Université Cheikh Anta Diop de Dakar
École Doctorale de Mathématiques et d'Informatique

Thèse de Doctorat Unique ès Sciences Mathématiques
Spécialité : Codage, Cryptologie, Algèbre et Applications

présentée pour obtenir le grade de

Docteur de l'Université Cheikh Anta Diop de Dakar

par

Abdoul Aziz Ciss

Arithmétique et Extracteurs Déterministes sur les Courbes Elliptiques

Soutenue le 03 Mars 2012 à l'amphi 7

Devant le jury composé de :

Président :	Mamadou Sangharé	Professeur	Univ. Cheikh A. Diop
Rapporteurs :	David Lubicz	Chercheur, HDR	Univ. Rennes 1
	Christophe Ritzenthaler	Maître de conf, HDR	Univ Aix-Marseille
Examinateurs :	Sidy Demba Touré	Maître de conférences	Univ. Cheikh A. Diop
	Cheikh T. Guèye	Maître de conférences	Univ. Cheikh A. Diop
	Oumar Diankha	Maître de conférences	Univ. Cheikh A. Diop
Directeur de thèse :	Djiby Sow	Maître de conférences	Univ. Cheikh A. Diop

DÉDICACES

Je dédie ce travail à mon père, feu Ibrahima Ciss. May God bless his soul ! A celle qui m'a toujours supporté et assisté, mon guide spirituel, ma très chère mère Lat Sall Niang. Que Dieu lui prête longue vie !

- *A mes sœurs Bineta, Rama et Penda.*
- *A mes neveux et nièces : Mafall, Massar, Fatou, Aïda, Mamy.*
- *A mon père Amadou Télémaque Sow et sa femme Aminata Guèye. Que Dieu bénisse leur famille !*
- *A toutes ces merveilleuses personnes avec qui j'ai passé des moments inoubliables et sans qui ce travail n'aurait jamais vu le jour, je veux dire mon frère Abou Beckr Gaye, Adama Ndiaye, Sidy Samb, Moustapha Wade, François Tine, Abdourahmane Fall, Babacar Diop, Tidiane et Moussa Télémaque, Ismaïla, Abdourahmane Fall et Ousmane Coulibaly, Thiali Badiane, Mansour Diongue, Pape Oumar Thiam.*
- *A ma grand mère, mes cousin(e)s, oncles et tantes.*
- *A mes étudiants du Master Transmission des Données et Sécurité de l'Information et ceux de l'École Supérieure des Sciences Appliquées.*

Que l'Eternel vous bénisse !

REMERCIEMENTS

Je tiens à remercier vivement Monsieur le Professeur **Mamadou Sangharé** pour l'honneur qu'il m'a fait en acceptant de présider mon jury de thèse.

Je tiens à remercier sincèrement le Docteur **Djiby SOW** qui a dirigé mes travaux, en lui exprimant d'abord ma profonde gratitude pour tout ce qu'il a fait pour moi, mais aussi le remercier très sincèrement pour sa disponibilité entière de me recevoir à n'importe quel moment, ensuite pour l'excellente formation que j'ai reçue auprès de lui sur tous les plans (didactique, recherche). J'ai apprécié tout particulièrement sa générosité grandiose, sa patience, et sa capacité d'écoute.

Je remercie très sincèrement **David Lubicz** et **Christophe Ritzenthaler** pour avoir accepté d'être rapporteurs de cette thèse et examinateurs dans ce jury.

J'exprime ma profonde gratitude à **Cheikh Thiécoumba Guèye**, **Sidy demba Touré** et **Oumar Diankha** pour l'honneur qu'ils me font en acceptant de siéger dans le jury de cette thèse.

Je tiens aussi à remercier l'Institut de Recherche Mathématique de Rennes (IRMAR), à travers Marie Françoise Roye et David Lubicz, pour l'opportunité qu'il m'ont offerte de séjourner dans leur labo, d'avancer dans mes travaux de recherche et de terminer la rédaction de cette thèse.

Je remercie tous les membres du Laboratoire d'Algèbre, de Cryptologie, de Géométrie Algébrique et Applications (LACGAA) et mes compagnons de recherche, je veux dire Seydina Omar Ndiaye, Ahmed Ould Khalifa, Ahmed Youssef, Amadou Tall, Mamadou G. Camara, Demba Sow, Régis F. Babindamana, Jean R. Tsiba, Mame Demba Cissé, Ali Y. Sangharé, Mamadou Mboup, Chérif Dème.

Mention spéciale à **Omar Diao** et à **Mouhamadou Lamine Diouf**.

Table des matières

Chapitre 1
INTRODUCTION GÉNÉRALE

En 1979, Diffie et Hellman publient leur papier révolutionnaire : *New Directions in Cryptography* [DH76], dans lequel ils introduisent le concept de cryptographie à clé publique. Avant ce tournant très important de la cryptographie moderne, les cryptosystèmes conventionnels étaient basés sur les techniques symétriques dans lesquels un secret commun est utilisé pour chiffrer les données envoyées par une partie à une autre. Contrairement à ce type de cryptosystèmes, Diffie et Hellman proposent une méthode asymétrique : une partie A fournit une clé publique, avec laquelle les autres parties peuvent chiffrer les messages qui lui sont destinés. L'utilisateur A détient une clé privée correspondante (aucun autre utilisateur ne connaît la clé privée à part A), avec laquelle A peut déchiffrer ces messages. Cette nouvelle technique règle le problème du partage de clés à travers un canal non sécurisé, problème qui apparaît fréquemment dans les cryptosystèmes à clés secrètes. Même si ces derniers sont plus efficaces du point de vue de la quantité de données à chiffrer, les cryptosystèmes à clés publiques permettent le partage de clés sécurisé, les signatures numériques et l'authentification. La sécurité des cryptosystèmes, comme ceux proposés par Diffie et Hellman, reposent sur l'existence de fonctions à sens unique à trappe. Calculer de telles fonctions est une opération facile alors que leur inversion est quasiment impossible. L'exponentiation d'un entier modulo un nombre premier q est l'un des exemples les plus importants [DH76]. La sécurité des cryptosystèmes basés sur cette fonction repose sur l'impossibilité de résoudre le *problème du logarithme discret* (DLP) dans un sous-groupe multiplicatif d'un corps fini $\mathbb{F}_q$, où q est un nombre premier suffisamment grand. Le problème du logarithme discret dans tout groupe G est défini comme suit : étant donnés a, y des éléments de G, trouver, s'il existe, l'entier x tel que $y = a^x$. Pour un groupe abélien, le DLP peut être formulé de façon additive : étant donnés P et Q dans un groupe abélien G, trouver x tel que $Q = [x]P$

(P additionné à lui même x fois). Lorsque le DLP est difficile à résoudre dans un groupe G, alors G peut être utilisé pour mettre en œuvre des protocoles comme indiqué par Diffie et Hellman.

Il a été suggéré indépendamment par Miller [Mil86] et Koblitz [Kob87] d'utiliser le groupe des points rationnels d'une courbe elliptique définie sur un corps fini pour mettre en œuvres les cryptosystèmes à clés publiques ou le protocole d'échange de clés de Diffie-Hellman. Plus tard, Koblitz proposa aussi dans [Kob89] le groupe de Picard d'une courbe hyperelliptique sur un corps fini. Depuis lors, les cryptosystèmes basés sur les courbes elliptiques et sur les courbes hyperelliptiques et les algorithmes pour résoudre le DLP dans les groupes correspondants sont intensément étudiés et sont largement utilisés. En pratique, on travaille avec des sous-groupes d'ordre premier. La taille d'un tel sous-groupe doit être suffisamment grande de sorte que le DLP soit impossible à résoudre avec tous les algorithmes connus. Le DLP sur une courbe est plus difficile que sur un corps fini de même ordre. Par conséquent, les courbes ont l'avantage d'avoir le même niveau de sécurité avec des paramètres plus petits.

En cryptographie, il est important de

- trouver un modèle de courbe elliptique avec une arithmétique efficiente,
- trouver un extracteur d'aléa déterministe, optimal et efficace sur les corps finis et sur les courbes elliptiques.

Notre contribution dans cette thèse se situe dans ces deux axes de recherche. Concrètement, nous avons contribué sur trois points :

1. Nous avons construit un extracteur d'aléa déterministe sur le corps fini $\mathbb{F}_{p^n}$. De plus, nous avons montré qu'on peut l'utiliser pour dériver une clé secrète à la suite d'un protocole d'échange de clé Diffie-Hellman.
2. Nous avons aussi montré qu'on peut avoir les résultats du (1) sur une courbe elliptique définie sur $\mathbb{F}_{p^n}$. Nous avons résolu en même temps les conjectures de Farashahi *et al.* sur les extracteurs d'aléa sur les courbes elliptiques.
3. Nous avons calculé de façon efficace le couplage de Tate sur les courbes

elliptiques de Huff proposées par Wu et Feng dans [WF10].

Extraction d'aléa sur les corps finis

Dans plusieurs protocoles et schémas cryptographiques, il est indispensable de pouvoir dériver une chaîne de bits aléatoire à partir d'un élément aléatoire d'un groupe donné. C'est le cas de l'échange de clés de Diffie-Hellman [DH76] qui est le protocole le plus connu et permettant à des parties de s'accorder sur un élément aléatoire dans un sous-groupe cyclique H d'un groupe G, engendré par un élément g d'ordre premier t. La sécurité du protocole de Diffie-Hellman repose sur le problème décisionnel de Diffie-Hellman (DDH) [Bon98], qui établit qu'il n'existe pas d'algorithme efficace permettant de distinguer les deux distributions (g^a, g^b, g^{ab}) et (g^a, g^b, g^c) dans G^3, où $1 \leq a, b, c \leq t$ sont choisis de façon aléatoire. Sous l'hypothèse DDH, on peut ainsi s'accorder sur un secret partagé parfaitement aléatoire. Il suffit donc de dériver de ce secret une chaîne de bits uniforme pour des utilisations symétriques. Différentes approches ont été proposées pour résoudre ce problème de dérivation de clés.

Une méthode classique pour transformer un élément aléatoire d'un groupe en une chaîne de bits aléatoire consiste à appliquer une fonction de hachage (MD5 ou SHA-1) à l'élément Diffie-Hellman, mais dans ce cas l'indistinguabilité ne peut être prouvée que dans le modèle de l'oracle aléatoire [BR93]. Une alternative aux fonctions de hachage, sûre dans le modèle standard, est l'utilisation d'extracteurs d'aléa.

En 1998, Boneh *et al.* proposent dans [BV96] d'extraire les bits de poids fort ou de poids faible de l'élément Diffie-Hellman. En 1999, Håstad *et al.*, [HILL99], via le Leftover Hash Lemma, proposent un extracteur d'aléa probabiliste qui peut extraire l'entropie de n'importe quel source d'aléa ayant une min-entropie suffisante. Cette technique et ses variantes [FPZ08, GKR04] requièrent l'utilisation de fonctions pseudo-aléatoires et d'un aléa supplémentaire, ce qui constitue un

défaut pour des utilisations pratiques.
En 2000, Carneti *et al.* [CFK$^+$00] ont montré, dans un sens statistique, que les k bits de poids fort de g^{xy} sont indistinguables d'une chaîne de bits aléatoire de longueur k, étant donnés les k bits de poids fort de g^x et de g^y. Mais, en 2001, Boneh *et al.* ont noté que cette technique ne peut pas être utilisée en pratique puisque dans plusieurs protocoles, l'attaquant connaît tout de g^x et de g^y.
En 2008, Fouque *et al.* montrent dans [FPSZ06], sous l'hypothèse DDH, que les k bits de poids fort d'un élément aléatoire d'un sous-groupe G de $\mathbb{Z}_p^*$ sont indistinguables d'une chaîne de bits aléatoire de même longueur. Pour prouver ce résultat, les auteurs ont borné la distance statistique en évaluant la norme L_1 par le biais de sommes d'exponentielles.
A Eurocrypt'09, Chevalier *et al.* [CFPZ09] ont étudié l'extracteur déterministe proposé dans [FPSZ06] et ont aussi proposé un extracteur déterministe très simple sur le groupe des points d'une courbe elliptique définie sur $\mathbb{Z}_p^*$. Ils utilisent cette fois ci la norme L_2 et les sommes d'exponentielles. Avec leur technique, on peut extraire deux fois le nombre de bits que [FPSZ06]. Remarquons que tous ces travaux ont été effectués sur le corps $\mathbb{F}_p$, avec p un nombre premier.
Nous avons étendu les résultats de Chevalier *et al.* sur les corps non premiers $\mathbb{F}_{p^n}$, avec p un nombre premier et n un entier positif plus grand que 1. Nous présentons dans cette thèse un nouvel extracteur déterministe très simple pour un sous-groupe multiplicatif G d'un corps fini $\mathbb{F}_{p^n}$. En particulier, on montre, sous l'hypothèse DDH dans le corps fini $\mathbb{F}_{2^n}$, que les the k-premiers coefficients dans $\mathbb{F}_2$ (les k bits de poids faibles) d'un élément aléatoire d'un sous-groupe de $\mathbb{F}_{2^n}^*$ sont indistinguables d'une chaîne de bits aléatoire de longueur k.

Extraction d'aléa sur les courbes elliptiques

L'extraction d'aléa à partir d'un point d'une courbe elliptique est utilisée dans plusieurs applications cryptographiques. Par exemple, on peut utiliser un extrac-

teur déterministe pour dériver une clé symétrique, dans les protocoles d'échanges de clés ou pour fabriquer des générateurs aléatoires cryptographiquement sûrs. Prenons le cas de l'échange de clés Diffie-Hellman sur une courbe elliptique E. A la fin de ce protocole dans un sous-groupe cyclique G de E, Alice et Bob s'accordent sur un point aléatoire $K_{AB} \in G$ qui est indistinguable, sous l'hypothèse décisionnelle de Diffie-Hellman, de tout autre élément de G. La clé secrète utilisée pour chiffrer et authentifier les données doit être une chaîne de bits uniformément aléatoire. Par conséquent, on ne peut pas utiliser directement le secret commun K_{AB} comme clé de session.

Une solution classique est d'utiliser une fonction de hachage, comme dans le cas des corps finis, pour convertir un point aléatoire de G en une chaîne de bits aléatoire de longueur fixe. Là aussi, l'indistinguabilité ne peut être prouvée sous l'hypothèse décisionnelle de Diffie-Hellman. Il est alors nécessaire dans ce cas de faire appel à l'oracle aléatoire. Plusieurs résultats dans ce sens peuvent être retrouvés dans [DGKR04, HILL99].

Une alternative aux fonctions de hachage consiste à utiliser un extracteur déterministe comme dans le cas des corps finis, mais en considérant cette fois-ci un sous-groupe G d'une courbe elliptique E. Un extracteur déterministe pour une courbe elliptique E est une fonction qui convertit un point uniformément aléatoire de E en une chaîne de l bits avec une distribution proche de l'uniforme.

Plusieurs extracteurs déterministes ont été proposés sur les courbes elliptiques. L'un d'entre eux est celui de Gürel [GÖ5]. Cet extracteur, étant donné un point P de $E(\mathbb{F}_{q^2})$, où q est une puissance d'un nombre premier impair, renvoie la moitié des bits de l'abscisse du point P. Si le point P est uniformément aléatoire, alors les bits extraits de P sont indistinguables d'une chaîne de bits aléatoire de même longueur [GÖ5]. Dans le même papier, l'auteur propose aussi un extracteur pour une courbe elliptique définie sur un corps premier $\mathbb{F}_p$, mais celui-ci renvoie moins de la moitié des bits de l'abscisse du point aléatoire considéré.

En 2007, R. R. Farashahi et R. Pellikaan [FP07] ont proposé un bon extracteur déterministe pour les courbes (hyper)elliptiques définies sur l'extension quadra-

tique du corps fini $\mathbb{F}_{q^2}$, avec $q \neq 2$, et améliore en même temps les résultats de Gürel. Dans leurs travaux, ils établissent une conjecture sur l'extraction d'aléa sur une courbe $\mathcal{C}$ (affine, plane, absolument irréductible, non singulière) définie sur un corps $F_q n$ (non nécessairement quadratique) par $y^m = f(x)$. Ils ont laissé la preuve de cette conjecture comme problème ouvert. Nous avons montré dans [CS11] que cette conjecture est vraie dans le cas où la courbe $\mathcal{C}$ est une courbe elliptique.

En 2008, R. R. Farashahi, R. Pellikaan et A. Sidorenko [FPS08] ont étudié le cas binaire en considérant l'extension quadratique d'un corps de caractéristique paire. En fait, ils présentent deux extracteurs déterministes efficaces pour une courbe elliptique $E(\mathbb{F}_{2^N})$, où $N = 2l$ et l est un entier positif. Étant donné un point P sur $E(\mathbb{F}_{2^N})$, leurs extracteurs renvoient le premier ou le second coefficient dans $\mathbb{F}_{2^l}$ de l'abscisse de P. Les auteurs ont aussi établi une conjecture similaire à celle de [FP07] pour une courbe elliptique définie sur un corps binaire $\mathbb{F}_{2^n}$, avec aucune restriction sur l'entier n. Nous avons aussi démontré dans [CS11] que cette conjecture est vraie.

En effet, nous avons proposé un extracteur déterministe très simple, noté $\mathcal{D}_k$ pour une courbe elliptique E définie sur un corps fini $\mathbb{F}_{q^n}$ (où q est un nombre premier et n un entier positif sans aucune restriction, n peut être premier en particulier) par $y^2+(a_1x+a_3)y = x^3+a_2x^2+a_4x+a_6$. Étant donné un point $P \in E(\mathbb{F}_{q^n})$, $\mathcal{D}_k$ extrait les k premiers coefficients dans $\mathbb{F}_q$ de l'abscisse du point P (où l'abscisse x de P est un élément de $\mathbb{F}_{q^n}$ considéré comme un espace vectoriel de dimension n sur $\mathbb{F}_q$).

