3.3 Loi de groupe pour $\mathbf{E}_{a,b}(\mathbb{F}_q[e])$

La courbe elliptique $\mathbf{E}_{a,b}(\mathbb{F}_q[e])$ est munie d'une structure de groupe abélien. L'addition des points dans ce groupe est donnée explicitement par le théorème suivant :

2. On peut prendre z' quelconque dans $\mathbb{F}_q$.
3. On peut prendre x' quelconque dans $\mathbb{F}_q$.

Théorème 3.3.1 *L'ensemble* $(\mathbf{E}_{a,b}(\mathbb{F}_q[e]),+)$ *est un groupe abélien d'élément neutre le point* $[0:1:0]$ *et dont la loi « + » est définie par* $[X_1:Y_1:Z_1]+[X_2:Y_2:Z_2]=[X_3:Y_3:Z_3]$, *avec :*

1. *Si* $[X_1:Y_1:Z_1]=[X_2:Y_2:Z_2]$, *alors :*

$$\begin{aligned}
X_3 =& (Y_1Y_2 - 3bZ_1Z_2 - a(X_1Z_2+X_2Z_1))(X_1Y_2+X_2Y_1) + (Y_1Z_2+Y_2Z_1)(a^2Z_1Z_2 - aX_1X_2 \\
& - 3b(X_1Z_2+X_2Z_1)) ; \\
Y_3 =& Y_1^2Y_2^2 + 3aX_1^2X_2^2 + \left(9bX_1X_2 - a^2X_2Z_1\right)(X_1Z_2+X_2Z_1) - Z_1Z_2(3ab(X_1Z_2+X_2Z_1) \\
& + a^2X_1X_2 + \left(a^3+9b^2\right)Z_1Z_2) ; \\
Z_3 =& (X_1Y_2+X_2Y_1)(3X_1X_2+aZ_1Z_2) + (Y_1Y_2+3bZ_1Z_2+a(X_1Z_2+X_2Z_1))(Y_1Z_2+Y_2Z_1).
\end{aligned}$$

2. *Si* $[X_1:Y_1:Z_1]\neq[X_2:Y_2:Z_2]$, *alors :*

$$\begin{aligned}
X_3 =& (X_1Y_2 - X_2Y_1)(Y_1Z_2+Y_2Z_1) + (Y_1Y_2 - 3bZ_1Z_2 - a(X_1Z_2+X_2Z_1))(X_1Z_2 - X_2Z_1) ; \\
Y_3 =& (3X_1X_2+aZ_1Z_2)(X_2Y_1 - X_1Y_2) + (3bZ_1Z_2 - Y_1Y_2 + a(X_1Z_2+X_2Z_1))(Y_1Z_2 - Y_2Z_1) ; \\
Z_3 =& (3X_1X_2+aZ_1Z_2)(X_1Z_2 - X_2Z_1) + (Y_2Z_1+Y_1Z_2)(Y_2Z_1 - Y_1Z_2) .
\end{aligned}$$

Preuve. Le Théorème peut être démontré en utilisant les formules explicites de W. Bosma et H. Lenstra [7, pages : 236–238]. □

Remarque 3.3.4 *Soit* $P=[X:Y:Z]\in\mathbf{E}_{a,b}(\mathbb{F}_q[e])$. *L'opposé du point* P *est le point noté* $-P$ *et donné par* $-P=[X:-Y:Z]$.

3.4 Conclusion

Dans ce chapitre, nous avons étudié en caractéristique supérieure ou égale à 5, les courbes elliptiques définies sur l'anneau $\mathbb{F}_q[e]$, où $e^3=e^2$, par l'équation de Weierstrass $Y^2Z=X^3+aXZ^2+bZ^3$. Le but de ce chapitre était d'avoir un bagage théorique suffisant pour la réalisation des cryptosystèmes sur ce type d'anneaux. Dans cette étude, nous avons remarqué que la propriété d'isomorphisme entre la courbe elliptique $\mathbf{E}_{a,b}(\mathbb{F}_q[e])$ et le produit cartésien $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)\times E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$ établie pour $e^2=e$, n'est plus valable pour $e^3=e^2$.

4 Applications cryptographiques

Sommaire

4.1 Préliminaires 57
4.1.1 Introduction 57
4.1.2 Terminologie 59
4.1.3 Principe d'Auguste Kerckhoffs (1883) 61
4.1.4 Objectifs de la cryptographie 61
4.1.5 Cryptanalyse 62
4.1.6 Sécurité des cryptosystèmes 63
4.1.7 Signature numérique 64
4.2 Algorithmes cryptographiques 64
4.2.1 Algorithmes symétriques 65
4.2.2 Algorithmes asymétriques 67
4.3 Protocoles d'échange de clefs 68
4.3.1 Problème du logarithme discret 68
4.3.2 Protocole de Diffie-Hellman 70
4.3.3 Cryptosystème d'ElGamal 71
4.3.4 Chiffrement RSA 72
4.4 Cryptographie sur les courbes elliptiques 73
4.4.1 Échange de clefs Diffie-Hellman 74
4.4.2 Cryptosystème d'ElGamal 75
4.5 Chiffrement entièrement homomorphe 75
4.5.1 Introduction 75
4.5.2 Premier cryptosystème 78
4.5.3 Deuxième cryptosystème 81
4.5.4 Sécurité de ces cryptosystèmes 85
4.5.5 Conclusion 85

Dans ce chapitre, nous introduisons deux systèmes de chiffrement entièrement homomorphes basés sur les courbes elliptiques étudiées aux chapitres précédents :

- ◇ Le premier cryptosystème est basé sur un anneau de matrices carrées. La construction de cet anneau est basé sur la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$ étudiée au chapitre 2. Ce cryptosystème fait l'objet d'une étude publié dans [9].
- ◇ Le deuxième cryptosystème est basé sur l'anneau $\mathbb{F}_q[e]$ où $e^3 = e^2$; et dont le protocole d'échange de clés est basé sur Diffie-Hellman pour la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$ étudiée au chapitre 3. Les résultats concernant ce cryptosystème sont publiés dans [13].

Pour arriver à cet objectif, nous commençons par des rappels élémentaires sur la cryptographie selon la hiérarchie suivante :

- ◇ Introduction (vision générale sur la cryptographie).
- ◇ Préliminaires sur la cryptographie (terminologie, objectifs de la cryptographie, signature numérique, ...).
- ◇ Algorithmes cryptographiques (symétriques et asymétriques).
- ◇ Protocoles d'échange de clés (Diffie-Hellman, ElGamal et RSA).
- ◇ Cryptographie sur les courbes elliptiques (Diffie-Hellman et ElGamal pour les courbes elliptiques).
- ◇ Chiffrement entièrement homomorphe (on introduit dans cette section les deux cryptosystèmes mentionnés ci-dessus.).

Comme il y a assez de références sur la cryptographie, les références suivantes sont adoptées pour la rédaction de ce chapitre :

- ◇ Pour un aperçu historique sur la cryptographie [30, 35].
- ◇ Pour des références de bases sur la cryptographie [37, 64, 68, 83, 112, 127, 130].
- ◇ Pour la cryptographie sur les courbes elliptiques [24, 41, 69, 82, 139].
- ◇ Pour la cryptographie homomorphe [19, 48, 141].

4.1 Préliminaires

4.1.1 Introduction

L'historien en cryptographie *David Kahn* [60] considère l'humaniste *Leon Battista Alberti* [46, 98] comme le « père de la cryptographie occidentale », grâce à trois avancées significatives : « la plus ancienne théorie occidentale de cryptanalyse, l'invention de la substitution polyalphabétique et l'invention du code de chiffrement [128] »[1].

Bien qu'éminemment stratégique, la cryptographie est restée pendant très longtemps un art, pour ne devenir une science qu'au 21e siècle. Avec l'apparition de l'informatique, son utilisation se démocratise de plus en plus.

La cryptographie classique [126] est utilisée depuis *l'Antiquité*[2] [30] dans plusieurs domaines comme le domaine militaire [66], le domaine commercial [97, 99] et dans la protection de la

1. `https://fr.wikipedia.org/wiki/Cryptographie`.
2. Une époque de l'histoire.

vie privée [1, 57]. Cette cryptographie est basée sur les caractères (lettres, numéros et symboles) où les différents algorithmes cryptographiques remplaçaient des caractères par d'autres ou transposaient les caractères. Les meilleurs systèmes faisaient les deux opérations plusieurs fois.

La cryptographie d'aujourd'hui [5, 66, 126] est une des disciplines de la *cryptologie* [16, 78], recouvrant l'ensemble des techniques et méthodes permettant le chiffrement et le déchiffrement des messages entre deux entités ou personnes de l'indiscrétion des espions (aussi appelés adversaires, attaquants, intercepteurs, intrus, opposants, oreilles indiscrètes, cryptanalystes, décrypteurs ou tout simplement ennemis), afin d'en préserver la confidentialité, l'authentification et l'intégrité des données. L'une des méthodes les plus anciennes de la cryptographie est *la cryptographie symétrique* (également dite à clé secrète). Cette cryptographie, permet à la fois de chiffrer et de déchiffrer des messages à l'aide d'un concept fondamental appelé « clé secrète », car toute la sécurité de l'ensemble est directement liée au fait que cette clé n'est connue que par l'expéditeur et le destinataire. La cryptographie symétrique se caractérise par une grande rapidité, et elle est largement utilisée pour protéger les informations dans de nombreux systèmes informatiques modernes. Par exemple, la *norme de chiffrement avancé* AES (Advanced Encryption Standard), aussi connue sous le nom de *Rijndael* [28, 29] est le nouveau standard de chiffrement pour les organisations du gouvernement des États-Unis. L'AES a remplacé le standard de chiffrement de données DES (Data Encryption Standard) [26], qui avait été développé par IBM (International Business Machines) dans les années 1970 en tant que norme de chiffrement symétrique et ensuite adopté comme norme américaine en 1977 par le Bureau national des normes [3] pour la protection des données non classifiées.

Le développement le plus récent dans l'histoire de la cryptographie a eu lieu en 1976, lorsque Whitfield Diffie et Martin Hellman ont présenté au public à la « National Computer Conference » le concept révolutionnaire de la cryptographie à clé publique (ou *la cryptographie asymétrique*) [34], qui a été publié quelques mois plus tard sous le titre « New Directions in Cryptography » [33]. Cet article fournissait également une nouvelle méthode pour résoudre des problèmes liés à la distribution et la génération de la clé secrète dans la cryptographie symétrique. Bien que les auteurs n'aient pas encore réalisé un système de chiffrement à clé publique à l'époque, mais ils ont présenté le premier cryptosystème à clé publique, qui a permis à deux personnes de se communiquer secrètement dans le cadre d'une communication publique sans canal secret prédéterminé. Cette invention et ceux qui suivent ont révolutionné le domaine de la cryptographie et le monde de la communication numérique.

Depuis 1976, plusieurs algorithmes à clef publique ont été proposés où seuls quelques-uns d'entre eux sont sûrs et pratiques. Ces algorithmes sont en général basés sur des problèmes mathématiques considérés calculatoirement difficiles à résoudre [4]. Le système Merkle-Hellman [86] est généralement considéré comme la première réalisation pratique d'un système de chiffrement à clef publique [83] ; il a cependant été prouvé non sûr par Shamir en 1982 [114]. Le premier algorithme à clef publique sûr et pratique a été introduit en 1978 par Ronald Rivest, Adi Shamir

3. Maintenant appelé NIST(National Institute of Standards and Technology).
4. Nécessitent un temps exponentiel ou sous exponentiel.

et Leonard Adleman et porte le nom de RSA (Rivest-Shamir-Adleman) [111]. Le cryptosystème RSA est rapidement devenu le cryptosystème à clef publique le plus connu et le plus largement utilisé. Une autre catégorie de systèmes puissants et pratiques de la cryptographie à clé publique a été découverte par T. ElGamal en 1985 [40].

L'une des contributions les plus importantes de la cryptographie à clé publique est la signature numérique. En 1991, la première norme internationale pour les signatures numériques a été basée sur le système à clé publique RSA. En 1994, le gouvernement américain a adopté la norme de signature numérique DSS (Digital Signature Standard), basé sur le système à clé publique ElGamal.

La sécurité des systèmes cryptographiques modernes est généralement basée sur des problèmes mathématiques. Par exemple, l'échange de clés de Diffie-Hellman et le chiffrement ElGamal sont basés sur le *problème du logarithme discret*, alors que le chiffrement RSA est basé sur le *problème de factorisation* des grands entiers en nombres premiers. Bien que les cryptosystèmes basés sur le problème du logarithme discret aient été dans les yeux du public beaucoup moins que RSA, le problème du logarithme discret a reçu une considérable attention dans le milieu de la recherche.

Le développement rapide de nouvelles technologies pousse les chercheurs à utiliser de nouveaux outils mathématiques pour construire des cryptosystèmes toujours plus sûrs. La recherche de nouveaux systèmes à clés publiques, d'améliorations des mécanismes cryptographiques existants et de preuves de sécurité se poursuit à un rythme rapide, où diverses normes et infrastructures impliquant la cryptographie sont en cours de mise en place. Des produits de sécurité sont en cours de développement pour répondre aux besoins de sécurité d'une société à forte intensité d'information.

4.1.2 Terminologie

Le mot *cryptographie* vient des mots en grec ancien [5] *kruptos* qui signifie « caché » et *graphein* qui signifie « écrire ». Beaucoup des termes de la cryptographie utilisent la racine « crypt », ou des dérivés du terme « chiffre ». Dans ce qui suit, nous allons lister un ensemble de termes que nous rencontrons très souvent en cryptographie :

- **Cryptologie :** est la branche des mathématiques qui traite de la cryptographie et de la cryptanalyse.
- **Cryptanalyse :** est l'art de déchiffrer des messages chiffrés.
- **Cryptographie :** est la science de garder le secret de messages par étude et conception des procédés de chiffrement des informations.
- **Attaque :** est une tentative de cryptanalyse.
- **Texte en clair :** est le message envoyé par l'expéditeur. L'ensemble des textes en clair est noté par $\mathcal{M}$.
- **Chiffrement (ou cryptage) :** est le processus de transformer un message en clair en un message incompréhensible. On note ce processus par une fonction Enc .

5. L'étape historique de la langue grecque qui s'étend du 9e siècle av. J.-C. au 8e siècle.

- **Cryptogramme (ou texte chiffré) :** est le résultat obtenu par un processus de chiffrement. L'ensemble des cryptogrammes est noté par $\mathcal{C}$; et pour tout $m \in \mathcal{M}$, on écrit $\text{Enc}(m) = c$ où $c \in \mathcal{C}$ est le chiffré de m.
- **Déchiffrement (ou décryptage) :** est le processus de reconstruction du texte en clair à partir du texte chiffré. On note ce processus par une fonction Dec, où pour tout $m \in \mathcal{M}$, on a $\text{Dec}\,(c) = m$ avec c est le chiffré de m.
- **Algorithme cryptographique :** est une fonction mathématique utilisée pour le chiffrement et le déchiffrement.
- **Algorithme restreint :** est un algorithme cryptographique dont la sécurité est basée sur le fait que celui-ci est tenu secret.
- **Clef :** est une valeur utilisée dans un algorithme cryptographique afin de chiffrer une donnée. L'ensemble des clefs est noté $\mathcal{K}$.
- **Cryptographie moderne :** se base sur la notion de *clefs* où l'algorithme cryptographique peut être publié et analysé (principe de Kerckhoffs (1883) [66]).
- **Cryptosystème ou système cryptographique :** est l'ensemble composé d'un algorithme cryptographique, de tous les messages en clairs, de tous les messages chiffrés et de l'espace des clés [112].
- **Protocole :** est une série d'étapes, impliquant deux ou plusieurs participants, conçu pour accomplir une tâche.
- **Protocole cryptographique :** est un protocole qui utilise des algorithmes cryptographiques dont le but de faire impossible apprendre plus de ce qui est prévu dans le protocole.
- **Protagonistes traditionnels :**
  - **Alice et Bob :** souhaitent se transmettre des informations où Alice est l'émetteur et Bob est le destinataire.
  - **Oscar :** un opposant qui souhaite espionner Alice et Bob.

