UNIVERSITÉ ASSANE SECK DE ZIGUINCHOR

UFR SCIENCES ET TECHNOLOGIES

DÉPARTEMENT DE MATHÉMATIQUES

Mémoire de Master

DOMAINE : SCIENCES ET TECHNOLOGIES
MENTION : MATHÉMATIQUES ET APPLICATIONS
SPÉCIALITÉ : MATHÉMATIQUES PURES
OPTION : GÉOMÉTRIE ALGÉBRIQUE

Thème :

Courbes d'Edwards et Applications

Présenté par :

Adama POUYE

Sous la direction de : **Dr. Moussa FALL**
Sous la supervision de : **Pr. Oumar SALL**

Soutenu publiquement le 27 janvier 2024 devant le jury composé de :

Thomas GUEDENON	Professeur assimilé	Président du Jury	UASZ
Oumar SALL	Professeur Titulaire	Superviseur	UASZ
Mansour SANE	Maître de Conférences Titulaire	Examinateur	UASZ
Moussa FALL	Maître de Conférences Titulaire	Directeur	UASZ

Année universitaire : 2022-2023

Remerciement

Je voudrais tout d'abord exprimer toute ma reconnaissance à mon directeur de mémoire Docteur Moussa FALL, qui m'a donné la chance de travailler avec lui, et dont ses nombreuses suggestions m'ont aidé à clarifier et mieux présenter les idées développées dans ce mémoire. Je tiens également à exprimer ma profonde gratitude au Professeur Oumar SALL qui a supervisé ce travail. Je le remercie pour ses remarques scientifiques constructives et ses grandes qualités humaines. Je tiens à remercier Professeur Thomas GUEDENON, d'avoir accepté de présider le jury et Docteur Mansour SANE d'avoir accepté d'être membres du jury.
Je voudrais remercier aussi Professeur Youssou FAYE du département d'informatique pour sa disponibilité, ses qualités scientifiques et ses conseils.
Qu'il me soit permis également de remercier tous les enseignants du département de mathématiques, sans oublier l'ensemble des étudiants du département de mathématiques.
Mes remerciements vont aussi à tous ceux qui ont contribué de près ou de loin à la réalisation de ce travail.
Je profite de cette occasion pour remercier aussi mes prédécesseurs Docteur Sény DIATTA, Monsieur Abdourahmane DIATTA et Monsieur Moustapha CAMARA pour l'aide et l'amitié qu'ils m'ont apporté, ainsi que les échanges et discussions autour des mathématiques.
Merci à tous mes amis, en particulier Mouhamadou Racine NDIAYE, Mouhamadou Seydina MBAYE, Abdarhamane Koné, Omar PANE, Siaka DIEME, Malang BADIANE, Maurice DIATTA, Demba FALL, Youssouf MBALLO, Boubacar BALDE, Sokhna Mouhsinatou MBACKE, Aminata BA, Moustapha TOURE, Cheikh FALL, pour divers services qu'ils m'ont rendus ; je leur adresse à tous un joyeux salut amical.

DÉDICACES

☞ À notre cher et bien aimé **CHEIKH AHMADOU BAMBA KHADIM RASSOUL**,

Je voudrais, après avoir rendu grâce à **DIEU** et prié sur son prophète **Mouhamad (PSL)**, adresser mes remerciements à mon guide spirituel **Cheikh Ahmadou BAMBA** qui m'a enseigné les valeurs du travail et de l'acquisition du savoir. C'est grâce à ses écrits que j'ai eu la force qui m'a animé durant tout mon parcours de formation. Puisse **DIEU** l'élève au rang de ses élus et que celui-ci accepte mon allégeance renouvelée d'être parmi ses fidèles serviteurs **mouride**.

☞ A mon père Moussa POUYE,

Vous m'avez toujours soutenu sans faille moralement et financièrement durant mes années les plus difficiles à l'université. Je réitère toute mon affection et ma disponibilité envers vous. Je n'oublierai jamais tout ce que tu as fait pour moi, depuis ma naissance jusqu'à nos jours pour toute l'estime et l'admiration que j'ai pour toi, je te dédie ce travail. QU' ALLAH, le tout Puissant, vous accorde une longue vie.

☞ A ma maman Khoyane SAGNE,

Tous les mots du monde ne sauraient exprimer l'immense amour que je vous porte, ni la profonde gratitude que je vous témoigne pour tous les efforts et les sacrifices que vous n'avez jamais cessé de consentir pour mon instruction et mon bien-être. C'est à travers vos encouragements que j'ai opté pour cette noble chemin et c'est à travers vos critiques que je me suis réalisé. J'espère avoir répondu aux espoirs que vous avez fondus en moi. Je vous rends hommage par ce modeste travail en guise de reconnaissance éternelle et de mon infime amour. Que Dieu le Tout-puissant, vous garde et procure la santé, le bonheur et une longue vie pour que vous demeuriez le flambeau illuminant le chemin de vos enfants.

☞ A mes papas, mes très chers frères et sœurs, mes cousins et mes épouses..., Babacar POUYE, Aliou POUYE, Ndiaga POUYE, Assane POUYE, Cheikh POUYE, Rokhi POUYE, Papa NGOM, Penda NGOM, Yacine NGOM, Khoyane POUYE, Ndeye SENE, Mouhamed POUYE, Mame Diarra POUYE, Sokhna Maye POUYE, Ndiabou POUYE,...

Je n'oublierai jamais vos conseils, vos prières et vos soutiens sans cesse en tout moment. Vous

aviez toujours été présent dans les moments les plus difficiles de ma vie. Je ne peux pas exprimer à travers ses lignes mes sentiments d'amour et de tendresse envers vous. Je vous souhaite tous une longue vie et de santé.

☞ A mes amis, Mansour FAYE, Abdou NDIAYE, Aliou Badara SARR, Ndiague POUYE, Douda SENE, Cheikh BOP, Ameth SENE,...

C'est plus que des amis, c'est une famille, je remercie le bon Dieu de vous avoir mis sur mon chemin et je souhaite que cette compagnie demeure à jamais jusqu'au paradis. Merci mes frères pour l'amour et la considération que vous me portez, ce travail est le vôtre, trouvez en ma reconnaissance et ma profonde gratitude.

Résumé

Dans ce mémoire, nous étudions les courbes d'Edwards standards et leurs généralisations appelées courbes d'Edwards tordues définies sur un corps k de caractéristique différente de 2 d'équations affines $ax^2 + y^2 = 1 + dx^2y^2$ où $a, d \in k$ et $d(d-1) \neq 0$.
Dans un premier temps, nous avons d'une part utilisé le plongement de Segré pour désingulariser les courbes d'Edwards et d'autre part donné les formules de la loi de groupe de ces courbes, ensuite nous avons montré que les courbes d'Edwards sont birationnellement équivalentes aux courbes de Montgomery d'équations affines $By^2 = x^3+Ax^2+x$ où $A, B \in k$ et $B(A^2-4) \neq 0$
Dans un deuxième temps, nous avons présenté d'abord les formules de la loi de groupe sur les corps finis, ensuite étudié la cryptographie sur les courbes d'Edwards et enfin montrer que les algorithmes sont plus efficaces sur les courbes d'Edwards que sur les courbes elliptiques sous forme de Weierstrass d'équation affine : $y^2 = x^3+ax+b$ avec $a, b \in k$ et $-16(4a^3+27b^2) \neq 0$.

Table des matières

Introduction générale

En 2007, Harold M. Edwards a apporté une contribution significative dans le domaine des courbes elliptiques. Il a présenté une nouvelle forme pour ces courbes sur un corps dont la caractéristique est différente de 2. Ce travail peut être trouvé dans son article référencé comme [9]. Edwards a montré que cette forme spécifique simplifie les formules utilisées pour les courbes elliptiques. Plus précisément, cela simplifie grandement la loi d'addition de ces courbes, la rendant plus complète et unifiée.
La famille des courbes elliptiques décrites par Edwards reste le modèle le plus couramment utilisé dans les systèmes cryptographiques. Elles ont été proposées pour les applications cryptographiques par Bernstein et Lange (voir [3]). Ces courbes définies sur des corps finis, servent non seulement à des fins pratiques en termes de mesures de sécurité, mais sont également largement étudiées en raison de leurs propriétés mathématiques faciles à établir. Edwards a prouvé que toute courbe elliptique sur un corps algébriquement clos k peut être exprimée d'une manière particulière sous la forme :

$$x^2 + y^2 = c^2(1 + x^2y^2) \; ; \quad c \in k \; et \; c^5 - c \neq 0.$$

Ces équations affines sont des équations de courbes appelées courbes d'Edwards. Elles ont été généralisées dans [3] par Bernstein et Lange sous d'autres formes appelées courbes d'Edwards tordues dont les équations affines sont :

$$ax^2 + y^2 = 1 + dx^2y^2 \; ; \quad a, \, d \in k \; et \; d(d-1) \neq 0.$$

Les courbes d'Edwards tordues peuvent être considérées comme des courbes elliptiques spéciales qui sont écrites sous une nouvelle forme. Elles ont des avantages cryptographiques sur les courbes elliptiques dans la forme usuelle de Weierstrass.
L'objectif de ce mémoire est d'étudier les courbes d'Edwards sous leurs formes générales et leurs applications en cryptographie.
Nous présentons dans le premier chapitre les outils fondamentaux en géométrie algébrique qui

sont nécessaires pour la compréhension de ce mémoire.
Dans le second chapitre, nous étudions d'une part les propriétés sur les courbes d'Edwards, notamment les formules d'addition et de doublement sur la loi de groupe et d'autre part, nous prolongeons l'étude de ces courbes sur les corps finis en s'inspirant des travaux de Daniel J. Bernstein et Tanja Lange (voir [3]) qui ont prouvé qu'il y a plus de courbes utilisées sous la forme suivante en cryptographie :

$$x^2 + y^2 = c^2(1 + dx^2y^2) \; ; \quad c, \, d \in k; \; c^5 - c \neq 0 \; et \; d(d-1) \neq 0.$$

Ensuite, nous avons prouvé que toutes les courbes de cette forme sont isomorphes aux courbes de la forme :

$$x^2 + y^2 = 1 + dx^2y^2 \; ; \quad d(d-1) \neq 0.$$

Enfin, nous étudions dans le dernier chapitre leurs applications en cryptographie. Dans cette partie, nous présentons la conception de protocoles de sécurité des données afin de donner une comparaison avec le modèle de Weierstrass.

Chapitre 1

Préliminaires

Le but de ce chapitre est de rassembler quelques notions de géométrie algébrique qui seront utilisées dans ce mémoire. Nous utilisons les références, comme par exemples : D. Abramovic, J. Harris, [1], P. A. Griffiths [14], Daniel Perrin [7] et J. H. Silverman [13].