Nous montrons que $\mathcal{D}_k$ est un extracteur déterministe efficace pour la courbe elliptique $E(\mathbb{F}_q n)$. Notre approche est un peu similaire à celui développée par C. Chevalier, P. Fouque, D. Pointcheval et S. Zimmer dans [CFPZ09], où ils proposent une extraction d'aléa très simple à partir d'un élément Diffie-Hellman dans un sous-groupe d'une courbe elliptique définie sur le corps fini $\mathbb{F}_p$.

Couplages sur les courbes de Huff

Depuis leur introduction en cryptographie par Koblitz [Kob87], Miller [Mil86] et Menezes [Men94], les courbes elliptiques sont intensément utilisées du fait qu'elles permettent d'avoir des tailles de clés très petites et que le problème du logarithme discret est plus difficile sur le groupe des points d'une courbe elliptique que sur $(\mathbb{Z}/p\mathbb{Z})^*$. De plus, un intérêt majeur fût porté sur les couplages sur les courbes elliptiques puisque ces derniers permettent de mettre en œuvre des protocoles et de cryptanalyser certains systèmes basés sur le logarithme discret.
On sait que les courbes elliptiques peuvent être représentées sous différentes formes. Ce qui induit naturellement différentes propriétés arithmétiques. Plusieurs modèles de courbes elliptiques ont été proposés pour accélérer les calculs, notamment la multiplication scalaire qui dépend du coût des opérations d'addition et de duplication.
Récemment, Joye, Tibouchi et Vergnaud on réintroduit dans [JTV10] un modèle pour les courbes elliptiques. Ce modèle a été étudié pour la première fois par Huff en 1948 dans [Huf48] dans le but d'étudier un problème diophantien. On peut donner une liste des différentes versions du modèle de Huff.

1. Les courbes elliptiques de Huff (par Huff lui même dans [Huf48]) sur un corps K, $\mathrm{char}(K) \neq 2$, de la forme

$$ax(y^2 - 1) = by(x^2 - 1) \text{ avec } a^2 - b^2 \neq 0,$$

2. Une première généralisation (par Joye, Tibouchi et Vergnaud dans [JTV10]) sur un corps K, $\mathrm{char}(K) \neq 2$:

$$ax(y^2 - d) = by(x^2 - d) \text{ avec } abd(a^2 - b^2) \neq 0,$$

3) Une seconde généralisation (par Wu et Feng dans [WF10]) sur un corps K, $\mathrm{char}(K) \neq 2$:

$$x(ay^2 - 1) = y(bx^2 - 1) \text{ avec } ab(a - b) \neq 0,$$

3. Les courbes elliptiques binaires de Huff (par Joye, Tibouchi et Vergnaud [JTV10]) sur un corps K, $\mathrm{char}(K) = 2$:

$$ax(y^2 + y + 1) = by(x^2 + x + 1) \text{ avec } abcd(a^2c - b^2d) \neq 0,$$

4. Les courbes elliptiques binaires de Huff généralisées (par Devigne et Joye [DJ11]) sur un corps d K, $\mathrm{char}(K) = 2$:

$$ax(y^2 + fy + 1) = by(x^2 + fx + 1) \text{ avec } abf(a - b) \neq 0.$$

La contribution dans cette thèse, concernant les courbes de Huff, est d'étudier le calcul du couplage de Tate sur les courbes elliptiques de Huff proposées par Wu et Feng dans [WF10].

Chapitre 2
PRÉLIMINAIRES

Dans ce chapitre, nous donnons les définitions et les résultats fondamentaux dont on aura besoin dans les chapitres qui suivent. Nous rappellerons essentiellement les notions de bases sur les variétés algébriques, la construction de quelques extracteurs déterministes sur les courbes (hyper)elliptiques.

2.1 Généralités sur les courbes planes

Dans cette section, nous donnons une brève introduction sur les courbes planes. Il sera question dans ce chapitre de définir les courbes affines et les courbes projectives, de discuter des concepts généraux et des propriétés avant de terminer avec les courbes (hyper)elliptiques. Nous ne donnons pratiquement pas de preuves pour les théorèmes énoncés dans ce chapitre puisque nous avons juste besoin de certains résultats que nous allons utiliser dans les chapitres qui suivent. Pour les preuves, se référer à [Har77], [Ful69], [Lor96], [Sti93], [Sil86], [FL05].

2.1.1 Courbes affines et courbes projectives

Soit $\mathbb{F}$, un corps parfait et $\overline{\mathbb{F}}$, sa clôture algébrique. Pour un entier positif n donné, le n-espace affine $\mathbb{A}^n(\overline{\mathbb{F}})$ est défini comme étant $\mathbb{A}^n(\overline{\mathbb{F}}) = \overline{\mathbb{F}}^n$. L'espace $\mathbb{A}^1(\overline{\mathbb{F}})$ est appelé *droite affine* et l'espace $\mathbb{A}^2(\overline{\mathbb{F}}) = \overline{\mathbb{F}} \times \overline{\mathbb{F}}$ est appelé *plan affine*. Pour toute extension $\mathbb{F} \subseteq \tilde{\mathbb{F}} \subseteq \overline{\mathbb{F}}$ de $\mathbb{F}$, on appelle $\mathbb{A}^n(\tilde{\mathbb{F}}) = \tilde{\mathbb{F}}^n$ l'ensemble des points $\tilde{\mathbb{F}}$-rationnels de $\mathbb{A}^n(\overline{\mathbb{F}})$. Étant donné un polynôme $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ à n variables, on peut évaluer f en un point $P = (a_1, a_2, \ldots, a_n) \in \mathbb{A}^n(\overline{\mathbb{F}})$ en $f(P) = f(a_1, a_2, \ldots, a_n) \in \overline{\mathbb{F}}$.

Définition 2.1.1. *Soit $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ un polynôme à n-variables. Définissons*

l'ensemble algébrique $\mathcal{C}_f$ *par*

$$\mathcal{C}_f := \{P \in \mathbb{A}^n(\overline{\mathbb{F}}), f(P) = 0\}.$$

Pour toute extension $\tilde{\mathbb{F}}$ *de* $\mathbb{F}$ *(*$\mathbb{F} \subseteq \tilde{\mathbb{F}} \subseteq \overline{\mathbb{F}}$*), l'ensemble*

$$\mathcal{C}_f(\tilde{\mathbb{F}}) := \{P \in \mathcal{C}_f, P \in \mathbb{A}^n(\tilde{\mathbb{F}})\}$$

des points de coordonnées dans $\tilde{\mathbb{F}}$ *est appelé* ensemble des points $\tilde{\mathbb{F}}$-rationnels de $\mathcal{C}_f$.

Dans ce manuscrit, on considère principalement les ensembles $\mathcal{C}_f \subseteq \mathbb{A}^2(\overline{\mathbb{F}})$. On notera ainsi, $\mathbb{F}[x, y]$ l'anneau des polynômes à deux variables sur $\mathbb{F}$.

Définition 2.1.2. *Soit* $f \in \mathbb{F}[x, y]$*, un polynôme. L'ensemble* $\mathcal{C}_f$ *est appelé courbe affine plane. Le* degré *de* $\mathcal{C}_f$ *est défini comme étant le degré de* f*.*

Exemple 2.1.3. *Une* droite affine plane *est une courbe affine plane de degré 1. Elle est donnée par un polynôme*

$$l := ax + by + c$$

de degré 1, c'est-à-dire $(a, b) \neq (0, 0)$*. Notons que la droite est déterminée uniquement à partir de deux points distincts.*
Une courbe affine plane de degré 2 sera appelée conique *affine plane. Elle est donnée par un polynôme*

$$f_C = c_1x^2 + c_2y^2 + c_3xy + c_4x + c_5y + c_6 \in \mathbb{F}[x, y]$$

de degré 2, c'est-à-dire $(c_1, c_2, c_3) \neq (0, 0, 0)$*.*
Une courbe affine plane de degré 3 sera appelée cubique*.*

Soit $P = (a_1, a_2, \ldots, a_{n+1}) \in \mathbb{A}^{n+1}(\overline{\mathbb{F}})$ un point sur $(n + 1)$-espace affine. Supposons que $P \neq (0, 0, \ldots, 0)$. Alors, P définit une unique droite passant par lui même et l'origine $(0, 0, \ldots, 0)$. Définissons la relation d'équivalence $\sim$

sur $\mathbb{A}^{n+1}(\overline{F})\backslash\{(0,0,\ldots,0)\}$ comme suit : deux points $P=(a_1,a_2,\ldots,a_{n+1})$ et $Q=(b_1,b_2,\ldots,b_{n+1})$ sont équivalents (on note $P\sim Q$), s'il existe $\lambda\in\overline{\mathbb{F}}^*$ tel que

$$(a_1,a_2,\ldots,a_{n+1})=\lambda(b_1,b_2,\ldots,b_{n+1})=(\lambda b_1,\lambda b_2,\ldots,\lambda b_{n+1}).$$

On note la classe d'équivalence d'un élément $P=(a_1,a_2,\ldots,a_{n+1})$ par

$$P^{\sim}:=(a_1:a_2:\ldots:a_{n+1})=\{Q\in\mathbb{A}^{n+1}(\overline{\mathbb{F}}),Q\sim P\}.$$

On définit le *n-espace projectif* $\mathbb{P}^n(\overline{\mathbb{F}})$ comme étant l'ensemble des classes d'équivalence :

$$\mathbb{P}^n(\overline{F}):=\{P^{\sim},(0,0,\ldots,0)\neq P\in\mathbb{A}^{n+1}(\overline{\mathbb{F}})\}.$$

L'ensemble $\mathbb{P}^1(\overline{\mathbb{F}})$ est appelé *droite projective*. L'ensemble $\mathbb{P}^2(\overline{\mathbb{F}})$ est appelé *plan projectif*. Une classe d'équivalence $P^{\sim}$ est appelée *point projectif*. L'ensemble des points $\tilde{\mathbb{F}}$-rationnels de $\mathbb{P}^n(\overline{\mathbb{F}})$ pour $\mathbb{F}\subseteq\tilde{\mathbb{F}}\subseteq\overline{F}$ est défini comme étant

$$\mathbb{P}^n(\tilde{\mathbb{F}}):=\{P^{\sim}=(a_1:a_2:\ldots a_{n+1}),\exists\lambda\in\overline{\mathbb{F}}^* \text{ avec } \lambda a_i\in\tilde{F} \text{ pour tout } i\}.$$

Le n-espace affine $\mathbb{A}^n(\overline{\mathbb{F}})$ peut être plongé dans le n-espace projectif en identifiant par exemple le point $(a_1,a_2,\ldots,a_n)\in\mathbb{A}^n(\overline{\mathbb{F}})$ au point $(a_1:a_2:\ldots:a_n:1)\in\mathbb{P}^n(\overline{\mathbb{F}})$

Lemme 2.1.4. *Soit* $U_{n+1}:=\{(a_1:a_2:\ldots:a_{n+1})\in\mathbb{P}^n(\overline{\mathbb{F}}),a_{n+1}\neq 0\}\subseteq\mathbb{P}^n(\overline{\mathbb{F}})$. *Alors, la fonction*

$$\begin{aligned}\varphi_{n+1}:U_{n+1}&\longrightarrow\mathbb{A}^n(\overline{\mathbb{F}})\\(a_1:a_2:\ldots:a_{n+1})&\longmapsto(\frac{a_1}{a_{n+1}},\frac{a_2}{a_{n+1}},\ldots,\frac{a_n}{a_{n+1}})\end{aligned}$$

est une bijection.

Démonstration. Voir [Har77]. □

La fonction réciproque est donnée par

$$(a_1,a_2,\ldots,a_n)\longmapsto(a_1:a_2:\ldots:a_n:1)$$

A partir de ce moment, on peut considérer $\mathbb{A}^n(\overline{\mathbb{F}})$ comme un sous-ensemble de $\mathbb{P}^n(\overline{\mathbb{F}})$. Lorsqu'on parle d'un point sur $\mathbb{P}^n(\overline{\mathbb{F}})$, on notera P la classe de $P^\sim$ par abus de notation.

Pour définir une courbe projective, nous devons d'abord expliquer ce que veut dire "un point est un zéro d'un polynôme". Un polynôme peut s'annuler pour un représentant donné d'un point projectif et ne pas s'annuler pour un autre, raison pour laquelle on considère des *polynômes homogènes*. Les monômes d'un polynôme homogène ont tous le même degré. Ainsi,

$$f(\lambda a_1, \lambda a_2, \ldots, \lambda a_{n+1}) = \lambda^d f(a_1, a_2, \ldots, a_{n+1})$$

pour un polynôme homogène $f \in \mathbb{F}[x_1, x_2, \ldots, x_{n+1}]$ de degré d. Ceci montre, pour un polynôme homogène donné, que tous les représentants d'un point projectif sont tous des zéros ou ne le sont pas.

Dans ce qui suit, les polynômes et les variables seront écrits en lettres majuscules pour distinguer les cas affines et les cas projectifs.

Définition 2.1.5. *Soit $F \in \mathbb{F}[X_1, X_2, \ldots, X_{n+1}]$ un polynôme homogène à $n+1$ variables. Définissons l'ensemble algébrique*

$$\mathcal{C}_F := \{P \in \mathbb{P}^n(\overline{\mathbb{F}}), F(P) = 0\}.$$

Pour toute extension $\mathbb{F} \subseteq \tilde{\mathbb{F}} \subseteq \overline{\mathbb{F}}$ de $\mathbb{F}$, l'ensemble

$$\mathcal{C}_F(\tilde{\mathbb{F}}) := \{P \in \mathcal{C}_F, P \in \mathbb{P}^n(\tilde{\mathbb{F}})\}$$

des points rationnels de l'espace projectif sur $\tilde{\mathbb{F}}$ est appelé ensemble des points $\tilde{\mathbb{F}}$-rationnels de $\mathcal{C}_F$

Définition 2.1.6. *Soit $F \in \mathbb{F}[X, Y, Z]$ un polynôme. L'ensemble projectif $\mathcal{C}_F$ est appelé courbe projective plane. Son degré est défini comme étant celui de F.*

Exemple 2.1.7. *On utilise les mêmes terminologies que pour les courbes affines. Une* droite projective plane *est une courbe projective plane de degré 1. Elle est donnée par un polynôme*

$$L = aX + bY + c,$$

où au moins un des coefficients a, b, c est différent de 0.
Une conique projective plane *est une courbe projective plane de degré 2 donnée par un polynôme*

$$F_C = a_1X^2 + a_2Y^2 + a_3Z^2 + a_4XY + a_5XZ + a_6YZ,$$

où au moins un des coefficients $a_1, a_2, \ldots, a_6$ *est non nul.*
Les courbes projectives planes de degré 3 sont appelées des cubiques projectives planes

Soit $F \in \mathbb{F}[X_1, X_2, \ldots, X_{n+1}]$ un polynôme homogène. On définit le *deshomogénéisé* F_* de F par rapport à x_{n+1} comme étant

$$F_*(x_1, x_2, \ldots, x_n) := F(x_1, x_2, \ldots, x_n, 1) \in \mathbb{F}[x_1, x_2, \ldots, x_n].$$

Réciproquement, pour un polynôme $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ de degré d, on définit l'*homogénéisé* de f comme étant

$$f^*(X_1, X_2, \ldots, X_{n+1}) := X_{n+1}^d f(\frac{X_1}{X_{n+1}}, \frac{X_2}{X_{n+1}}, \ldots, \frac{X_n}{X_{n+1}}) \in \mathbb{F}[X_1, X_2, \ldots, X_{n+1}].$$

Notons que $(f^*)_* = f$ pour tout polynôme $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$. Si X_{n+1} ne divise pas F, alors $(F_*)^* = F$.
Grâce à l'homogénéisation, la déshomogénéisation et l'application φ_n, on peut associer à toute courbe affine plane une courbe projective et réciproquement. Toute courbe projective $\mathcal{C}_F$ contient la courbe affine $\mathcal{C}_{F_*}$. Les points qui sont sur $\mathcal{C}_F$ et qui ne sont pas sur $\mathcal{C}_{F_*}$, c'est-à-dire, les points de la forme $(a_1 : a_2 : \ldots : a_n : 0)$, sont appelés points infinis.

Remarque 2.1.8. *A travers ce document, on utilisera les notations bien connues* $\mathcal{C}_f : f = 0$ *et* $\mathcal{C}_F : F = 0$ *pour les courbes planes.*

Les courbes, comme définies ici, sont des ensembles algébriques spéciaux (voir [Har77] et [Ful69]). Un ensemble algébrique est l'ensemble des zéros d'une collection de polynômes. Les ensembles algébriques sont les fermés d'une topologie sur

les n-espaces affine et projectif, c'est la *topologie de Zariski* [Har77]. Les espaces affine et projectif sont équipés ainsi d'une structure d'espace topologique et on définit la notion d'irréductibilité comme suit : Un ensemble X non vide d'un espace topologique est dit irréductible s'il ne peut être exprimé comme union de deux de ses sous ensembles, chacun d'eux étant un fermé dans X [Har77]. Pour un ensemble algébrique, cela signifie qu'il ne peut être exprimé comme une union de deux sous-ensembles algébriques non triviaux. Notons aussi que la topologie de Zariski dépend du corps de base (corps de définition de la courbe). Un ensemble algébrique qui est irréductible sur $\mathbb{F}$ peut être réductible sur une extension de $\mathbb{F}$. Si l'ensemble algébrique reste irréductible sur toute extension de $\mathbb{F}$, c'est-à-dire s'il est irréductible sur $\overline{\mathbb{F}}$, on dira alors qu'il est absolument irréductible.