La figure suivante illustre le schéma de communication entre Alice et Bob :

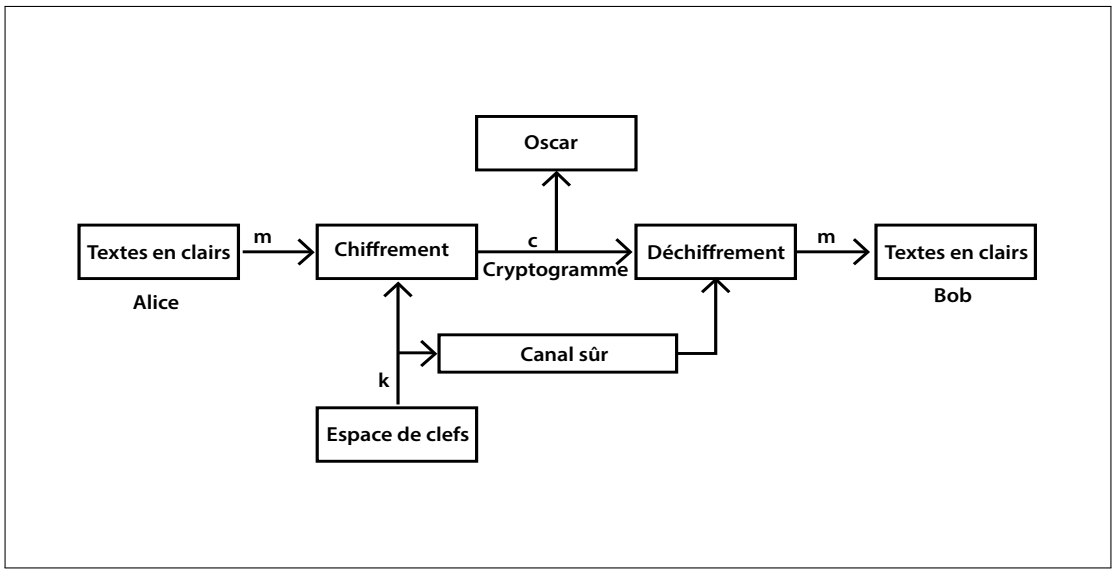

FIGURE 4.1: Schéma de communication entre Alice et Bob.

4.1.3 Principe d'Auguste Kerckhoffs (1883)

En 1883, Auguste Kerckhoffs (1835 - 1903) posa le principe de la cryptographie moderne « la cryptographie militaire » paru dans le « journal des sciences militaires » [66]. Dans cet article, il a énoncé six principes fondamentaux que doit respecter un système cryptographique pour assurer une communication confidentielle [6] :

1. Le système doit être matériellement, sinon mathématiquement indéchiffrable.
2. Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi.
3. La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants.
4. Il faut qu'il soit applicable à la correspondance télégraphique.
5. Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes.
6. Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.

Aujourd'hui, les deux premiers principes sont toujours en vigueur. Pour le troisième, tous les systèmes modernes fonctionnent avec des clés plus ou moins longues (de 64 à 2048 bits suivant le type de code et la sécurité demandée) et sont donc assez faciles à transmettre secrètement. Pour le quatrième principe, il suffit de remplacer télégraphique par communications électroniques. Les deux derniers principes n'ont plus d'intérêt, car n'importe quel ordinateur peut chiffrer ou déchiffrer un message. Ce qui est appelé aujourd'hui « principe de Kerckhoffs » est essentiellement le second principe qui exprime que la sécurité d'un cryptosystème ne doit reposer que sur le secret de la clé. Autrement dit, tous les autres paramètres doivent être supposés publiquement connus et plus précisément :

- La sécurité repose sur le secret de la clef et non sur le secret de l'algorithme.
- Le déchiffrement sans la clef doit être impossible (en un temps raisonnable).
- Trouver la clef à partir du clair et du chiffré est impossible (en un temps raisonnable).

4.1.4 Objectifs de la cryptographie

La cryptographie moderne a pour objectif de garantir un certain nombre de services liés aux sécurités de communications (voir [135, p. 9]) :

1. **Confidentialité :** a pour but d'assurer qu'un message clair soit transformé en un message chiffré, de manière à ce que l'expéditeur et le destinataire sont les seuls qui puissent lire le message en clair.
2. **Authentification :** identifier l'expéditeur du message de façon efficace. Le destinataire d'un message doit pouvoir s'assurer de son origine. Un intrus ne doit pas être capable de se faire passer pour quelqu'un d'autre.

6. `https://fr.wikipedia.org/wiki/Principe_de_Kerckhoffs`

3. **Intégrité :** le destinataire doit être sûr que le message envoyé par l'expéditeur n'a pas été modifié durant la transmission. Un intrus doit être incapable de faire passer un faux message pour une légitime.
4. **Non-répudiation ou protocole de signature :** se décompose des trois sous-protocoles suivants :
   (a) **Non-répudiation d'origine :** l'expéditeur ne peut nier avoir écrit le message et il peut prouver qu'il ne l'a pas fait, si c'est effectivement le cas.
   (b) **Non-répudiation de réception :** le destinataire ne peut nier avoir reçu le message et il peut prouver qu'il ne l'a pas reçu, si c'est effectivement le cas.
   (c) **Non-répudiation de transmission :** l'émetteur du message ne peut nier avoir envoyé le message et il peut prouver qu'il ne l'a pas fait, si c'est effectivement le cas.

Pour un exemple illustrant ces services, supposons qu'Alice veut envoyer un message à Bob, alors :

1. Alice veut être certaine que :
   (a) **Confidentialité :** aucune personne non autorisée ne peut prendre connaissance des messages qu'elle envoie.
   (b) **Intégrité :** son message ne sera pas falsifié par un attaquant malveillant.
   (c) **Non-répudiation :** Bob a bien pris connaissance de son message et ne pourra pas nier l'avoir reçu.
2. Bob veut être certain que :
   (a) **Confidentialité :** aucune personne autre que lui n'a accès au contenu du message.
   (b) **Authentification :** le message reçu vient bien d'Alice.
   (c) **Intégrité :** le message n'a pas été falsifié par un attaquant malveillant.
   (d) **Non-répudiation :** Alice ne pourra pas nier avoir envoyé le message.

4.1.5 Cryptanalyse

La cryptanalyse [35, 78] est la science de la reconstitution du texte en clair sans connaître la clef de déchiffrement. Le but de la cryptanalyse est d'étudier les systèmes cryptographiques suivant le principe de Kerckhoffs, afin de mettre en évidence les faiblesses d'un cryptosystème qui peuvent éventuellement faciliter les attaques contre celui-ci. Une cryptanalyse réussie peut fournir soit le texte en clair, soit la clef de déchiffrement.

En cryptanalyse, il y a quatre types génériques d'attaques cryptanalytiques qui reposent sur l'hypothèse où le cryptanalyste (qui pratique la cryptanalyse) dispose de la connaissance complète de l'algorithme de chiffrement. Ces attaques sont énumérées ci-dessous (voir [112, pp. 5–6]&[129, p. 22]) :

1. **Attaque à texte chiffré seulement :** le cryptanalyste dispose du texte chiffré de plusieurs messages chiffrés par le même algorithme et il doit retrouver le texte en clair de plus grands nombres de messages possibles ou mieux encore de trouver les clefs qui ont

été utilisées pour chiffrer les messages ; ce qui permettrait de déchiffrer d'autres messages chiffrés avec ces mêmes clefs.

2. **Attaque à texte en clair connu :** le cryptanalyste a non seulement accès aux textes chiffrés de plusieurs messages, mais aussi aux textes en clairs correspondants. La tâche de cryptanalyste est de retrouver la (ou les) clef(s) utilisée(s) pour chiffrer ces messages ou un algorithme qui permet de déchiffrer n'importe quel nouveau message chiffré avec la même clef.
3. **Attaque à texte en clair choisi :** le cryptanalyste a non seulement accès aux textes chiffrés et aux textes en clair, mais de plus, il peut choisir les textes en clair à chiffrer. Cette attaque est plus efficace que l'attaque à texte en clair connu, car le cryptanalyste peut choisir des textes en clair qui donneront plus d'informations sur la clef. La tâche consiste à retrouver les clefs utilisées pour chiffrer ces messages ou un algorithme qui permet de déchiffrer n'importe quel nouveau message chiffré avec la même clef.
4. **Attaque à texte en clair choisi adaptative :** c'est un cas particulier de l'attaque à texte en clair choisi où le cryptanalyste peut adapter ses choix en fonction des textes chiffrés précédents.

La complexité d'une attaque est mesurée de l'une des manières suivantes [112, pp. 8–9] :

1. **Complexité en information :** la quantité d'informations nécessaires en entrée pour l'algorithme.
2. **Complexité en temps :** le temps nécessaire pour achever l'attaque.
3. **Complexité en espace :** la quantité de mémoire nécessaire à l'attaque.

Comme règle de base, la complexité d'une attaque est prise comme le minimum de ces trois facteurs.

4.1.6 Sécurité des cryptosystèmes

Les différents algorithmes cryptographiques ont des niveaux de sécurité divers, plus ou moins difficile à casser. Lars Knudsen a classé les différentes manières de casser un algorithme en ordre décroissant de sévérité (voir [67, pp. 44–45]) :

1. **Cassage complet :** un cryptanalyste trouve la clef k telle que pour tout message en clair m, on a $\mathrm{Dec_k}(c_m) = m$, où c_m est le chiffré de m.
2. **Obtention globale :** un cryptanalyste trouve un algorithme de remplacement $\mathcal{A}$ équivalant à $\mathrm{Dec_k}(\mathcal{C})$ sans connaitre k.
3. **Obtention locale :** un cryptanalyste trouve le texte en clair d'un message chiffré qu'il a intercepté.
4. **Obtention d'information :** un cryptanalyste glane quelques informations à propos du texte en clair ou de la clef.

La cryptographie se préoccupe des cryptosystèmes invulnérables par calcul. Un cryptosystème est considéré invulnérable par calcul s'il ne peut pas être cassé avec les ressources disponibles actuellement et dans le futur.

4.1.7 Signature numérique

La signature numérique (analogue électronique d'une signature manuscrite) est un mécanisme qui permet de garantir l'intégrité d'un document électronique et d'en authentifier l'auteur. Elle permet au destinataire d'identifier l'expéditeur du document. En plus, elle garantit le document d'être altéré entre l'émetteur et le récepteur. Une signature numérique doit donc être [113] :

1. **Authentique :** l'identité du signataire doit pouvoir être retrouvée de manière certaine. La signature convainc le destinataire que le signataire a délibérément signé le document.
2. **Infalsifiable :** la signature ne peut pas être falsifiée. La signature est la preuve que le signataire a délibérément signé le document (quelqu'un ne peut se faire passer pour un autre.).
3. **Non réutilisable :** la signature fait partie du document signé. Une personne malintentionnée ne peut déplacer la signature sur un autre document.
4. **Inaltérable :** une fois le document signé, il ne peut plus être modifié.
5. **Irrévocable :** toute personne signataire ne peut nier sa signature.

Comme exemples de signatures numériques, on cite la signature numérique d'ElGamal [40], la signature numérique RSA [111] et la signature numérique DSS donnée par NIST et décrite d'une manière détaillée dans [108]. Une modification de la signature d'ElGamal est donnée par Claus-Peter Schnorr dans [113].

4.2 Algorithmes cryptographiques

Les algorithmes restreints sont très populaires pour les applications à bas niveau de sécurité où les utilisateurs ne se soucient pas des problèmes de sécurité inhérents à leur système, et donc ces algorithmes ne présentent plus qu'un intérêt historique, car de nos jours, ils sont inadéquats pour les besoins actuels de sécurité.

Pour résoudre le problème de sécurité dans les algorithmes restreints, les opérations de chiffrement et de déchiffrement dans la cryptographie moderne se font à l'aide d'une clef k et sont notées respectivement $\mathrm{Enc_k}$ et $\mathrm{Dec_k}$. De plus, pour tout message en clair m, les opérations $\mathrm{Enc_k}$ et $\mathrm{Dec_k}$ doivent vérifier les égalités suivantes : $\mathrm{Enc_k}(m) = c$; $\mathrm{Dec_k}(c) = m$ et $\mathrm{Dec_k}(\mathrm{Enc_k}(m)) = m$.

Avec ces données, la définition formelle d'un cryptosystème est la suivante (voir [130, Définition 2.1, p. 15]) :

Définition 4.2.1 *Un cryptosystème est un quintuplet* $(\mathcal{M}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, *où :*

1. $\mathcal{M}$ *est un ensemble fini dit « espace de textes en clairs » ;*
2. $\mathcal{C}$ *est un ensemble fini dit « espace de textes chiffrés » ;*
3. $\mathcal{K}$ *est un ensemble fini dit « espace de clefs » ;*
4. $\mathcal{E}$ *est l'ensemble des opérations de chiffrement de* $\mathcal{M}$ *dans* $\mathcal{C}$ *;*
5. $\mathcal{D}$ *est l'ensemble des opérations de déchiffrement de* $\mathcal{C}$ *dans* $\mathcal{M}$ *;*

qui satisfaisant, pour tout $k \in \mathcal{K}$, il existe une fonction de chiffrement $\mathrm{Enc_k} \in \mathcal{E}$ *et une fonction de déchiffrement* $\mathrm{Dec_k} \in \mathcal{D}$ *telles que* $\mathrm{Dec_k}(\mathrm{Enc_k}(m)) = m$ *pour tout message en clair* $m \in \mathcal{M}$.

La figure suivante, illustre le schéma d'un cryptosystème :

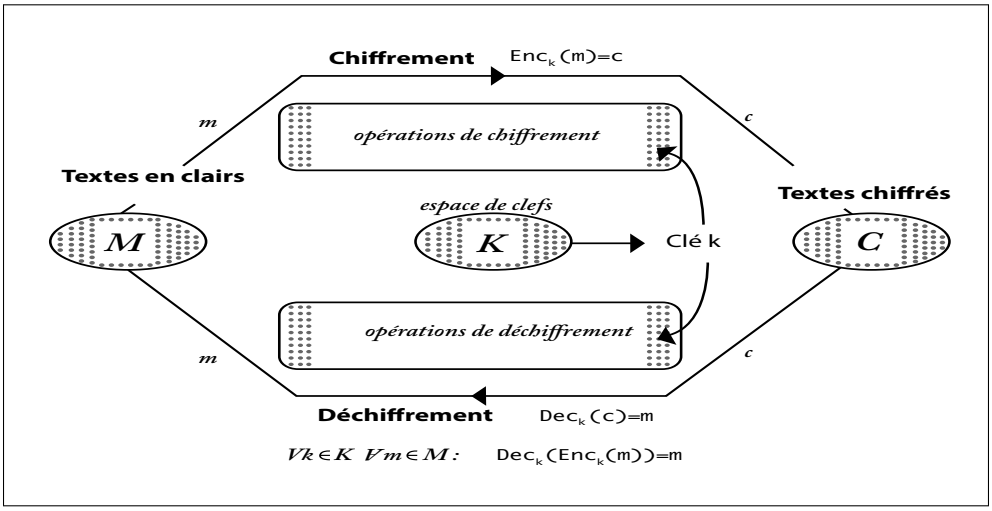

FIGURE 4.2: Schéma d'un cryptosystème.

Certains cryptosystèmes utilisent des clefs différentes ; une clef k_1 est utilisée pour le chiffrement et une clef k_2 est utilisée pour le déchiffrement. Un tel cryptosystème doit vérifier $\mathrm{Enc_{k_1}}(m) = c$; $\mathrm{Dec_{k_2}}(c) = m$ et $\mathrm{Dec_{k_2}}(\mathrm{Enc_{k_1}}(m)) = m$ pour tout $m \in \mathcal{M}$.

Avec ces algorithmes, toute la sécurité réside dans la (ou les) clef(s) et non dans les détails de l'algorithme et donc ces algorithmes peuvent être connus des attaquants sans mettre en danger la sécurité du système. Les algorithmes à base de clefs sont de deux types principaux : *algorithmes à clef secrète* et *algorithmes à clef publique.*

4.2.1 Algorithmes symétriques

Les *algorithmes symétriques (ou à clef secrète)* sont des algorithmes où la clef de chiffrement peut être calculée à partir de la clef de déchiffrement ou vice-versa. Dans la plupart des cas, la clef de chiffrement et la clef de déchiffrement sont identiques. Le chiffrement et le déchiffrement dans un cryptosystème à clef secrète se déroulent comme suit (voir [112, p. 28]) :

1. Alice et Bob choisissent un algorithme cryptographique ;
2. Alice et Bob se mettent d'accord sur une clef ;
3. Alice chiffre son texte en clair à l'aide de l'algorithme choisi et avec la clef secrète sélectionnée ;
4. Alice envoie le texte chiffré à Bob ;
5. Bob déchiffre le texte chiffré avec le même algorithme et la même clef secrète.