1.1 Espace affine et Espace projectif

1.1.1 Espace affine

Soient k un corps de nombres parfait et $\overline{k}$ une clôture algébrique de k. Nous définissons d'abord l'espace affine de dimension n sur k.

Définition 1.1.1 *On appelle espace affine de dimension n sur k l'ensemble*

$$\mathbb{A}^n = \mathbb{A}^n\left(\overline{k}\right) = \left\{(x_1, \cdots, x_n) \,|\, x_i \in \overline{k}\right\}.$$

L'ensemble des points k-rationnels de $\mathbb{A}^n$ est l'ensemble

$$\mathbb{A}^n(k) = \{(x_1, \cdots, x_n) \,|\, x_i \in k\}.$$

Si $x = (x_1, \cdots, x_n) \in \mathbb{A}^n$, alors les x_i sont les coordonnées de x.
A cette espace affine, on associe l'anneau $\overline{k}[X_1, \cdots, X_n]$ des polynômes à n variables par l'application :

$$P : x \longrightarrow P(x_1, \cdots, x_n).$$

Si x est un point de $\mathbb{A}^n$ et si $P(X_1, \cdots, X_n)$ est un polynôme de l'anneau précédent, on note $P(x) = P(x_1, \cdots, x_n)$.

1.1.2 Espace projectif

La motivation de la définition du plan projectif est "d'augmenter" le plan affine pour que deux droites quelconques se coupent. Pour ce faire, l'idée est d'ajouter un élément pour chaque direction ; deux droites parallèles s'intersecteront, alors par définition au "point" déterminé par leur direction. Formellement, on introduit la construction suivante : Soient k un corps et n un entier naturel. On considère la relation d'équivalence $\sim$ définie par : pour tous $x, y \in k^{n+1} - \{0\}$, on a : $x \sim y \Leftrightarrow \exists \lambda \in k^* : y = \lambda x$. Ainsi, on $x \sim y$ si et seulement si x et y sont colinéaires.

Définition 1.1.2 *On appelle espace projectif noté $\mathbb{P}^n(k)$ ou $\mathbb{P}(k^{n+1})$ l'espace des classes d'équivalence sur $k^{n+1} - \{0\}$ par la relation $\sim$. S'il y a pas de confusion sur k on note $\mathbb{P}^n$ ou bien de $\mathbb{P}^n(k)$.*

Une classe d'équivalence de $\{(\lambda x_0, \cdots, \lambda x_n)\,,\ \lambda \in k^*\}$ est notée $[x_0, \cdots, x_n]$ mais nous utiliserons dans la suite la notation $(x_0, \cdots, x_n)$.
Les scalaires $x_0, \cdots, x_n$ sont appelés coordonnées homogènes pour les points correspondants dans $\mathbb{P}^n$. L'ensemble des points k-rationnels dans $\mathbb{P}^n$ est l'ensemble

$$\mathbb{P}^n(k) = \{(x_0, x_1, \cdots, x_n) \,|\, x_i \in k\}\,.$$

La droite projective $\mathbb{P}^1$ s'interprète comme l'ensemble des directions de $\mathbb{A}^2$. Pour interpréter les dimensions supérieures, on remarque le fait suivant : Le n-espace projectif $\mathbb{P}^n$ est en bijection avec l'ensemble $\mathbb{A}^n \cup \mathbb{P}^{n-1}$. En particulier, $\mathbb{P}^2 = \mathbb{A}^2 \cup \mathbb{P}^1$, donc le plan projectif peut effectivement se voir comme le plan affine auquel on a ajouté l'ensemble des directions. On appellera points affines les éléments de la forme $(x_0, \cdots, x_{n-1}, 1)$ et points à l'infini ceux de la forme $(x_0, \cdots, x_{n-1}, 0)$.

1.2 Les courbes affines planes et les courbes projectives

1.2.1 Les courbes affines planes

Définition 1.2.1 *Une courbe affine plane $\mathcal{C}$ est un ensemble de points $(x, y) \in \mathbb{A}^2(k)$ dont les coordonnées vérifient une équation de la forme :*

$$f(x, y) = 0$$

où f est un polynôme non constant de $\overline{k}[X,Y]$. On note $\mathcal{C} = V(f)$. Le degré de $\mathcal{C}$ est celui du polynôme f.

Exemple 1.2.1 *(de courbes affines planes)*

a) Une droite affine D est une courbe affine plane d'équation $ax + by + c = 0$.

b) Une conique ou quadrique affine est une courbe affine $\mathcal{C}$ d'équation $f(x,y) = 0$, où f est un polynôme de degré 2 :

$$f(x,y) = \sum_{0\leq i,\ j,\ i+j\leq 2} a_{i,j}x^i y^j;$$

c) Une cubique affine est une courbe affine $\mathcal{C}$ d'équation $P(x,y) = 0$, où P est un polynôme de degré 3 :

$$P(x,y) = \sum_{0\leq i,\ j,\ i+j\leq 3} a_{i,j}x^i y^j;$$

d) Une quartique affine est une courbe affine $\mathcal{C}$ d'équation $P(x,y) = 0$, où P est un polynôme de degré 4 :

$$P(x,y) = \sum_{0\leq i,\ j,\ i+j\leq 4} a_{i,j}x^i y^j;$$

où les coefficients $a_{i,j}$ sont dans k.

1.2.2 Les courbes projectives planes

Définition 1.2.2 *Une courbe projective plane $\mathcal{C}$ est l'ensemble des points $P(X,Y,Z) \in \mathbb{P}^2$ dont les coordonnées vérifient une équation de la forme :*

$$F(X,Y,Z) = 0$$

où F est un polynôme homogène non constant de $\overline{k}[X,Y,Z]$. On note $\mathcal{C} = V(F)$, le degré de $\mathcal{C}$ est le degré du polynôme F.

Il est utile de savoir faire le lien entre les notions affines et projectives d'une courbe algébrique, d'où l'intérêt d'introduire la notion d'homogénéisation.

1.2.3 Homogénéisation

On a la proposition suivante qui donne le lien entre les notions affines et projectives d'une courbe algébrique plane.

Proposition 1.2.1 *Soient $\mathcal{C} = V(F)$ une courbe projective plane avec F un polynôme de $\overline{k}[X,Y,Z]$ de degré d, homogène et non constant, si $\mathcal{C}$ rencontre $\mathbb{A}^2$, alors $\mathcal{C} \cap \mathbb{A}^2$ est une courbe affine plane et $\mathcal{C} \cap \mathbb{A}^2 = V(f)$ avec $f(X,Y) = F(X,Y,1) \in \overline{k}[X,Y]$.*
Soit $\mathcal{C} = V(f)$ une courbe affine plane avec f un polynôme de degré d. La plus petite courbe projective plane contenant $\mathcal{C}$ est $\overline{\mathcal{C}} = V(F)$ avec F le polynôme homogène de $\overline{k}[X,Y,Z]$ défini par : $F(X,Y,Z) = Z^d f(\frac{X}{Z}, \frac{Y}{Z})$.

La courbe $\overline{\mathcal{C}}$ dans $\mathbb{P}^2$ est la complétion projective de $\mathcal{C}$ dans $\mathbb{A}^2$. Les points de $\overline{\mathcal{C}}$ dans le plan projectif privés des points de $\mathcal{C}$ dans le plan affine sont les points à l'infini. On notera la courbe ou sa complétion projective par $\mathcal{C}$ dans la suite.
Le passage de l'équation affine à l'équation projective est appelé homogénéisation et le passage inverse est appelé déshomogénéisation.

Exemple 1.2.2 *Dans le plan affine la courbe*

$$\mathcal{C} : y^3 - x(x-1)(x-2)(x-3) = 0$$

a pour équation homogène dans le plan projectif

$$\mathcal{C} : Y^3Z - X(X-Z)(X-2Z)(X-3Z) = 0.$$

Si une courbe est singulière on a souvent besoin de connaitre la multiplicité de la courbe aux points de singularité.

1.2.4 Point singulier et Point lisse

On a la définition suivante dans le plan affine :

Définition 1.2.3 *Un point (a,b) d'une courbe plane d'équation $\mathcal{C} : f(x,y) = 0$ est dit singulier si :*

$$\frac{\partial f}{\partial x}(a,b) = \frac{\partial f}{\partial y}(a,b) = 0.$$

Un point (a,b) d'une courbe $\mathcal{C} : f(x,y) = 0$ est dit lisse si :

$$\left(\frac{\partial f}{\partial x}(a,b), \frac{\partial f}{\partial y}(a,b)\right) \neq (0,0).$$

Ainsi on :
– La tangente en un point lisse (a, b) à $\mathcal{C}$ est la droite d'équation :

$$(x-a)\frac{\partial f}{\partial x}(a,b) + (y-b)\frac{\partial f}{\partial y}(a,b) = 0.$$

– Une courbe $\mathcal{C}$ dont tous les points sont lisses est dite lisse.

On a de façon analogue dans le plan projectif la définition suivante :

Définition 1.2.4 . *Un point $P(a, b, c)$ d'une courbe $\mathcal{C} : F(X, Y, Z) = 0$ est dit singulier si :*

$$\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = 0.$$

Un point $P(X, Y, Z)$ d'une courbe $\mathcal{C} : F(X, Y, Z) = 0$ est dit lisse si :

$$\left(\frac{\partial F}{\partial X}(P), \frac{\partial F}{\partial Y}(P), \frac{\partial F}{\partial Z}(P)\right) \neq (0,\, 0,\, 0).$$

Par conséquent :
– La courbe $\mathcal{C}$ est lisse si tous ses points sont lisses.
– L'équation de la tangente à la courbe en un point lisse P est donnée par la formule suivante :

$$X\frac{\partial F}{\partial X}(P) + Y\frac{\partial F}{\partial Y}(P) + Z\frac{\partial F}{\partial Z}(P) = 0.$$

1.2.5 Multiplicité

Définition 1.2.5 *Soient $P(a, b)$ un point de $\mathcal{C}$ et $f(x, y) = 0$ une équation de $\mathcal{C}$ qui peut s'écrire sous la forme polynomiale en $X - a$ et $Y - b$ dont les coefficients sont dans k, c'est-à-dire :*

$$f(X, Y) = f_m(X - a, Y - b) + \cdots + f_d(X - a, Y - b)$$

où les f_i sont des polynômes homogènes de degré i en $X - a$ et $Y - b$.
Le plus petit entier m tel que $f_m \neq 0$ est la multiplicité de $\mathcal{C}$ ou de f au point P. Elle est notée $m_P(\mathcal{C})$.