Définition 2.1.9. *Une courbe définie sur $\mathbb{F}$ est dit absolument irréductible si elle ne peut être exprimée comme union de deux sous-ensembles algébriques distincts sur $\overline{\mathbb{F}}$.*
Pour une courbe plane $\mathcal{C}_F$, on peut déterminer son irréductibilité en considérant le polynôme F. Un polynôme sur $\mathbb{F}$ est dit absolument irréductible s'il est irréductible en tant que polynôme de $\overline{\mathbb{F}}$.

Lemme 2.1.10. *Une courbe affine plane $\mathcal{C}_f$ (resp : une courbe projective plane) est absolument irréductible si f (resp : F) est absolument irréductible.*

Démonstration. Voir [FL05]. □

Tout espace algébrique peut être écrit de façon unique comme une union d'espaces algébriques irréductibles distincts dont aucun n'est contenu dans un autre ([Har77], [Ful69]). Ces sous-ensembles sont appelés *composantes irréductibles* de l'ensemble algébrique. Pour une courbe affine plane $\mathcal{C}_f$ sur $\overline{\mathbb{F}}$, la factorisation joue le rôle de la décomposition en composantes irréductibles [Ful69].

2.1.2 Singularité et droites tangentes

Dans cette sous-section, on ne considère que les courbes planes, c'est-à-dire les courbes définies par un polynôme $f \in \mathbb{F}[x, y]$ ou par un polynôme homogène $F \in \mathbb{F}[X, Y, Z]$.

Définition 2.1.11. *Soit $\mathcal{C}_f$ une courbe affine, $f \in \mathbb{F}[x, y]$. Un point P sur $\mathcal{C}_f$ est dit* point singulier *si les deux dérivées partielles de f s'annulent en P, c'est-à-dire*

$$\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0$$

Définition 2.1.12. *Soit $\mathcal{C}_F$ une courbe projective, $F \in \mathbb{F}[X, Y, Z]$. Un point $P \in \mathcal{C}_F$ est dit* singulier *si les trois dérivées partielles de F s'annulent en P. Autrement dit,*

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

Définition 2.1.13. *Soit $\mathcal{C}$ une courbe affine ou projective. Si $P \in \mathcal{C}$ est un point singulier alors, $\mathcal{C}$ est dite* singulière *en P. Dans le cas contraire, le point P est dit* non singulier *et la courbe* non singulière *en P.*
La courbe $\mathcal{C}$ est dite non singulière *si elle n'a pas de points singuliers.*

Lemme 2.1.14. *Soit $P = (X_P : Y_P : Z_P) \in \mathcal{C}_F$ un point de la courbe projective $\mathcal{C}_F$ tel que $Z_P \neq 0$. Alors, P est singulier si et seulement si le point $(X_P/Z_p, Y_P/Z_P)$ est singulier sur $\mathcal{C}_{F_*}$*

Démonstration. Voir [Lor96]. □

Lorsqu'on a un point non singulier sur une courbe, il y a une unique tangente à la courbe en ce point. Cette tangente est donnée par les dérivées partielles du polynôme définissant la courbe de la manière suivante.

Définition 2.1.15. *Soit $\mathcal{C}_f$ une courbe affine, $f \in \mathbb{F}[x, y]$ et $P = (x_P, y_P) \in \mathcal{C}_f$ un point non singulier. La droite*

$$t_{f,P} : \frac{\partial f}{\partial x}(P)(x - x_P) + \frac{\partial f}{\partial y}(P)(y - y_P) = 0$$

est appelée droite tangente à $\mathcal{C}_f$ au point P.

Définition 2.1.16. *Soit $\mathcal{C}_F$ une courbe projective, $F \in \mathbb{F}[X,Y,Z]$ et $P = (X_P, Y_P, Z_P) \in \mathcal{C}_F$ un point non singulier. La droite*

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

est appelée droite tangente à $\mathcal{C}_F$ au point P.

Remarque 2.1.17. *Notons que les polynômes décrivant les tangentes dans les définitions précédentes sont de degré 1 puisque le point P est non singulier, en particulier ils sont non nuls. Les polynômes définissant les tangentes projectives dépendent du représentant du point, mais puisque les dérivées partielles sont des polynômes homogènes de degré 1, la tangente est donnée de façon unique [Lor96]. On peut définir la tangente projective en $P = (X_P : Y_P : Z_P)$ comme*

$$T_{F,P} : \frac{\partial F}{\partial X}(P)(X - X_P) + \frac{\partial F}{\partial Y}(P)(Y - Y_P) + \frac{\partial F}{\partial Z}(P)(Z - Z_P) = 0$$

Soit $P = (x_P, y_P) \in \mathcal{C}_f$ un point non singulier. Alors d'après le Lemme 2.1.14, il s'en suit que $P^* = \varphi_3^{-1}(P) = (x_P : y_P : 1)$ est un point non singulier de la courbe $\mathcal{C}_{f^*}$ et la tangente $T_{f^*,P}$ est donnée par l'homogénéisé de $t_{f,P}$ [Lor96].

2.1.3 Nombre d'intersections et Théorème de Bézout

On notera simplement $\mathbb{A}^2 = \mathbb{A}^2(\mathbb{F})$. Soit $\overline{\mathbb{F}}(\mathbb{A}^2) := \overline{\mathbb{F}}(x,y) = \mathrm{Quot}(\overline{\mathbb{F}}[x,y])$ le corps des fonctions rationnelles à deux variables. Ses éléments sont des fonctions rationnelles dans $\mathbb{A}^2$, c'est-à-dire des fractions de polynômes dans $\overline{\mathbb{F}}[x,y]$. Pour un point $P \in \mathbb{A}^2$, on définit

$$\mathcal{O}_P(\mathbb{A}^2) = \{g/h \in \overline{\mathbb{F}}(\mathbb{A}^2), h(P) \neq 0\}.$$

Le sous-anneau $\mathcal{O}_P(\mathbb{A}^2) \subseteq \overline{\mathbb{F}}(\mathbb{A}^2)$ est un anneau local avec

$$\mathcal{M}_P = \{g/h \in \mathcal{O}_P(\mathbb{A}^2), g(P) = 0\}$$

comme idéal maximal (voir [Sti93]).
Soit $f, g \in \mathcal{O}_P(\mathbb{A}^2)$ et soit (f,g) l'idéal dans $\mathcal{O}_P(\mathbb{A}^2)$ engendré par f et g. Alors,

$\mathcal{O}_P(\mathbb{A}^2)/(f,g)$ est un espace vectoriel sur $\mathbb{F}$.
Soit $\mathbb{P}^2 := \mathbb{P}^2(\overline{\mathbb{F}})$. De façon similaire, on définit le corps des fonctions rationnelles

$$\overline{\mathbb{F}}(\mathbb{P}^2) = \{G/H, G, H \in \mathbb{F}[X,Y,Z] \text{ homogènes, } H \neq 0, \deg(G) = \deg(H)\} \cup \{0\}$$

comme étant le corps des fonctions rationnelles homogènes, c'est-à-dire des quotients de polynômes de même degré. Pour un point P, on définit

$$\mathcal{O}_P(\mathbb{P}^2) := \{G/H \in \overline{\mathbb{F}}(\mathbb{P}^2), H(P) = 0\}.$$

L'anneau $O_P(\mathbb{P}^2)$ est un anneau local, avec

$$\mathcal{M}_P(\mathbb{P}^2) := \{G/H \in O_P(\mathbb{P}^2), G(P) = 0\}$$

comme idéal maximal (voir [Sti93]).
Notons que $\overline{\mathbb{F}}(\mathbb{P}^2)$ est isomorphe sur $\overline{\mathbb{F}}$ à $\overline{\mathbb{F}}(\mathbb{A}^2)$, par conséquent les anneaux locaux en P et en $\varphi_3(P)$ sont isomorphes pour $P \in U_3$. On mappe un polynôme homogène $F \in \mathbb{F}[X,Y,Z]$ de degré d dans $\mathcal{O}_P(\mathbb{P})$ en choisissant une droite projective L ne passant pas par P et en posant $F_\times := F/L^d$. Si $P \in U_3$, c'est-à-dire si P est un point tel que $Z \neq 0$, on peut choisir $L = Z$ et $F_\times$ est le deshomogénéisé usuel F_*. Soit $F, G \in \mathbb{F}[X,Y,Z]$ homogènes, alors $F_\times, G_\times \in \mathcal{O}_P(\mathbb{P}^2)$. Si $(F_\times, G_\times)$ est l'idéal engendré par $F_\times$ et $G_\times$, alors l'anneau $\mathcal{O}_P(\mathbb{P}^2)/(F_\times, G_\times)$ est un $\overline{\mathbb{F}}$-espace vectoriel.

Définition 2.1.18. *Soit $f, g \in \mathbb{F}[x,y]$ et $P \in \mathbb{A}^2(\overline{\mathbb{F}})$. Le nombre d'intersections entre $\mathcal{C}_f$ et $\mathcal{C}_g$ au point P est défini comme étant*

$$I(P, \mathcal{C}_f \cap \mathcal{C}_g) := \dim_{\overline{\mathbb{F}}}(\mathcal{O}_P(\mathbb{A}^2)/(f,g)),$$

où (f,g) est l'idéal dans $\mathcal{O}_P(\mathbb{A}^2)$ engendré par f et g.
Soit $F, G \in \mathbb{F}[X,Y,Z]$ deux polynômes homogènes et $P \in \mathbb{P}^2(\overline{\mathbb{F}})$. Le nombre d'intersections entre $\mathcal{C}_F$ et $\mathcal{C}_G$ au point P est défini comme étant

$$I(P, \mathcal{C}_F \cap \mathcal{C}_G) := \dim_{\overline{\mathbb{F}}}(\mathcal{O}_P(\mathbb{P}^2)/(F_\times, G_\times)),$$

où (f,g) est l'idéal dans $\mathcal{O}_P(\mathbb{A}^2)$ engendré par f et g.

Il est clair, pour un point projectif $P \in U_3$ donné, que

$$I(P, \mathcal{C}_F \cap \mathcal{C}_G) = I(\varphi_3(P), \mathcal{C}_{F_*} \cap \mathcal{C}_{G_*}).$$

Le nombre d'intersections est l'unique entier satisfaisant les sept propriétés données dans [Ful69]. Nous ne donnerons que quelques unes de ces propriétés.

Lemme 2.1.19. *Le nombre d'intersection décrit dans la Définition 2.1.18 satisfait les propriétés suivantes :*

1. $\infty > I(P, \mathcal{C}_f \cap \mathcal{C}_g) > 0$ *pour tout* f, g *et* P *tels que* $\mathcal{C}_f$ *et* $\mathcal{C}_g$ *s'intersectent proprement en* P, *c'est-à-dire qu'elles n'ont pas de composantes communes qui passent en* P. *Si les courbes ne s'intersectent pas proprement en* P, *alors* $I(P, \mathcal{C}_f \cap \mathcal{C}_g) = \infty$
2. $I(P, \mathcal{C}_f \cap \mathcal{C}_g) = 0$ *si et seulement si* $P \notin \mathcal{C}_f \cap \mathcal{C}_g$. *Le nombre d'intersection dépend uniquement du nombre de composantes de* $\mathcal{C}_f$ *et de* $\mathcal{C}_g$ *qui passent par* P.
3. $I(P, \mathcal{C}_f \cap \mathcal{C}_g) \geq m_P(\mathcal{C}_f) m_P(\mathcal{C}_G)$, *avec égalité si et seulement si* $\mathcal{C}_f$ *et* $\mathcal{C}_g$ *n'ont pas de tangente commune en* P. *En particulier, si* P *est un point singulier sur* $\mathcal{C}_f$ *et sur* $\mathcal{C}_g$, *alors* $I(P, \mathcal{C}_f \cap \mathcal{C}_g) = 1$ *si et seulement si* $\mathcal{C}_f$ *et* $\mathcal{C}_g$ *n'ont pas de tangente commune en* P.

Démonstration. Voir [Ful69]. □

Le théorème suivant, connu sous le nom de Théorème de Bézout nous renseigne sur le nombre d'intersections entre deux courbes pour un degré donné.

Theorème 2.1.20 (Théorème de Bézout)**.** *Soit* $F, H \in \mathbb{F}[X, Y, Z]$ *deux polynômes homogènes de degrés respectifs* d *et* e *tels que* $\mathcal{C}_F$ *et* $\mathcal{C}_G$ *n'aient aucune composante commune. Alors,*

$$\sum_{P \in \mathcal{C}_F \cap \mathcal{C}_G} I(P, \mathcal{C}_F \cap \mathcal{C}_G) = d.e$$

Démonstration. Voir [Ful69], [Har77]. □

2.1.4 Fonctions, morphismes et twists

Soit $\mathcal{C}_f$ une courbe affine absolument irréductible, définie par un polynôme $f \in \mathbb{F}[x, y]$. Soit $(f) \subseteq \overline{\mathbb{F}}[x, y]$ l'idéal engendré par f. Alors, (f) est un idéal premier et l'anneau

$$\overline{\mathbb{F}}[\mathcal{C}_f] := \overline{\mathbb{F}}[x, y]/(f)$$

est intègre. Il est appelé *anneau des coordonnées* de $\mathcal{C}_f$.

Définition 2.1.21. *Le corps des fractions*

$$\overline{\mathbb{F}}(\mathcal{C}_f) := \mathrm{Quot}(\overline{\mathbb{F}}[\mathcal{C}_f])$$

est appelé corps de fonctions *de* $\mathcal{C}_f$.
Les éléments du corps de fonctions sont appelés des fonctions rationnelles *et sont des quotients de polynômes modulo le polynôme définissant la courbe.*
On définit par $\mathbb{F}[\mathcal{C}_f]$*, l'anneau des coordonnées de* $\mathcal{C}_f$ *sur* $\mathbb{F}$ *et par* $\mathbb{F}(\mathcal{C}_f)$ *le corps de fonctions de* $\mathcal{C}_f$ *sur* $\mathbb{F}$ *comme des sous-ensembles respectifs de* $\overline{\mathbb{F}}[\mathcal{C}_f]$ *et de* $\overline{\mathbb{F}}(\mathcal{C}_f)$*. Le corps* $\mathbb{F}$ *est contenu dans* $\mathbb{F}(\mathcal{C}_f)$*.*

Les éléments dans $\overline{\mathbb{F}}(\mathcal{C}_f)$ définissent des fonctions dans $\mathcal{C}_f$ puisque les polynômes dans $\overline{\mathbb{F}}$ sont des applications $\mathbb{A}^2(\overline{\mathbb{F}}) \longrightarrow \overline{\mathbb{F}}$. Sur l'espace projectif, la situation est différente puisqu'un polynôme dans $\overline{\mathbb{F}}[X, Y, Z]$ donne des valeurs différentes lorsqu'il est évalué en différents représentants d'un point projectif donné.
Soit $\mathcal{C}_F$ une courbe projective, absolument irréductible, définie par un polynôme homogène irréductible $F \in \mathbb{F}[X, Y, Z]$. Notons (F), l'idéal engendré par F. Comme dans le cas affine, on définit l'anneau des coordonnées homogènes par $\overline{\mathbb{F}}_{hom}[\mathcal{C}_F] := \overline{\mathbb{F}}[X, Y, Z]/(F)$. C'est un anneau intègre. Notons $\overline{\mathbb{F}}_{hom}(\mathcal{C}_F) = \mathrm{Quot}(\overline{\mathbb{F}}_{hom}[\mathcal{C}_F])$, l'anneau quotient. Un élément $g \in \overline{\mathbb{F}}_{hom}[\mathcal{C}_F]$ est appelé *forme* s'il existe un polynôme G tel que $g = G + (F)$.

Définition 2.1.22. *Le corps des fonctions de $\mathcal{C}_f$ est le sous-corps de $\overline{\mathbb{F}}_{hom}(\mathcal{C}_F)$ donné par*

$$\overline{\mathbb{F}}(\mathcal{C}_F) = \{g/h, g, h \in \overline{\mathbb{F}}_{hom}[\mathcal{C}_F] \text{ formes de même degré, avec } h \neq 0\} \cup \{0\}.$$

Le corps de fonctions $\mathbb{F}(\mathcal{C}_F)$ sur $\mathbb{F}$ est défini comme étant le corps fixe sous l'action du groupe de Galois $\mathcal{G}_{\overline{\mathbb{F}}/\mathbb{F}}$ sur $\overline{\mathbb{F}}_{hom}(\mathcal{C}_F)$. Les éléments de $\mathbb{F}(\mathcal{C}_F)$ définissent des fonctions sur $\mathcal{C}_F$ puisqu'ils sont représentés sous forme de quotients de même degré. Par conséquent, la valeur d'un tel élément est indépendante du représentant choisi d'un point projectif donné.

L'application $\varphi_3 : U_3 \longrightarrow \mathbb{A}^2(\overline{\mathbb{F}}),\ P = (X_P, Y_P, Z_P) \longmapsto (X_P/Z_P, Y_P/Z_P)$ induit un isomorphisme

$$(\varphi_3^{-1})^* : \overline{\mathbb{F}}(\mathcal{C}_F) \longrightarrow \overline{\mathbb{F}}(\mathcal{C}_{F_*})$$

sur $\overline{\mathbb{F}}$.
Ainsi, le corps de fonction d'une courbe projective est isomorphe au corps des fonctions d'une courbe affine donnée par la déshomogénéisation (voir [Lor96], [Sti93]).