Les opérations de chiffrement et de déchiffrement dans ces algorithmes vérifient $\mathrm{Enc_k}(m) = c$ et $\mathrm{Dec_k}(c) = m$ pour tous $k \in \mathcal{K}$ et $m \in \mathcal{M}$.

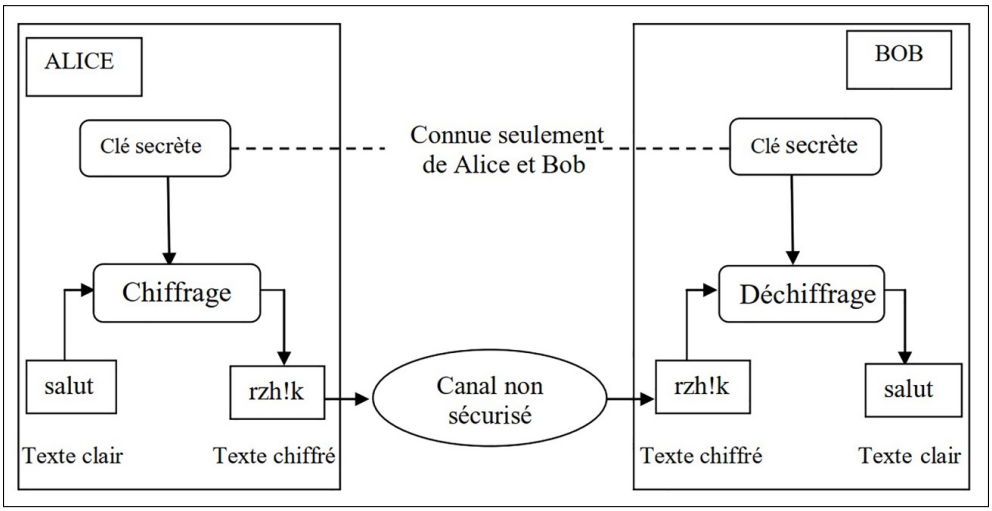

FIGURE 4.3: Chiffrement et déchiffrement symétrique.

La sécurité de ce cryptosystème est basée sur deux secrets, à savoir : l'algorithme utilisé et la clef choisie. Si un espion peut mettre la main sur les deux premières étapes, il aura ce qu'il lui faut. Un bon cryptosystème est un système où la sécurité est inhérente à la connaissance de la clef et non pas à celle de l'algorithme. C'est pourquoi, la gestion des clefs est un problème assez important en cryptographie. Avec un algorithme à clef secrète, Alice et Bob peuvent faire la première étape en public, mais ils doivent réaliser la deuxième discrètement. Autrement dit, la clef choisie entre Alice et Bob doit rester toujours secrète avant (pendant et après) l'échange des données. Les algorithmes symétriques peuvent être classés en deux types [64, 83, 115] :

- **Algorithmes de chiffrement en continu :** l'opération de chiffrement opère sur le texte en clair bit par bit. Par exemple, l'algorithme RC4 [109], conçu par Ronald Rivest, et qui est utilisé notamment par le protocole WEP (Wired Equivalent Privacy) du Wi-Fi (Wireless Fidelity).
- **Algorithmes de chiffrement par blocs :** l'opération de chiffrement opère sur le texte en clair par groupes de bits, qu'on appelle *blocs*. Par exemple, l'algorithme DES [7] chiffre un bloc de textes en clair de 64 bits en utilisant une clef de 56 bits, pour obtenir un bloc de textes chiffré de 64 bits.

Les algorithmes symétriques sont rapides et adaptés à la transmission de grandes quantités de données, mais ils présentent les inconvénients ci-dessous, qui les rendent inappropriés dans de nombreuses applications (voir [82, pp. 2–3]&[112, p. 29]) :

- **La distribution de clefs :** la sécurité des algorithmes symétriques repose sur la clef elle-même et donc, si celle-ci est compromise (volée, devinée, achetée, etc.), alors tout adversaire peut chiffrer ou déchiffrer des messages dans ce cryptosystème. L'expéditeur et le destinataire sont obligés de se mettre d'accord sur la même clef qui doit être gardée secrète avant tout échange de données.
- **La gestion de clefs :** dans un réseau de n utilisateurs, chaque paire d'utilisateurs doivent partager une clef secrète, pour un total de $n(n-1)/2$ clefs. Si n est grand, le nombre de clefs devient alors ingérable.

7. Pour les attaques sur ce cryptosystème, on peut se référer à [116].

- **Absence de signature numérique :** dans un cryptosystème à clef secrète, Alice et Bob ont les mêmes capacités de cryptage et de décryptage, et donc Bob ne peut pas convaincre Oscar que le message qu'il a reçu d'Alice en fait provient d'Alice.

Pour combler ces trois lacunes dans la cryptographie à clef secrète, W. Diffie et M. Hellman ont inventé les algorithmes à clef publique.

4.2.2 Algorithmes asymétriques

Les *algorithmes asymétriques (ou à clef publique)* [93] sont inventés en 1976 par Whitfield Diffie et Martin Hellman [33] pour résoudre les lacunes précédentes des algorithmes symétriques et notamment le problème du partage des clefs et le besoin de les changer avant toute transmission de données. Les algorithmes à clef publique sont conçus de telle manière que la clef de chiffrement (dite « clef publique ») soit différente de la clef de déchiffrement (dite « clef privée » ou « clef secrète »). Les algorithmes asymétriques sont dits à clef publique parce que la clef de chiffrement est rendue publique (n'importe qui, peut utiliser la clef de chiffrement pour chiffrer un message), alors que la clef de déchiffrement demeure secrète (seul celui qui possède la clef de déchiffrement peut déchiffrer le message résultant.).

Dans les cryptosystèmes asymétriques, l'expéditeur et le destinataire n'ont plus besoin de partager des clefs secrètes via une voie de transmission sécurisée, ce qui permet d'échanger des messages de manière sécurisée sans aucun dispositif de sécurité. Le chiffrement et le déchiffrement dans cette cryptographie se font de la manière suivante (voir [112, pp. 31–32]) :

1. Alice et Bob choisissent un cryptosystème à clef publique ;
2. Bob envoie sa clef publique à Alice ;
3. Alice chiffre son texte en clair à l'aide de la clef publique de Bob ;
4. Alice envoie le texte chiffré à Bob ;
5. Bob déchiffre le texte chiffré d'Alice avec sa clef privée.

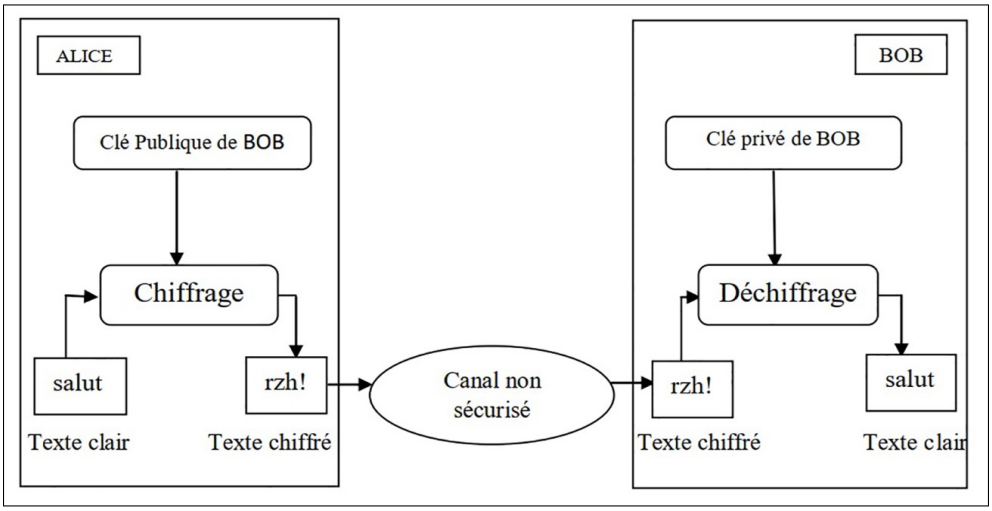

FIGURE 4.4: Chiffrement et déchiffrement asymétrique.

La sécurité des algorithmes asymétriques repose sur des problèmes mathématiques considérés calculatoirement difficiles à résoudre dans un temps raisonnable. Les plus populaires de ces algorithmes sont :

1. L'algorithme de Diffie-Hellman [33], qui a donné naissance à la cryptographie à clef publique. La sécurité de cet algorithme repose sur la difficulté de résoudre le problème du logarithme discret [139, Chap. 5].
2. L'algorithme RSA inventé en 1977 par Ronald Rivest, Adi Shamir et Leonard Adleman [111]. RSA est la première réalisation pratique d'un cryptosystème à clef publique. La sécurité de ce cryptosystème repose sur la difficulté de factoriser des grands entiers en nombres premiers.
3. L'algorithme d'ElGamal basé sur le problème du logarithme discret de son inventeur egyptien Taher Elgamal [40]. Le cryptosystème ElGamal est adapté pour le chiffrement et la signature numérique.
4. Les algorithmes basés sur les courbes elliptiques ECC (Elliptic Curve Cryptography), où la sécurité repose sur le problème du logarithme discret dans le groupe des points d'une courbe elliptique définie sur un corps fini. L'utilisation de courbes elliptiques en cryptographie a été suggérée indépendamment par Neal Koblitz [69] et Victor S. Miller [87] en 1985.
5. L'algorithme de signature numérique DSA (Digital Signature Algorithm)[72], élaboré par David Kravitz en 1993 et adapté seulement pour la signature numérique.

4.3 Protocoles d'échange de clefs

L'échange de la clef privée entre Bob et Alice dans la cryptographie asymétrique se fait via un canal public à l'aide des protocoles d'échange de clefs qui sont généralement difficiles à casser (aucun espion ne peut s'informer de la clef privée échangée.). La sécurité de nombreux protocoles actuels repose sur des problèmes mathématiques qui sont difficiles à résoudre tels que le problème du logarithme discret (voir [79, 135] &[139, Chap. 5]) et le problème de factorisation des entiers en produit de nombres premiers [96].

4.3.1 Problème du logarithme discret

La cryptographie à clef publique est basée sur une notion fondamentale dite « fonctions à sens unique » où une fonction f est dite à sens unique, si f est facile à calculer, mais plus difficile à inverser. Autrement dit, f est à sens unique, si pour toute valeur x il est facile de calculer $f(x)$ en un temps polynomial en x, mais en connaissant $f(x)$ il est très difficile de trouver x.

En cryptographie un message chiffré par une fonction à sens unique, personne ne peut le déchiffrer, ce qui signifie que les fonctions à sens unique n'ont pas d'une grande utilité. Pour qu'on puisse utiliser des fonctions à sens unique en cryptographie à clef publique, on lui ajoute une information supplémentaire qui nous permet facilement de trouver x si on connaît $f(x)$. Ce type de fonctions s'appelle *fonctions à sens unique avec trappe*. Avec une fonction à sens unique

avec trappe, le chiffrement est le sens facile de la fonction et se fait à l'aide de la clef publique (tout le monde peut chiffrer un message.) et le déchiffrement est le sens difficile de la fonction où personne ne peut déchiffrer le message sans connaître la trappe qui n'est autre que la clef privée.

D'un point de vue mathématique, il n'y a pas de preuves que des fonctions à sens unique existent [15, 42]. Cependant, il existe plusieurs fonctions que nous pouvons facilement calculer, mais à ce jour nous ne connaissons pas de moyen simple pour les inverser.

Exemple 4.3.1 *Soit p un nombre premier et soit $x \in \mathbb{F}_p$ où $\mathbb{F}_p$ est le corps fini de p éléments. L'exponentiation modulaire en base x dans $\mathbb{F}_p$ est la fonction $f : \mathbb{Z} \longrightarrow (\mathbb{F}_p)^*$ définie par $f(n) = x^n \mod p$. Étant donné n, il est facile de calculer $f(n)$, mais étant donné un élément $y \in \mathbb{F}_p$, il est très difficile de trouver l'entier n tel que $y = x^n$ et surtout lorsque p est assez grand. En effet, tous les algorithmes connus pour inverser cette fonction, nécessitent un temps de calcul non-polynomial en* $\log(p)$ *; alors f est une fonction à sens unique. Le plus petit entier positif n qui vérifie $y = x^n$ s'appelle* le logarithme discret *en base x de y et se note* $\log_x(y)$.

Définition 4.3.1 *Soit G un groupe multiplicatif fini d'ordre n et soit g un générateur de G. Pour tout élément $a \in G$, le logarithme discret en base g de a est l'unique entier $0 \leqslant m < n$ tel que $g^m = a$. On note $m = \log_g(a)$.*

Exemple 4.3.2 *Dans le groupe multiplicatif du corps fini $\mathbb{F}_{97}$, on a $5^{32} \equiv 35 \mod 97$, et donc $\log_5(35) = 32$ dans G.*

L'algorithme évident de calcul des puissances successives de g jusqu'à trouver m est de complexité $O(n)$ opérations dans G, et donc cet algorithme est inefficace si n est grand. *Le problème du logarithme discret* (PLD) dans un groupe G est de trouver un algorithme de calcul efficace pour le logarithme discret dans G. Le PLD est un problème généralement difficile à résoudre en dépendance du groupe choisi [81, 94, 100]. Malheureusement, nous n'avons aucune preuve formelle que le problème du logarithme discret sur un ordinateur classique est difficile [127, Chap. 3.2.1]. De plus, Peter Shor [119] a montré que si l'on pouvait construire un ordinateur quantique suffisamment compliqué, il pourrait résoudre le problème du logarithme discret dans un temps limité par une fonction polynomiale du nombre de chiffres égale au nombre d'éléments de G.

Le problème du logarithme discret a reçu beaucoup d'attention ces dernières années et de nombreuses techniques ont été conçues :

- Algorithmes qui fonctionnent en groupes arbitraires (méthode racine carrée) [102].
- Algorithmes qui fonctionnent en groupes arbitraires, mais exploitent la structure du sous-groupe (méthode Pohlig-Hellman) [101].
- Méthodes de calcul d'indice [25, 27, 50, 77, 80, 87, 103].
- Méthodes qui exploitent les isomorphismes entre les groupes [85].

Le problème du logarithme discret permet de construire des cryptosystèmes d'un grand intérêt pour la cryptographie à clef publique et cela provient du fait que le calcul des logarithmes

discrets est difficile, tandis que calculer l'opération inverse de l'exponentiation modulaire peut se faire facilement.

4.3.2 Protocole de Diffie-Hellman

En 1976, W. Diffie et M. Hellman [33] dans leur document fondateur « New directions in cryptography » sur la cryptographie à clef publique ont décrit pour première fois un algorithme pour le problème de distribution des clés de la cryptographie symétrique. Nous décrivons ce protocole, connu sous le nom de *protocole de Diffie-Hellman*, en terme d'un groupe arbitraire G de la façon suivante (voir [82, p. 3]) :

1. Alice et Bob se mettent d'accord sur un générateur g d'un groupe multiplicatif fini G (peut-être un corps fini ou le groupe de points d'une courbe elliptique) ;
2. Alice choisit un entier a et calcule g^a, puis l'envoie à Bob ;
3. Bob choisit un entier b et calcule g^b, puis l'envoie à Alice ;
4. Alice calcule $\left(g^b\right)^a$;
5. Bob calcule $(g^a)^b$.

La clé privée entre Alice et Bob est $K = g^{ab} = g^{ba}$ et les autres clefs G, g, g^a et g^b sont publiques.

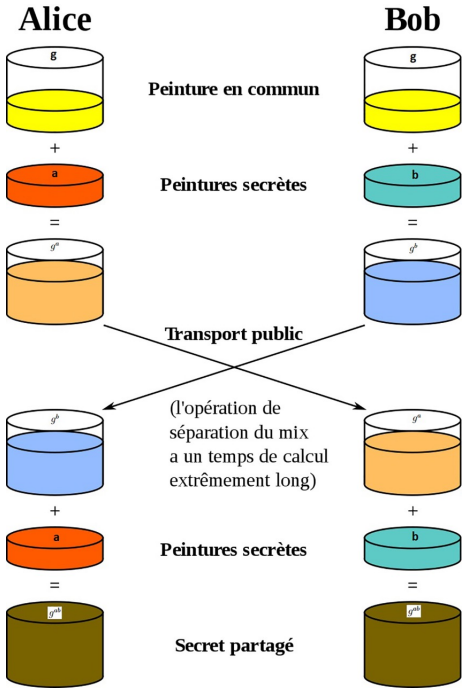

FIGURE 4.5: Echange de clés Diffie-Hellman.