Si $m_P(\mathcal{C}) = 1$, alors P est un point régulier et si $m_P(\mathcal{C}) \neq 1$, alors P est un point singulier (ou multiple) de $\mathcal{C}$.
En particulier :

- si $m_P(\mathcal{C}) = 2$, alors P est point singulier double ;
- si $m_P(\mathcal{C}) = 3$, alors P est point singulier triple.

Dans la suite, on est souvent amené à déterminer l'intersection de deux courbes. Le théorème de Bézout nous renseigne sur le cardinal de leur intersection.

1.2.6 Le théorème de Bézout

Proposition 1.2.2 *(Bézout faible)*
Soient deux courbes planes $\mathcal{C}$ et $\mathcal{C}'$ d'équations respectives $f = 0$ et $g = 0$ de degrés respectifs m et n. Alors

- *soient les polynômes f et g ont un facteur commun ;*
- *soit $\#(\mathcal{C} \cap \mathcal{C}') \leq mn$.*

On suppose maintenant que le corps est algébriquement clos, alors on a le théorème de Bézout suivant :

Théorème 1.2.1 *Soient $\mathcal{C}$ et $\mathcal{C}'$ deux courbes projectives planes de degrés respectifs n et m, sans composantes irréductibles communes. Alors elles s'intersectent en mn points (comptés avec multiplicités).*

Voir le livre de Daniel Perin [7] pour la preuve.

1.3 Les courbes elliptiques

1.3.1 Rappels sur les corps finis

Définition 1.3.1 *Un corps F est dit fini si son cardinal (nombre d'éléments) est fini. Le nombre d'éléments est l'ordre du corps souvent noté q qui peut être représenté par la puissance d'un nombre premier c'est-à-dire $q = p^n$, où p est un nombre premier, appelé la caractéristique du corps, et $n \in \mathbb{N}$.*

L'étude de la cryptographie sur les courbes elliptiques portera essentiellement sur les deux types de corps suivants :
— **Corps premier** : un corps est dit premier, noté F_p s'il n'a pas de sous-corps autre que lui-même. Les $\mathbb{Z}/p\mathbb{Z}$ avec p premier sont des corps premiers finis. Le corps est constitué des nombres entiers $\{0, 1, 2, \cdots, p-1\}$.
— **Corps binaire** : un corps fini d'ordre 2^n est un corps binaire, noté F_{2^n} qu'on peut construire en utilisant une représentation polynômiale, les éléments du corps sont des polynômes binaires et les degrés sont inférieurs à n :
$F_{2^n} = \left\{a_{n-1}Z^{n-1} + a_{n-2}Z^{n-2} + \cdots + a_1 Z + a_0 \mid a_i \in \{0, 1\}\right\}$.

1.3.2 Équation de Weierstrass

Une courbe elliptique sur un corps k est la donnée d'une équation affine de la forme :

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

avec les coefficients a_1, a_2, a_3, a_4, a_6 appartenant à k, cette équation est appelée forme de Weierstrass. Ces coefficients sont choisis de sorte que E soit lisse et admet un unique point à l'infini noté O_E.
Lorsque k est de caractéristique strictement supérieur à 3 le changement de variables :

$$(x, y) \longmapsto \left(x - \frac{a_1^2 + 4a_2}{12}, y - \frac{a_1}{2}\left(\frac{a_1^2 + 4a_2}{12} - \frac{a_1}{2}\right)\right)$$

permet de simplifier l'équation de Weierstrass sous la forme :

$$E_W : y^2 = x^3 + ax + b$$

avec $a, b \in k$ et $\triangle = -16(4a^3 + 27b^2) \neq 0$, où $\triangle$ est le discriminant de cette courbe (critère de non singularité).

1.3.3 Loi de groupe

Supposons que E soit une courbe elliptique définie sur un corps fini k, noté E/k. Il existe une loi appelée **Sécante-tangente**, qui a deux points $P = (x_p, y_p)$ et $Q = (x_q, y_q)$ de E/k associe un troisième point de E/k.
L'ensemble des points $E(k) \cup \{O\}$ fourni par cette loi représentée par $+$ forme un groupe commutatif. Ce groupe se compose de deux opérations basées sur le doublement et l'addition de deux points différents sur la courbe.
Nous définissons cela géométriquement en considérant deux points $P = (x_p, y_p)$ et $Q = (x_q, y_q)$ différents du point à l'infini de la courbe elliptique sur le corps fini k.

- L'addition de deux points $(P + Q)$ avec $P \neq Q$ consiste à prendre le symétrique du point d'intersection de la droite (PQ) avec la courbe par rapport à l'axe des abscisses.
- Le doublement d'un point est le cas d'addition où $P = Q$ on prend, alors le symétrique du point d'intersection de la tangente en P avec la courbe elliptique. Dans ce cas P et Q sont symétriques par rapport à l'axe des abscisses, la droite (PQ) coupe la courbe au point à l'infini (le zéro du groupe) et donc $Q = -P$.

Les figures suivantes décrivent géométriquement les opérations de la loi de groupe.

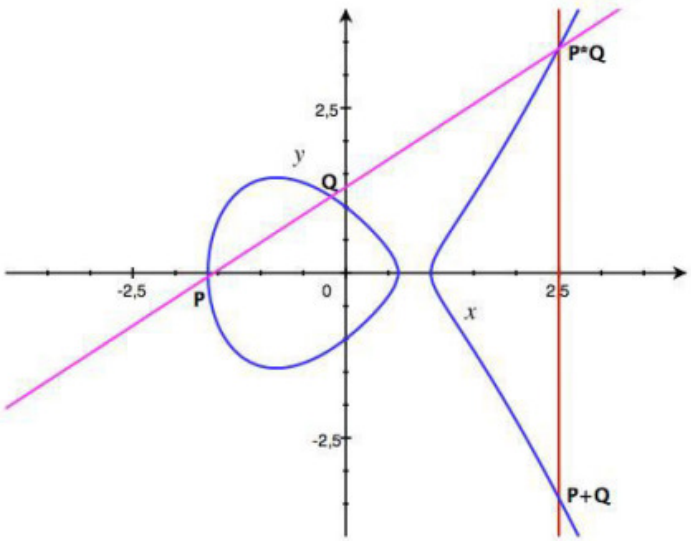

FIGURE 1.1 – Addition de points

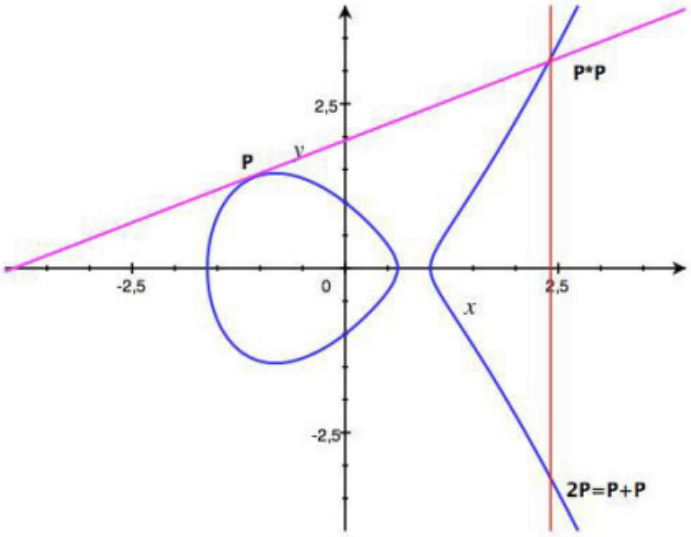

FIGURE 1.2 – Doublement de points

Ces opérations peuvent être calculées de façon algébrique, selon la nature du corps de base la formule d'addition diffère. Soit $k = \mathbb{F}_p$ le corps fini à q éléments, avec $q = p^m$ une puissance avec $m > 3$, considérons l'équation simplifiée de Weierstrass. L'addition $P+Q = (x_{pq}, y_{pq})$ ou le doublement de points $2P = P + Q = (x_{pq}, y_{pq})$, si $P = Q$ se calcule à travers les équations suivantes :

$$\begin{cases} x_{pq} = \lambda^2 - x_p - x_q, \\ y_{pq} = \lambda(x_p - x_{pq}) - y_p, \end{cases}$$

où le scalaire λ est donné par les formules suivantes :

$$\begin{cases} \lambda = \dfrac{y_q - y_p}{x_q - x_p}, \ si \ P \neq Q \\ \lambda = \dfrac{3x_p^2 + a}{2y_p}, \ si \ P = Q. \end{cases}$$

Chapitre 2

Les Courbes d'Edwards

Edwards a introduit deux formes de courbes : les courbes d'Edwards standards et les courbes d'Edwards tordues. Avant d'aborder les courbes d'Edwards tordues, nous passons brièvement en revue les courbes d'Edwards les plus connues et leurs opérations de loi de groupe.

2.1 Définitions des Courbes d'Edwards

La forme originale d'une courbe d'Edwards, proposée par Harold Edwards en 2007, est la forme normale suivante (voir [9]) :

Définition 2.1.1 *Une courbe d'Edwards sur un corps k de caractéristique différente de 2 est une courbe d'équation affine de la forme :*

$$x^2 + y^2 = c^2 + c^2x^2y^2$$

où $c \in k$ *et* $c^5 - c \neq 0$.

En faisant quelques changement sur le paramètre c, on obtient la définition suivante des courbes d'Edwards donnée par Bernstein et Lange (voir [3]).

Définition 2.1.2 *Une courbe d'Edwards sur un corps k de caractéristique différente de 2 est une courbe d'équation affine de la forme :*

$$x^2 + y^2 = 1 + dx^2y^2$$

où $d \in k$ *et* $d(d-1) \neq 0$.

Nous retiendrons dans la suite cette définition précédente comme celle des courbes d'Edwards. Les courbes d'Edwards sont des quartiques possédant deux points singuliers qui sont les deux points à l'infini que nous notons $\infty+ = (0,1,0)$ et $\infty- = (1,0,0)$ de multiplicité 2.
La désingularisée d'une courbe d'Edwards est donc une courbe plane lisse qui est l'intersection de deux quadriques $XY = ZT$ et $X^2 + Y^2 = Z^2 + dT^2$.
Elles possèdent le point k-rationnel $(0,1,1,0)$ dans l'espace projectif, ce sont donc des courbes elliptiques. Ainsi la définition rigoureuse d'une courbe d'Edwards est la suivante :

Définition 2.1.3 *Soient k un corps de caractéristique différente de 2 et $d \in k$ avec $d(d-1) \neq 0$. On appelle courbes d'Edwards les courbes elliptiques définies par l'intersection dans $\mathbb{P}^3$ de deux quadriques suivantes $XY = ZT$ et $X^2 + Y^2 = Z^2 + dT^2$.*

2.2 Désingularisation des courbes d'Edwards

Pour désingulariser une courbe d'Edwards, on utilise le plongement de Segré.