La localisation de l'anneau des coordonnées au point P est le sous-anneau de $\overline{\mathbb{F}}(\mathcal{C}_F)$ donné par

$$\mathcal{O}_P(\mathcal{C}_F) = \{g/h \in \overline{\mathbb{F}}(\mathcal{C}_F), h(P) \neq 0\}.$$

C'est un anneau local avec

$$\mathcal{M}_P(\mathcal{C}_F) = \{g/h \in \mathcal{O}_P(\mathcal{C}_F), g(P) = 0\}$$

comme idéal maximal. Si P est non singulier, alors $\mathcal{O}_P(\mathcal{C}_F)$ est un anneau de valuation discrète et dans ce cas on peut définir une valuation sur $\mathcal{O}_P(\mathcal{C}_F)$.

Définition 2.1.23. *Soit $P \in \mathcal{C}_F$ un point non singulier. La valuation sur $\mathcal{O}_P(\mathcal{C}_F)$ définie par*

$$\begin{aligned} \mathrm{ord}_P : O_P(\mathcal{C}_F) &\longrightarrow \mathbb{N}^* \\ \phi &\longmapsto \max\{m \in \mathbb{Z}, \phi \in \mathcal{M}_P(\mathcal{C}_F)^m\} \end{aligned}$$

est appelée ordre *de* ϕ *en* P

L'application "ordre" peut être étendue sur tout le corps de fonctions en définissant

$$\mathrm{ord}_P : \overline{\mathbb{F}}(\mathcal{C}_F) \longrightarrow \mathbb{Z}, \quad \phi = f/g \longmapsto \mathrm{ord}(f) - \mathrm{ord}(g).$$

Un élément $t \in \overline{\mathbb{F}}(\mathcal{C}_F)$ avec $\mathrm{ord}_P(t) = 1$ est appelé *uniformisante* pour $\mathcal{C}_F$ en P.

Puisque les ensembles algébriques sont définis par des polynômes, les applications naturelles définies entre eux sont aussi des polynômes. En terme de topologie de Zariski, on considère des applications qui sont continues par rapport à cette topologie.
Un morphisme de courbes affines est une application $\varphi : \mathcal{C}_f \longrightarrow \mathcal{C}_g$ donnée par un pair de polynômes (φ_x, φ_y) de $\overline{\mathbb{F}}[x, y]$ qui à tout point $P \in \mathcal{C}_f$ associe le point $(\varphi_x(P), \varphi_y(P)) \in \mathcal{C}_g$. Si $\varphi_x, \varphi_y \in \mathbb{F}[x, y]$, on dira que φ est définie sur $\mathbb{F}$. Tout morphisme entre courbes induit un morphisme d'algèbres $\varphi^* : \overline{\mathbb{F}}[\mathcal{C}_g] \longrightarrow \overline{\mathbb{F}}[\mathcal{C}_f]$ sur $\overline{\mathbb{F}}$ entre les anneaux de coordonnées. D'après [FL05], φ^* est injective si et seulement si φ est surjective, et si φ^* est surjective alors φ est injective. L'application φ^* est un isomorphisme si elle admet un inverse qui est un morphisme. Dans ce cas, φ^* est un isomorphisme d'algèbres sur $\overline{\mathbb{F}}$ (voir [FL05]).

On ne considère maintenant que des courbes projectives en tenant compte du fait que les cas affines peuvent être obtenus avec la déshomogénéisation. Soit $\mathcal{C}_F$ et $\mathcal{C}_G$ deux courbes projectives, absolument irréductibles, définies sur $\mathbb{F}$.
Une application rationnelle de $\mathcal{C}_F$ dans $\mathcal{C}_G$ est une application $\phi : \mathcal{C}_F \longrightarrow \mathcal{C}_G$ donnée par un triplet (ϕ_X, ϕ_Y, ϕ_Z), avec $\phi_X, \phi_Y, \phi_Z \in \overline{\mathbb{F}}(\mathcal{C}_F)$, telle que pour tout point $P \in \mathcal{C}_F$, on a

$$\phi(P) = (\phi_X(P), \phi_Y(P), \phi_Z(P)) \in \mathcal{C}_G,$$

lorsque ϕ_X, ϕ_Y et ϕ_Z sont définies en P. On dit que ϕ est définie sur $\mathbb{F}$ s'il existe $\lambda \in \overline{\mathbb{F}}^*$ tel que $\lambda\phi_X, \lambda\phi_Y, \lambda\phi_Z \in \mathbb{F}(\mathcal{C}_F)$.

Définition 2.1.24. *Deux courbes $\mathcal{C}_F$ et $\mathcal{C}_G$ sont équivalentes birationnellement s'il existe une application $\phi : \mathcal{C}_F \longrightarrow \mathcal{C}_G$ et une application $\varphi : \mathcal{C}_G \longrightarrow \mathcal{C}_F$ telles que les applications $\varphi \circ \phi$ et $\phi \circ \varphi$ soit les applications identités sur $\mathcal{C}_F$ et $\mathcal{C}_G$ respectivement. Dans ce cas, ϕ est appelée* application birationnelle.

Une application rationnelle $\phi : \mathcal{C}_F \longrightarrow \mathcal{C}_G$ est dite régulière en P s'il existe une fonction rationnelle $g \in \overline{\mathbb{F}}(\mathcal{C}_F)$ telle que $g\phi_X, g\phi_Y, g\phi_Z$ soient définies en P et si au moins une des valeurs $g\phi_X(P), g\phi_Y(P), g\phi_Z(P)$ n'est pas nulle.

Définition 2.1.25. *Un morphisme entre $\mathcal{C}_F$ et $\mathcal{C}_G$ est une application rationnelle $\phi : \mathcal{C}_F \longrightarrow \mathcal{C}_G$ qui est régulière en tout point $P \in \mathcal{C}_F$. L'application ϕ est un isomorphisme s'il existe un morphisme $\varphi : \mathcal{C}_F \longrightarrow \mathcal{C}_G$ tel que $\varphi \circ \phi$ et $\phi \circ \varphi$ soient les applications identités sur $\mathcal{C}_F$ et $\mathcal{C}_G$ respectivement. Soit* $\mathrm{Mor}(\mathcal{C}_F, \mathcal{C}_G)$*, l'ensemble des morphismes de $\mathcal{C}_F$ dans $\mathcal{C}_G$ et* $\mathrm{Mor}(\mathcal{C}_F, \mathcal{C}_G)$*, l'ensembles des isomorphismes de $\mathcal{C}_F$ dans $\mathcal{C}_G$. L'ensemble des morphismes et l'ensembles des isomorphismes définis sur $\mathbb{F} \subseteq \tilde{\mathbb{F}} \subseteq \overline{\mathbb{F}}$ sont notés respectivement* $\mathrm{Mor}_{\tilde{\mathbb{F}}}(\mathcal{C}_F, \mathcal{C}_G)$ *et* $\mathrm{Isom}_{\tilde{\mathbb{F}}}(\mathcal{C}_F, \mathcal{C}_G)$*. Les courbes $\mathcal{C}_F$ et $\mathcal{C}_G$ sont isomorphes sur $\tilde{\mathbb{F}}$ s'il existe un isomorphisme entre elles sur $\tilde{\mathbb{F}}$.*

Remarque 2.1.26. *Soit $\phi : \mathcal{C}_F \longrightarrow \mathcal{C}_G$ une application rationnelle, avec $\mathcal{C}_F$ et $\mathcal{C}_G$ deux courbes projectives, non singulières, absolument irréductibles. Alors, ϕ est un morphisme [Sil86]. Si $\phi : \mathcal{C}_F \longrightarrow \mathcal{C}_G$ est un morphisme, alors ϕ est soit constant, soit surjectif [Sil86]. Par composition, ϕ induit une injection de corps de fonctions*

$$\phi^* : \overline{\mathbb{F}}(\mathcal{C}_G) \longrightarrow \overline{\mathbb{F}}(\mathcal{C}_F), \quad f \longmapsto f \circ \phi,$$

(voir [Sil86]).
Le degré d'extension $[\overline{\mathbb{F}}(\mathcal{C}_F) : \phi^*(\overline{\mathbb{F}}(\mathcal{C}_G))]$ est appelé degré *de ϕ.*

Définition 2.1.27. *Soit $\mathcal{C}$, une courbe projective, non singulière, définie sur $\mathbb{F}$. Une courbe non singulière $\mathcal{C}'$, définie sur $\mathbb{F}$ est appelé* twist *de $\mathcal{C}$ si $\mathcal{C}'$ est isomorphe à $\mathcal{C}$ sur $\overline{\mathbb{F}}$. Ce qui signifie, en d'autres termes, que l'ensemble* $\mathrm{Isom}(\mathcal{C}, \mathcal{C}')$ *n'est*

pas vide. On note Twist$(\mathcal{C}/\mathbb{F})$*, l'ensemble des classes d'isomorphismes sur* $\mathbb{F}$ *des courbes qui sont des twists de* $\mathcal{C}$ *sur* $\mathbb{F}$*.*

Si $\mathcal{C}'/\mathbb{F}$ est un twist de $\mathcal{C}/\mathbb{F}$, alors il existe un isomorphisme $\psi \in \mathrm{Isom}(\mathcal{C}, \mathcal{C}')$ et une extension finie $\tilde{\mathbb{F}}$ de $\mathbb{F}$ tels que ψ soit défini sur $\mathbb{F}$.

Définition 2.1.28. *Soit* $\mathcal{C}$ *une courbe projective, définie sur* $\mathbb{F}$ *et* $\mathcal{C}'/\mathbb{F}$ *un twist de* $\mathcal{C}$*. Le degré d'extension minimal pour lequel il existe un isomorphisme* $\psi \in \mathrm{Isom}(\mathcal{C}, \mathcal{C}')$ *qui est défini sur* $\tilde{\mathbb{F}}$*, avec* $[\tilde{\mathbb{F}} : \mathbb{F}] = d$*, est appelé* degré *du twist* $\mathcal{C}'$*. Un twist de degré 2 est appelé* twist quadratique*, un twist de degré 3 est appelé* twist cubique*, ainsi de suite.*

Remarque 2.1.29. *L'ensemble* Twist$(\mathcal{C}/\mathbb{F})$ *est déterminé par le groupe de Galois* $\mathcal{G}_{\overline{\mathbb{F}}/\mathbb{F}}$ *et le groupe* Isom$(\mathcal{C})$ *des isomorphismes de* $\mathcal{C}$ *dans lui même. Pour plus de détails, se référer à [Sil86].*

2.1.5 Diviseurs, groupe de Picard, genre

Dans cette sous-section, nous définissons le groupe de Picard $\mathrm{Pic}^0_{\mathbb{F}}(\mathcal{C})$ de la courbe $\mathcal{C}$. Ce groupe est utilisé dans les applications cryptographiques basées sur les courbes planes pour mettre en œuvres des protocoles liés au problème du logarithme discret. Pour sa description, nous suivons [Sil86] et [FL05].

Soit $\mathcal{C}/\mathbb{F}$ une variété (courbe projective, irréductible) non singulière, définie sur $\mathbb{F}$ par $F(X, Y, Z) = 0$. Le groupe des diviseurs de $\mathcal{C}$, noté Div$(\mathcal{C})$, est le groupe abélien libre engendré par les points de $\mathcal{C}$.
Un élément $D \in \mathrm{Div}(\mathcal{C})$ est exprimée comme une somme formelle

$$D = \sum_{P \in \mathcal{C}} n_P(P),$$

où $n_P \in \mathbb{Z}$ pour tout P et $n_P = 0$ sauf pour un nombre fini de P. D est appelé *diviseur* de $\mathcal{C}$. L'entier $\deg(D) = \sum_{P \in \mathcal{C}} n_P$ est appelé *degré* du diviseur D. L'ensemble des points tels que $n_P \neq 0$ est appelé *support* de D. Le sous-groupe de

$\mathrm{Div}(\mathcal{C})$ de tous les diviseurs de degré 0 est noté

$$\mathrm{Div}^0(C) := \{D \in \mathrm{Div}(\mathcal{C}), \deg(D) = 0\}.$$

A un élément non nul ϕ du corps de fonctions $\overline{\mathbb{F}}(\mathcal{C})$ on associe le diviseur $\mathrm{div}(\phi) = \sum_{P \in \mathcal{C}} \mathrm{ord}_P(\phi)(P)$. Un diviseur $D \in \mathrm{Div}(\mathcal{C})$ est dit *principal* s'il existe une fonction $\phi \in \overline{\mathbb{F}}(\mathcal{C})^*$ telle que $D = \mathrm{div}(\phi)$. On note $\mathrm{Princ}(\mathcal{C})$ l'ensemble des diviseurs principaux. Le degré d'un diviseur principal est égal à 0 [Sil86]. Notons que $\mathrm{Princ}(\mathcal{C}) \subseteq \mathrm{Div}^0(\mathcal{C})$ est un sous-groupe de $\mathrm{Div}^0(\mathcal{C})$.

Définition 2.1.30. *Le groupe de Picard est défini par*

$$\mathrm{Pic}^0(\mathcal{C}) := \mathrm{Div}^0(\mathcal{C})/\mathrm{Princ}(\mathcal{C}).$$

Le sous-groupe de $\mathrm{Pic}^0(\mathcal{C})$ *fixé par le groupe de Galois* $\mathcal{G}_{\bar{\mathbb{F}}/\mathbb{F}}$ *est le groupe des classes de diviseurs définis sur* $\mathbb{F}$ *et noté* $\mathrm{Pic}^0_{\mathbb{F}}(\mathcal{C})$.

Remarque 2.1.31. *Il existe une variété projective, non singulière et absolument irréductible* $J_{\mathcal{C}}$*, définie sur* $\mathbb{F}$ *telle que* $J_{\mathcal{C}}(\tilde{\mathbb{F}})$ *soit isomorphe à* $\mathrm{Pic}^0_{\overline{\mathbb{F}}}(\mathcal{C})^{\mathcal{G}_{\bar{\mathbb{F}}/\tilde{\mathbb{F}}}}$ *pour toute extension* $\mathbb{F} \subseteq \tilde{\mathbb{F}} \subseteq \overline{\mathbb{F}}$*. La variété* $J_{\mathcal{C}}$ *est appelée* Jacobienne *de* $\mathcal{C}$*. Elle a une structure de groupe et la loi de groupe peut être décrite par un morphisme* $J_{\mathcal{C}} \times J_{\mathcal{C}} \longrightarrow J_{\mathcal{C}}$*. C'est aussi un groupe algébrique. Un groupe algébrique projectif est appelé* variété abélienne*.*

Nous allons maintenant introduire la notion de *genre* d'une courbe. Cette notion apparaît dans le théorème important Riemann-Roch dont nous présenterons une version simplifiée comme dans [FL05].
Pour se faire, nous avons besoin de définir un ordre partiel sur $\mathrm{Div}(\mathcal{C})$ comme suit : un diviseur $D = \sum_{P \in \mathcal{C}} n_P(P)$ est dit positif ou effectif si $n_P \geq 0$ pour tout $P \in \mathcal{C}$, et on écrira dans ce cas $D \geq 0$. Soit D_1 et $D_2 \in \mathrm{Div}(\mathcal{C})$. Alors, on écrit $D_1 \geq D_2$ si $D_1 - D_2 \geq 0$. Cette notation est très utile pour décrire les zéros et

les pôles d'une fonction rationnelle. Par exemple, l'inégalité $\mathrm{div}(\phi) \geq (P) - 5Q$ signifie que la fonction ϕ a un zéro d'ordre au moins 1 au point P et un pôle d'ordre au plus 5 au point Q. L'inégalité $\mathrm{div}(\phi) \geq -2P$ signifie que ϕ a un pôle d'ordre au plus 2 en P. Soit $D \in \mathrm{Div}(\mathcal{C})$ un diviseur de $\mathcal{C}$. Définissons l'ensemble

$$\mathcal{L}(D) := \{\phi \in \overline{\mathbb{F}}(\mathcal{C}), \mathrm{div}(\phi) \geq -D\} \cup \{0\}.$$

$\mathcal{L}(D)$ est un $\overline{\mathbb{F}}$-espace vectoriel de dimension finie [Sti93]. On note $l(D) := \dim_{\overline{\mathbb{F}}}(\mathcal{L}(D))$ sa dimension.

Theorème 2.1.32 (Riemann-Roch)**.** *Soit $\mathcal{C}/\mathbb{F}$ une courbe absolument irréductible et non singulière. Il existe alors un entier $g \geq 0$ tel que pour tout diviseur $D \in \mathrm{Div}(\mathcal{C})$*

$$l(D) \geq \deg(D) - g + 1.$$

Si $D \in \mathrm{Div}(\mathcal{C})$ et $\deg(D) \geq 2g - 2$, alors $l(D) = \deg(D) - g + 1$.

Démonstration. Voir [FL05], [Sil86], [Sti93], [Har77]. □

Définition 2.1.33. *L'entier g du théorème ci-dessus est appelé* genre *de $\mathcal{C}$.*

2.1.6 Courbes elliptiques

Cette sous-section est consacrée aux courbes elliptiques. On résumera les principaux résultats dont on a besoin dans les chapitres qui suivent. On considère que $\mathbb{F}$ est un corps parfait.

Définition 2.1.34. *Une* courbe elliptique *sur $\mathbb{F}$ est une courbe projective, non singulière, absolument irréductible, de genre 1 sur $\mathbb{F}$ avec au moins un point rationnel $O \in E(\mathbb{F})$.*

En utilisant le Théorème de Riemann-Roch 2.1.32, on peut montrer que toute courbe elliptique est isomorphe à une courbe plane donnée par une équation spéciale appelée *équation de Weierstrass*.