La difficulté de ce protocole dépend de la difficulté de calculer des logarithmes discrets dans le groupe G (le calcul de a et b) par rapport à la facilité de calcul d'exponentiation modulaire dans le même groupe (le calcul de g^a et g^b). Le problème de la reconstitution de g^{ab} à partir des clefs publiques uniquement est couramment appelé le *problème de Diffie-Hellman*.

Jusqu'à présent, on ne sait pas en général, si le problème de Diffie-Hellman est équivalent au problème du logarithme discret. En effet, le sens trivial de cette équivalence est que la résolution du problème du logarithme discret dans G, implique facilement la résolution du problème de Diffie-Hellman, alors que la réciproque n'est pas encore démontré sauf dans un cas spécial du groupe G où le résultat a été montré par B. Den Boer en 1990 [32]. Par ailleurs, il existe des groupes où le problème de Diffi-Hellman est facile, mais où on n'a pas d'algorithmes efficaces pour résoudre le problème du logarithme discret [58]. L'équivalence entre le problème de Diffie-Hellman et le problème du logarithme discret est largement admis et supposé être le cas et pour cette raison nous disons que la sécurité de Diffie-Hellman est basée sur la difficulté du DLP.

Pour le cas du groupe de points d'une courbe elliptique définie sur un corps fini, le problème du logarithme discret est exponentiel ; alors qu'il est sous exponentiel sur les corps finis et donc un espion ne peut pas calculer g^{ab} dans un temps raisonnable. En pratique, pour que le protocole de Diffie-Hellman ne soit pas cassé par les meilleurs algorithmes de résolution du logarithme discret, il faut que le groupe de départ soit bien choisi et que les nombres utilisés soient suffisamment grands [8] pour éviter une attaque par recherche exhaustive.

4.3.3 Cryptosystème d'ElGamal

Le cryptosystème d'ElGamal est un protocole asymétrique inventé par Taher ElGamal en 1985 [9] [40] pour le chiffrement et la signature numérique. La sécurité de ce protocole est basée sur le problème du logarithme discret et le problème de Diffie-Hellman [83, Chap. 8, Note 8.23]. Le cryptosystème d'ElGamal pour le chiffrement se compose de trois algorithmes et se décrit en terme d'un groupe fini G de la façon suivante (voir [82, p. 8]) :

- **Génération de clefs :** cette étape est réalisée par Bob (le destinataire) et provoque la création de deux clefs : la clef publique et la clef privée.
  1. Il choisit un groupe fini G d'ordre n et un générateur g de G ;
  2. Il choisit un entier a entre 1 et $n-1$ (clef secrète de Bob) ;
  3. Il calcule $A = g^a$ dans G.

  Bob pourra alors publier sa clef publique (G, g, n, A) et garder secrète sa clef privée a.
- **Chiffrement d'un message :** si Alice veut écrire à Bob un message m encodé comme un élément du groupe G, il le chiffre de la façon suivante :
  1. Il récupère la clef publique (G, g, n, A) de Bob ;
  2. Il choisit au hasard un entier k entre 1 et $n-1$;
  3. Il calcule $y_1 = g^k$ et $y_2 = m.A^k$;
  4. Il envoie $c = (y_1, y_2)$ à Bob.
- **Déchiffrement d'un message :** pour que Bob puisse déchiffrer le message d'Alice c, il utilise sa clef privée a et calcul $y_2.y_1^{n-a}$ qui n'est rien d'autre que le message en clair d'Alice. En effet, on a :

$$y_2.y_1^{n-a} = m.A^k.\left(g^k\right)^{n-a} = m.g^{ak}.g^{kn}.g^{-ak} = m.g^{ak}.\left(g^n\right)^k.g^{-ak} = m.g^{ak}.g^{-ak} = m.$$

Pour une mise en œuvre sûre et efficace de ce cryptosystème, le groupe G et le générateur g de G devraient être choisis pour satisfaire les deux conditions suivantes :

- Pour l'efficacité, le groupe G doit être choisi de telle sorte que les opérations de calcul soient faciles à appliquer ;
- Pour la sécurité, le problème du logarithme discret dans le groupe G doit être difficile à résoudre.

8. Pour le cas des corps finis, la caractéristique du corps doit être de l'ordre de 300 chiffres et a et b doivent être de l'ordre de 100 chiffres.

9. A été présenté pour la première fois en 1984 dans le *Workshop on the Theory and Application of Cryptographic Techniques CRYPTO'84.*

En particulier, pour le cas des corps finis $\mathbb{F}_p$ [10] avec p un nombre premier, un choix de p de l'ordre de 1024 bits permet de résister aux méthodes de résolution de DLP sur $\mathbb{F}_p$ [83, Chap. 8, Note 8.24]. Plus tard, certains autres groupes ont été considérés, comme le groupe multiplicatif du corps fini $\mathbb{F}_{2^n}$, où n est un entier positif ; le groupe de points d'une courbe elliptique sur un corps fini [69, 87] ; le jacobien d'une courbe hyperelliptique définie sur un corps fini [70] ; le groupe de matrices non-singulières sur un corps fini [95] ; le groupe de classes d'un corps quadratique imaginaire [17] et le groupe de points des courbes elliptiques définies sur certains anneaux finis [20, 22, 134, 137, 138].

4.3.4 Chiffrement RSA

L'algorithme RSA a été inventé en 1977 par Ronald Rivest, Adi Shamir et Leonard Adleman [111] et fut la première réalisation pratique d'un algorithme asymétrique basé sur l'échange de clefs de Diffie-Hellman. Le cryptosystème RSA est conçu pour le chiffrement et la signature numérique. Le chiffrement RSA est composé des trois algorithmes suivants [127, pp. 56–57] :

- **Génération de clefs :** cette étape est réalisée par le destinataire (Bob) et provoque la création de deux clefs : la clef publique qui sert à chiffrer le message en clair et la clef privée qui sert à le déchiffrer selon l'algorithme suivant :
  1. Il choisit deux grands nombres premiers distincts p et q ;
  2. Il calcule leur produit $n = pq$;
  3. Il calcule l'indicateur d'Euler [11] $\varphi(n) := (p-1)(q-1) = n + 1 - p - q$;
  4. Il choisit un entier naturel e premier avec n ;
  5. Il calcule l'entier $d \leqslant \varphi(n)$ tel que $d \equiv e^{-1} \mod \varphi(n)$.

  La clé publique est le couple (n, e) et la clé privée est le couple (n, d). Le destinataire pourra alors publier sa clef publique et garder secrets p, q et d.
- **Chiffrement d'un message :** si Alice veut écrire un message à Bob, il crypte son message grâce à la clef publique de Bob (n, e) par l'algorithme suivant :
  1. Il récupère la clé publique de Bob (n, e) ;
  2. Il encode son message comme un entier m entre 0 et $n - 1$;
  3. Il calcule $c \equiv m^e \mod n$, puis il l'envoie à Bob.
- **Déchiffrement d'un message :** pour que Bob puisse déchiffrer le message c d'Alice, il doit utiliser sa clef privée (n, d) pour calculer $c^d \mod n$ et il retrouve bien le message en clair d'Alice. En effet, il existe $k \in \mathbb{Z}$ tel que $ed = 1 + k\varphi(n)$, d'où :

$$c^d \equiv m^{ed} \mod n \equiv m.\left(m^{\varphi(n)}\right)^k \mod n \equiv m \mod n.$$

Pour chiffrer un message m, il est nécessaire de le découper en blocs numériques tels que chaque bloc ait une taille [12] unique modulo n (voir[83, p. 287]).

10. Taher ElGamal a décrit son cryptosystème en utilisant le groupe multiplicatif du corps fini $\mathbb{F}_p$.
11. $\varphi(n)$ est l'ordre du groupe des éléments inversibles de l'anneau $(\mathbb{Z}/pq\mathbb{Z})$.
12. Avec des données binaires, on choisit la plus grande puissance de 2 inférieure à n.

L'exemple suivant illustre le chiffrement RSA avec de petits nombres premiers :

Exemple 4.3.3 *Prenons* $p = 47$ *et* $q = 59$. *Alors :*

- $n = 2773$.
- $\varphi(n) = 2668$.
- *On choisit* $e = 17$.
- $d \equiv \frac{1}{17} \mod 2668 = 157$.
- *La clef publique est* $(17, 2773)$ *et la clef privée est* $d = 157$.
- *Soit à chiffrer l'entier* $m = 66$. *Alors* $c \equiv 66^{17} \mod 2773 = 872$.
- *Le déchiffré de* c *est* $m \equiv 872^{157} \mod 2773 = 66$.

Le chiffrement RSA a résisté depuis à des années de cryptanalyse intensive. Bien que la cryptanalyse n'ait jamais prouvé la sécurité ou la non-sécurité de RSA, si on peut trouver d à partir de e et n, on peut facilement casser RSA. Pour trouver d, il faut trouver l'inverse modulaire de e modulo $(p-1)(q-1)$, ce que l'on ne sait pas faire sans connaître les entiers p et q, c'est-à-dire la décomposition de n en facteurs premiers. La sécurité de RSA dépend donc de la factorisation d'un entier en produit de deux nombres premiers.

Les spécialistes dans ce domaine croient (absence d'une preuve connue pour ceci) que casser le système RSA équivaut à factoriser n, où beaucoup de progrès ont été réalisés dans la conception d'algorithmes efficaces pour la factorisation des entiers [74, 76, 75, 105]. Mathématiquement, il n'a jamais été prouvé que vous devez factoriser n pour calculer m à partir de c et e. Il est concevable qu'un tout autre moyen de cryptanalyse de RSA soit découvert.

4.4 Cryptographie sur les courbes elliptiques

La cryptographie asymétrique basée sur les courbes elliptiques définies sur les corps finis a été suggérée pour la première fois en 1985, de manière indépendante, par Neal Koblitz [69] et Victor S Miller [87]. L'idée dans cette cryptographie est que l'ensemble des points rationnels d'une courbe elliptique forment un groupe abélien pour l'addition [13] des points, ce qui permet de donner des modifications d'autres systèmes de chiffrement asymétriques existants (ElGamal par exemple) sur ce groupe, plutôt qu'un corps fini. En outre, le problème du logarithme discret dans ce groupe est considéré comme très difficile [14] par rapport à celui d'un corps finis de même ordre que ce groupe.

L'utilisation des courbes elliptiques en cryptographie permet d'améliorer la sécurité des cryptosystèmes, où ils peuvent fournir un niveau de sécurité équivalent avec des longueurs de clefs plus courtes que les autres systèmes existants [24], ce qui est un facteur important dans la réalisation de certaines applications comme la conception de systèmes de cartes à puce [52], où la mémoire et la puissance de traitement sont limitées. Le tableau suivant montre la performance en longueur de clefs, de la cryptographie sur les courbes elliptiques par rapport à RSA pour un

13. Revient à quelques opérations arithmétiques dans le corps considéré.
14. Il n'y a pas d'attaque connue de complexité sous exponentielle.

même niveau de sécurité [15] :

	Taille des clés en bits				
ECC	160	224	256	384	512
RSA	1024	2048	3072	7680	15360

TABLE 4.1: Longueur de clefs entre ECC et RSA.

Un autre avantage à tirer de l'utilisation des courbes elliptiques est que chaque utilisateur peut sélectionner une courbe $E(K)$ différente, même si tous les utilisateurs utilisent le même corps fini K. Par conséquent, tous les utilisateurs ont besoin du même matériel pour effectuer l'arithmétique du corps, alors que la courbe E peut être modifiée périodiquement pour une sécurité supplémentaire.

Pour la cryptographie sur les courbes elliptiques, on utilise la version additive du logarithme discret, définie par :

Définition 4.4.1 *Soit G un groupe additif fini d'ordre n et soit g un générateur de G. Pour tout élément $a \in G$, le logarithme discret en base g de a est l'unique entier $0 \leqslant m < n$ tel que $mg = a$.*

Dans cette section, nous allons présenter pour la cryptographie sur les courbes elliptiques, un analogue de Diffie-Hellman pour le partage de clefs et d'ElGamal pour le chiffrement. Dans la suite, on désigne par $E(\mathbb{F}_q)$, le groupe des points $\mathbb{F}_q$-rationnels d'une courbe elliptique E définie sur le corps fini $\mathbb{F}_q$, où q est une puissance d'un nombre premier p.

4.4.1 Échange de clefs Diffie-Hellman

L'échange de clés Diffie-Hellman pour le groupe de points d'une courbe elliptique, se décrit de la façon suivante (voir [139, pp. 170–171]) :

1. Alice et Bob se mettent d'accord sur un nombre premier p, une courbe elliptique E sur $\mathbb{F}_q$ et sur un point P du groupe $E(\mathbb{F}_q)$;
2. Alice choisit un entier a et calcul aP, puis l'envoie à Bob ;
3. Bob choisit un entier b et calcul bP, puis l'envoie à Alice ;
4. Alice calcule $a(bP)$;
5. Bob calcule $b(aP)$.

La clé privée entre Alice et Bob est $K = abP$.

Sans doute, un adversaire ne peut pas trouver K sans résoudre le problème du logarithme discret. Pour E, P et p bien choisis, l'expérience suggère que le problème du logarithme discret dans $E(\mathbb{F}_q)$ est beaucoup plus difficile que le problème du logarithme discret dans $\mathbb{F}_q$ (voir [127, p. 138]).

15. `https://www.keylength.com/fr/`

4.4.2 Cryptosystème d'ElGamal

Le cryptosystème d'ElGamal pour le chiffrement et déchiffrement sur une courbe elliptique, se décrit par les trois algorithmes suivants (voir [139, pp. 174–175]) :

- **Génération de clefs :**
  1. Bob Choisit une courbe elliptique E et un point P de $E(\mathbb{F}_q)$;
  2. Bob Choisit un entier positif b et calcule bP.

  Bob publie q, E, P et bP et garde secret b.
- **Chiffrement d'un message :** si Alice veut écrire un message secret M à Bob, alors :
  1. Alice encode son message secret M en un point $m \in E$;
  2. Alice choisit au hasard un entier k et calcul kP, kbP et $m + kbP$;
  3. Alice envoie à Bob $c = (kP, m + kbP)$ et garde secret la clef k.
- **Déchiffrement d'un message :** pour que Bob puisse déchiffre le message c d'Alice, il doit utiliser sa clef secrète b pour calculer bkP et $-bkP$, puis il retrouve m par la formule $m = -bkP + (m + bkP)$.

4.5 Chiffrement entièrement homomorphe

Dans cette section, on va décrire deux systèmes de chiffrement entièrement homomorphe sur un anneau non commutatif. Le premier cryptosystème [9] est basé sur un anneau non commutatif de matrices carrées construit à partir de la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$, où $e^2 = e$; alors que le deuxième cryptosystème [13] est basé sur l'anneau $\mathbb{F}_q[e]$, où $e^3 = e^2$. La sécurité de ces cryptosystèmes repose sur le problème du logarithme discret pour les courbes elliptiques et le problème de recherche du conjugué dans un anneau non commutatif R, qui consiste à trouver $x \in R$ en connaissant seulement un élément y de la forme hxh^{-1}, où h est un élément inversible dans R. Le problème de recherche du conjugué est à la base de la sécurité d'un protocole d'échange de clés introduit en 2001 et souvent appelé protocole « AAFGl [2] ».

4.5.1 Introduction

Depuis la découverte de la cryptographie à clé publique par W. Diffie et M. Hellman dans l'année 1976 [33], la nécessité d'une confidentialité totale des données numériques est devenue de plus en plus forte, surtout depuis qu'Internet est devenu un élément indispensable de notre vie privée et professionnelle. Pour cela, la question d'une sécurisation maximale des systèmes de chiffrement s'est posée au cours des dernières décennies. Le chiffrement *homomorphe* et particulièrement *entièrement homomorphe* FHE (Fully Homomorphic Encryption), est une forme de chiffrement qui permet d'effectuer des calculs spécifiques sur des textes chiffrés et de générer un résultat chiffré qui, une fois déchiffré, correspond au résultat des opérations effectuées sur les textes en clairs.