2.2.1 Plongement de Segré

Soient $X = (X_0, \cdots, X_n) \in \mathbb{P}^n$ et $Y = (Y_0, \cdots, Y_m) \in \mathbb{P}^n$. On désigne par $k[X,Y]$ l'anneau $k[X_0, \cdots, X_n, Y_0, \cdots, Y_m]$.

Définition 2.2.1 *Un polynôme $F \in k[X,Y]$ est bihomogène de bidegré (d,e) s'il vérifie, pour tous $\lambda, \mu \in k$,*

$$F(\lambda X_1, \cdots, \lambda X_n, \mu Y_1, \cdots, \mu Y_m) = \lambda^d \mu^e F(X_1, \cdots, X_n, Y_1, \cdots, Y_m).$$

Considérons S une partie quelconque de $k[X,Y]$ formée des polynômes bihomogènes. On note :

$$V(S) = \{(x,y) \in \mathbb{P}^n \times \mathbb{P}^m \mid \forall F \in S, F(x,y) = 0\},$$

le sous-ensemble de $\mathbb{P}^n \times \mathbb{P}^m$ formé par l'ensemble des zéros communs à tous les polynômes de S. Les sous-ensembles de ce type sont des sous-variétés projectives.
Fixons deux entiers naturels n et m strictement positifs et considérons le produit $\mathbb{P}^n \times \mathbb{P}^m$ des espaces projectifs de dimensions respectives n et m avec le système de coordonnées homogènes de $\mathbb{P}^N$ où $N = (n+1)(m+1) - 1 = nm + n + m$. On peut maintenant donner la définition.

Définition 2.2.2 *On fixe un corps k et deux entiers naturels m, n et on considère le produit fibré $\mathbb{P}^n \times \mathbb{P}^m$ des espaces projectifs de dimensions m et n. Alors il existe un morphisme de variétés algébriques*

$$f : \mathbb{P}^n \times \mathbb{P}^m \longrightarrow \mathbb{P}^{nm+n+m},$$

qui est une immersion fermée (i.e. f induit un isomorphisme sur son image) qui est une sous-variété fermée de $\mathbb{P}^{nm+n+m}$. De plus, au niveau des points rationnels, on a :

$$f((x_0, \ldots, x_n), (y_0, \ldots, y_m)) = (x_0y_0, x_0y_1, \ldots, x_0y_m, x_1y_0, \ldots, x_ny_m).$$

Cette immersion est appelée le plongement de Segré (voir [12]) .

2.2.2 Désingularisation

Nous allons construire un morphisme birationnel sur le corps k entre la définition rigoureuse des courbes d'Edwards donnée par la définition 2.1.3 et les courbes d'Edwards (singulières) données par la définition 2.1.2. L'idée est de remarquer que la donnée supplémentaire du produit $p(x, y) = xy$ définit un plongement dans $\mathbb{P}^3$.
On représente les points $(x, y) \in \mathbb{A}^1 \times \mathbb{A}^1$ par les points $((x, w); (y, z)) \in \mathbb{P}^1 \times \mathbb{P}^1$.
Considérons le plongement de segré définie par :

$$f : \mathbb{P}^1 \times \mathbb{P}^1 \longrightarrow \mathbb{P}^3, \qquad f((x, w), (y, z)) = (xy, xz, wy, wz).$$

Soit (x, y) un point sur la courbe d'équation affine

$$E_{d_1} : x^2 + y^2 = 1 + dx^2y^2.$$

En appliquant les permutations $(xy, xz, wy, wz) \leftrightarrow (xz, yw, xy, wz)$ et en effectuant les changements $X = xz$, $Y = yw$, $T = xy$, $Z = wz$; ces derniers vérifient l'équation :

$$(xy)^2 + (xz)^2 = (wy)^2 + d(wz)^2 \Longleftrightarrow X^2 + Y^2 = Z^2 + dT^2 \; et \; XY = ZT.$$

Donc $(X, Y, T, Z) \in \mathbb{P}^3$ vérifie l'équation de la courbe elliptique lisse d'équation projective

$$E_{d_2} : X^2 + Y^2 = Z^2 + dT^2 \; et \; XY = ZT.$$

On en déduit que E_{d_2} est une désingularisation de la courbe E_{d_1}.

2.3 Loi de groupe sur les courbes d'Edwards

Dans la référence [4], Daniel J. Bernstein et Tanja Lange montrent que cette famille de courbes a sa forme d'addition et de doublement unifiée qui donne une loi d'addition complète sous la condition que le paramètre d ne soit pas un carré dans le corps k.
Nous présentons dans cette section la loi de groupe sur les courbes d'Edwards en coordonnées affines et en cordonnées projectives (voir [4]) qui donne la formule d'addition de deux points.

2.3.1 Formules en coordonnées affines

Soit E_d une courbe d'Edwards donnée par $E_d : x^2+y^2 = 1+dx^2y^2$ telle que $dx^2y^2 \neq \pm 1$. Soit $P_i = (x_i, y_i)$ un point de la courbe E_d, alors $-P_i = (-x_i, y_i), \forall i \in \mathbb{N}$. Soit maintenant $P_1 + P_2 = P_3$ avec $P_i = (x_i, y_i) \in E_d$ pour $i = 1, 2, 3$. Dans ce cas :

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3) = \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right).$$

Le point $(0, 1)$ est l'élément neutre et est appelé point à l'infini. Le point $-(x_1, y_1) = (-x_1, y_1)$ est l'élément opposé de (x_1, y_1). Notons que ces éléments sont différents de l'identité et de l'inverse de la forme de Weierstrass (voir [8]). Pour tous points (x_1, y_1) et (x_2, y_2) dans E_d, cette loi est complète et fortement unifiée lorsque $dx_1y_1x_2y_2 \neq \pm 1$: les dénominateurs ne sont jamais nuls et il n'y a pas d'exception pour les doublements, les inverses, etc. Le doublement d'un point sur une courbe d'Edwards est donné simplement par :

$$2(x_1, y_1) = \left(\frac{2x_1y_1}{1 + dx_1^2y_1^2}, \frac{y_1^2 - x_1^2}{1 - dx_1^2y_1^2} \right).$$

Ces formules en coordonnées affines nous permettent de déduire les formules en cordonnées projectives par homogénéisation.

2.3.2 Formules en coordonnées projectives

Soient X, Y, Z des éléments de k avec $Z \neq 0$ tels que $(x, y) = (\frac{X}{Z}, \frac{Y}{Z})$, E_d devient, alors :

$$E_d : Z^2(X^2 + Y^2) = Z^4 + dX^2Y^2.$$

Ainsi dans leur article (voir [5]), Daniel J. Berntein et Tanja Lange présentent la loi d'addition comme suite :

- $-(X, Y, Z) = (-X, Y, Z)$;
- $\infty = (0, 1, 0)$ ou $\infty = (1, 0, 0)$;

- $\begin{cases} X_3 = Z_1Z_2(X_1Y_2 + X_2Y_1)(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2) \\ Y_3 = Z_1Z_2(Y_1Y_2 - X_1X_2)(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2) \\ Z_3 = Z_1^4Z_2^4 - (dX_1X_2Y_1Y_2)^2. \end{cases}$

En effet, en posant $(x, y) = \left(\frac{X}{Z}, \frac{Y}{Z}\right)$, alors la formule

$$(x_3, y_3) = \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}\right)$$

devient $\left(\frac{X_3}{Z_3}, \frac{Y_3}{Z_3}\right) =$

$$\left(\frac{Z_1Z_2(X_1Y_2 + X_2Y_1)(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)}{Z_1^4Z_2^4 - (dX_1X_2Y_1Y_2)^2}, \frac{Z_1Z_2(Y_1Y_2 - X_1X_2)(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2)}{Z_1^4Z_2^4 - (dX_1X_2Y_1Y_2)^2}\right).$$

Par identification, on trouve les expressions de $X_3, Y_3\, et\, Z_3$ ci-dessus .

2.4 Quatre points spéciaux

L'équation d'une courbe d'Edwards est symétrique en ce sens que les rôles de x et y peuvent être intervertis. Si l'on a une solution (x, y), il s'ensuit que $(\pm x, \pm y)$ et $(\pm y, \pm x)$ sont également des solutions. Il est facile de trouver quatre solutions à l'équation, à savoir $(0, 1), (0, -1), (1, 0)\, et\, (-1, 0)$.

Avec ces quatre points on peut créer un groupe d'automorphismes D_4, donné par :

$S : P \dashrightarrow \pm P + Q$ où $Q \in \{(0, 1), (0, -1), (1, 0), (-1, 0)\}$.

Ce groupe est constitué :

— des réflexions sur les droites passant par $(0, 0)$ et les points Q ;

— des droites $x = \pm y$;

— des rotations sur un angle de $\dfrac{n\pi}{2}$ pour $0 \leqslant n \leqslant 3$.

Ainsi , D_4 est composé de 8 éléments.

Les opérations de S peuvent être considérées comme les deux opérations changeant les rotations r de x et y et changeant les signes de x et /ou y. On a ainsi,

— $(x, y) + (0, 1) = (x, y)$ et $(-x, y) + (0, 1) = (-x, y)$;

— $(x, y) + (0, -1) = (-x, -y)$ et $(-x, y) + (0, -1) = (x, -y)$.

Notons que les points $(0, 1), (0, -1), (1, 0)\, et\, (-1, 0)$ appartiennent à la courbe d'Edwards E_d.

Les huit résultats pour $S(x, y)$ sont représentés sur la figure suivante :

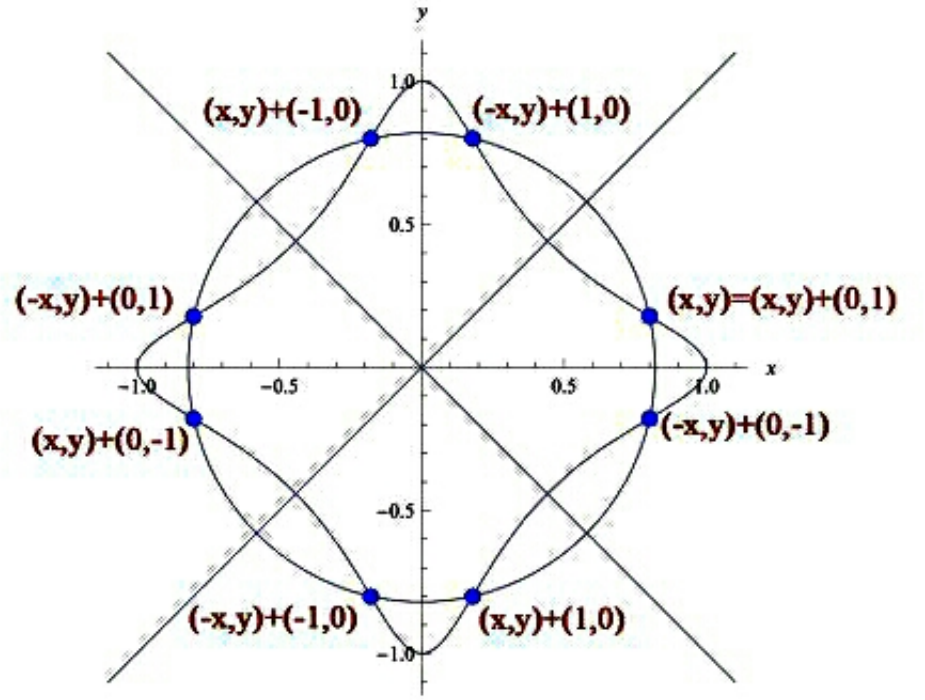

FIGURE 2.1 – La courbe d'Edwards pour $d = -16$.