Proposition 2.1.35. *Soit E une courbe elliptique définie sur $\mathbb{F}$. Alors, E est isomorphe à une courbe $\mathcal{C}$ donnée par l'équation de Weierstrass*

$$\mathcal{C} : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{2.1}$$

avec $a_1, a_2, \ldots, a_6 \in \mathbb{F}$. L'image du point O par l'isomorphisme correspondant est le point $(0 : 1 : 0)$.
Réciproquement, toute courbe non singulière donnée par une équation de Weierstrass 2.1 est une courbe elliptique définie sur $\mathbb{F}$. On peut prendre $O = (0 : 1 : 0)$.

Démonstration. Voir [Sil86]. □

Une courbe elliptique est une courbe projective mais on utilise souvent l'équation affine correspondante :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2.2}$$

On peut facilement voir, en considérant l'équation projective de la courbe, que le point $(0 : 1 : 0)$ est le seul point à l'infini sur E.
Si $\mathrm{char}(F) \neq 2$, on peut utiliser la transformation

$$(x, y) \longmapsto (x', y') = (x, y + \frac{1}{2}(a_1x + a_3))$$

et obtenir après substitution la courbe

$$E' : y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4},$$

où $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$ et $b_6 = a_3^3 + 4a_6$.
La transformation ci-dessus est un $\mathbb{F}$-isomorphisme $E \longrightarrow E'$ [Flo5a]. Si de plus $\mathrm{char}(K) \neq 2, 3$ on peut utiliser la transformation

$$(x, y) \longmapsto (x', y') = (x + \frac{b_2}{12}, y)$$

et l'équation de la courbe devient

$$E" : y^2 = x^3 - \frac{c_4}{48}x - \frac{c_6}{864},$$

où $c_4 = b_2^2 - 24b_4$ et $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$.
Définissons

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 = \frac{1}{4}(b_2b_6 - b_4^2),$$

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \quad \text{et} \quad j = \frac{c_4^3}{\Delta}.$$

La quantité Δ est appelée *discriminant de la courbe* E, j est appelé *j-invariant* de E. On utilise aussi la notation $j(E) = j$.
La courbe E'' est isomorphe à E. On peut donc assumer si $\text{char}(\mathbb{F}) \neq 2, 3$ que E est donnée par l'*équation de Weierstrass réduite*

$$E : y^2 = x^3 + ax + b, \qquad a, b \in \mathbb{F}. \tag{2.3}$$

Dans ce cas, le discriminant et le j-invariant sont donnés par

$$\Delta = -16(4a^3 + 27b^2) \quad \text{et} \quad j = -1728\frac{(4a)^3}{\Delta}.$$

Le discriminant permet de savoir si une courbe donnée par l'équation 2.1.6 est singulière ou non. La courbe E est non singulière si et seulement si $\Delta \neq 0$ [Sil86]. Le j-invariant détermine la classe d'isomorphisme d'une courbe elliptique puisque deux courbes elliptiques sont isomorphes sur $\mathbb{F}$ si et seulement si elles ont le même j-invariant [Sil86].

Exemple 2.1.36. *Soit $\mathbb{F}$ un corps de caractéristique différente de 2 et de 3, et $f = y^2 - x^3 - b$, $0 \neq b \in \mathbb{F}$. On considère la courbe $E = \mathcal{C}_f : y^2 = x^3 + b$ sur $\mathbb{F}$. Le discriminant $\Delta = -16.27b^2$ est non nul puisqu'aucun des facteurs n'est nul dans $\mathbb{F}$. Ainsi, E est non singulière et décrit une courbe elliptique. Le j-invariant $j = 0$. Par conséquent, toutes les courbes $E : y^2 = x^3 + b$ avec $b \neq 0$ sont des courbes elliptiques. Elles sont toutes isomorphes sur $\mathbb{F}$ puisqu'elles ont le même j-invariant.*

Proposition 2.1.37. *Soit E une courbe elliptique. Pour tout diviseur $D \in \text{Div}^0(E)$, il existe un unique point P tel que $D \sim (P) - (O)$. Notons $\sigma(D)$ ce point. Il s'en*

FIGURE 2.1: Une courbe elliptique

suit que pour tous diviseurs $D_1, D_2 \in \mathrm{Div}^0(E)$, $\sigma(D_1) = \sigma(D_2)$ *si et seulement si* $D_1 \sim D_2$. *L'application* σ *est surjective et induit ainsi une bijection*

$$\sigma : \mathrm{Pic}^0(E) \longrightarrow E$$

Démonstration. Voir [Sil86]. □

Puisque $\mathrm{Pic}^0(E)$ est un groupe abélien, la bijection de la proposition précédente induit une structure de groupe abélien sur E. Les ensembles E et $\mathrm{Pic}^0(E)$, en tant que groupes, sont isomorphes. Lorsque E est donnée par une équation de Weierstrass, la loi de groupe peut être exprimée en fonction des points impliqués. On donne dans ce qui suit les formules de la loi de groupe dans les cas $\mathrm{char}(\mathbb{F}) \neq 2, 3$) pour une courbe elliptique donnée par une équation de Weierstrass réduite.

Lemme 2.1.38. *Considérons* $\mathrm{char}(\mathbb{F}) \neq 2, 3$ *et soit* $E : y^2 = x^3 + ax + b$ *une courbe elliptique définie sur* $\mathbb{F}$. *Notons* $+$ *la loi de groupe sur* E.

1. *Pour tout* $P \in E$, $P + O = P$, *c'est-à-dire* O *est l'élément neutre.*

2. *Si* $P = (x_1, y_1)$ *alors,* $(x_1, y_1) + (x_1, -y_1) = O$*, c'est-à-dire l'opposé de* P *est le point* $-P = (x_1, -y_1)$.

3. *Si* $P_1 = (x_1, y_1)$ *et* $P_2 = (x_2, y_2)$*, avec* $P_1 \neq -P_2$*, on définit*

$$\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1) & \text{si } P_1 \neq P_2, \\ (3x_1^2 + a)/(2y_1) & \text{si } P_1 = P_2. \end{cases}$$

Alors, $P_1 + P_2 = P_3 = (x_3, y_3)$*, avec*

$$x_3 = \lambda^2 - x_1 - x_2 \quad \text{et} \quad y = \lambda(x_1 - x_3) - y_1$$

Démonstration. Voir [Sil86], [FL05]. □

Remarque 2.1.39. *La loi de groupe sur une courbe elliptique a une interprétation géométrique à partir de laquelle peuvent être dérivées le formules ci-dessus. Pour additionner deux points* P_1 *et* P_2*, on considère la droite* L *passant par ces deux points. Si les deux points sont confondus, on prend la tangente à la courbe en* P_1*. La droite* L *intersecte la courbe en un troisième point. Le symétrique de ce point par rapport à l'axe des abscisses donne le point* P_3.

On considère maintenant les morphismes entre courbes elliptiques qui sont compatibles avec la loi de groupe. Soit E_1 et E_2, deux courbes elliptiques, O_1 et O_2, leurs éléments neutres respectifs. Un morphisme $\varphi : E_1 \longrightarrow E_2$, avec $\varphi(O_1) = O_2$, est appelé *isogénie*. S'il existe une isogénie entre deux courbes elliptiques E_1 et E_2, on dira que les ces courbes sont isogènes. Les isogénies sont des morphismes de groupes [Sil86]. On note $\mathrm{Hom}(E_1, E_2)$ l'ensemble des isogénies de E_1 dans E_2. Le sous-ensemble des isogénies définies sur $\mathbb{F}$ est noté $\mathrm{Hom}_{\mathbb{F}}(E_1, E_2)$.
L'ensemble $\mathrm{Hom}(E_1, E_2)$ est un groupe abélien puisque E_2 est un groupe abélien. Si $E_1 = E_2$ alors $\mathrm{Hom}(E_1, E_2)$ est un anneau.

Définition 2.1.40. *L'ensemble des endomorphismes* $\mathrm{End}(E)$ *d'une courbe elliptique est défini comme étant* $\mathrm{End}(E) = \mathrm{Hom}(E, E)$*. Les éléments inversibles de* $\mathrm{End}(E)$ *sont appelés des* automorphismes *de* E *et l'ensemble de tous les automorphismes de* E *est noté* $\mathrm{Aut}(E)$.

$\mathrm{Aut}(E)$ *muni de la composition est un groupe. L'ensemble des endomorphismes et l'ensemble des automorphismes de* E *sur* $\mathbb{F}$ *sont notés respectivement* $\mathrm{End}_{\mathbb{F}}(F)$ *et* $\mathrm{Aut}_{\mathbb{F}}(E)$.

Exemple 2.1.41. *Pour* $m \in \mathbb{Z}$, *définissons l'application* $[m] : E \longrightarrow E$ *sur* $E/\mathbb{F}$ *comme suit : soit* $P \in E$ *un point arbitraire. Si* $m = 0$ *alors,* $[m]P = O$. *Si* $m > 0$ *alors,* $[m]P = P + P + \ldots + P$, m *fois. Enfin, si* $m < 0$ *alors,* $[m]P = -[-mP]$. *L'application* $[m]$ *est un endomorphisme sur* $\mathbb{F}$, *c'est-à-dire* $[m] \in \mathrm{End}_{\mathbb{F}}(E)$.

Définition 2.1.42. *Soit* $0 \neq m \in \mathbb{Z}$. *Le noyau de l'application* $[m]$ *est noté*

$$E[m] := Ker([m]) = \{P \in E, [m]P = O\}.$$

$E[m]$ *est appelé* sous-groupe de m-torsion de E. *Les éléments de* $E[m]$ *sont appelés des* points de m-torsion. *L'ensemble des points de* m*-torsion* $\mathbb{F}$*-rationnels est noté* $E(\mathbb{F})[m]$.

Lemme 2.1.43. *Soit* E *une courbe elliptique définie sur* $\mathbb{F}$ *et* $0 \neq m \in \mathbb{Z}$. *Supposons que* $\mathrm{char}(\mathbb{F}) \neq 0$ *ou* $\mathrm{char}(\mathbb{F}) \wedge m = 1$. *Alors,*

$$E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

En particulier, si $m > 0$ *alors* $E[m]$ *est un* $\mathbb{F}_m$ *espace vectoriel de dimension 2.*

Démonstration. Voir [Sil86]. □

L'anneau des endomorphismes d'une courbe elliptique est un anneau intègre de caractéristique 0 [Sil86]. Puisque toutes les applications $[m]$ sont dans $\mathrm{End}(E)$, alors pour tout $m \in \mathbb{Z}$, l'anneau $\mathbb{Z}$ peut être plongé dans $\mathrm{End}(E)$. Par conséquent, l'anneau des endomorphismes d'une courbe elliptique contient toujours une copie de $\mathbb{Z}$.

On considère maintenant les courbes elliptiques définies sur un corps fini. Posons $\mathbb{F} = \mathbb{F}_q$, un corps fini d'ordre q. Soit $p = \mathrm{char}(\mathbb{F}_q)$ la caractéristique de $\mathbb{F}_q$.

Alors q est une puissance de p. L'ensemble $E(\mathbb{F}_q)$ des points $\mathbb{F}_q$-rationnels de E est fini. Le *théorème de Hasse* donne une borne pour le cardinal de $E(\mathbb{F}_q)$.

Theorème 2.1.44 (Hasse)**.** *Soit E une courbe elliptique définie sur $\mathbb{F}_q$. Alors,*

$$\#E(\mathbb{F}_q) = q + 1 - t, \qquad où \;\; |t| \leq 2\sqrt{q}.$$

Démonstration. Voir [Sil86]. □

Les groupes utilisés en cryptographie sont des groupes cycliques d'ordre un nombre premier très grand. Soit E une courbe elliptique définie sur $\mathbb{F}_q$ avec $n = \#E(\mathbb{F}_q)$. Soit $r \neq p$ un nombre premier divisant n.

Définition 2.1.45. *Le* degré de plongement *de E par rapport à r est le plus petit entier k tel que $r|q^k - 1$.*
Si r ne divise pas $(q-1)$, le degré de plongement détermine la plus petite extension de $\mathbb{F}_q$ sur laquelle tous les points de r-torsion de E sont définis.

Theorème 2.1.46. *Soit E une courbe elliptique définie sur $\mathbb{F}_q$, $n = \#E(\mathbb{F}_q)$, r un entier tel que r divise n et r ne divise pas $(q-1)$. Alors, $E[r] \subseteq E(\mathbb{F}_q^k)$ si et seulement si $r|q^k - 1$.*

Démonstration. Voir [BK98]. □

2.1.7 Courbes elliptiques de Huff

Dans cette sous-section, nous introduisons les courbes elliptiques de Huff. Ces courbes, utilisées en 1948 par Huff pour résoudre une équation diophantienne [Huf48], ont été réintroduites par Joye, Tibouchi et Vergnaud dans [JTV10]. Dans [JTV10], les auteurs montrent que les courbes de Huff sont résistantes face aux attaques à canaux cachés. Ils ont aussi montré comment calculer le couplage de Tate sur ces courbes. Nous aborderons la notion de couplage plus loin.

FIGURE 2.2: Courbe de Huff $2x(y^2-1) = y(x^2-1)$ sur $\mathbb{R}$.

Soit $\mathbb{F}$, un corps de caractéristique différente de 2. Une courbe elliptique de Huff sur $\mathbb{F}$ est une courbe $\mathcal{H}_{a,b}$ donnée

$$\mathcal{H}_{a,b} : ax(y^2-1) = by(x^2-1),$$

où $a, b \in \mathbb{F}^*$ et $a^2 \neq b^2$.
Sur cette courbe, l'opposé du point $P = (x, y)$ est le point $-P = (-x, -y)$. Il y a trois points à l'infini. Il s'agit de $(1 : 0 : 0)$, $(0 : 1 : 0)$ et $(a : b : 0)$ en coordonnées projectives. Ce sont les trois points d'ordre 2 sur la courbe. Une loi de groupe sur une courbe elliptique de Huff peut être définie de la manière suivante : soit $P_1 = (x_1, y_1)$ et $P_2 = (x_2, y_2)$ deux points de $\mathcal{H}_{a,b}$. Alors,

$$P_1 + P_2 = \left(\frac{(x_1 + x_2)(1 + y_1y_2)}{(1 + x_1x_2)(1 - y_1y_2)}, \frac{(y_1 + y_2)(1 + x_1x_2)}{(1 - x_1x_2)(1 + y_1y_2)} \right).$$

Le point $(0, 0)$ est l'élément neutre pour l'addition. Cette addition est unifiée, c'est-à-dire qu'elle peut même être utilisée pour calculer le point $2P$ étant donné $P \in \mathcal{H}_{a,b}$. De plus, si le point $P \in \mathcal{H}_{a,b}(\mathbb{F})$ est un point d'ordre impair, alors l'addition est complète sur le sous-groupe engendré par P.

Dans [JTV10], les auteurs ont aussi introduit le twist quadratique du modèle de Huff. Ce twist est donné par :

$$\mathcal{H}^d_{a,b} : ax(y^2 - d) = by(x^2 - d).$$

La loi de groupe sur ce twist est définie de la manière suivante : si $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in \mathcal{H}^d_{a,b}$, alors

$$P_1 + P_2 = \left(\frac{d(x_1 + x_2)(d + y_1y_2)}{(d + x_1x_2)(d - y_1y_2)}, \frac{d(y_1 + y_2)(d + x_1x_2)}{(d - x_1x_2)(d + y_1y_2)} \right).$$

Wu et Fung donnent une généralisation des courbes elliptiques de Huff dans [WF10] en introduisant la nouvelle forme :

$$\tilde{\mathcal{H}}_{a,b} : x(ay^2 - 1) = y(bx^2 - 1),$$

avec $ab(a - b) \neq 0$. Ce nouveau modèle contient les courbes de Huff ordinaires comme cas particulier.
Sur la forme généralisée $\tilde{\mathcal{H}}_{a,b}$, si $a = \mu^2$ et $b = \nu^2$ sont des carrés dans $\mathbb{F}$, on peut poser $x' = \nu x$ et $y' = \mu y$. Ainsi, $\mu x'(y'^2 - 1) = \nu y'(x'^2 - 1)$.
Ce qui veut dire que les courbes de la forme $ax(y^2 - 1) = by(x^2 - 1)$ sont inclues dans la famille de courbes $x(ay^2 - 1) = y(bx^2 - 1)$, où a et b sont des carrés dans $\mathbb{F}$. Notons que $\tilde{\mathcal{H}}_{a,b}$ est une courbe elliptique lisse si $ab(a - b) \neq 0$.

Theorème 2.1.47. *Soit $\mathbb{F}$ un corps de caractéristique différente de 2 et soit a, b des éléments de $\mathbb{F}$ avec $a \neq b$. Alors, la courbe*

$$\tilde{\mathcal{H}}_{a,b} : X(aY^2 - Z^2) = Y(bX^2 - Z^2)$$

est isomorphe à la courbe elliptique

$$V^2W = U(U + aW)(U + bW)$$

avec le changement de variables $\varphi(X, Y, Z) = (U, V, W)$, où $U = bX - aY$, $V = (b - a)Z$ et $W = Y - X$. L'application inverse est donnée par $\psi(U, V, W) = (X, Y, Z)$, avec $X = U + aW$, $Y = U + bW$ et $Z = V$.

En coordonnées affines, la courbe de Huff $x(ay^2-1)=y(bx^2-1)$ définie sur $\mathbb{F}$ est isomorphe à la courbe elliptique $y^2=x(x+a)(x+b)$ sur $\mathbb{F}$.