La propriété d'homomorphe de divers cryptosystèmes peut être utilisée pour créer des systèmes de vote électronique sécurisés, des systèmes privés de recherche d'informations sur des

données chiffrées [16] et permettre une utilisation généralisée de l'informatique pour le cloud computing [17] en garantissant la confidentialité des données traitées. Plus largement, le chiffrement entièrement homomorphe améliore la capacité de calcul sécurisé sur les données chiffrées. Le RSA est le premier système de chiffrement à clé publique ayant une propriété d'homomorphe. Toutefois, pour des raisons de sécurité, le RSA doit ajouter des bits aléatoires à un message avant de le chiffrer, ce qui fait perdre à la RSA sa propriété d'homomorphe.

Le chiffrement homomorphe est un outil très utile qui présente un certain nombre d'applications [18] intéressantes sur le texte chiffré pour pouvoir manipuler le texte en clair en utilisant uniquement leur cryptogramme. Ce qui serait vraiment utile, c'est de pouvoir utiliser simultanément l'addition et la multiplication, ce qui permettrait de manipuler davantage le texte en clair en modifiant le texte chiffré. En fait, cela permettrait à une personne non-fiable ne disposant pas de la clé secrète, de calculer efficacement toute fonction calculable sur le texte chiffré lorsqu'elle ne dispose que du texte chiffré. Ce type de chiffrement est dit entièrement homomorphe et il a été introduit par R. Rivest, L. Adleman et M. Dertouzos en 1978 [110]. Malheureusement, peu après sa publication, des mesures de sécurité importantes ont été trouvées dans le système de chiffrement RSA [111]. La recherche des cryptosystèmes entièrement homomorphes a commencé et le problème de la construction d'un système avec ses propriétés est restée sans réponse jusqu'en 2009, lorsque Gentry [48] a présenté son résultat décisif.

Le chiffrement entièrement homomorphe permet d'assurer la confidentialité, la non-répudiation et l'intégrité des données dans les processus de communication et de stockage, comme la possibilité de déléguer les calculs à des parties non-fiables. Si un utilisateur pouvait prendre un problème défini dans un système algébrique et le chiffrer en un problème d'un autre système algébrique différent, d'une manière que le déchiffrement vers le système algébrique original est difficile, l'utilisateur pourrait alors chiffrer des calculs coûteux et les envoyer à la partie non-fiable pour effectuer le calcul correspondant dans le second système algébrique et renvoyer le résultat à l'utilisateur. Après avoir reçu le résultat, l'utilisateur peut le déchiffrer en une solution dans le système algébrique original, tandis que la partie de non-fiable ne sait pas quel calcul a été réellement effectué. En bref, un système de chiffrement est entièrement homomorphe si pour toute fonction de chiffrement Enc(), les opérations $\mathrm{Enc}(x+y)$ et $\mathrm{Enc}(x.y)$ sont faciles à calculer à partir de $\mathrm{Enc}(x)$ et $\mathrm{Enc}(y)$.

Avant de donner la définition formelle d'un système de chiffrement entièrement homomorphe, nous donnons tout d'abord la définition d'un système de chiffrement à clé publique [33] :

Définition 4.5.1 *Un système de chiffrement à clé publique consiste en trois algorithmes probabilistes de temps polynomiaux $(\mathcal{K}, \mathcal{E}, \mathcal{D})$, où :*

1. **$\mathcal{K}$ est l'algorithme de génération des clés :** *prend un paramètre de sécurité k comme entrée et produit une paire de clés (pk, sk), où pk désigne la clé publique utilisée pour le chiffrement et sk est la clé privée (ou clé secrète) utilisée pour le déchiffrement. On suppose que pk et sk ont chacun une longueur d'au moins k, et que k peut être déterminé*

16. Cas des moteurs de recherches.
17. La nouvelle forme de stockage de données du 21e siècle.
18. Généralement l'addition ou la multiplication, où une seule opération est possible.

à partir de pk et sk.

2. $\mathcal{E}$ **est l'algorithme de chiffrement :** *prend en entrée une clé publique pk et un message m à partir d'un espace de message en clairs sous-jacent* $\mathcal{M}$*, et produit en sortie un message chiffré c d'un espace de message chiffré sous-jacent* $\mathcal{C}$*. On note une fonction de chiffrement par* $\mathrm{Enc}_{\mathrm{pk}}$ *et on écrit* $\mathrm{Enc}_{\mathrm{pk}}(m) = c$*, ou tout simplement* $\mathrm{Enc}_{\mathrm{k}}(m) = c$*, s'il n'y a pas d'ambiguïté sur la clé utilisée.*

3. $\mathcal{D}$ **est l'algorithme de déchiffrement :** *est un algorithme déterministe, qui prend en entrée une clé privée sk et un message chiffré c, et produit en sortie un message clair m. On note une fonction de déchiffrement par* $\mathrm{Dec}_{\mathrm{sk}}$ *et on écrit* $\mathrm{Dec}_{\mathrm{sk}}(c) = m$*, ou tout simplement* $\mathrm{Dec}_{\mathrm{k}}(c) = m$*, s'il n'y a pas d'ambiguïté sur la clé utilisée.*

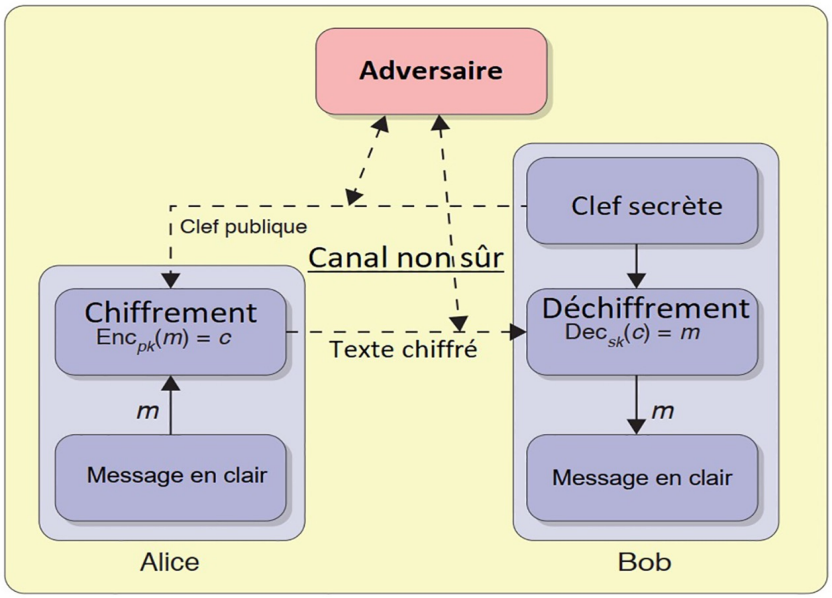

FIGURE 4.6: Système de chiffrement à clé publique.

Remarque 4.5.1 *Comme le but d'un système de chiffrement, n'est rien d'autre que de retrouver le texte en clair original, alors l'identité* $\mathrm{Dec}_{\mathrm{sk}} \circ \mathrm{Enc}_{\mathrm{pk}}(m) = m$ *doit être toujours vérifiée, pour toute paire de clés* (pk, sk) *et tout message en clair* m*.*

Un système de chiffrement homomorphe est un système de chiffrement permettant de faire des calculs sur les données chiffrées. Formellement, on a :

Définition 4.5.2 *(voir [141, pp. 27–28]).*
Un système de chiffrement asymétrique $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ *est dit homomorphe, si pour toute entrée k et pour toute paire de clés* (pk, sk) *produite à partir de k, il est possible de définir des groupes* $(\mathcal{M}, \bullet)$ *et* $(\mathcal{C}, \circ)$ *tels que :*

(i) L'espace des clairs $\mathcal{M}$ *et tous les chiffrés par* $\mathrm{Enc}_{\mathrm{pk}}$ *sont des éléments de* $\mathcal{C}$ *;*

(ii) Pour tous c_1 *et* c_2 *dans* $\mathcal{M}$*, on a* $\mathrm{Dec}_{\mathrm{sk}}(c_1 \circ c_2) = \mathrm{Dec}_{\mathrm{sk}}(c_1) \bullet \mathrm{Dec}_{\mathrm{sk}}(c_2)$*.*

Définition 4.5.3 *(voir [141, pp. 48–49]).*
Un système de chiffrement asymétrique $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ est dit entièrement homomorphe, si :

(i) L'espace des messages en clairs est un anneau $(\mathcal{M}, +, \times)$;

(ii) L'espace des messages chiffrés est un anneau $(\mathcal{C}, \oplus, \otimes)$;

(iii) Pour tous $m_1, m_2 \in \mathcal{M}$ et pour toute paire de clés (pk, sk) produite à partir de $\mathcal{K}$, on a :

$$\mathrm{Dec}_{\mathrm{sk}}\left(\mathrm{Enc}_{\mathrm{pk}}(m_1) \oplus \mathrm{Enc}_{\mathrm{pk}}(m_2)\right) = m_1 + m_2 \text{ et } \mathrm{Dec}_{\mathrm{sk}}\left(\mathrm{Enc}_{\mathrm{pk}}(m_1) \otimes \mathrm{Enc}_{\mathrm{pk}}(m_2)\right) = m_1 \times m_2.$$

Remarque 4.5.2 *Si $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ est un système de chiffrement symétrique, nous aurons une seule clé pour le chiffrement et le déchiffrement. Dans ce cas les clés pk et sk seront identiques.*

4.5.2 Premier cryptosystème

Dans cette sous-section nous décrivons un système de chiffrement entièrement homomorphe sur un anneau non commutatif R [9]. L'anneau R est construit à partir de la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$ étudiée au deuxième chapitre pour le cas particulier où la caractéristique p est un nombre premier supérieur ou égale à 5. Nous rappelons que la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$ est l'ensemble des points projectifs $[X : Y : Z] \in \mathbb{P}^2(\mathbb{F}_q[e])$ qui vérifient l'équation de Weierstrass $Y^2Z = X^3 + aXZ^2 + bZ^3$, où $(a, b) \in (\mathbb{F}_q[e])^2$ sont tels que $4a^3 + 27b^2$ est inversible dans l'anneau $\mathbb{F}_q[e]$.

4.5.2.1 L'anneau R

Soit $P \in E_{a,b}(\mathbb{F}_q[e])$ un point d'ordre n tel que le logarithme discret dans le groupe engendré par P soit difficile. Nous définissons l'ensemble R par : $R = \left\{ \begin{pmatrix} x & tP \\ 0 & y \end{pmatrix} | x, y, t \in \{0, 1, \cdots, n-1\} \right\}$.

Soient $X = \begin{pmatrix} x & tP \\ 0 & y \end{pmatrix}$ et $Y = \begin{pmatrix} z & rP \\ 0 & w \end{pmatrix}$. On définit sur R, les lois de composition internes « $+$ » et « $*$ » par : $X + Y = \begin{pmatrix} x+z & (t+r)P \\ 0 & y+w \end{pmatrix}$ et $X * Y = \begin{pmatrix} x & (tw+xr)P \\ 0 & yw \end{pmatrix}$.

Lemme 4.5.1 *$(R, +, *)$ est un anneau non commutatif d'unité $1_R = \begin{pmatrix} 1 & [0:1:0] \\ 0 & 1 \end{pmatrix}$.*

Preuve. Nous vérifions facilement que :

(i) $(R, +)$ est un groupe commutatif d'élément neutre le point $\begin{pmatrix} 0 & [0:1:0] \\ 0 & 0 \end{pmatrix}$; et l'opposé de tout point $\begin{pmatrix} a & xP \\ 0 & b \end{pmatrix}$ est le point $\begin{pmatrix} -a & -xP \\ 0 & -b \end{pmatrix}$.

(ii) La loi « $*$ » est associative, distributive à gauche et à droite par rapport à la loi « $+$ » et d'unité l'élément $\begin{pmatrix} 1 & [0:1:0] \\ 0 & 1 \end{pmatrix}$.

(iii) La loi « $*$ » est non commutative.

□

Lemme 4.5.2 *Un élément* $X = \begin{pmatrix} a & xP \\ 0 & b \end{pmatrix} \in R$ *est inversible si, et seulement si* $a \wedge n = 1$ *et* $b \wedge n = 1$. *Dans ce cas, l'inverse de* X *est donné par :* $X^{-1} = \begin{pmatrix} a^{-1} & -a^{-1}b^{-1}xP \\ 0 & b^{-1} \end{pmatrix}$.

Preuve. Soient $X = \begin{pmatrix} a & xP \\ 0 & b \end{pmatrix} \in R$. Si X est inversible, alors il existe $Y = \begin{pmatrix} c & yP \\ 0 & d \end{pmatrix} \in R$ tel que $X * Y = Y * X = \begin{pmatrix} 1 & [0:1:0] \\ 0 & 1 \end{pmatrix}$; et donc $ac \equiv 1 \mod n$ et $bd \equiv 1 \mod n$. D'où $a \wedge n = 1$ et $b \wedge n = 1$.

Réciproquement, si $a \wedge n = 1$ et $b \wedge n = 1$, alors on vérifie facilement que $\begin{pmatrix} a^{-1} & -a^{-1}b^{-1}xP \\ 0 & b^{-1} \end{pmatrix}$ est l'inverse de X. □

Lemme 4.5.3 *Soit* $X = \begin{pmatrix} a & xP \\ 0 & b \end{pmatrix} \in R$ *et soit* k *un entier strictement positif. L'élément* X^k *défini par* $X^k = \underbrace{X * X * \cdots * X}_{k \text{ fois l'élément } X.}$ *est donné par :* $X^k = \begin{pmatrix} a^k & \alpha_k xP \\ 0 & b^k \end{pmatrix}$, *où* $\alpha_k = \sum_{i+j=k-1} a^i b^j$.

Preuve. La propriété est évidente pour $k = 1$.

Supposons que $X^k = \begin{pmatrix} a^k & \alpha_k xP \\ 0 & b^k \end{pmatrix}$, où k est un entier strictement positif et $\alpha_k = \sum_{i+j=k-1} a^i b^j$. Alors :

$$X^{k+1} = X^k * X = \begin{pmatrix} a^k & \alpha_k xP \\ 0 & b^k \end{pmatrix} * \begin{pmatrix} a & xP \\ 0 & b \end{pmatrix} = \begin{pmatrix} a^{k+1} & \left(a^k + \alpha_k b\right) xP \\ 0 & b^{k+1} \end{pmatrix} = \begin{pmatrix} a^{k+1} & \alpha_{k+1} xP \\ 0 & b^{k+1} \end{pmatrix}.$$

Ainsi, le Lemme est montré. □

4.5.2.2 Description du cryptosystème basé sur R

L'objectif d'un protocole de génération de clés est de permettre à deux ou plusieurs entités de se communiquer sur un réseau ouvert avec une clé secrète partagée. La clé peut être ensuite

utilisée dans une cryptographie symétrique pour atteindre certains objectifs cryptographiques tels que la confidentialité ou l'intégrité des données. Le cryptosystème basé sur R qu'on va décrire, se décompose en trois algorithmes :

- **Algorithme de génération des clés :** la clé secrète K entre Alice et Bob est générée par le protocole d'échange de clés de Diffie-Hellman pour les courbes elliptiques :
  1. Alice et Bob s'accordent sur un nombre premier $p \geqslant 5$, un point $P \in E_{a,b}(\mathbb{F}_q[e])$ d'ordre fini n et choisissent deux entiers x et y dans l'ensemble $\{0, 1, \cdots, n-1\}$ qui sont premiers avec n ;
  2. Alice choisit un entier secret $n_a \leqslant n-1$, calcule $n_a P$ et l'envoie à Bob ;
  3. Bob choisit un entier secret $n_b \leqslant n-1$, calcule $n_b P$ et l'envoie à Alice ;
  4. Alice calcule $n_a n_b P$ et Bob calcule $n_b n_a P$;
  5. La clé privée entre Alice et Bob est $K = \begin{pmatrix} x & Q \\ 0 & y \end{pmatrix}$, où $Q = n_a n_b P$.