2.5 Courbes d'Edwards tordues

Une courbe d'Edwards tordue est une généralisation d'une courbe d'Edwards. Cette généralisation a été présentée par Daniel J. Bernstein Lange dans leur article (voir [2]).

Définition 2.5.1 *Soient k un corps de caractéristique $p \neq 2$ et $a, d \in k$ tels que $a \neq 0$ et $d(d-1) \neq 0$, alors la généralisation d'une courbe d'Edwards est donnée par l'équation :*

$$E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2.$$

La courbe $E_{a,d}$ est appelée courbe d'Edwards tordue. Leurs équations projectives sont données par :

$$E_{a,d} : (aX^2 + Y^2)Z^4 = Z^4 + dX^2Z^2.$$

On a la proposition suivante :

Proposition 2.5.1 *La courbe d'Edwards tordue $E_{a,d}$ et la courbe d'Edwards standard E_d sont birationnellement équivalentes.*

Preuve 2.5.1 *Considérons l'application :*

$$\varphi : k^2 \longrightarrow \left(k(\sqrt{a})\right)^2$$
$$(x, y) \longmapsto (\frac{x}{\sqrt{a}}, y).$$

Cette application permet de créer un isomorphisme de $E_{1,\frac{d}{a}}$ à $E_{a,d}$ dans $k(\sqrt{a})$.

Dans certain cas, il est plus facile de manipuler $E_{a,d}$ pour éviter de calculer $\frac{d}{a}$ comme il se fait dans le cas non généralisé où on utilise $E_{1,\frac{d}{a}}$.

Exemple 2.5.1 *Voici la représentation d'une courbe d'Edwards tordue.*

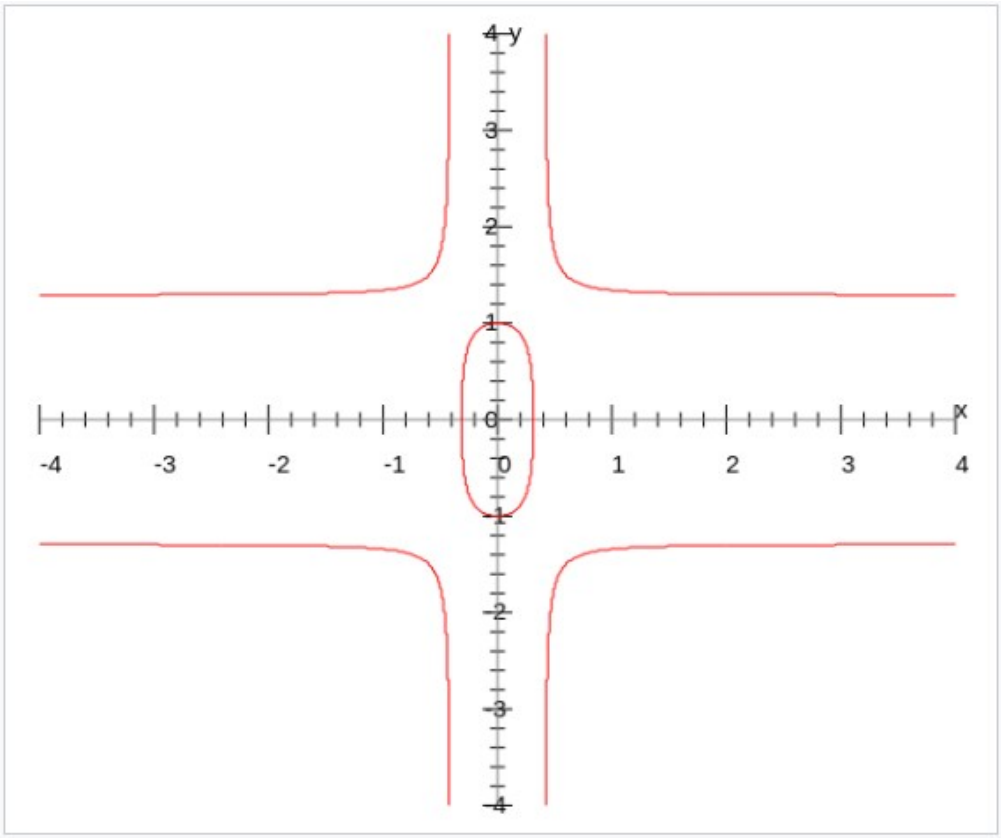

FIGURE 2.2 – La courbe d'Edwards tordue pour $a = 10$ et $d = 6$

Comme dans le cas standard, les courbes d'Edwards tordues ont aussi leur formule d'addition et de doublement unifiées et aussi la loi est complète sous condition que le paramètre a soit un carré dans k et que d ne le soit pas.
En coordonnées affines, la loi est donnée dans la définition suivante :

Définition 2.5.2 *Soient* $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ *et* $P_3 = (x_3, y_3)$ *des points de* $E_{a,d}$. *Alors la loi d'addition est donnée par :*

- $-(x, y) = (-x, y)$;
- $\infty = (0, 1)$;
- $P_1 + P_2 = P_3$; *avec* $(x_3, y_3) = \left(\dfrac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \dfrac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \right)$.

En particulier :
$2P_1 = P_3$ *avec* $(x_3, y_3) = \left(\dfrac{2x_1y_1}{1 + dx_1^2y_1^2}, \dfrac{y_1^2 - ax_1^2}{1 - dx_1^2y_1^2} \right) = \left(\dfrac{2x_1y_1}{1 + x_1^2 + y_1^2}, \dfrac{y_1^2 - ax_1^2}{2 - ax_1^2 - y_1^2} \right)$.

En coordonnées projectives la loi est définie par :

Définition 2.5.3 *Soient* $P_1 = (X_1, Y_1, Z_1), P_2 = (X_2, Y_2, Z_2)$ *et* $P_3 = (X_3, Y_3, Z_3)$, *alors la loi d'addition est donnée par :*

- $-(X, Y, Z) = (-X, Y, Z)$;
- $\infty = (0, 1, 1)$;
- $\begin{cases} X_3 = Z_1Z_2(X_1Y_2 + X_2Y_1)(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2) \\ Y_3 = Z_1Z_2(Y_1Y_2 - aX_1X_2)(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2) \\ Z_3 = Z_1^4Z_2^4 + (dX_1X_2Y_1Y_2)^2. \end{cases}$

2.6 Équivalence birationnelle entre les courbes d'Edwards tordues et les courbes de Montgomery

Les courbes de Montgomery d'équations affines $By^2 = x^3 + Ax^2 + x$ où $A, B \in k$ et $B(A^2 - 4) \neq 0$, comparées à celles d'Edwards forment une famille de courbes avec des propriétés particulièrement similaires.
En particulier, les courbes d'Edwards ont un point d'ordre 4 et d'ordre 2 respectivement en $(1, 0)$ et en $(0, -1)$. Les courbes de Montgomery ont un point d'ordre 2 en $(0, 0)$ et, sur les corps finis, au moins un point d'ordre 2 en $(0, 0)$ et en $(0, -1)$, ou un point d'ordre 4 se doublant $(0, 0)$ ou

bien deux autres points d'ordre 2.
Les mêmes règles s'appliquent pour les courbes d'Edwards tordues.
Pour chaque courbe d'Edwards tordue, il existe une équivalence birationnelle avec une courbe de Montgomery à un changement de coordonnés prés. En effet, soit

$$E_{a,d} : au^2 + v^2 = 1 + du^2v^2,$$

une courbe d'Edwards tordue, considérons l'application suivante :

$$\begin{aligned} \varphi : k^2 &\longrightarrow (k - \{1\})^2 \\ (x, y) &\longmapsto \left(\frac{1+v}{1-v}, \frac{1+v}{u(1-v)} \right). \end{aligned}$$

D'autre part, posons

$$A = 2\frac{a+d}{a-d} \quad et \quad B = \frac{4}{a-d}$$

les paramètres satisfont :

$$a = \frac{A+2}{B} \quad et \quad b = \frac{A-2}{B}.$$

Si $A = 0$, alors $a + b = a - b$ donc $b = 0$, contradiction ; si $a = -2$ dans ce cas $a = 0$, d'où une contradiction. Donc $E_{A,B}$ est une courbe de Montgomery. Cette application donne un isomorphisme qui permet de passer d'une courbe d'Edwards tordue à une courbe de Montgomery de la forme :

$$E_{A,B} : By^2 = x^3 + Ax^2 + x.$$

De même, on passe de la courbe de Montgomery à la courbe d'Edwards tordue en posant

$$u = \frac{x}{y} \quad et \quad v = \frac{x-1}{x+1}.$$

Avec des paramètres donnés par :

$$a = \frac{A+2}{B} \quad et \quad b = \frac{A-2}{B}.$$

Notons que les cas exceptionnels c'est-à-dire $v = 0$ et $u = 1$ ne se produisent que pour un nombre fini de points (u, v) sur $E_{A,B}$.

2.7 Courbes d'Edwards sur F_{2^m}

Bernstein Lange et Rezaeian Farashahi dans [6] ont introduit les courbes d'Edwards sur les corps finis F_{2^m} où m est un entier non nul. Nous présentons quelques résultats tirés de leur article de référence [6].