Loi de groupe sur $x(ay^2-1)=y(bx^2-1)$:

Soit $y=y_1+\lambda(x-x_1)=\lambda x+\mu$ l'équation de la droite passant par P_1 et P_2, deux points de la courbe, où λ est la pente. On obtient d'après l'équation de la courbe $x(a(\lambda x+\mu)^2-1)=(\lambda x+\mu)(bx^2-1)$. Soit $S=P_1+P_2=(x_3,y_3)$. Alors,

$$P_1+P_2=\left(\frac{(x_1+x_2)(ay_1y_2+1)}{(bx_1x_2+1)(ay_1y_2-1)},\frac{(y_1+y_2)(bx_1x_2+1)}{(bx_1x_2-1)(ay_1y_2+1)}\right).$$

Considérons maintenant P_1 et P_2 en coordonnées projectives, c'est-à-dire $P_1=(X_1,Y_1,Z_1)$ et $P_2=(X_2,Y_2,Z_2)$, et $U=O=(0,0,1)$ comme élément neutre de la loi d'addition. Soit $S=P_1+P_2=(X_3,Y_3,Z_3)$. Alors,

$$\begin{cases} X_3=\big(X_1Z_2+X_2Z_1\big)\big(aY_1Y_2+Z_1Z_2\big)^2\big(Z_1Z_2-bX_1X_2\big),\\ Y_3=\big(Y_1Z_2+Y_2Z_1\big)\big(bX_1X_2+Z_1Z_2\big)^2\big(Z_1Z_2-aY_1Y_2\big),\\ Z_3=(b^2X_1^2X_2^2-Z_1^2Z_2^2)(a^2Y_1^2Y_2^2-Z_1^2Z_2^2). \end{cases}$$

Soit **m**, **s** et **c** les coûts respectifs de la multiplication, de l'élévation au carré et de la multiplication par une constante. Posons $M_1=X_1X_2$, $M_2=Y_1Y_2$, $M_3=Z_1Z_2$, $C_1=bM_1$ et $C_2=aM_2$.

1. $M_4=(X_1+Z_1)(X_2+Z_2)-M_1-M_3$, $\quad M_5=(Y_1+Z_1)(Y_2+Z_2)-M_2-M_3$
2. $M_6=(M_3-C_1)(M_3+C_2)$, $\quad M_7=(M_3+C_1)(M_3-C_2)$.

Ainsi, $X_3=M_4M_6(M_3+C_2)$, $Y_3=M_5M_7(M_3+C_1)$ et $Z_3=M_6M_7$. Par conséquent, l'addition des points P_1 et P_2 peut être effectuée en $12\mathbf{m}+2\mathbf{c}$, où les $2\mathbf{c}$ représentent le coût de la multiplication par les constantes a et b.

La formule d'addition peut aussi être utilisée pour calculer le point $2P=(x_3,y_3)$ étant donné $P=(x_1,y_1)$. On a ainsi,

$$x_3=\frac{2x_1(ay_1^2+1)}{(bx_1^2+1)(ay_1^2-1)} \quad \text{et} \quad y_3=\frac{2y_1(bx_1^2+1)}{(bx_1^2-1)(ay_1^2+1)}.$$

En coordonnées projectives et avec $U=O=(0,0,1)$ comme élément neutre, le point $2P$ peut être évalué en $7\mathrm{m}+5\mathrm{s}+2\mathrm{c}$.

2.1.8 Courbes hyperelliptiques

Dans cette sous-section, nous donnons une brève introduction sur les courbes hyperelliptiques. On considérera principalement les courbes hyperelliptiques de genre 2. On considère aussi que $\mathbb{F}$ est un corps parfait.

Définition 2.1.48. *Une courbe projective non singulière $\mathcal{C}/\mathbb{F}$ de genre g est appelée* courbe hyperelliptique *de genre g si son corps de fonctions $\mathbb{F}(\mathcal{C})$ est une extension séparable de degré 2 du corps des fonctions rationnelles $\mathbb{F}(x)$, c'est-à-dire $[\mathbb{F}(\mathcal{C}) : \mathbb{F}(x)] = 2$.*

A l'aide du théorème de Riemann-Roch, on peut voir qu'une courbe hyperelliptique peut être donnée par l'équation d'une courbe affine plane non singulière [FL05].

Proposition 2.1.49. *Le corps de fonction d'une courbe hyperelliptique de genre g sur $\mathbb{F}$ est le corps de fonction d'une courbe affine plane non singulière donnée par*

$$\mathcal{C} : y^2 + h(x)y = f(x),$$

où $h(x), f(x) \in \mathbb{F}[x]$, $\deg(f) \in \{2g+1, 2g+2\}$ et $\deg(h) \leq g+1$.

Démonstration. Voir [FL05]. □

Remarque 2.1.50. *Si $\deg(f) = 2g+1$ et char$(\mathbb{F}) \neq 2$, l'équation de la courbe peut être transformée en $y^2 = f(x)$ [FL05]. Dans ce cas, un point $P = (x_P, y_P)$ est dit singulier si $y_p = 0$ et x_P est une racine double de $f(x)$. Par conséquent, une courbe hyperelliptique définie sur un corps de caractéristique différente de 2 peut être décrite par $\mathcal{C} : y^2 = f(x)$, où f n'admet que des racines simples dans $\overline{\mathbb{F}}[x]$.*

A partir de cette définition, on peut considérer une courbe elliptique comme une

FIGURE 2.3: Une courbe hyperelliptique

courbe hyperelliptique de genre 1. Mais si $g > 1$, les points de $\mathcal{C}$ ne forment pas un groupe. Par conséquent, on utilise le groupe de Picard $\mathrm{Pic}^0(\mathcal{C})$ ou en d'autres termes, la Jacobienne de $\mathcal{C}$ pour des utilisations cryptographiques. Le théorème suivant donne une très jolie représentation des éléments de $\mathrm{Pic}^0(\mathcal{C})$.

Theorème 2.1.51 (Représentation de Mumford)**.** *Soit* $\mathcal{C} : y^2+h(x)y = f(x)$*, une courbe hyperelliptique de genre* g*, avec* $f, h \in \mathbb{F}[x]$*,* $\deg(f) = 2g+1$ *et* $\deg(h) \leq g$*. Soit* $\mathbb{F} \subseteq \tilde{\mathbb{F}} \subseteq \overline{\mathbb{F}}$ *une extension de* $\mathbb{F}$*. Alors, tout élément non trivial de* $\mathrm{Pic}^0_{\tilde{\mathbb{F}}}(E)$ *peut être représenté par un unique couple de polynômes* $(u(x), v(x))$*,* $u, v \in \tilde{F}[x]$*, où*

1. u *est un polynôme unitaire,*
2. $\deg(v) \leq \deg(u) \leq g$ *,*
3. $u | v^2 + vh - f$*.*

Démonstration. Voir [FL05]. □

Remarque 2.1.52. *L'arithmétique dans $Pic^0_{\tilde{\mathbb{F}}}(\mathcal{C})$ avec la représentation de Mumford peut être réalisée en utilisant l'algorithme de Cantor [Can87] ou [DL05]. La représentation de Mumford montre aussi que le groupe de Picard $Pic^0_{\overline{\mathbb{F}}_q}(\mathcal{C})$ d'une courbe hyperelliptique définie sur un corps fini est fini.*

On identifie $J_{\mathcal{C}}$ à $\mathrm{Pic}^0(\mathcal{C})$. Rappelons que les éléments de $J_{\mathcal{C}}$ sont des classes de diviseurs. On note $\overline{D}$ la classe du diviseur D. Un endomorphisme de $J_{\mathcal{C}}$ est un morphisme de variétés abéliennes $J_{\mathcal{C}} \longrightarrow J_{\mathcal{C}}$, c'est-à-dire un morphisme de groupes. en particulier, il fixe l'élément neutre de $J_{\mathcal{C}}$.
On note $\mathrm{End}(J_{\mathcal{C}})$, l'ensemble des endomorphismes de $J_{\mathcal{C}}$ et par $\mathrm{End}_{\tilde{\mathbb{F}}}(J_{\mathcal{C}})$ l'ensemble des endomorphismes de J_C définis sur $\tilde{\mathbb{F}}$, pour $\mathbb{F} \subseteq \tilde{\mathbb{F}} \subseteq \overline{\mathbb{F}}$.

Exemple 2.1.53. *Un endomorphisme très important de $J_{\mathcal{C}}$ est l'application $[m] : J_{\mathcal{C}} \longrightarrow J_{\mathcal{C}}$, pour $m \in \mathbb{Z}$. A une classe de diviseurs $\overline{D}$, on associe $[m]\overline{D} = \overline{D} + \overline{D} + \ldots + \overline{D}$, m fois. Le noyau de $[m]$ est noté*

$$J_{\mathcal{C}}[m] = \{\overline{D} \in J_{\mathcal{C}}, [m]\overline{D} = \overline{O}\},$$

où $\overline{O}$ est la classe du diviseur $D = O$. Pour tout $\mathbb{F} \subseteq \tilde{F} \subseteq \overline{\mathbb{F}}$, le sous-ensemble des diviseurs $\tilde{\mathbb{F}}$-rationnels de $J_{\mathcal{C}}$ est noté $J_{\mathcal{C}}(\tilde{\mathbb{F}})[m]$.

2.1.9 Extracteurs déterministes

Définition 2.1.54 (Probabilité de collision)**.** *Soit S un ensemble fini et X une variable aléatoire sur S. La probabilité de collision de X, notée $Col(X)$, est la probabilité*

$$Col(X) = \sum_{s \in S} Pr[X = s]^2.$$

Si X et X' sont des variables aléatoires identiquement distribuées sur S, alors la probabilité de collision de X peut être interprétée comme $Col(X) = Pr[X = X']$.

Définition 2.1.55 (Distance statistique)**.** *Soit X et Y deux variables aléatoires sur un ensemble fini S. La distance statistique $\Delta(X,Y)$ entre X et Y est définie comme étant*

$$\Delta(X,Y) = \tfrac{1}{2}\sum_{s\in S} |Pr[X=s] - Pr[Y=s]|.$$

Soit U_S une variable aléatoire uniformément distribuée sur S. Alors une variable aléatoire X sur S est dite δ-uniforme si

$$\Delta(X,U_S) \leq \delta.$$

Lemme 2.1.56. *Soit X une variable aléatoire sur un ensemble fini S de cardinal $|S|$ et soit $\epsilon = \Delta(X,U_S)$ la distance statistique entre X et U_S, où U_S est la variable aléatoire uniformément distribuée sur S. Alors,*

$$Col(X) \geq \frac{1+4\epsilon^2}{|S|}.$$

Pour prouver ce lemme on a besoin du résultat suivant.

Lemme 2.1.57. *Soit S un ensemble et $(\alpha_x)_{x\in S}$ une suite de nombres réels. Alors*

$$\frac{\left(\sum_{x\in S}|\alpha_x|\right)^2}{|S|} \leq \sum_{x\in S}\alpha_x^2. \tag{2.4}$$

Démonstration. Cette inégalité est une conséquence directe de celle de Cauchy-Schwarz :

$$\sum_{x\in S}|\alpha_x| = \sum_{x\in S}|\alpha_x|.1 \leq \sqrt{\sum_{x\in S}\alpha_x^2}\sqrt{\sum_{x\in S}1^2} \leq \sqrt{|S|}\sqrt{\sum_{x\in S}\alpha_x^2}.$$

Le résultat peut être déduit facilement. □

Si X est une variable aléatoire sur S et si on considère que $\alpha_x = Pr[X=x]$, alors puisque la somme des probabilités est égale à 1 et $Col(X) = \sum_{x\in S} Pr[X=x]^2$, on a

$$\frac{1}{|S|} \leq Col(X). \tag{2.5}$$

On peut maintenant donner la preuve du Lemme 2.1.56

Démonstration. Si $\epsilon = 0$, alors le résultat est une conséquence facile de l'équation 2.5. Supposons que $\epsilon \neq 0$. Définissons

$$q_x = |Pr[X = x] - 1/|S||/2\epsilon.$$

On a alors $\sum_x q_x = 1$ et d'après l'équation 2.4, on a :

$$\begin{aligned}\frac{1}{|S|} &\leq \sum_{x \in S} q_x^2 = \sum_{x \in S} \frac{(Pr[X = x] - 1/|S|)^2}{4\epsilon^2} = \frac{1}{4\epsilon^2}\left(\sum_{x \in S} Pr[X = x]^2 - 1/|S|\right) \\ &\leq \frac{1}{4\epsilon^2}(Col(X) - 1/|S|).\end{aligned}$$

D'où le résultat. □

Définition 2.1.58. *Soit S et T deux ensembles finis. Soit Ext une fonction $Ext : S \longrightarrow T$. On dit que Ext est un (T, δ)-extracteur déterministe pour S si $Ext(U_S)$ est δ-uniforme sur T. En d'autres termes,*

$$\Delta(Ext(U_S), U_T) \leq \delta.$$

2.1.10 Le Leftover Hash Lemma

Dans cette sous-section nous rappelons le Leftover Hash Lemma [HILL99, GKR04] qui est l'extracteur déterministe le plus célèbre dans la littérature. Cet extracteur requiert l'utilisation de familles de fonctions de hachage universelles.

Définition 2.1.59 (Guessing probability)**.** *Soit $\mathcal{V}$ un ensemble de cardinal N et soit X une variable aléatoire à valeurs dans $\mathcal{V}$. La "guessing probability" $\gamma(X)$ de X est définie comme étant $\gamma(X) = \max\{P[X = v] : v \in \mathcal{V}\}$.*

Définition 2.1.60 (Familles de fonctions de hachage universelles)**.** *Soit $\mathcal{H} = \{h_i\}_i$ une famille de fonctions de hachage facilement calculables $h_i : \{0,1\}^n \longrightarrow \{0,1\}^k$, pour $i \in \{0,1\}^d$. On dit que $\mathcal{H}$ est une famille de fonctions de hachage universelles si pour tout $x \neq y$ dans $\{0,1\}^n$,*

$$\Pr_{i \in \{0,1\}^d}[h_i(x) = h_i(y)] \leq 1/2^k.$$

Theorème 2.1.61 (Leftover Hash Lemma)**.** *Soit $\mathcal{H}$ une famille de fonctions de hachage universelles de $\{0,1\}^n$ dans $\{0,1\}^k$.Soit i une variable aléatoire uniformément distribuée sur $\{0,1\}^d$, soit U_k une variable aléatoire uniformément distribuée sur $\{0,1\}^k$, et soit A une variable aléatoire sur $\{0,1\}^n$, avec i et A qui sont mutuellement indépendantes. Soit $\gamma = \gamma(A)$, alors*

$$\Delta(\langle i, h_i(A)\rangle, \langle i, U_k\rangle) \leq \frac{\sqrt{2^k\gamma}}{2}.$$

Démonstration. Voir [Sho05]. □

Pour plus de détails sur les extracteurs, se référer à [Sha02, TV00].

Chapitre 3
EXTRACTION D'ALÉA SUR LES CORPS FINIS

Dans ce chapitre, nous présentons un extracteur déterministe, simple et efficace pour un sous-groupe multiplicatif de $\mathbb{F}^*_{p^n}$, où p est un entier premier. En particulier, nous montrons que les k-premiers coefficients dans $\mathbb{F}_2$ d'un élément aléatoire d'un sous-groupe de $\mathbb{F}^*_{2^n}$ sont indistinguables d'une chaîne de bits de même longueur. Ainsi, sous l'hypothèse du problème décisionnel de Diffie-Hellman sur les corps binaires, on peut dériver de façon déterministe une chaîne de bits uniforme à partir d'une clé secrète après l'échange de clés Diffie-Hellman dans le modèle standard. Cet extracteur, qu'on a noté ici ext_k peut être utilisé dans n'importe quel protocole ou schéma de chiffrement ou de signature qui requiert la dérivation d'une chaîne de bits uniforme à partir d'un élément d'un corps binaire.
Ce chapitre est organisé comme suit : dans la première section, nous rappelons certaines constructions d'extracteurs pour les corps finis qui ont été proposés, dans la section 2 nous donnons quelques résultats importants que nous utiliserons dans la suite. La section 3 sera consacrée à la présentation, à l'analyse et les applications de notre nouvel extracteur.

3.1 Extraction d'aléa sur $\mathbb{F}_p$

Récemment, Fouque *et al.* ont proposé dans [FPSZ06] un extracteur d'aléa déterministe très simple pour les éléments Diffie-Hellman. Plus précisément, ils montrent que les k bits de poids fort (resp. de poids faible) d'un élément aléatoire d'un sous-groupe de $\mathbb{F}^*_p$ sont indistinguables d'une chaîne de bits aléatoire de même longueur. Leur extracteur est défini de la manière suivante :
Soit p un nombre premier de n bits, c'est-à-dire $2^{n-1} \leq p < 2^n$, soit G un sous-groupe de $\mathbb{F}^*_p$ d'ordre q avec $q \gg \sqrt{p}$, l un entier tel que $2^{l-1} \leq q < 2^l$ et soit X une variable aléatoire uniformément distribuée dans G. Soit k un entier et soit U_k

une variable aléatoire uniformément distribuée sur $\{0,1\}^k$. Si x est un entier, on note $\mathbf{lsb}_k(x)$ (resp. $\mathbf{msb}_k(x)$) les k bits de poids faible (resp. fort) de x.

Définition 3.1.1. *La fonction* $Ext_k : \{0,1\}^n \longrightarrow \{0,1\}^k, \quad c \longmapsto \mathbf{lsb}_k(c)$ *est appelée* (n,p,q,k)*-extracteur pour* G*.*

Theorème 3.1.2 ([FPSZ06])**.** *Avec les notations précédentes pour un* (n,p,q,k)*-extracteur pour* G *, on a*

$$\Delta(Ext_k(X), U_k) < \frac{2^k}{p} + \frac{2^k\sqrt{p}\log_2(p)}{q} < 2^{k+n/2+\log_2(n)+1-l}.$$

Corollaire 3.1.3 ([FPSZ06])**.** *Soit* e *un entier positif. Supposons que* $\log_2(q) > m = n/2+k+e+\log_2(n)+1$*. Alors,l'application* Ext_k *est un* $(m, 2^{-e})$*-extracteur déterministe pour* G*.*

Les auteurs montrent que si les paramètres $n = 1024$, $e = 80$ et que l'on veut extraire une clé de 128 bits d'un élément Diffie-Hellman dans un sous-groupe G de $\mathbb{F}_p^*$ avec la fonction Ext_k, alors G doit contenir 2^{713} éléments.