  Alice et Bob publient x, y, p, P et $E_{A,B}\left(\mathbb{F}_{p^d}[e]\right)$ et gardent comme secrets, les entiers n_a et n_b.
- **Algorithme de chiffrement :** si Alice veut envoyer un message m à Bob, alors :
  1. Il encode son message m en un point M de R ;
  2. Il utilise sa clé privée K et calcule $C = \mathrm{Enc_K}(M) = K * M * K^{-1}$;
  3. Il envoie à Bob le message chiffré C.
- **Algorithme de déchiffrement :** après avoir reçu le message chiffré C, Bob utilise sa clé privée K et calcule $\mathrm{Dec_K}(C) = K^{-1} * C * K$; et il retrouve bien, le message M d'Alice. En effet, pour tout $K \in \mathcal{C}$, on a :

$$\mathrm{Dec_K} \circ \mathrm{Enc_K}(M) = K^{-1} * \left(K * M * K^{-1}\right) * K = K^{-1} * K * (M) * K^{-1} * K = M.$$

Dans ce cryptosystème basé sur R, nous avons :

- **L'espace de textes en clairs :** $\mathcal{M} = R$.
- **L'espace de textes chiffrés :** $\mathcal{C} = R$.
- **L'espace des clés :** $\mathcal{K} = R^*$ (ensemble des éléments inversibles dans R).
- **L'ensemble des fonctions de chiffrement $\mathcal{E}$:** pour tout $K \in \mathcal{K}$, une fonction de chiffrement $\mathrm{Enc_K} : \mathcal{M} \longrightarrow \mathcal{C}$ est définie par : $\mathrm{Enc_K}(M) = K * M * K^{-1}$.
- **L'ensemble des fonctions de déchiffrement $\mathcal{D}$:** Pour tout $K \in \mathcal{K}$, une fonction de déchiffrement $\mathrm{Dec_K} : \mathcal{C} \longrightarrow \mathcal{M}$ est définie par : $\mathrm{Dec_K}(C) = K^{-1} * C * K$.

Proposition 4.5.1 *Le système de chiffrement $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ est entièrement homomorphe.*

Preuve. Soit K un élément de l'espace de clefs $\mathcal{K}$ et soient M_1 et M_2 deux éléments de l'espace des clairs $\mathcal{M}$. Pour toute paire $(\mathrm{Enc_K}, \mathrm{Dec_K}) \in \mathcal{E} \times \mathcal{D}$, nous avons :

$$\mathrm{Enc_K}(M_1) + \mathrm{Enc_K}(M_2) = K * (M_1 + M_2) * K^{-1} = \mathrm{Enc_K}(M_1 + M_2)$$

et

$$\mathrm{Enc_K}\left(M_1\right) * \mathrm{Enc_K}\left(M_2\right) = K * \left(M_1 * M_2\right) * K^{-1} = \mathrm{Enc_K}\left(M_1 * M_2\right).$$

Alors :

$$\mathrm{Dec_K}\left(\mathrm{Enc_K}\left(M_1\right) + \mathrm{Enc_K}\left(M_2\right)\right) = \mathrm{Dec_K} \circ \mathrm{Enc_K}\left(M_1 + M_2\right) = M_1 + M_2$$

et

$$\mathrm{Dec_K}\left(\mathrm{Enc_K}\left(M_1\right) * \mathrm{Enc_K}\left(M_2\right)\right) = \mathrm{Dec_K} \circ \mathrm{Enc_K}\left(M_1 * M_2\right) = M_1 * M_2.$$

D'où, le système de chiffrement $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ est entièrement homomorphe. □

4.5.3 Deuxième cryptosystème

Dans cette sous-section, nous présentons un autre système de chiffrement sur un anneau non commutatif noté R [13]. Nous nous intéressons en particulier au chiffrement basé sur le problème du conjugué dans R et le problème du logarithme discret dans le groupe de points de la courbe elliptique définie sur l'anneau $\mathbb{F}_q\left[e\right]$, où $e^3 = e^2$ (voir chapitre 3).

4.5.3.1 L'anneau R

Soit $\mathbb{F}_q$ un corps fini d'ordre q, où q est une puissance d'un nombre premier p supérieur ou égal à 5. Au chapitre 3, nous avons montré que l'ensemble $\mathbb{F}_q\left[e\right]$ des éléments de la forme $x_0 + x_1 e + x_2 e^2$, où $(x_0, x_1, x_2) \in \mathbb{F}_q^3$ et $e^3 = e^2$ est un anneau commutatif, unitaire et non-local pour les lois de composition internes « + » et « . » définies par :

Loi d'addition : $X + Y = (x_0 + y_0) + (x_1 + y_1)\, e + (x_2 + y_2)\, e^2$;

Loi de multiplication : $X.Y = x_0 y_0 + \delta_{XY} e + ((x_0 + x_1 + x_2)(y_0 + y_1 + y_2) - x_0 y_0 - \delta_{XY})\, e^2$;

où $X = x_0 + x_1 e + x_2 e^2, Y = y_0 + y_1 e + y_2 e^2$ et $\delta_{XY} = x_0 y_1 + x_1 y_0$.

Nous notons l'anneau $\mathbb{F}_q\left[e\right]$ par R et nous définissons sur R une autre loi de composition interne notée « $*$ » par : $X * Y = x_0 y_0 + (x_0 y_1 + x_1 y_2)\, e + x_2 y_2 e^2$.

Lemme 4.5.4 *$(R, +, *)$ est un anneau non commutatif d'unité $1_R = 1 + e^2$.*

Preuve. Évidente. □

Lemme 4.5.5 *Un élément $X = x_0 + x_1 e + x_2 e^2 \in R$ est inversible pour la loi $*$ si, et seulement si $x_0 x_2 \neq 0$. Dans ce cas, l'inverse de X est donné par : $X^{-1} = x_0^{-1} - x_1 x_0^{-1} x_2^{-1} e + x_2^{-1} e^2$.*

Preuve. Soient $X = x_0 + x_1 e + x_2 e^2 \in R$ et $Y = y_0 + y_1 e + y_2 e^2 \in R$. Comme $X * Y = x_0 y_0 + (x_0 y_1 + x_1 y_2)\, e + x_2 y_2 e^2$ et $Y * X = x_0 y_0 + (y_0 x_1 + y_1 x_2)\, e + x_2 y_2 e^2$, alors :

$$X * Y = Y * X = 1 + e^2 \Leftrightarrow \begin{cases} x_0 y_0 = 1 \\ x_0 y_1 + x_1 y_2 = y_0 x_1 + y_1 x_2 = 0 \\ x_2 y_2 = 1 \end{cases} \Leftrightarrow \begin{cases} x_0 \neq 0 \text{ et } y_0 = x_0^{-1} \\ y_1 = -x_1 x_0^{-1} x_2^{-1} \\ x_2 \neq 0 \text{ et } y_2 = x_2^{-1} \end{cases}.$$

Ainsi X est inversible si, et seulement si $x_0x_2 \neq 0$; et l'inverse de X est $X^{-1} = Y$. □

Lemme 4.5.6 *Soit $X = x_0+x_1e+x_2e^2 \in R$ et soit n un entier strictement positif. La puissance $X^n := \underbrace{X * X * \cdots * X}_{n \text{ fois l'élément } X}$ de X pour la loi $*$ est donnée par : $X^n = x_0^n + x_1 \sum_{i+j=n-1} x_0^i x_2^j e + x_2^n e^2$.*

Preuve. La propriété est évidente pour $n = 1$.
Supposons que $X^n = x_0^n+x_1 \sum_{i+j=n-1} x_0^i x_2^j e+x_2^n e^2$, où n est un entier supérieur ou égal à 1. Alors :

$$X^{n+1} = X*X^n = x_0x_0^n+\left(x_0x_1 \sum_{i+j=n-1} x_0^i x_2^j + x_1x_2^n\right) e+x_2x_2^n e^2 = x_0^{n+1}+x_1 \sum_{i+j=n} x_0^i x_2^j e+x_2^{n+1}e^2.$$

Ainsi, le Lemme est montré. □

4.5.3.2 Description du cryptosystème basé sur R

Soient A et B deux éléments de R tels que $4A^3 + 27B^2$ soit inversible dans l'anneau $(R, +, .)$ et soit $E_{A,B}(R)$ la courbe elliptique définie sur l'anneau $(R, +, .)$ (voir chapitre 3). Soit $(\mathcal{M}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ le cryptosystème défini par :

- **L'espace de textes en clairs :** $\mathcal{M} = \mathbb{F}_q$.
- **L'espace de textes chiffrés :** $\mathcal{C} = \mathbb{F}_q$.
- **L'espace des clés :** $\mathcal{K} = R$
- **L'ensemble des fonctions de chiffrement $\mathcal{E}$:** pour toute clé publique $pk = (a, b)$ d'éléments de $\mathbb{F}_q$, une fonction de chiffrement Enc_{pk} est définie par :

$$\begin{array}{rccl} \text{Enc}_{\text{pk}} : & \mathcal{M} & \longrightarrow & \mathcal{C} \\ & m & \longmapsto & \text{coeff}\left(k * \left(a + me + be^2\right) * k^{-1}, e\right) \end{array},$$

  où k est la clé privée entre Alice et Bob.
- **L'ensemble des fonctions de déchiffrement $\mathcal{D}$:** pour toute clé privée $sk = k \in \mathcal{K}$, une fonction de déchiffrement Dec_{sk} est définie par :

$$\begin{array}{rccl} \text{Dec}_{\text{sk}} : & \mathcal{C} & \longrightarrow & \mathcal{M} \\ & c & \longmapsto & \text{coeff}\left(k^{-1} * \left(a + ce + be^2\right) * k, e\right) \end{array}.$$

Dans ce cryptosystème, les algorithmes de génération des clés, de chiffrement et déchiffrement sont définis par :

- **Algorithme de génération des clés :** est basé sur le protocole d'échange des clés de Diffie-Hellman pour les courbes elliptiques :
  1. Alice et Bob se mettent d'accord sur un nombre premier $p \geqslant 5$ et un point P de la courbe elliptique $E_{A,B}(R)$ d'ordre connu ;

2. Alice choisit un entier secret $t < \text{ord}(P)$, calcule tP et envoie le résultat à Bob ;
3. Bob choisit un entier secret $l < \text{ord}(P)$, calcule lP et envoie le résultat à Bob ;
4. Alice calcule tlP et Bob calcule ltP ;
5. Si $tlP = ltP = [k : r : 1]$ avec k est inversible dans l'anneau $(R, +, *)$, alors la clé privée entre Alice et Bob est k. Sinon, on reprend l'algorithme à partir du deuxième point.

Alice et Bob publient p, P et $E_{A,B}(R)$ et gardent comme secrets, les entiers t et l.

- **Algorithme de chiffrement :** si Alice veut envoyer un message M à Bob, alors :
  1. Il encode son message M, en un entier $m \in \mathbb{F}_q$;
  2. Il choisit une clé publique sous forme d'une paire $pk = (a, b) \in \mathbb{F}_q \times \mathbb{F}_q$;
  3. Il utilise sa clé privée k et calcule $c = \text{Enc}_{\text{pk}}(m) = \text{coeff}\left(k * \left(a + me + be^2\right) * k^{-1}, e\right)$;
  4. Il envoie à Bob la clé publique pk et le message chiffré c.
- **Algorithme de déchiffrement :** après avoir reçu le message chiffré c et la clé publique pk, Bob utilise sa clé privée $sk = k$ et calcule $\text{Dec}_{\text{sk}}(c) = \text{coeff}\left(k^{-1} * \left(a + ce + be^2\right) * k, e\right)$; et il retrouve bien, le message m d'Alice.

Proposition 4.5.2 *Pour tout $m \in \mathbb{F}_q$, on a $\text{Dec}_{\text{sk}} \circ \text{Enc}_{\text{pk}}(m) = m$.*

Preuve. Soit $pk = (a, b) \in \mathbb{F}_q \times \mathbb{F}_q$ et soit $k = k_0 + k_1 e + k_2 e^2$ un élément inversible[19] dans l'anneau $(R, +, *)$. Pour tout $m \in \mathbb{F}_q$, on a :

$$\begin{aligned} k * \left(a + me + be^2\right) * k^{-1} &= k * a * k^{-1} + k * (me) * k^{-1} + k * \left(be^2\right) * k^{-1} \\ &= a - ak_1k_2^{-1}e + k_0mk_2^{-1}e + k_1bk_2^{-1}e + be^2 \\ &= a + \left(k_0mk_2^{-1} + k_1bk_2^{-1} - ak_1k_2^{-1}\right)e + be^2 \end{aligned}$$

et alors $c = \text{Enc}_{\text{pk}}(m) = \text{coeff}\left(k * \left(a + me + be^2\right) * k^{-1}, e\right) = k_0mk_2^{-1} + k_1k_2^{-1}(b - a)$.

D'autre part, on a :

$$\begin{aligned} k^{-1} * \left(a + ce + be^2\right) * k &= k^{-1} * a * k + k^{-1} * (me) * k + k^{-1} * \left(be^2\right) * k \\ &= a + ak_1k_0^{-1}e + k_0^{-1}ck_2e - k_1k_0^{-1}be + be^2 \\ &= a + \left(ak_1k_0^{-1} + k_0^{-1}ck_2 - k_1k_0^{-1}b\right)e + be^2 \end{aligned}$$

et donc :

$$\begin{aligned} \text{Dec}_{\text{sk}}(c) = \text{coeff}\left(k^{-1} * \left(a + ce + be^2\right) * k, e\right) &= ak_1k_0^{-1} + k_0^{-1}ck_2 - k_1k_0^{-1}b \\ &= ak_1k_0^{-1} + k_0^{-1}k_2\left(k_0mk_2^{-1} + k_1bk_2^{-1} - ak_1k_2^{-1}\right) - k_1k_0^{-1}b \\ &= ak_1k_0^{-1} + m + k_1k_0^{-1}b - ak_1k_0^{-1} - k_1k_0^{-1}b = m. \end{aligned}$$

Ainsi, nous avons montré que $\text{Dec}_{\text{sk}} \circ \text{Enc}_{\text{pk}}(m) = m$, pour tout $m \in \mathbb{F}_q$. □

19. Son inverse est donné par $k^{-1} = k_0^{-1} - k_1k_0^{-1}k_2^{-1}e + k_2^{-1}e^2$.

Proposition 4.5.3 *Le système de chiffrement $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ est homomorphe si, et seulement si $k = k_0 + k_2 e^2$ ou $a = b$.*

Preuve. Soit $pk = (a, b) \in \mathbb{F}_q \times \mathbb{F}_q$ et soit $k = k_0 + k_1 e + k_2 e^2$ un élément inversible dans l'anneau $(R, +, *)$. Pour toute paire $(m_1, m_2) \in \mathbb{F}_q \times \mathbb{F}_q$, on a :

$$\mathrm{Enc}_{\mathrm{pk}}(m_1 + m_2) = k_0 (m_1 + m_2) k_2^{-1} + k_1 k_2^{-1} (b - a)$$

et

$$\mathrm{Enc}_{\mathrm{pk}}(m_1) + \mathrm{Enc}_{\mathrm{pk}}(m_2) = k_0 (m_1 + m_2) k_2^{-1} + 2 k_1 k_2^{-1} (b - a) \ .$$

Alors :

$$\mathrm{Enc}_{\mathrm{pk}}(m_1 + m_2) = \mathrm{Enc}_{\mathrm{pk}}(m_1) + \mathrm{Enc}_{\mathrm{pk}}(m_2) \Leftrightarrow k_1 k_2^{-1} (b - a) = 0 \Leftrightarrow k_1 = 0 \text{ ou } a = b.$$

□

Corollaire 4.5.1 *Soit $k = k_0 + k_2 e^2$ un élément inversible dans l'anneau $(R, +, *)$. Pour tout $(m_1, m_2) \in \mathbb{F}_q \times \mathbb{F}_q$, on a :* $\mathrm{Enc}_{\mathrm{pk}}(m_1.m_2) = k_2 k_0^{-1} \mathrm{Enc}_{\mathrm{pk}}(m_1) . \mathrm{Enc}_{\mathrm{pk}}(m_2)$.