Définition 2.7.1 *Soient k un corps de caractéristique 2 et $d_1, d_2 \in k$ tels que $d_1(d_2+d_1^2+d_1) \neq 0$. La courbe d'Edwards binaires E_{B,d_1,d_2} est définie par l'équation affine*

$$E_{B,d_1,d_2} : d_1(x+y) + d_2(x^2+y^2) = xy + xy(x+y) + x^2y^2.$$

On définit ainsi la loi d'addition en affine et en projective sur les courbes d'Edwards binaires comme suit :

2.7.1 Formules en coordonnées affines

La loi d'addition est définie dans la proposition suivante :

Proposition 2.7.1 *Soient $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ et $P_3 = (x_3, y_3)$ des points sur $E_{a,d}$. Alors la loi d'addition est donnée par :*

- $-(x_1, y_1) = (y_1, x_1)$;
- $\infty = (0, 0)$;
- $P_1 + P_2 = P_3$; *avec*

$$x_3 = \frac{d_1(x_1+x_2) + d_2(x_1+y_1)(x_2+y_2) + (x_1+x_1^2)(x_2(y_1+y_2+1)+y_1y_2)}{d_1 + (x_1+x_1^2)(y_2+x_2)},$$

$$y_3 = \frac{d_1(y_1+y_2) + d_2(x_1+y_1)(x_2+y_2) + (y_1+y_1^2)(y_2(x_1+x_2+1)+x_1x_2)}{d_1 + (y_1+y_1^2)(y_2+x_2)},$$

d_1 et d_2 sont des éléments de k tels que $d_1 \neq 0$ et $d_2 \neq d_1^2 + d_1$.

2.7.2 Formules en coordonnées projectives

Soient X, Y, Z des éléments de k avec $Z \neq 0$ et $(x, y) = (\frac{X}{Z}, \frac{Y}{Z})$ l'équation E_{B,d_1,d_2} s'écrit en coordonnées projectives

$$E_{B,d_1,d_2} : d_1(X+Y)Z^3 + d_2(X^2+Y^2)Z^2 = XYZ^2 + XY(X+Y)Z + X^2Y^2.$$

La loi d'addition est donnée par la proposition suivante :

Proposition 2.7.2 *Soient les points de E_{B,d_1,d_2} de coordonnées $P_1 = (X_1, Y_1, Z_1)$, $P_2 = (X_2, Y_2, Z_2)$ et $P_3 = (X_3, Y_3, Z_3)$. Alors la loi d'addition est donnée par :*

- $-(X_1, Y_1, Z_1) = (-X_1, Y_1, Z_1)$;
- $\infty = (0, 0, 1)$;

- *On pose* $W_1 = X_1, Y_1,\ W_2 = (X_2, Y_2),\ A = X_1(X_1, Z_1), B = Y_1(Y_1 + Z_1),$ $C = Z_1 Z_2,\ D = W_2 Z_2,\ E = d_1 C^2,\ H = (d_1 Z_2 + d_2 W_2) W_1 C,\ I = d_1 C Z_1,$ $U = AD,\ V = E + BD\ et\ S = UV$

$$\begin{cases} X_3 = SY_1 + (H + X_2(I + A(Y_2 + Z_2)))VZ_1 \\ Y_3 = SX_1 + (H + Y_2(I + B(X_2 + Z_2)))UZ_1 \\ Z_3 = SZ_1. \end{cases}$$

Cette loi d'addition est complète lorsqu'il n'existe pas un nombre $t \in k$ tel que $t^2 + t + d_2 = 0$.

Chapitre 3

Courbes d'Edwards et Applications

3.1 Problème du logarithme discret

Considérons P un point d'ordre N ($N \in \mathbb{N}$) sur une courbe elliptique E définie sur un corps de nombres k et Q un point dans le sous-groupe H généré par P ($H =< P >$). Il existe un entier n dans l'ensemble $\{0, N-1\}$ tel que $Q = [n]P$ et est appelé le logarithme discret de Q en base P et on le note log_P. Pour chiffrer un message via une courbe elliptique, il est nécessaire de calculer l'entier n à partir des données publiques (H, P, Q). Cet algorithme consistant à calculer successivement P, $2P$, $3P...$, nP et nécessite de faire n additions dans $(E, +)$ ce qui n'est pas efficace. Ainsi, le problème du logarithme discret dans un ensemble est de trouver l'entier n à partir des données globales, et la sécurité du protocole basée sur la courbe elliptique dépend de la résolution de ce problème.

3.2 Le systèmes RSA

Actuellement, avec les progrès des nouvelles technologies de la communication, l'échange des informations confidentielles de manière sécurisée est devenu un besoin obligatoire. La cryptographie est une science ancienne toujours réinitialisée.
Ainsi le système RSA inventé par Ronald Rivest, Adi Samir et Leonard Adleman en 1977 (voir [15]) est un moyen de sécurisation de données à clé publique qui est un système universel servant dans plusieurs applications de ce domaine.
Le fonctionnement du système RSA est basé principalement sur le théorème ci-dessous :

Théorème 3.2.1 *Soient p et q deux nombres premiers, et posons $n = p \times q$. Soit e un entier*

premier avec $(p-1)\times(q-1)$*, alors il existe un entier* $d>0$ *et un entier* m *tels que :*

$$d\times e+m\times(p-1)(q-1)=1.$$

Notons au passage que si on choisit d *positif et inférieur à* $(p-1)(q-1)$*, alors* d *est unique. On note* a^m *le nombre* a *élevé à la puissance* m*, c'est-à-dire le nombre* a *multiplié par lui-même* m *fois. Pour tout entier* $a<n$ *premier avec* n*, le reste de la division de* $a^{e\times d}$ *par* n *est égal à* a*.*

Preuve 3.2.1 *Le reste de la division de* x *par* n *vaut* y *s'exprime en langage mathématique :* x *est congru à* y *modulo* n *et se note* $x\equiv y[n]$*. Cette notation est utilisée dans la suite de cette preuve.*
On appelle φ *la fonction indicatrice d'Euler, c'est-à-dire la fonction qui associe à tout entier naturel* n *le nombre de nombres premiers avec* n *dans l'ensemble* $\{1,\cdots,n\}$*.*
Pour un nombre premier p*, on a* $\varphi(p)=p-1$ *car seuls* 1 *et* p *ne sont pas premiers avec* p *dans l'ensemble* $\{1,\cdots,n\}$*.*
D'autre part, on a $\varphi(p\times q)=(p-1)\times(q-1)$ *pour* p *et* q *deux nombres premiers distincts. En effet, les seuls nombres entiers compris entre* 1 *et* $p\times q$ *qui ne sont pas premiers avec* $p\times q$ *sont les multiples de* p *ou de* q*. Il y a exactement* p *multiples de* q *dans* $\{1,\cdots,p\times q\}$ *et* q *multiples de* p*. L'entier* $p\times q$ *est à la fois multiple de* p *et de* q*, donc on a* $p+q-1$ *diviseurs de* $p\times q$ *distincts dans l'ensemble* $\{1,\cdots,p\times q\}$*, donc* $\varphi(p\times q)=p\times q-p-q+1=(p-1)(q-1)$*.*
Le petit théorème de Fermat généralisé nous assure que pour tout entier a *premier avec un entier* n*, on a :* $a^{\varphi(n)}\equiv 1[n]$*. Comme* e *est supposé premier avec* $(p-1)(q-1)$*, on sait d'après le théorème de Bezout qu'il existe un entier* d *tel que* $e\times d=1+m\times(p-1)(q-1)$*.*
Soit a *un nombre premier avec* $p\times q$*. On a*

$$\begin{aligned}a^{ed}&=a^{1+m\times(p-1)(q-1)}\\&=a\times(a^{\varphi(p\times q)})^m\\&\equiv a\times 1^m[p\times q]\\&=a.\end{aligned}$$

En utilisant le petit théorème de Fermat généralisé, on déduit, alors le protocole RSA pour le codage (voir [10]).

3.2.1 Génération de clés

Alice et Bob veulent communiquer sans que personne ne sache ce qu'ils veulent dire, alors Alice procède comme suite :

— elle choisit deux grands nombres suffisamment grands p et q ;
— ensuite, elle calcule $n = p * q$ et $\varphi(n) = \varphi(p * q) = (p-1)(q-1)$ et détermine e tel que $e \wedge \varphi(n) = 1$, c'est-à-dire $PGCD(e, \varphi(n)) = 1$;
— elle détermine d tel que $ed \equiv 1\, mod(\varphi(n))$;
— le couple (d, n) est la clé privée d'Alice et (e, n) sa clé publique.

3.2.2 Chiffrement

Bob procède ainsi :
— il prend la clé publique (e, n) d'Alice ;
— il choisit un message $M \in \mathbb{Z}/n\mathbb{Z}$;
— ensuite, il calcule $C = M^e \, mod\, n$ qui est le message chiffré et le transmet à Alice.

3.2.3 Déchiffrement

Alice déchiffre le message C en utilisant sa clé privée d puis calcule $C^d \, mod\, n = M^{ed}$, comme il existe m tel que $ed - m\varphi(n) = 1$ donc

$$\begin{aligned} C^d \, mod\, n &= M^{1+m\varphi(n)} \\ &= M(M^{\varphi(n)})^m \\ &= M(M^{(p-1)(q-1)})^m \\ &= M \times 1^m[p \times q] \\ &\equiv M. \end{aligned}$$

3.3 Cryptographie sur les courbes elliptiques (ECC)

L'abréviation ECC veut dire Elliptic Curve Cryptography qui signifie en français Cryptographie à Courbe Elliptique. Basée sur un système de courbes elliptiques, la cryptographie ECC peut générer des clés nettement plus courtes que les clés RSA pour des niveaux de sécurité équivalents.
ECC et RSA utilisent de grands nombres premiers, mais là où RSA est basé sur leur factorisation des entiers, ECC utilise le logarithme discret.
Les clés et les certificats ECC fonctionnent de la même façon que RSA en pratique mais utilisent un autre format.

Considérons G un groupe cyclique de $E(k)$ engendré par P un point de la courbe. On note

$$G =< P >= \{O,\, P,\, [2]P, \cdots,\, [n-1]P\} \subseteq E(k) \quad et \quad [n]P = O.$$

Pour tout entier m, l'opération $[m]P$ est appelée multiplication de P par un scalaire m. Pour simplifier les écritures dans les opérations, on notera souvent mP au lieu de $[m]P$.
On se donne $m \in \mathbb{Z}$ et $P, Q \in G$, alors :

$$Q = [m]P = \underbrace{P + \cdots + P}_{(m fois)}.$$

Cette opération est dite à sens unique car il est très difficile de trouver m connaissant P et $Q = [m]P$, alors qu'on retrouve facilement par calcul Q connaissant m et P. Ce problème difficile est appelé problème du logarithme discret (ECDLP). La sécurité de la majorité des crypto-systèmes à base de courbes elliptiques repose sur ce dernier. Pour optimiser ce calcul, on utilise la représentation binaire de m. Soit $(m_{n-1}, \cdots, m_1, m_0)$, la représentation binaire de m telle que $m_{n-1} \neq 0$, en utilisant la méthode de Hörner, on a :

$$\begin{aligned} mP &= \sum_{i=0}^{n-1} m_i 2^i P \\ &= m_0 P + m_1 2^1 P + K_2 2^2 P + \cdots + m_{n-1} 2^{n-1} P \\ &= m_0 P + 2(m_2 P + (\cdots + (2(m_{n-2} + 2(m_{n-1}))) \cdots)). \end{aligned}$$

Dans cette formule découle immédiatement un algorithme appelé doublement-et-addition, il fait n tours et fait un doublement quel que soit la valeur m_i et une addition que si la valeur de m_i vaut 1.