Dans [CFPZ09], Chevalier *et al.* améliorent la distance statistique et du coup, le nombre de bits que l'on peut extraire avec la fonction Ext_k avec une nouvelle technique décrite dans [CFPZ09]. Ils ont établit le théorème suivant :

Theorème 3.1.4. *Soit* p *un nombre premier de* n *bits, soit* G *un sous-groupe d'ordre* q *(avec* $l = \log_2(q)$*) de* $\mathbb{F}_p^*$*, soit* U_G *une variable aléatoire uniformément distribuée sur* G *et* k *un entier positif. Alors,*

$$\Delta(Ext_k(U_G), U_k) \leq \begin{cases} 2^{3n/4-l-1} & si\ p^{3/4} + 2^{(k-l)/2} \leq q, \\ 2^{(k+n+\log_2(n))/2-l} & si\ (2^{-8}p)^{2/3}) \leq q \leq p^{3/4}, \\ 2^{(k+n/2+\log_2(n)+4)/2-5l/8} & si\ p^{1/2} \leq q \leq (2^{-8}p)^{2/3}), \\ 2^{(k+n/4+\log_2(n)+4)/2-3l/8} & si\ (2^{16}p)^{1/3} \leq q \leq p^{1/2}. \end{cases}$$

Corollaire 3.1.5. *Soit e un entier positif et supposons que les inégalités*

$$k \leq \begin{cases} l-(2e+2) & \text{et } 2^e p^{3/4} \leq q, \\ 2l-(n+2e+\log_2(n)) & \text{et } (2^{-8}p)^{2/3} \leq q \leq 2^e p^{3/4}, \\ 5l/4-(n/2+2e+\log_2(n)+4) & \text{et } p^{1/2} \leq q \leq (2^{-8}p)^{2/3}, \\ 3l/4-(n/4+2e+\log_2(n)+4) & \text{et } (2^{16}p)^{1/3} \leq q \leq p^{1/2}. \end{cases}$$

soient vraies. Alors, l'application Ext_k est un $(U_G, 2^{-e})$-extracteur déterministe.

Cette fois-ci, on peut extraire une chaîne de 256 bits avec les paramètres $n = 1024$ et $e = 80$ mais avec $|G| \sim 2^{756}$.
Notons que dans ce qui précède, les auteurs ont proposé un extracteur déterministe et efficace sur les corps premiers $\mathbb{F}_p$. Leur approche n'inclut pas les corps $\mathbb{F}_{p^n}$. L'objet de notre contribution est de proposer un extracteur déterministe et efficace sur $\mathbb{F}_{p^n}$.

3.2 Sommes de caractères incomplètes sur les corps finis

Dans cette section, nous rappelons quelques résultats fondamentaux sur les sommes de caractères sur les corps finis. On note e_p le caractère sur $\mathbb{F}_p$ tel que, pour tout $y \in \mathbb{F}_p$, $e_p(y) = e^{\frac{2i\pi y}{p}} \in \mathbb{C}^*$, et ψ le caractère additif de $\mathbb{F}_{p^n}$ tel que pour tout $x \in \mathbb{F}_{p^n}$, $\psi(x) = e_p(\mathrm{Tr}(x))$, où $\mathrm{Tr}(x) = x + x^p + \ldots + x^{p^{n-1}}$ est la trace de $x \in \mathbb{F}_{p^n}$ dans $\mathbb{F}_p$.

Lemme 3.2.1. *Soit ψ un caractère additif de $\mathbb{F}_{p^n}$ et soit G un sous-groupe multiplicatif de $\mathbb{F}_{p^n}^*$. Considérons la somme de Gauss $T(a, G) = \sum_{x \in G} \psi(ax)$. Alors,*

$$\max_{a \in \mathbb{F}_{p^n}^*} |T(a, G)| \leq \sqrt{p^n}.$$

Démonstration. Voir [KS99] ou [Shp04]. □

Lemme 3.2.2. *Soit V un sous-groupe additif de $\mathbb{F}_{p^n}$ et soit ψ un caractère additif de $\mathbb{F}_{p^n}$. Alors,*

$$\sum_{y \in \mathbb{F}_{p^n}} \left| \sum_{z \in V} \psi(yz) \right| \leq p^n.$$

Démonstration. Voir [Win01]. □

Pour plus de détails sur les sommes de caractères, se référer à [KS99, LN83].

3.3 Extraction d'aléa sur $\mathbb{F}_{p^n}$

Dans cette section, nous proposons et prouvons la sécurité d'un extracteur déterministe et simple pour un sous-groupe G de $\mathbb{F}_{p^n}$. Le théorème central de cette section établit que les k-premiers coefficients dans $\mathbb{F}_p$ d'un élément aléatoire de G sont indistinguables d'un élément de groupe aléatoire de $\mathbb{F}_p^k$. Pour prouver ce théorème, nous utilisons les sommes d'exponentielles pour borner la distance statistique.

Considérons le corps fini $\mathbb{F}_{p^n}$, où p est premier et n est un entier positif plus grand que 1. Alors, $\mathbb{F}_{p^n}$ est un espace vectoriel de dimension n sur $\mathbb{F}_p$. Soit $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ une base de $\mathbb{F}_{p^n}$ sur $\mathbb{F}_p$. Ce qui veut dire que, tout élément x de $\mathbb{F}_{p^n}$ peut être représenté sous la forme $x = x_1\alpha_1 + x_2\alpha_2 + \ldots + x_n\alpha_n$, où $x_i \in \mathbb{F}_p$. Soit G un sous-groupe multiplicatif de $\mathbb{F}_{p^n}$. L'extracteur ext_k, pour un élément aléatoire x de G donné, renvoie les k-premiers coefficients dans $\mathbb{F}_p$ de x.

Définition 3.3.1. *Soit $G \subset \mathbb{F}_{p^n}^*$ un sous-groupe multiplicatif d'ordre q et soit k un entier positif plus petit que n. L'extracteur* ext_k *est défini comme étant la fonction*

$$\begin{aligned} \mathrm{ext}_k : G &\longrightarrow \mathbb{F}_p^k \\ x &\longmapsto (x_1, x_2, \ldots, x_k), \end{aligned}$$

où x est représenté sous la forme $x = x_1\alpha_1 + x_2\alpha_2 + \ldots + x_n\alpha_n$.

Le théorème suivant montre que ext_k est un bon extracteur d'aléa.

Theorème 3.3.2. *Soit $G \subset \mathbb{F}^*_{p^n}$ un sous-groupe multiplicatif d'ordre q. Alors,*

$$\Delta(\mathrm{ext}_k(U_G), U_{\mathbb{F}_q^k}) \leq \frac{\sqrt{p^{n+k}}}{2q},$$

où $1 < k < n$ est un entier positif, U_G est une variable aléatoire uniformément distribuée sur G et $U_{\mathbb{F}_p^k}$ est la distribution uniforme sur $\mathbb{F}_p^k$.

Démonstration. Définissons les ensembles

$$M = \{(x_{k+1}\alpha_{k+1} + x_{k+2}\alpha_{k+2} + \ldots + x_n\alpha_n), x_i \in \mathbb{F}_p\} \subset \mathbb{F}_{p^n},$$

et

$$A = \{(x, y) \in G^2 / \exists m \in M, x - y = m\}.$$

Construisons maintenant la fonction caractéristique

$$\mathbf{1}_{(x,y,m)} = \frac{1}{p^n} \times \sum_{a \in \mathbb{F}_q} \psi(a(x - y - m)),$$

qui est égale à 1 si $x - y = m$ et 0 sinon. Alors, le cardinal de l'ensemble A est donné par

$$|A| = \frac{1}{p^n} \times \sum_{x \in G} \sum_{y \in G} \sum_{m \in M} \sum_{a \in \mathbb{F}_p^n} \psi(a(x - y - m)).$$

Par conséquent,

$$\begin{aligned}
\mathrm{Col}(\mathrm{ext}_k(U_G)) &= \frac{|A|}{|G|^2} = \frac{|A|}{q^2} \\
&= \frac{1}{q^2 \times p^n} \times \sum_{x\in G}\sum_{y\in G}\sum_{m\in M}\sum_{a\in\mathbb{F}_p^n} \psi(a(x-y-m)) \\
&= \frac{1}{p^k} + \frac{1}{q^2 \times p^n} \times \sum_{x\in G}\sum_{y\in G}\sum_{m\in M}\sum_{a\in\mathbb{F}_{p^n}^*} \psi(a(x-y-m)) \\
&= \frac{1}{p^k} + \frac{1}{q^2 \times p^n} \times \sum_{a\in\mathbb{F}_{p^n}^*} \left(\sum_{x\in G}\psi(ax)\right)\left(\sum_{y\in G}\psi(-ay)\right)\sum_{m\in M}\psi(-am) \\
&= \frac{1}{p^k} + \frac{1}{q^2 \times p^n} \times \sum_{a\in\mathbb{F}_{p^n}^*} T(a,G).T(-a,G)\sum_{m\in M}\psi(-am) \\
&\leq \frac{1}{p^k} + \frac{1}{q^2 \times p^n} \times R^2 \times \sum_{a\in\mathbb{F}_{p^n}^*} \left|\sum_{m\in M}\psi(-am)\right|,
\end{aligned}$$

où $R = \max_{a\in\mathbb{F}_{p^n}^*} |T(a,G)|$ ..

Puisque

- $R \leq \sqrt{p^n}$, d'après le Lemme 3.2.1,
- and $\sum_{a\in\mathbb{F}_{p^n}^*} \left|\sum_{m\in M}\psi(-am)\right| \leq p^n$, d'après le Lemme 4.2.1,

on a les inégalités suivantes :

$$\mathrm{Col}(\mathrm{ext}_k(U_G)) \leq \frac{1}{p^k} + \frac{p^n}{q^2}.$$

Ainsi,

$$\frac{1 + 4\Delta^2(ext_k(U_G), U_{\mathbb{F}_p^k})}{p^k} \leq \frac{1}{p^k} + \frac{p^n}{q^2}.$$

Donc,

$$\Delta(\mathrm{ext}_k(U_G), U_{\mathbb{F}_p^k}) \leq \frac{\sqrt{p^{n+k}}}{2q}.$$

□

Corollaire 3.3.3. *Soit $p > 2$ un nombre premier et soit $G \subset \mathbb{F}_{p^n}^*$ un sous-groupe multiplicatif d'ordre q, avec $|q| = r$ et $|p| = m$. Si $e > 1$ et $k > 1$ sont deux entiers tels que*

$$k \leq \frac{2r - 2e - mn}{m},$$

alors ext_k *est un* $(U_G, \frac{1}{2^e})$*-extracteur déterministe.*

Démonstration. Puisque $k \leq \frac{2r-2e-mn}{m}$, on a

$$\frac{m(n+k)}{2} \leq r - e \Longleftrightarrow 2^{\frac{m(n+k)}{2}} \leq 2^r \times 2^{-e} \Longleftrightarrow \frac{2^{\frac{m(n+k)}{2}}}{2 \times 2^{r-1}} \leq 2^{-e}.$$

D'où $\Delta(\mathrm{ext}_k(U_G), U_{\mathbb{F}_p^k}) \leq 2^{-e}$. □

Pour les corps de caractéristique 2, on a le corollaire suivant.

Corollaire 3.3.4. *Soit $G \subset \mathbb{F}_{2^n}^*$ un sous-groupe multiplicatif d'ordre q avec $|q| = r$. Si $e > 1$ et $k > 1$ sont des entiers tels que*

$$k \leq 2r - 2e - n,$$

alors ext_k *est un* $(U_G, \frac{1}{2^e})$*-extracteur déterministe.*

Démonstration. On a

$$k \leq 2t - 2e - n \Leftrightarrow 2^{\frac{(n+k)}{2}} \leq 2^r 2^{-e}.$$

Puisque $p = 2$ et $2^{r-1} \leq q < 2^r$, on en déduit que $p^{\frac{(n+k)}{2}} \leq \frac{2^r}{2^e}$. Ainsi,

$$\frac{\sqrt{p^{n+k}}}{2 \times 2^{r-1}} \leq \frac{1}{2^e} \Longleftrightarrow \frac{\sqrt{p^{n+k}}}{2q} \leq \frac{1}{2^e}.$$

□

Remarque 3.3.5. *On a les mêmes résultats que précédemment si on considère cette fois-ci que l'extracteur* ext_k *renvoie les k derniers coefficients dans $\mathbb{F}_p$ d'un élément aléatoire d'un sous-groupe multiplicatif G de $\mathbb{F}_{p^n}^*$.*

3.4 Applications

Notre fonction ext_k peut extraire l'entropie de n'importe quel élément aléatoire d'un sous-groupe G multiplicatif d'un corps fini $\mathbb{F}_{p^n}$. Par conséquent, une application naturelle de celui-ci est la dérivation de clé à partir d'un élément aléatoire Diffie-Hellman dans un groupe DDH, $G \subset \mathbb{F}^*_{2^n}$. Après un échange de clé Diffie-Hellman, les parties s'accordent sur un élément aléatoire du sous-groupe G qui est indistinguable d'un élément uniformément distribué dans G, sous l'hypothèse DDH. Cependant, cet élément aléatoire ne suffit pas puisqu'on a besoin d'une chaîne de bits uniformément distribuée pour les schémas symétriques. Ainsi, on peut essayer d'extraire l'entropie contenue dans cet élément aléatoire Diffie-Hellman par le biais d'un extracteur d'aléa.

Supposons par exemple que l'on veut extraire une clé symétrique de 256 bits à partir d'un élément aléatoire après une échange de clés Diffie-Hellman dans un sous-groupe G de $\mathbb{F}_{2^n}$ avec une borne de sécurité de $2^{-e} = 2^{-80}$ comme dans le Leftover Hash Lemma. Alors, on peut choisir un entier premier $n = 811$ et consider un sous-groupe G d'ordre premier q avec $|q| = r = 615$. On obtient exactement une chaîne de 256 bits parfaitement aléatoire avec la borne de sécurité 2^{-80}. Notons que le sous-groupe G contient q éléments, avec $2^{615} \leq q < 2^{616}$.

Dans le tableau suivant, nous donnons la taille $q = |G|$ de G ,(avec $p = 2$ et $e = 80$) en fonction n(= premier) et du nombre de bits extraits k.

k (key)\\n (prime)	521	811	1021	1153
128	$\|q\| = 404$	$\|q\| = 549$	$\|q\| = 654$	$\|q\| = 720$
192	$\|q\| = 432$	$\|q\| = 581$	$\|q\| = 686$	$\|q\| = 752$
224	$\|q\| = 448$	$\|q\| = 597$	$\|q\| = 702$	$\|q\| = 768$
256	$\|q\| = 468$	$\|q\| = 615$	$\|q\| = 718$	$\|q\| = 783$

Conclusion

Dans ce chapitre, nous avons étendu l'étude de l'existence d'extracteurs déterministes pour un sous-groupe G d'un corps fini $\mathbb{F}_p$ à un corps de la forme $\mathbb{F}_{p^n}$ où p est un nombre premier et $n > 1$ un entier. L'extracteur, noté ext_k, étant donné un élément aléatoire d'un sous-groupe multiplicatif G de $\mathbb{F}_{p^n}$, renvoie les k premiers (resp. k derniers) coefficients dans $\mathbb{F}_p$ de cet élément. Cet extracteur marche pour tout corps fini $\mathbb{F}_{p^n}$ dans lequel l'hypothèse DDH est vérifiée. Par conséquent, si la taille q de G est très grande, on peut toujours dériver une clé symétrique à partir d'un élément Diffie-Hellman dans G. De façon générale, l'extracteur peut être utilisé dans n'importe quel protocole cryptographique qui requiert l'extraction de bits à partir d'un élément du corps $\mathbb{F}_p^n$.

Chapitre 4
EXTRACTION D'ALÉA SUR LES COURBES ELLIPTIQUES

Un extracteur déterministe pour une courbe elliptique est une fonction qui convertit un point aléatoire de la courbe en une chaîne de bits aléatoires avec une distribution proche de l'uniforme. Les extracteurs sont des outils très importants en cryptographie. Ils sont utilisés dans les fonctions de dérivation de clés, dans les protocoles d'échange de clés et pour construire des générateurs de nombres pseudo-aléatoires cryptographiquement sûrs.
Dans ce chapitre, nous présentons un extracteur déterministe et efficace pour une courbe elliptique E définie sur un corps fini $\mathbb{F}_q n$, où q est un nombre premier et n un entier positif. Notre extracteur, noté $\mathcal{D}_k$, étant donné un point aléatoire P sur la courbe E, renvoie les k-premiers $\mathbb{F}_q$-coordonnées de l'abscisse de P.
L'extracteur confirme en même temps les deux conjectures de R. R. Farashahi et R. Pellikaan dans [FP07] et de R. R. Farashahi, A. Sidorenko et R. Pellikaan dans [FPS08] sur l'extraction de bits à partir d'un point d'une courbe elliptique.
Ce chapitre est organisé comme suit :
Dans la première section, nous donnons un aperçu des différents extracteurs qui ont été proposés.
Dans la section 2, on rappelle quelques définitions et quelques théorèmes fondamentaux sur les sommes de caractères. Pour terminer, en section 3, nous décrivons notre nouvel extracteur qui résout les deux conjectures posées dans [FP07] et [FPS08].