Preuve. Soit $(m_1, m_2) \in \mathbb{F}_q \times \mathbb{F}_q$ et soit $k = k_0 + k_2 e^2$ un élément inversible dans l'anneau $(R, +, *)$. Alors :

$$\mathrm{Enc}_{\mathrm{pk}}(m_1) . \mathrm{Enc}_{\mathrm{pk}}(m_2) = k_0 m_1 k_2^{-1} . k_0 m_2 k_2^{-1} = k_0 \left(k_0 (m_1.m_2) k_2^{-1} \right) k_2^{-1} = k_0 \mathrm{Enc}_{\mathrm{pk}}(m_1.m_2) k_2^{-1}.$$

□

Corollaire 4.5.2 *Si $k = k_0 + k_0 e^2$, où $k_0 \in \mathbb{F}_q^*$, alors le système de chiffrement $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ est entièrement homomorphe.*

Preuve. Découle directement du corollaire précédent. □

Remarque 4.5.3 *Soit $(m_1, m_2) \in \mathbb{F}_q \times \mathbb{F}_q$ et soit $k = k_0 + k_2 e^2$ un élément inversible dans l'anneau $(R, +, *)$. Alors :* $\mathrm{Enc_k}(m_1). \mathrm{Enc_k}(m_2) = \mathrm{Enc_{k^2}}(m_1.m_2)$, *où $k^2 = k * k$.*

4.5.3.3 Exemple numérique

Soient les données suivantes :

q =12141680576410806693246636917646993166515042744075872007823827560868151782532553
1293 ;

a =1157920892373161954235709850086879078532699846656405640394575840079131296402 33 ;

b =9485687950320942729098935091911713411339877143809275006112365281928243580103559 57 ;

$$
\begin{aligned}
k =& 29642774844752946028434172162224104410437116074403984394101141506025761187823791 \\
&+ 72370055773322622139731865630429942408293740416025352524660990004945706029 17e \\
&+ 23714219875802356822747337729779283528349692859523187515280913204820608950258 \\
&9237e^2 \ ; \\
m =& 46316835694926478169428394003475163141307993866256225615783033603165251855 9817 \ ;
\end{aligned}
$$

alors, le chiffré de m est :

$$
\begin{aligned}
c =& 37599608055473163124466745634442328940635586913242365184093361109148436480978867 \\
&053 \ .
\end{aligned}
$$

4.5.4 Sécurité de ces cryptosystèmes

Dans les articles [9] et [13], l'état de l'art de la cryptographie basée sur un anneau est passée en revue, puis un nouveau problème cryptographique basé sur le problème du conjugué dans un anneau non commutatif a été proposé. Sur la base de ce problème, nous avons conçu deux nouveaux systèmes de chiffrement entièrement homomorphes.

Le processus de signature des systèmes basés sur un anneau est plus efficace que celui des systèmes basés sur RSA, tandis que le processus de vérification pour ces systèmes est nettement plus lent. Par conséquent, les signatures basées sur un anneau conviennent donc aux scénarios où le processus de signature doit être aussi rapide que possible, mais où des retards sont autorisés dans le processus de vérification (par exemple, dans les systèmes de paiement électronique hors ligne).

Les cryptosystèmes qu'on a décrit dans cette section sont à clé publique, où le protocole d'échange de clés se fait par Diffie-Hellman sur le groupe de points de la courbe elliptique définie sur l'anneau R. De ce fait, aucun autre tiers n'est capable de déterminer la clé privée ; et le seul moyen de calculer cette clé privée est de résoudre le problème de Diffie-Hellman, où le problème a été étudié minutieusement pendant des dizaines d'années, sans pour autant qu'aucune solution « facile » n'ait été proposée. Le moyen le plus efficace connu pour résoudre le problème de Diffie-Hellman est de résoudre le problème du logarithme discret, où ce problème est réputé être un problème plus difficile dans le groupe de points d'une courbe elliptique. De plus, le processus de déchiffrement d'un message est basé sur le problème de recherche du conjugué dans l'anneau non commutatif R, qui est aussi réputé être un problème difficile.

4.5.5 Conclusion

Les résultats expliqués dans cette section, montrent que le premier cryptosystème [9] est entièrement homomorphe, et que le deuxième [13] est entièrement homomorphe dans des cas précis. La sécurité de ces deux cryptosystèmes repose sur deux problèmes difficiles : le problème du logarithme discret dans le groupe des points d'une courbe elliptique et le problème de recherche du conjugué dans un anneau non commutatif.

La grande beauté est le fait que les cryptosystèmes entièrement homomorphes peuvent être largement utilisé dans la pratique, notamment dans le cloud computing, le commerce électronique, le vote électronique, etc.

Finalement, nous proposons aux lecteurs une question de grand intérêt qui peut donner forme à un nouvel article sur la cryptographie : comment transformer un message donné en un élément de l'anneau R ?

Conclusion générale et perspectives

Dans cette thèse, nous avons étudié des courbes elliptiques définies sur des anneaux finis et non-locaux dans le but d'introduire le bagage théorique nécessaire pour la conception des cryptosystèmes sûrs et efficaces sur ces structures.

Le premier chapitre était une introduction aux courbes elliptiques, où on a donné des prérequis de base pour la réalisation de cette thèse.

L'étude des propriétés algébriques de l'anneau $\mathbb{F}_q[e]$, où $e^2 = e$ dans le deuxième chapitre, nous a permis d'établir un isomorphisme entre les courbes elliptiques définies sur cet anneau et un produit cartésien de courbes elliptiques définies sur le corps fini $\mathbb{F}_q$ sous-jacent. Ce résultat est très important en cryptographie, du fait qu'il donne un nouvel algorithme de factorisation des grands entiers et il permet aussi, de voir que le problème du logarithme discret des courbes elliptiques définies sur cet anneau est équivalent à celui des courbes elliptiques définies sur le corps fini sous-jacent.

Dans le troisième chapitre, on a étudié les courbes elliptiques définies sur l'anneau non-local $\mathbb{F}_q[e]$, où $e^3 = e^2$ et q est une puissance d'un nombre premier supérieur ou égal à 5. Le but de ce chapitre était de concevoir les idées nécessaires pour une généralisation de l'étude des courbes elliptiques sur les anneaux de type $\mathbb{F}_q[e]$, où $e^{n+1} = e^n$ avec n un entier supérieur ou égal à 2.

Enfin, dans le quatrième chapitre, nous avons mis en œuvre les résultats théoriques trouvés aux chapitres précédents pour la construction de nouveaux systèmes de chiffrement entièrement homomorphe.

Ce travail s'ouvre sur d'autres questions et applications et il ouvre d'autres voies d'étude :

Perspectives de recherche :

1. Étant donné un entier positif n, est-ce qu'on peut trouver une courbe elliptique définie sur $\mathbb{F}_q[e]$ d'ordre n ? ce qui donnerait une nouvelle méthode de factorisation des entiers.

2. Étudier les courbes elliptiques définies sur l'anneau $\mathbb{F}_q[e]$, avec $e^n = e$, où n un entier positif.
3. Chercher s'il existe un isomorphisme entre la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$ étudiée au chapitre 3 et ses réductions sur $\mathbb{F}_q$.
4. Étudier la sécurité des cryptosystèmes entièrement homomorphes donnés au chapitre 4.
5. Étudier les attaques existantes sur ces courbes elliptiques.

Références bibliographiques

[1] Q. Alamélou. *Protocoles cryptographiques pour l'authentification numérique et le respect de la vie privée*. PhD thesis, Limoges, 2017.

[2] I. Anshel, M. Anshel, B. Fisher, and D. Goldfeld. New key agreement protocols in braid group cryptography. *Topics in Cryptology-CT-RSA 2001*, pages 13–27, 2001.

[3] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Mathematics of computation*, 61(203) :29–68, 1993.

[4] E. Bach. Number-theoretic algorithms. *Annual Review of Computer Science*, 4(1) :119–172, 1990.

[5] P. Barthélemy, R. Rolland, P. Véron, and R. Rolland. *Cryptographie : principes et mises en œuvre*. Hermès Science Publications, 2005.

[6] I. Blake, G. Seroussi, G. Seroussi, and N. Smart. *Elliptic curves in cryptography, volume 265*. Cambridge University Press, 1999.

[7] W. Bosma and H. Lenstra. Complete systems of two addition laws for elliptic curves. *Journal of Number Theory*, 53(2) :229–240, 1995.

[8] A. Boulbot, A. Chillali, and A. Mouhib. Elliptic curves over the ring $\mathbb{F}_q[e], e^3 = e^2$. *Gulf Journal of Mathematics*, 4(4) :123–129, 2016.

[9] A. Boulbot, A. Chillali, and A. Mouhib. Cryptographic protocols on the non-commutative ring R. *International Journal of Mathematical and Computational Methods*, 2 :138–141, 2017.

[10] A. Boulbot, A. Chillali, and A. Mouhib. Elliptic curve over a finite ring generated by 1 and an idempotent element e with coefficients in the finite field $\mathbb{F}_{3^d}$. *Boletim da Sociedade Paranaense de Matemática*, pages 1–19, 2018.

[11] A. Boulbot, A. Chillali, and A. Mouhib. Elliptic curve over a finite ring of characteristic two. *(soumis).*, 2020.

[12] A. Boulbot, A. Chillali, and A. Mouhib. Elliptic curves over the ring R. *Boletim da Sociedade Paranaense de Matemática*, 38(3) :193–201, 2020.

[13] A. Boulbot, M. Elhassani, A. Chillali, and A. Mouhib. Fully homomorphic encryption scheme on a non commutative ring *R. In International Conference on Intelligent Systems and Advanced Computing Sciences (ISACS)*, pages 1–4. IEEE, 2019.

[14] P. Boyer. *Petit compagnon des nombres et de leurs applications*, volume 125 of Mathématiques en Devenir. Calvage et Mounet, 2019.

[15] G. Brassard. A time-luck tradeoff in relativized cryptography. *Journal of Computer and System Sciences*, 22(3) :280–311, 1981.

[16] G. Brassard and C. Goutier. *Cryptologie contemporaine*. Masson Paris, 1993.

[17] J. Buchmann and H. C. Williams. A key-exchange system based on imaginary quadratic fields. *Journal of Cryptology*, 1(2) :107–118, 1988.

[18] L. S. Charlap, D. P. Robbins, and R. Coley. *An elementary introduction to elliptic curves*. Center for Communications Research, Institute for Defense Analysis, 1988.

[19] A. Chatterjee and K. M. M. Aung. *Fully homomorphic encryption in real world applications*. Springer, 2019.

[20] A. Chillali. Cryptography over elliptic curve of the ring $\mathbb{F}_q[\epsilon], \epsilon^4 = 0$. *World Academy of Science, Engineering and Technology*, 78, 2011.

[21] A. Chillali. *Cryptosystème à clef publique et courbes elliptiques sur l'anneau* $\mathbb{F}_q[\epsilon]$, $\epsilon^n = 0$. PhD thesis, Université Sidi Mohamed Ben Abdellah, faculté des sciences et techniques-Fès, 2013.

[22] A. Chillali and M. Boulagouaz. Methods of encryption keys : example of elliptic curve. *Journal of Communications and Computer Engineering*, 3(1) :7–11, 2013.

[23] H. Cohen. *A course in computational algebraic number theory*, volume 138. Springer Verlag, 1993.

[24] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren. *Handbook of elliptic and hyperelliptic curve cryptography*. Chapman & Hall/CRC press, 2005.

[25] D. Coppersmith. Fast evaluation of logarithms in fields of characteristic two. *IEEE Transactions on Information Theory*, 30(4) :587–594, 1984.

[26] D. Coppersmith. The data encryption standard (DES) and its strength against attacks. *IBM Journal of Research and Development*, 38(3) :243–250, 1994.

[27] D. Coppersmith, A. M. Odlzyko, and R. Schroeppel. Discrete logarithms in $GF(p)$. *Algorithmica*, 1(1-4) :1–15, 1986.

[28] J. Daemen and V. Rijmen. Reijndael : The Advanced Encryption Standard. *Dr. Dobb's Journal : Software Tools for the Professional Programmer*, 26(3) :137–139, 2001.

[29] J. Daemen and V. Rijmen. *The design of Rijndael : AES-the Advanced Encryption Standard*. Springer Science & Business Media, 2013.

[30] C. Daremberg and E. Saglio. *Dictionnaire des antiquités grecques et romaines : d'après les textes et les monuments*, volume 3. Hachette, 1904.

[31] H. Davenport. *The higher arithmetic : An introduction to the theory of numbers*. Cambridge University Press, 1999.

[32] B. Den Boer. Diffie-Hellman is as strong as discrete log for certain primes. *Advances in Cryptology–CRYPTO 88. Lecture Notes in Computer Science*, 403 :530–539, 1990.

[33] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6) :644–654, 1976.

[34] W. Diffie and M. E. Hellman. Multiuser cryptographic techniques. *In Proceedings of the June 7-10, 1976, National Computer Conference and Exposition*, pages 109–112. ACM, 1976.

[35] J. F. Dooley. *History of cryptography and cryptanalysis*. History of Computing. Springer, 1st edition, 2018.

[36] Y. Driencourt and J. F. Michon. Elliptic codes over fields of characteristics 2. *Journal of Pure and Applied Algebra*, 45(1) :15–39, 1987.

[37] G. Dubertret. *Initiation à la cryptographie*. Vuibert Informatique, 2000.

[38] S. R. Dusse and J. B. S. Kaliski. A cryptographic library for the Motorola DSP56000. *Lecture Notes in Computer Science*, 473 :230–244, 1991.

[39] H. Eberle. A high-speed DES implementation for Network Applications. *Advances in Cryptology - CRYPT0'92*, page 521, 1992.

[40] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4) :469–472, 1985.

[41] A. Enge. *Elliptic curves and their applications to cryptography : an introduction*. Kluwer Academic Publishers, 1999.

[42] P. Fahn and M. Robshaw. *Results from the RSA factoring challenge*. Technical Report TR–501, Version 1.3, RSA Laboratories, 1995.

[43] A. Fiat and A. Shamir. How to prove yourself : practical solutions to identification and signature problems. *Advances in Cryptology-CRYPTO'86, LNCS*, 263 :186–194, 1987.

[44] F. Fontein. *Elliptic curves over rings with a point of view on cryptography and factoring*. PhD thesis, Universitat Oldenburg, Diplomstudiengang Mathematik, 2005.

[45] W. Fulton. *Algebraic curves : an introduction to algebraic geometry*. Addison-Wesley, 1989.

[46] F. Furlan. *Studia albertiana : lectures et lecteurs de LB Alberti*. Vrin, 2003.

[47] P. Gaudry. An algorithm for solving the discrete logarithm problem on hyperelliptic curves. *Advances is Cryptology-EUROCRYPTO 2000*, pages 19–34, 2000.

[48] C. Gentry. Fully homomorphic encryption using ideal lattices. *In ACM Symposium on Theory of Computing*, 2009, pages 169–178, 2009.

[49] S. Goldwasser and J. Kilian. Almost all primes can be quickly certified. *In Proceedings of the* 8th *Annual ACM Symposium on Theory of Computing*, pages 316–329, 1986.

[50] D. M. Gordon. Discrete logarithms in $GF(p)$ using the number field sieve. *SIAM Journal on Discrete Mathematics*, 6(1) :124–138, 1993.

[51] A. Guillevic. *Arithmetic of pairings on algebraic curves for cryptography*. PhD thesis, Ecole Normale Supérieure de Paris - ENS Paris, 2013.

[52] L. C. Guillou, M. Ugon, and J.-J. Quisquater. The smart card : A standardized security device dedicated to public cryptology. *Contemporary Cryptology : the Science of Information Integrity. IEEE Press, Piscataway, NJ*, 16, 1992.

[53] G. Harper, A. Menezes, and S. Vanstone. Public-key cryptosystems with very small key lengths. *In Advances in Cryptology-EUROCRYPT'92*, pages 163–173. Springer-Verlag, 1993.

[54] M. H. Hassib. *Courbes elliptiques sur un anneau de caractéristique 3 et cryptographie*. PhD thesis, Université Moulay Ismail, Faculté des Sciences et Techniques Errachidia, 2015.

[55] M. H. Hassib, A. Chillali, and M. A. Elomary. Elliptic curves over a chain ring of characteristic 3. *Journal of Taibah University for Science*, 9(3) :276–287, 2015.

[56] M. J. Jacobson, A. Menezes, and A. Stein. Solving elliptic curve discrete logarithm problems using Weil descent. *IACR Cryptology ePrint Archive*, 2001 :41, 2001.

[57] A. Jambert. *Outils cryptographiques pour la protection des contenus et de la vie privée des utilisateurs*. PhD thesis, Université de Bordeaux, 2011.

[58] A. Joux and K. Nguyen. Separating decision Diffie-Hellman from computational Diffie-Hellman in cryptographic groups. *Journal of Cryptology*, 16(4) :239–247, 2003.

[59] A. Joux and V. Vitse. Elliptic curve discrete logarithm problem over small degree extension fields. *Journal of Cryptology*, 26(1) :119–143, 2013.

[60] D. Kahn. *La guerre des codes secrets*. Inter Editions, 1980.