Algorithme 1 : : Left-to-right (doublement-et-addition)
Entrées : P∈ E et $m = (m_{n-1} \cdots m_1 m_0)_2$
Sortie :[m]P
1.$P_0 \longleftarrow O$
2.$P_1 \longleftarrow P$
3.pour $i \longleftarrow n-1$ à 0 faire
4.$P_0 \longleftarrow [2]P_0$
5.si $m_i = 1$ alors
6.$P_0 \longleftarrow P_0 + P_1$
7.**retourner** P_0

3.3.1 Génération des clés ECC

Pour générer des clés d'ECC, Alice et Bob doivent effectuer les étapes suivantes :

❶ Alice et Bob choisissent une courbe elliptique et le point P de la courbe (point commun) ;

❷ Alice choisit un grand nombre premier m_a (clé privée) et calcule les coordonnées du point Q_a (clé publique) telles que $Q_a = m_a P$ et le même processus pour Bob $Q_b = m_b P$;

❸ Alice et Bob échangent des clés publiques Q_a et Q_b.

3.3.2 ECC pour chiffrer des données

Pour chiffrer un message clair M, les étapes suivantes doivent être suivies :

❶ Alice convertit le message M en une liste de points à partir de la courbe utilisée ;

❷ elle choisit un grand nombre entier m et une liste de messages chiffrés ;

❸ elle donne le premier élément de la liste du message chiffré : $P * m$;

❹ pour toutes les lettres du message clair, elle ajoute élément $L + Q_b * m$ à la liste des messages chiffrés tel que L est le point de chaque lettre.

3.3.3 ECC pour déchiffrer des données

Pour déchiffrer le message chiffré (la liste des points) les étapes suivantes doivent être suivies :

❶ Bob calcule le point S tel que S est le premier élément du message chiffré$*$ la clé privée b (message chiffré$*b$) ;

❷ une liste de messages chiffrés ;

❸ pour tous les points du message chiffré, on ajoute l'élément $L_c - S$ à la liste de messages déchiffrés tel que L_c, c'est le point chiffré de chaque lettre $L_c - S = L + (Q_b * b * m) = L$.

3.3.4 La méthode d'El Gamal pour les courbes elliptiques

Alice veut envoyer un message secret à Bob, tout d'abord, Bob fabrique une clé publique de la manière suivante : il choisit une courbe elliptique E définie sur un corps fini $\mathbb{F}_p$ de sorte que le problème du logarithme discret soit plus difficile à résoudre sur $E(\mathbb{F}_p)$ que sur $\mathbb{F}_p$. Il choisit un point P sur E tel que l'ordre de P soit un grand nombre premier et un nombre entier s secret. Ensuite, il calcule $B = sP$. La courbe E, le corps fini $\mathbb{F}_p$ et les points P et B sont les

clés publiques de Bob et sa clé secrète est s.
Pour envoyer le message, Alice procède comme suite :

❶ Alice prend la clé publique de Bob ;
❷ Alice convertit son message en un point $M \in E(\mathbb{F}_p)$;
❸ Alice choisit un nombre entier secret m et calcule $M_1 = mP$;
❹ ensuite, elle calcule $M_2 = M + mB$;
❺ Alice transmet M_1 et M_2 à Bob ;
❻ Bob, pour déchiffrer le message, il calcule $M = M_1 - sM_2$,

$$M_1 - sM_2 = (M + mB) - s(mP) = M + m(sP) - smP = M.$$

Voici le processus de cryptographie sur les courbes elliptiques

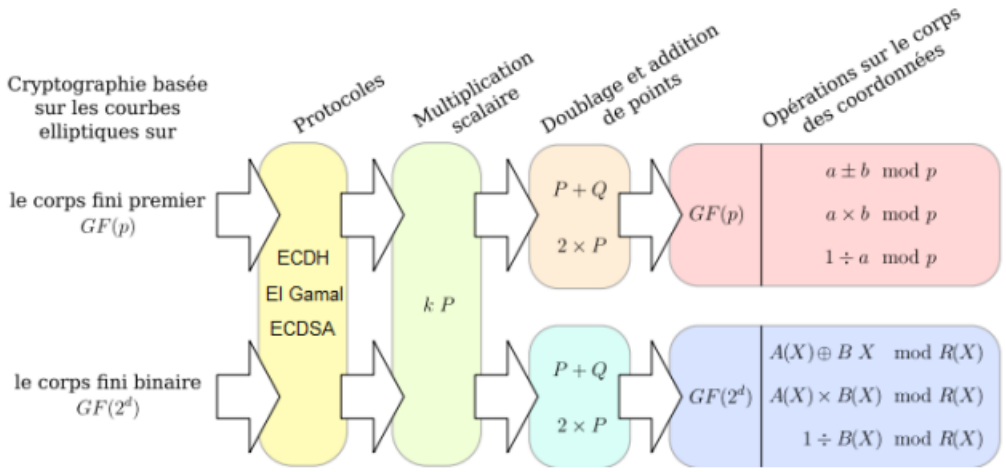

FIGURE 3.1 – Cryptographie basée sur les courbes elliptiques.

Actuellement, on ne connaît pas de moyen plus rapide qui permet de retrouver le message initial en ne sachant que ce qui est rendu public du système de cryptage. Donc, à priori la fiabilité de ce genre de cryptogramme repose fortement sur des progrès faits en matière de résolution du logarithme discret.

3.3.5 Niveaux de performances des courbes d'Edwards

Dans le contexte des applications en cryptographie, nous montrons dans cette section comment les courbes elliptiques sous la forme d'Edwards standard et la forme d'Edwards tordue accélèrent le chiffrement dans les algorithmes cryptographiques. Afin de mesurer le coût selon

le type d'opération utilisé, nous comptons le nombre de multiplications (M), de quadratures (S), d'additions (a) et de multiplications par les paramètres d'Edwards (D) qui interviennent dans les opérations de base (addition et doublement) des points de la courbe. Les formules d'addition pour les courbes d'Edwards et les courbes d'Edwards tordues impliquent toutes des inversions qui sont très coûteuses et leurs chiffrements sont plus lourds que les additions (a), les multiplications (M) ou les mises au carré (S). Par exemple, « la base de données de formules explicites » (voir [4]). Contient un tableau de coûts qui suppose qu'une inversion de champ coûte autant 100 multiplications de corps (M).
Dans ce qui suit, nous discuterons des formules pouvant éviter les inversions.

❶ Formule sans inversion

a **Addition sur une courbe d'Edwards tordue** :

Dans le cadre d'une application en cryptographie les performances de cette dernière vont dépendre des performances du système de coordonnées pour additionner ou pour doubler les points de la courbe. Cela consiste à éviter les inversions en passant aux coordonnées projectives afin de se débarrasser des dénominateurs. La somme de deux points (X_1, Y_1, Z_1) et (X_2, Y_2, Z_2) sur une courbe d'Edwards tordue équivaut à

$$(X_1, Y_1, Z_1) + (X_2, Y_2, Z_2) = (X_3, Y_3, Z_3),$$

avec $A = Z_1.Z_2$; $B = A^2$; $C = X_1.X_2$; $D = Y_1.Y_2$; $E = dC.D$; $F = B - E$; $G = B + E$;

$$\begin{aligned} X_3 &= A.F((X_1 + Y_1).(X_2 + Y_2) - C - D); \\ Y_3 &= A.G(D - aC); \\ Z_3 &= F.G. \end{aligned}$$

Ces formules optimisent la somme totale en $10M + 1S + 2D + 7a$, où les $2D$ sont des multiplications par a et une par d. Si $Z_2 = 1$, alors la multiplication $A = Z_2Z_1 = Z_1$, il est possible d'omettre Z_2 en fonction de l'addition mixte et de prendre $1D$ de moins, soit $9M + 1S + 2D + 7a$.

b **Doublement sur une courbe d'Edwards tordue** :

Le doublement est le cas où $(x_1, y_1) = (x_2, y_2)$. Étant donné un point (x_1, y_1) sur la courbe

$$E_{a,b} : ax^2 + y^2 = 1 + dx^2y^2.$$

En remplaçant $dx_1^2y_1^2$ par $ax^2 + y^2 - 1$ dans la formule suivante :

$$(x_1, y_1) + (x_1, y_1) = \left(\frac{2x_1y_1}{1 + dx_1^2y_1^2}, \frac{y_1^2 - ax_1^2}{1 - dx_1^2y_1^2} \right),$$

on obtient

$$= \left(\frac{2x_1y_1}{ax_1^2 + y_1^2}, \frac{y_1^2 - ax_1^2}{2 - (ax_1^2 + y_1^2)} \right).$$

Cette substitution permet de réduire le degré du dénominateur de 4 à 2, ce qui traduit par des doublement plus rapides comme suit : $B = (X_1, Y_1)^2$; $C = X_1^2$; $D = Y_1^2$; $E = aC$; $F = E + D$;$H = Z_1^2$; $J = F - 2H$.

$$X_3 = (B - C - H);$$
$$Y_3 = F.(C - D);$$
$$Z_3 = F.J.$$

Et la complexité correspondante est : $3M + 4S + 1D + 7a$, où $1D$ est la multiplication par a et $2H$ est calculé comme $H + H$.

❷ Effacement des dénominateurs en coordonnées projectives.

Considérons $E_{a,b}$: $a\overline{x}^2 + \overline{y}^2 = 1 + d\overline{x}^2\overline{y}^2$ une courbe d'Edwards tordue. Pour donner une approche alternative de l'arithmétique sur les courbes d'Edwards tordues $E_{a,b}$ dans le cas où a n'est pas un carré dans k, on passe à une courbe d'Edwards $E_{1,\frac{d}{a}}$ par l'isomorphisme donné par φ définie par

$$\varphi\,(\overline{x},\ \overline{y}) = \left(\sqrt{a}\overline{x},\ \overline{y}\right) = (x,\ y).$$

Les formules de la loi de groupe sur $E_{1,\frac{d}{a}}$ sont obtenues en utilisant $10M + 1S + 3D + 7a$ additions, $3D$ multiplications, deux par a et une par d.