[61] B. S. Kaliski. A Pseudo-Random bit generator based on elliptic logarithms. *Lecture Notes in Computer Science*, pages 84–103, 1987.

[62] B. S. Kaliski. *Elliptic curves and cryptography : A pseudorandom bit generator and other tools*. PhD thesis, Massachusetts Institute of Technology, 1988.

[63] B. S. Kaliski. One-Way permutations on elliptic curves. *Journal of Cryptology*, 3(3) :187–199, 1991.

[64] J. Katz and Y. Lindell. *Introduction to modern cryptography*. Chapman & Hall/CRC Cryptography and Network Security Series. 2e édition, 2015.

[65] J. Katz, A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone. *Handbook of applied cryptography*. CRC press, 1996.

[66] A. Kerckhoffs. La cryptographie militaire. *Journal des Sciences Militaires*, 9 :5–38, 1883.

[67] L. R. Knudsen. *Block ciphers-analysis, design and applications*. Aarhus Universitet. Department of Computer Science, 1994.

[68] N. Koblitz. *A course in number theory and cryptography*, volume 114. Springer-Verlag, 1987.

[69] N. Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177) :203–209, 1987.

[70] N. Koblitz. Hyperelliptic cryptosystems. *Journal of Cryptology*, 1(3) :139–150, 1989.

[71] N. Koblitz and A. J. Menezes. A survey of public-key cryptosystems. *SIAM review*, 46(4) :599–634, 2004.

[72] D. W. Kravitz. *Digital Signature Algorithm*, July 27 1993. US Patent 5,231,668.

[73] H. W. Lenstra and A. K. Lenstra. Algorihtms in number theory. *Handbook of Theoretical Computer Science*, pages 673–715, 1990.

[74] H. W. Lenstra and C. Pomerance. A rigorous time bound for factoring integers. *Journal of the American Mathematical Society*, 5(3) :483–516, 1992.

[75] H. W. Lenstra. Elliptic curves and number-theoretic algorithms. *Proceedings of the International Congress of Mathematicians*, Berkeley, California, USA, 1986.

[76] H. W. Lenstra. Factoring integers with elliptic curves. *Annals of Mathematics*, pages 649–673, 1987.

[77] R. Lovorn. *Rigorous, subexponential algorithms for discrete logarithms over finite fields.* PhD thesis, University of Georgia, 1992.

[78] B. Martin. *Codage, cryptologie et applications.* PPUR Presses Polytechniques, 2004.

[79] U. M. Maurer and S. Wolf. Diffie-Hellman oracles. *In Annual International Cryptology Conference*, pages 268–282. Springer, 1996.

[80] K. McCurley. Cryptographic key distribution and computation in class groups. *Proceedings of NATO ASI Number Theory and Applications*, pages 459–479, 1989.

[81] K. McCurley. The discrete logarithm problem, cryptology and computational number theory. *In Proc. Symposia in Applied Mathematics*, volume 42, pages 49–74. AMS, 1990.

[82] A. J. Menezes. *Elliptic curve public key cryptosystems*, volume 234 of The Kluwer International Series in Engineering and Computer Science. Springer Science+Business Media, LLC, 1st edition, 1993.

[83] A. J. Menezes, J. Katz, P. C. Van Oorschot, and S. A. Vanstone. *Handbook of applied cryptography.* CRC press Series on Discrete Mathematics and Its Applications, 1996.

[84] A. J. Menezes, T. Okamoto, and S. A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions on Information Theory*, 39(5) :1639–1646, 1993.

[85] A. J. Menezes and S. A. Vanstone. A note on cyclic groups, finite fields, and the discrete logarithm problem. *Applicable Algebra in Engineering, Communication and Computing*, 3(1) :67–74, 1992.

[86] R. Merkle and M. Hellman. Hiding information and signatures in trapdoor knapsacks. *IEEE Transactions on Information Theory*, 24(5) :525–530, 1978.

[87] V. S. Miller. Use of elliptic curves in cryptography, *Advances in Cryptology Proc. of CRYPTO'85. LNCS*, 218 :417–426, 1986.

[88] S. Miyaguchi. Fast encryption algorithm for the RSA cryptographic system. *Proceedings of Compcon 82, IEEE Press*, pages 672–678, 1982.

[89] S. M. Molleví. *Corbes el. liptiques modul ni aplicacions criptografiques*. PhD thesis, Universitat Politècnica de Catalunya (UPC), 1997.

[90] P. L. Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Mathematics of Computation*, 48(177) :243–264, 1987.

[91] P. L. Montgomery. *An FFT extension of the elliptic curve method of factorization*. PhD thesis, UCLA, 1992.

[92] G. L. Mullen and D. Panario. *Handbook of finite fields*. Chapman and Hall/CRC, 2013.

[93] J. Nechvatal. *Computer security : public-key cryptography*. NIST, 1991.

[94] A. Odlyzko. Discrete logarithms and their cryptographic significance. *Advances in Cryptography, Proceding of EUROCRYPT 84*, 209 :224–314, 1985.

[95] R. Odoni, V. Varadharajan, and P. Sanders. Public key distribution in matrix rings. *Electronics Letters*, 20(9) :386–387, 1984.

[96] T. Okamoto. A new public-key cryptosystem as secure as factoring, *Advances in Cryptology-Proceedings of EUROCRYPTO'98. Lecture Notes in Computer Science*, 1403 :308–318, 1998.

[97] F. S. M. Onana. *Vie privée en commerce électronique*. ProQuest, 2005.

[98] M. Paoli, L. B. Alberti, and F. Choay. *Leon Battista Alberti, 1404-1472*. Les Éd. de l'Imprimeur, 2004.

[99] J.-P. Paquin and R. Paquin. Une analyse stratégique des communications de l'avenir : la cryptographie à clé révélée. *Théories et Pratiques Actuelles du Management*, page 93, 1990.

[100] C. Pierrot. *Le logarithme discret dans les corps finis*. PhD thesis, Paris 6, 2016.

[101] S. Pohlig and M. Hellman. An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance (Corresp.). *IEEE Transactions on Information Theory*, 24(1) :106–110, 1978.

[102] J. M. Pollard. Monte Carlo methods for index computation (*mod p*). *Mathematics of Computation*, 32(143) :918–924, 1978.

[103] C. Pomerance. Fast, rigorous factorization and discrete logarithm algorithms. *Discrete Algorithms and Complexity, Elsevier*, pages 119–143, 1987.

[104] C. Pomerance. Very short primality proofs. *Mathematics of Computation*, pages 315–322, 1987.

[105] C. Pomerance. Factoring. *In Proc. Symposia in Applied Mathematics, Providence*, volume 42, pages 27–48. American Mathematical Society, 1990.

[106] C. Pomerance and S. Goldwasser. *Cryptology and computational number theory*, volume 42. American Mathematical Soc., 1990.

[107] G. Poupard. *Authentification d'entité, de message et de clés cryptographiques : théorie et pratique*. PhD thesis, École Polytechnique, 2000.

[108] R. L. Rivest. Debating encryption standards. *Communications of the ACM*, 35(7) :32–54, 1992.

[109] R. L. Rivest. The RC4 encryption algorithm, 1992. *RSA Data Security Inc*, 25, 2016.

[110] R. L. Rivest, L. Adleman, and M. L. Dertouzos. On data banks and privacy homomorphisms. *Foundations of Secure Computation*, 1978.

[111] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2) :120–126, 1978.

[112] B. Schneier. *Applied cryptography : protocols, algorithms, and source code in C*. John Wiley & Sons, 20th edition, 2015.

[113] C.-P. Schnorr. Efficient signature generation by smart cards. *Journal of Cryptology*, 4(3) :161–174, 1991.

[114] A. Shamir. A polynomial-time algorithm for breaking the basic Merkle-Hellman cryptosystem. *IEEE Transactions on Information Theory*, 30(5) :699–704, 1984.

[115] A. Shamir. Stream ciphers : dead or alive ?. *Advances in Cryptology-ASIACRYPT 2004*, pages 25–36, 2004.

[116] A. Shamir and E. Biham. Differential cryptanalysis of the full 16-round DES. *In Advances in Cryptology-Proceedings of CRYPTO'92*. Springer-Verlag, 1993.

[117] C. E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27(3) :379–423, 1948.

[118] C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4) :656–715, 1949.

[119] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2) :303–332, 1999.

[120] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106. Springer-Verlag, 1986.

[121] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151. Springer-Verlag, 1994.

[122] J. H. Silverman and J. T. Tate. *Rational points on elliptic curves*, volume 9. Springer-Verlag, 1992.

[123] R. D. Silverman and S. S. Wagstaff. A practical analysis of the elliptic curve factoring algorithm. *Mathematics of Computation*, 61(203) :445–462, 1993.

[124] G. J. Simmons. The smart card : A standardized security device dedicated to public cryptology. *Wiley-IEEE Press*, 1992.

[125] S. Singh. *Histoire des codes secrets : de l'Egypte des pharaons à l'ordinateur quantique*. Livre de Poche, 2000.

[126] M. Smid and D. Branstad. The data encryption standard : past and future, *In Contemporary Cryptology : The Science of Information Integrity*, IEEE Press, pages 43–64, 1991.

[127] W. Stein. *Elementary number theory : primes, congruences, and secrets*. Springer Science & Business Media, 2009.

[128] J. Stern. *Science du secret (La)*. Odile Jacob, 1998.

[129] D. Stinson and S. Vaudenay. *Cryptographie-Théorie et pratique*. Vuibert, Paris, 2e édition, 2001.

[130] D. R. Stinson and M. Paterson. *Cryptography : Theory and Practice*. CRC Press, 4th edition, 2018.

[131] A. Tadmori. *Courbes elliptiques sur des anneaux commutatifs finis et applications*. PhD thesis, Université Mohammed Premier, Faculté des Science Oujda, 2016.

[132] A. Tadmori, A. Chillali, and M. Ziane. Elliptic curve over spir of characteristic two. *International Conference on Applied Mathematics and Computational Methods (AMCM 2013)*, pages 41–45.

[133] A. Tadmori, A. Chillali, and M. Ziane. Normal form of the elliptic curve over the finite ring. *Journal of Mathematics and System Science*, 4(3) :194–196, 2014.

[134] A. Tadmori, A. Chillali, and M. Ziane. Cryptography over the elliptic curve $E_{a,b}(A_3)$. *Journal of Taibah University for Science*, 9(3) :326–331, 2015.

[135] W. Trappe and L. C. Washington. *Introduction to cryptography with coding theory*. Pearson Education International, 2nd edition, 2006.

[136] M. Tsfasman and S. G. Vladut. Algebraic-geometric codes. *Mathematics and its Applications (Soviet Series)*, 58, 1991.

[137] S. A. Vanstone and R. J. Zuccherato. Elliptic curve cryptosystems using curves of smooth order over the ring $\mathbb{Z}_n$. *IEEE Transactions on Information Theory*, 43(4) :1231–1237, 1997.

[138] M. Virat. *Courbes elliptiques sur un anneau et applications cryptographiques*. PhD thesis, Université Nice Sophia Antipolis, 2009.

[139] L. C. Washington. *Elliptic curves : number theory and cryptography*. Chapman & Hall/CRC, 2nd edition, 2008.

[140] A. Wiles. Modular elliptic curves and fermat's last theorem. *Annals of Mathematics*, 141(3) :443–551, 1995.

[141] X. Yi, R. Paulet, and E. Bertino. *Homomorphic encryption and applications*, volume 3. Springer, 2014.

Index

A

algorithme
- asymétrique, 67
- cryptographique, 60, 64
- de chiffrement en continu, 66
- de chiffrement par blocs, 66
- de Diffie-Hellman, 68
- d'ElGamal, 68
- DSA, 68
- ECC, 68
- restreint, 60
- RSA, 68
- symétrique, 65

Alice, 60

attaque, 59
- à texte chiffré seulement, 62
- à texte en clair choisi, 63
- à texte en clair choisi adaptative, 63
- à texte en clair connu, 63
- cryptanalytique, 62

authentification, 61

B

Bob, 60

C

cassage complet, 63

chiffrement, 59
- à clé publique , 76
- entièrement homomorphe, 78
- homomorphe, 77
- RSA, 72

clef, 60

complexité
- d'une attaque, 63
- en espace, 63
- en information, 63
- en temps, 63

confidentialité, 61

courbe
- affine plane, 6
- elliptique affine, 9
- elliptique projective, 11
- elliptique sur un anneau fini, 23
- projective plane, 8
- singulière, 6

cryptage, 59

cryptanalyse, 62

cryptogramme, 60

cryptographie, 59
- moderne, 60
- sur les courbes elliptiques, 73

cryptologie, 59

cryptosystème, 60, 64
- basé sur R, 79, 82
- d'ElGamal, 71, 75

D

déchiffrement, 60

décryptage, 60

Diffie-Hellman pour ECC, 74

discriminant d'une courbe elliptique, 9
distribution de clefs, 66
droite tangente, 6

E
équation de Weierstrass
affine, 9
projective, 11

F
fonction
à sens unique, 68
avec trappe, 69
formes normales d'une courbe elliptique
affine, 10
projective, 11
formules affines d'addition
pour $\mathrm{char}\,(\mathbf{K}) \neq 2, 3$, 15
pour $\mathrm{char}\,(\mathbf{K}) = 2$, 14
pour $\mathrm{char}\,(\mathbf{K}) = 3$, 15
formules projectives d'addition
pour $\mathrm{char}\,(\mathbf{K}) \neq 2, 3$, 18
pour $\mathrm{char}\,(\mathbf{K}) = 2$, 20
pour $\mathrm{char}\,(\mathbf{K}) = 3$, 19

G
gestion de clefs, 66

I
intégrité, 62

L
logarithme discret, 69, 74
loi de groupe pour
$E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_{3^d})$, 37
$E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_{3^d})$, 37
$E_{a,b}(\mathbb{F}_{3^d}[e])$, 38, 42
$E_{a,b}(\mathbb{F}_q[e])$, 35, 37, 54

N
non-répudiation, 62
de réception, 62
de transmission, 62
d'origine, 62

O
obtention
d'information, 63
globale, 63
locale, 63
Oscar, 60

P
plan
affine, 6
projectif, 7
projectif sur un anneau, 22
point
non-singulier, 6
singulier, 6, 8
points **K**-rationnels, 9
polynôme
homogène, 8
irréductible, 6
problème
de Diffie-Hellman, 70
du conjugué, 75
du logarithme discret, 68, 69
protagonistes traditionnels, 60
protocole, 60
cryptographique, 60
de Diffie-Hellman, 70
de signature, 62
d'échange de clefs, 68

S
schéma
de communication, 60
d'un cryptosystème, 65
sécurité des cryptosystèmes, 63
basés sur R, 85
signature
numérique, 64
authentique, 64
inaltérable, 64
infalsifiable, 64
irrévocable, 64
non réutilisable, 64

système cryptographique, 60

T

texte
    chiffré, 60
    en clair, 59
triplet primitif, 21

Z

zéro d'un polynôme, 6

Résumé

Le but de cette thèse est d'étudier les applications cryptographiques des courbes elliptiques définies sur des anneaux finis et non-locaux.

Dans le premier chapitre, nous avons donné sous forme d'une introduction aux courbes elliptiques, des préliminaires nécessaires à l'élaboration de cette thèse.

Dans le deuxième chapitre, nous avons étudié des courbes elliptiques définies sur l'anneau $\mathbb{F}_q[e]$, où $e^2 = e$ et $\mathbb{F}_q$ est un corps fini d'ordre $q = p^d$, avec p un nombre premier et d un entier positif. Le résultat essentiel, que nous avons montré, est l'isomorphisme entre la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$ et le groupe $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q) \times E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$. Ce résultat nous a permis de munir la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$ d'une structure de groupe et de donner explicitement sa loi du groupe.

Dans le troisième chapitre, nous avons étudié les courbes elliptiques définies sur l'anneau $\mathbb{F}_q[e]$, où $e^3 = e^2$ et q est une puissance d'un nombre premier supérieur ou égal à 5. Après avoir classifié les points dans ces courbes elliptiques, nous avons donné explicitement leur loi de groupe.

Enfin, dans le quatrième chapitre, nous avons donné deux systèmes de chiffrement entièrement homomorphes sur ces courbes.

Mots clés : Anneau fini, Anneau non-local, Caractéristique, Corps finis, Courbes elliptiques, Cryptographie, Chiffrement entièrement homomorphe, Équation de Weierstrass, Isomorphisme, Logarithme discret.