En posant $A = Z_1.Z_2$; $B = aA^2$; $H = aA$; $C = X_1.X_2$; $D = Y_1.Y_2$; $E = dC.D$; $F = B - E$; $G = B + E$.

On obtient

$$X_3 = H.F((X_1 + Y_1).(X_2 + Y_2) - C - D);$$
$$Y_3 = H.G(C - D);$$
$$Z_3 = F.G.$$

Le doublement sur $E_{1,\frac{b}{a}}$ utilise $3M + 4S + 6a$. Si $a = 1$ dans la sous-section précédente, les formules d'addition pour $E_{1,\frac{b}{a}}$ sont plus rapides (on économise une multiplication par a) que doubler par $E_{a,b}$.

❸ Coordonnées d'Edwards tordues inversées.

L'arithmétique en coordonnées d'Edwards tordues inversées ou dans le cas $a = 1$ nous permet d'économiser $1M$ en plus comparé aux coordonnées standards. Ainsi on a :

a **Addition :**

La somme de deux points utilise $9M + 1S + 2D + 7a$, où les $2D$ sont une multiplication par a et une par b.

Posons $A = Z_1.Z_2$; $B = dA$; $C = X_1.X_2$; $D = Y_1.Y_2$; $E = C.D$; $H = C - aD$; $I = (X_1 + Y_1).(X_2 + Y_2) - C - D$.

La somme de $(X_1, Y_1, Z_1) + (X_2, Y_2, Z_2)$ donne :

$$\begin{aligned} X_3 &= (E + B).H; \\ Y_3 &= (E - B).I; \\ Z_3 &= A.H.I. \end{aligned}$$

b **Doublement :**

Pour doubler un point de la courbe, le nombre total d'opérations est : $3M + 4S + 2D + 6a$, où les $2D$ sont une multiplication par a et une par $2d$, avec $A = X_1^2$; $B = Y_1^2$; $U = aB$; $C = A + U$; $D = A - U$; $E = (X_1 + Y_1)^2 - A - B$.

$$\begin{aligned} X_3 &= C.D; \\ Y_3 &= E.(C - 2dZ_1^2); \\ Z_3 &= D.E. \end{aligned}$$

❹ Le modèle de Weierstrass.

Les courbes de Weierstrass sur $\mathbb{F}_p$ sont définies par l'équation :

$$E_W : y^2 = x^3 + ax + b.$$

Considérons l'ensemble

$$E(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p \mid y^2 = x^3 + ax + b\} \cup \{O\},$$

cet ensemble possède une structure de groupe. Cette structure fait apparaître deux types d'opérations : $P + Q$ et $2P$ qu'on peut résoudre graphiquement.

De plus $P + Q$ n'est pas possible si $Q \neq \pm P$ et généralement des formules différentes sont nécessaires pour effectuer ces opérations.

Les formules d'addition (ADD) et de doublement (DBL) sont rappelées dans le tableau suivant :

Coordonnées	Jacobiennes $(x = \frac{x}{z^2}; y = \frac{y}{z^3})$	Projectives $(X = \frac{x}{z}; Y = \frac{y}{z})$
ADD	$ZZ_1 = Z_1^2$	$U_1 = X_1.Z_2$
	$ZZ_2 = Z_2^2$	$U_2 = X_2.Z_1$
	$U_1 = X_1.ZZ_2$	$S_1 = Y_1.Z_2$
	$U_2 = X_2.ZZ_1$	$S_2 = Y_2.Z_1$
	$S_1 = Y_1.ZZ_2Z_2$	$ZZ = Z_1.Z_2$
	$S_2 = Y_2.ZZ_1Z_1$	$T = U_1 + U_2$
	$H = U_2 - U_1$	$TT = T^2$
	$I = (2.H)^2$	$M = S_1 + S_2$
	$J = H.I$	$R = T.T - U_1U_2 + aZZ^2$
	$r = 2(S_2 - S_1)$	$F = ZZ.M$
	$V = U_1.I$	$L = M.F$
	$S = 2.S_1.J$	$LL = L^2$
	$T = ZZ_1 + ZZ_2$	$G = (T + L)^2 - TT - LL$
	$U = (Z_1 + Z_2)^2$	$W = 2.R^2 - G$
	$X_3 = r^2 - J - 2V$	$X_3 = 2.F.W$
	$Y_3 = r.(V - X_3) - S$	$Y_3 = R.(G - 2.W) - 2LL$
	$Z_3 = M^2 - 2.S$	$Z_3 = 4F^3$
Coûts	11M+5S+13a	11M+6S+16a+1D
DBL	$XX = X_1^2$	$XX = X_1^2$
	$YY = Y_1^2$	$ZZ = Z_1^2$
	$t_0 = YY^2$	$w = a.ZZ + 3XX$
	$ZZ = Z_1^2$	$s = 2.Y_1.Z_1$
	$t_1 = (X_1 + YY)^2$	$ss = s^2$
	$S = 2(t_1 - XX - t_0)$	$Z_3 = s.ss$
	$M = 3.XX + aZZ^2 =$	$R = Y_1.s$
	$X_3 = M^2 - 2S$	$RR = R^2$
	$U = S - X_3$	$B = (X_1 + R)^2 - XX - RR$
	$Y_3 = M.U - 8.t_0$	$h = w^2 - 2.B$
	$V = YY + ZZ$	$X_3 = h.s$
	$Z_3 = (Y_1 + Z_1)^2 - V$	$Y_3 = w.(B - h) - 2RR$
Coûts	1M+8S+16a+1D	5M+6S+12a+1D

3.4 Comparaison

À titre de comparaison, les algorithmes les plus rapides connus pour les courbes elliptiques sont utilisés avec le modèle d'Edwards. En effet, le processeur effectue moins d'opérations lorsque ce modèle est comparé avec le modèle de Weierstrass. Ce dernier, pour additionner deux points de la courbe utilise en coordonnées projectives 11 multiplications scalaires, 6 opérations de corps et 16 additions de corps alors que celle d'Edwards tordue économise le temps en utilisant 10 multiplications de corps, 1 opération de corps des cordonnées et 7 additions de corps des coordonnées. Maintenant, pour doubler un point, le modèle d'Edwards tordue reste encore le modèle le plus rapide pour chiffrer comparé à celle de Weierstrass avec une différence de 2 multiplications de corps, 2 opérations de corps des coordonnées et 5 additions de corps. Le modèle d'Edwards standard est presque pareil que dans le cas tordu, la sommation de deux points de la courbe a un gain d'opérations pour des additions de champs si on double deux points de la courbe. Bref, les courbes d'Edwards ont un caractère supplémentaire que les formules d'additions sont complètes, c'est-à-dire elles fonctionnent pour n'importe quelle paire de points d'entiers sur les courbes. Certaines additions ont été présentées comme fortement unifiées et sont très utiles pour la protection contre les attaques par canal latéral.
L'évolution rapide de la technologique de l'information force les industries des équipements à augmenter régulièrement la taille minimale des clés RSA. L'ANSSI (Agence nationale de la sécurité des systèmes d'information en France) recommande le 4096-bit depuis 2020. La taille des clés a un impact significatif sur les performances des équipements.
Le tableau suivant présente l'équivalence ECC / RSA (voir [11]) :

Taille des clés RSA (bits)	Taille des clés ECC (bits)
1024	160
2048	224
3072	256
7680	384
15360	521

Conclusion

Dans ce mémoire, nous nous sommes intéressés à l'étude des propriétés des courbes elliptiques sous forme d'Edwards en plus nous avons donné les autres formes qui dérivent de ce modèle standard. Ensuite, nous avons étudié leurs applications en cryptographie. Ces travaux ont permis également de voir comment cette nouvelle forme des courbes elliptiques interviennent dans l'accélération arithmétique et dans la réduction des opérations lors d'un doublement ou d'addition des points de la courbe. Il serait intéressant de poursuivre les recherches pour explorer d'autres techniques d'addition et de doublement des points de la courbe afin de minimiser davantage la complexité des opérations de calcul et ainsi de sécurisé aux mieux les systèmes d'informations à moindre effort.

Bibliographie

[1] D. Abramovic, J. Harris, Varieties and curves in Wd(C), composio Math. 78 (1991) 227-238.

[2] D. J. Bernstein, P. Birkner,M. Joye, T. Lange et C. Peters : Twisted edwards curves. Progress in Cryptology AFRICACRYPT 2008, pages 389-405, 2008.

[3] D. J. Bernstein and T. Lange. Faster addition and doubling on elliptic curves. In Advances in cryptology—ASIACRYPT 2007, volume 4833 of Lecture Notes in Comput. Sci., pages 29–50. Springer, Berlin, 2007.

[4] D. J. Bernstein et T. Lange : Inverted edwards coordinates. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, pages 20 -27, 2007.

[5] D. J. Bernstein et T. Lange : Performance evaluation of a new coordinate system for elliptic curves. 2007.

[6] D. J. Bernstein, T. Lange, and Reza R. Farashahi. Binary Edwards curves. In CHES, 08 : Proceeding of the 10th international workshop on Cryptographic Hardware and Embedded Systems, pages 244–265, Berlin, Heidelberg, 2008. Springer-Verlag.

[7] D. Perrin. Géométrie algébrique, une introduction. Inter-éditions, Paris, 1995.

[8] E. Breir ; M. Joye : Weierstrass Elliptic Curve and side-channel Attacks. In Public Key Cryptography, (PKC), volume 2274 of LNCS, pages 335-345, 2002.

[9] Edwards, Harold M. A Normal Form for Elliptic Curves. American Mathematical Society 44.3 (2007) : 393-422. Web. http ://www. ams.org/journals/bull/2007-44-03/S0273-0979-07-01153-6/S0273-0979-07-01153-6.pdf.

[10] https ://interstices.info/nombres-premiers-et-cryptologie-lalgorithme-rsa/
Page visitée le 05/01/2024.

[11] https ://www.tbs -certificats.com/FAQ/fr/explications-ECC.html.
Page visitée le 05/01/2024.

[12] https ://fr.wikipedia.org/w/index.php. (Plongement de segré)
Page visitée le 05/01/2024.

[13] J. H. Silverman. The arithmetic of elliptic curves. Graduate Texts in Mathematics. Springer-Verlage, New York, 1986.

[14] P. A. Griffiths,Introduction to algebraic curves , Translations of mathematical monographs volume 76. American Mathematical Society,Providence (1989).

[15] Ronald Rivest, Adi Shamir et Leonard Adleman, A method for obtaining digital signatures and public-key cryptosystems, communications of the ACM, vol. 21, n0 2, 1978, p.120-126.

[16] S. Pontie. Sécurisation matérielle pour la cryptographie à base de courbes elliptiques. Thèse de Doctorat, Université Grenoble Alpes, 2016.