4.1 État de l'art

Un extracteur déterministe pour une courbe elliptique est une fonction qui convertit un point uniformément aléatoire sur la courbe en une chaîne de bits aléatoire de longueur fixe. Plusieurs extracteurs ont été proposés, parmi lesquels

celui de Gürel dans [GÖ5]. Il est défini de la manière suivante.

Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_{q^2} \cong \mathbb{F}_q[t]/(t^2 - c)$, où q est un nombre premier et c n'est pas un résidu quadratique dans $\mathbb{F}_q$. Alors $\mathbb{F}_{q^2}$ peut être considéré comme un espace vectoriel sur $\mathbb{F}_q$ muni de la base naturelle $\{1, t\}$. Ainsi, tout élément $z \in \mathbb{F}_{q^2}$ peut s'écrire sous la forme $z = z_0 + z_1 t$, avec $z_0, z_1 \in \mathbb{F}_q$. L'extracteur dans [GÖ5] est définie comme une fonction

$$\mathcal{H} : E(\mathbb{F}_{q^2}) \longrightarrow \mathbb{F}_q, \quad (x, y) \longmapsto x_0,$$

où $x = x_0 + x_1 t$ avec $x_0, x_1 \in \mathbb{F}_q$.
Le théorème suivant donne une estimation de la taille de $\mathcal{H}^{-1}(z)$, pour tout $z \in \mathbb{F}_q$.

Theorème 4.1.1. *Soit E une courbe elliptique définie sur $\mathbb{F}_{q^2}$ par une équation affine $Y^2 = X^3 + aX + b$. Soit $\mathbb{F}_{q^2} \cong \mathbb{F}_q[t]/(t^2 - c)$, où c n'est pas un résidu quadratique sur $\mathbb{F}_q$. Alors, pour tout $z \in \mathbb{F}_q$*

$$|\#\mathcal{H}^{-1}(z) - (q+1)| \leq 20\sqrt{q} + 14,$$

et

$$m \leq \mathcal{H}^{-1}(0) \leq M,$$

où $m = \min(2(q+1) - 4\sqrt{q}, (q+1) - 20\sqrt{q} - 14)$ et $M = \max(2(q+1) + 4\sqrt{q}, (q+1) + 20\sqrt{q} + 14)$.

Démonstration. Voir [GÖ5]. □

Soit D la distribution

$$D = \{P \in_R E, X = \mathcal{H}(P)\}.$$

Lemme 4.1.2. *Soit U_q la distribution uniforme sur $\mathbb{F}_q$. Alors,*

$$\Delta(D, U_q) \leq \frac{21\sqrt{2}}{\sqrt{2^l}},$$

avec q s'écrivant sous la forme $q = 2^l - \lambda$, $\lambda \in [1, 2^{l/2}]$.

Démonstration. Voir [GÖ5]. □

Dans la même logique, Farashahi et Pellikaan proposent deux extracteurs $\mathcal{H}_0$ et $\mathcal{H}_1$ pour une courbe elliptique définie sur $\mathbb{F}_{2^n}$, où $n = 2l$ [FPS08].

Soit E une courbe elliptique définie sur $\mathbb{F}_{2^n}$, c'est-à-dire

$$E(\mathbb{F}_{2^n}) = \{(x, y)\ \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}, y^2 + xy = f(x)\} \cup \{O\},$$

où $f(x) = x^3 + ax^2 + b$, $a, b \in \mathbb{F}_{2^n}^*$ et O est le point à l'infini.
Soit $n = 2l$, l étant un entier arbitraire strictement positif. Alors, $\mathbb{F}_{2^n}$ est une extension quadratique de $\mathbb{F}_{2^l}$. On peut ainsi écrire $\mathbb{F}_{2^n} \cong \mathbb{F}_{2^l}[t]/(t^2 + t + c)$, où $t^2+t+c \in \mathbb{F}_{2^l}[t]$ est un polynôme unitaire irréductible. Tout $x \in \mathbb{F}_{2^n}$ peut s'écrire sous la forme $x = x_0 + x_1 t$, avec $x_0, x_1 \in \mathbb{F}_{2^l}$.

Définition 4.1.3. *Les extracteurs $\mathcal{H}_0$ et $\mathcal{H}_1$ sont définis comme étant des fonctions*

$$\mathcal{H}_0 : E(\mathbb{F}_{2^n}) \longrightarrow \mathbb{F}_{2^l}, \quad (x, y) \longmapsto x_0$$

et

$$\mathcal{H}_1 : E(\mathbb{F}_{2^n}) \longrightarrow \mathbb{F}_{2^l}, \quad (x, y) \longmapsto x_1$$

avec $\mathcal{H}_0(O) = \mathcal{H}_1(O) = 0$.

Les deux théorèmes suivants donnent une estimation de $\#\mathcal{H}_0^{-1}(z)$ et de $\#\mathcal{H}_1^{-1}(z)$ pour $z \in \mathbb{F}_{2^l}$.

Theorème 4.1.4. *Pour tout $z \in \mathbb{F}_{2^l}$,*

$$|\#\mathcal{H}_0^{-1}(z) - 2^l| \leq 2 \left\lfloor 2^{(l+2)/2} \right\rfloor$$

et pour $z = 0$

$$|\#\mathcal{H}_0^{-1}(0) - (2^l + 1)| \leq \left\lfloor 2^{(l+2)/2} \right\rfloor.$$

Démonstration. Voir [FPS08] □

Theorème 4.1.5. *Pour tout* $z \in \mathbb{F}_{2^l}$,

$$|\#\mathcal{H}_1^{-1}(z) - (2^l + 1)| \leq \left\lfloor 2^{(l+2)/2} + 1 \right\rfloor,$$

pour $z = 0$ *et* $b_1 \neq 0$ *avec* $b = b_0 + b_1 t$, *on a*

$$|\#\mathcal{H}_1^{-1}(0) - (2^l + 1)| \leq 1$$

et si $z = 0$ *et* $b_1 = 0$ *alors,*

$$|\#\mathcal{H}_1^{-1}(0) - (2^l + 1)| \leq 2^l - 1.$$

Démonstration. Voir [FPS08]. □

Corollaire 4.1.6. $\mathcal{H}_0$ *et* $\mathcal{H}_1$ *sont des extracteurs* $O(\frac{1}{\sqrt{2^l}})$*-déterministes pour* $E(\mathbb{F}_{2^n})$.

Démonstration. Voir [FPS08]. □

Dans le même papier, les auteurs ont posé une conjecture concernant la généralisation de $\mathcal{H}_0$ pour une courbe elliptique $E(\mathbb{F}_{2^n})$, où n est un entier positif arbitraire.

Soit E une courbe elliptique définie sur $\mathbb{F}_{2^n}$, avec n un entier strictement positif. En particulier, n peut être un nombre premier. Un élément $x \in \mathbb{F}_{2^n}$ peut être représenté par la chaîne de bits $(x_1, x_2, \ldots, x_n)$. Considérons l'extracteur

$$ext_k : E(\mathbb{F}_{2^n}) \longrightarrow \{0,1\}^k, \quad (x, y) \longmapsto (x_1, x_2, \ldots, x_k),$$

avec $1 \leq k \leq n$.
Soit X la variable aléatoire sur $\{0,1\}^k$ définie par

$$X = ext_k(P), \quad \text{pour } P \in_R E(\mathbb{F}_{2^n}).$$

Conjecture 4.1.7. *La variable aléatoire* X *est statistiquement proche de la variable uniforme* U_k *:*

$$\Delta(X, U_k) \leq \frac{g}{\sqrt{2^{n-k}}},$$

où g *est une constante.*

Nous avons confirmé cette conjecture dans [CS11].

Dans [FP07], Farashahi et Pellikaan proposent une extracteur déterministe efficace Ext pour une courbe (hyper)elliptique définie sur $\mathbb{F}_{q^2}$, où q est une puissance d'un nombre premier. Leurs travaux ont amélioré les résultats dans [Gö5].
Soit $\mathcal{C}$ une courbe affine, plane, non singulière, absolument irréductible, définie sur $\mathbb{F}_{q^2}$, avec $q = p^k$ où p est un nombre premier et k un entier strictement positif.

Définition 4.1.8. *L'extracteur Ext est définie comme étant une fonction*

$$Ext : \mathcal{C}(\mathbb{F}_{q^2}) \longrightarrow \mathbb{F}_q, \quad (x, y) \longmapsto x_0,$$

où $x \in \mathbb{F}_{q^2}$ est représenté sous la forme $x = x_0 + x_1 t$.

La proposition suivante montre que Ext est un bon extracteur pour $\mathcal{C}(\mathbb{F}_{q^2})$.

Proposition 4.1.9. *Soit X une variable aléatoire sur $\mathbb{F}_q$ définie par*

$$X = Ext(P) \quad pour \quad P \in_R \mathcal{C}(\mathbb{F}_{q^2}).$$

Alors X est statistiquement proche de la variable uniforme $U_{\mathbb{F}_q}$, en d'autres termes

$$\Delta(X, U_{\mathbb{F}_q}) = O\left(\frac{1}{\sqrt{q}}\right)$$

Démonstration. Voir [FP07]. □

Ils ont aussi posé une conjecture sur Ext. Considérons le corps fini $\mathbb{F}_{q^n}$, où q est une puissance d'un nombre premier et n un entier strictement positif. Alors $\mathbb{F}_{q^n}$ peut être considéré comme un espace vectoriel sur $\mathbb{F}_q$. Soit $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ une base de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$. Alors, tout élément $x \in \mathbb{F}_{q^n}$ peut être représenté sous la forme $x = x_1\alpha_1 + x_2\alpha_2, \ldots + x_n\alpha_n$, où les $x_i \in \mathbb{F}_q$.
Soit $\mathcal{C}$ une courbe affine non singulière, absolument irréductible, définie sur $\mathbb{F}_{q^n}$ par l'équation $y^m = f(x)$, où $f \in \mathbb{F}_{q^n}[x]$ est un polynôme unitaire de degré d et m un entier divisant $q - 1$.

Définition 4.1.10. *Soit k un entier positif plus petit que n. On définit*

$$ext_k : \mathcal{C}(\mathbb{F}_{q^n}) \longrightarrow \mathbb{F}_q^k, \quad (x, y) \longmapsto (x_1, x_2, \ldots, x_k),$$

avec $x = x_1\alpha_1 + x_2\alpha_2 + \ldots + x_n\alpha_n$ et $x_i \in \mathbb{F}_q$.

Soit X_k la variable aléatoire sur $\mathbb{F}_q^k$ définie par

$$X_k = ext_k(P) \text{ pour } P \in \mathcal{C}(\mathbb{F}_{q^n}).$$

Conjecture 4.1.11. *La variable aléatoire X_k est $\frac{c}{\sqrt{q^{n-k}}}$-uniforme sur $\mathbb{F}_q^k$, avec c une constante dépendant de m, n et de d :*

$$\Delta(X_k, U_{\mathbb{F}_q^k}) \leq \frac{c}{\sqrt{q^{n-k}}}.$$

Nous avons prouvé dans [CS11] que cette conjecture était vraie si $\mathcal{C}$ est courbe elliptique.

4.2 Sommes de caractères et courbes elliptiques

Dans cette section, nous rappelons quelques notions sur les sommes de caractères sur les courbes elliptiques que nous utiliserons dans la suite

4.2.1 Sommes de caractères

Dans ce qui suit, on note e_q le caractère sur $\mathbb{F}_q$ tel que pour tout $x \in \mathbb{F}_q$

$$e_q(x) = e^{\frac{2i\pi x}{q}} \in \mathbb{C}^*.$$

On note $\Psi = \mathrm{Hom}(\mathbb{F}_{q^n}, \mathbb{C}^*)$, le groupe des caractères additifs sur $\mathbb{F}_{q^n}$. Un caractère $\psi \in \Psi$ peut être écrit sous la forme $\psi(z) = e_q(\mathrm{Tr}(\alpha z))$, pour tout $z\ in \mathbb{F}_{q^n}$, où $\mathrm{Tr}(x)$ est la trace de $x \in \mathbb{F}_{q^n}$ dans $\mathbb{F}_q$ (see [KS00]).

Lemme 4.2.1. *Soit V un sous-groupe additif de $\mathbb{F}_{p^n}$. Alors,*

$$\sum_{\psi\in\Psi}\left|\sum_{z\in V}\psi(z)\right| \leq p^n.$$

Démonstration. Voir [Win01]. □

4.2.2 Courbes elliptiques et sommes de caractères

Soit E une courbe elliptique définie sur $\mathbb{F}_{q^n}$ et donnée par l'équation de Weierstrass

$$y^2 + (a_1x + a_3)y = x^3 + a_2x^2 + a_4x + a_6.$$

On note $E(\mathbb{F}_{q^n})$, le groupe des éléments de E sur $\mathbb{F}_{q^n}$. Le cardinal de $E(\mathbb{F}_{q^n})$ est noté N. N satisfait

$$|N - (q^n + 1)| \leq 2\sqrt{q^n}.$$

On note $\mathbb{F}_{q^n}[E]$, l'anneau des coordonnées de de E sur $\mathbb{F}_{q^n}$ et $\mathbb{F}_{q^n}(E)$ le corps de fonction de E sur $\mathbb{F}_{q^n}$. $\mathbb{F}_{q^n}[E] = \mathbb{F}_{q^n}[x,y]/(h(x,y))$, où $h(x,y) = y^2 + (a_1x + a_3)y - x^3 - a_2x^2 - a_4x - a_6$ est irréductible.
On note aussi $\mathbb{F}_{q^n}(E)$ le corps de fractions de $\mathbb{F}_{q^n}[E]$. Pour tout point $P \in E(\mathbb{F}_{q^n}) - \{\infty\}$, on note $P = (x(P), y(P))$, où $x(P)$ et $y(P)$ sont les coordonnées du point P.
Si $f \in \mathbb{F}_{q^n}(E)$, on note $\deg(f)$ son degré, qui est $\sum_{i=1}^{s} n_i \deg(P_i)$ si $\sum_{i=1}^{s} n_iP_i$ est le diviseur des pôles de f. On note $\Omega = \mathrm{Hom}(E(\mathbb{F}_{q^n}), \mathbb{C}^*)$, le groupe des caractères sur $E(\mathbb{F}_{q^n})$, et ω_0 le caractère trivial qui est tel que $\omega_0(P) = 1$ pour tout $P \in E(\mathbb{F}_{q^n})$. Pour un sous-groupe G de $E(\mathbb{F}_{q^n})$, on définit

$$S(\omega,\psi,f,E(\mathbb{F}_{q^n})) = \sum_{P\in E(\mathbb{F}_{q^n})} \omega(P)\psi(f(P))$$
$$S(\omega,\psi,f,G) = \sum_{P\in G} \omega(P)\psi(f(P))$$

et

$$S(\psi, f, E(\mathbb{F}_{q^n})) = S(\omega_0, \psi, f, E(\mathbb{F}_{q^n})) = \sum_{P \in E(\mathbb{F}_{q^n})} \psi(f(P))$$
$$S(\psi, f, G) = S(\omega_0, \psi, f, G) = \sum_{P \in G} \psi(f(P))$$

où $\omega \in \Omega$, $\psi \in \Psi$ et $f \in \mathbb{F}_{q^n}(E)$. En particulier, nous nous intéresserons aux sommes avec $f = x$.
Dans [KS00], D. R. Kohel et I. E. Shparlinski énoncent le théorème et le corollaire suivants qui donnent une borne pour $S(\omega, \psi, f, E(\mathbb{F}_{q^n}))$.

Theorème 4.2.2. *(see [KS00]) Soit E une courbe elliptique sur $\mathbb{F}_{q^n}$, $f \in \mathbb{F}_{q^n}(E)$, $\omega \in \Omega$ et $\psi \in \Psi$ un caractère non trivial. Alors,*

$$S(\omega, \psi, f, E(\mathbb{F}_{q^n})) \leq 2 \deg(f) \sqrt{q^n}.$$

Et en particulier, si $f = x$, $\deg(f) = 2$ et

$$S(\psi, f, E(\mathbb{F}_{q^n})) \leq 4\sqrt{q^n}.$$

Corollaire 4.2.3. *Soit E une courbe elliptique définie sur $\mathbb{F}_{q^n}$ et G un sous-groupe de $E(\mathbb{F}_{q^n})$, $\omega \in \Omega$ et $\psi \in \Psi$ des caractères non triviaux. Alors,*

$$S(\omega, \psi, f, G) \leq 2 \deg(f) \sqrt{q^n}.$$

Et en particulier, si $f = x$, $\deg(f) = 2$ et

$$S(\psi, f, G) \leq 4\sqrt{q^n}.$$

Dans la section suivante, nous utilisons cette borne de $S(\omega, \psi, f, E(\mathbb{F}_{q^n}))$ pour montrer que $\mathcal{D}_k$ est un bon extracteur d'aléa pour $E(\mathbb{F}_{q^n})$.

4.3 Extraction d'aléa dans $E(\mathbb{F}_{q^n})$

Considérons le corps fini $\mathbb{F}_{q^n}$, où q est un nombre premier et n un entier positif. Alors, $\mathbb{F}_{q^n}$ est un espace vectoriel de dimension n sur $\mathbb{F}_q$. Soit $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ une base de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$. Ce qui signifie que tout élément x de $\mathbb{F}_{q^n}$ peut être représenté sous la forme $x = x_1\alpha_1 + x_2\alpha_2 + \ldots + x_n\alpha_n$, où $x_i \in \mathbb{F}_q$. Soit E une courbe elliptique définie sur $\mathbb{F}_{q^n}$ par l'équation de Weierstrass

$$y^2 + (a_1x + a_3)y = x^3 + a_2x^2 + a_4x + a_6.$$

L'extracteur $\mathcal{D}_k$, où k est un entier positif plus petit que n,étant donné un point P sur $E(\mathbb{F}_{q^n})$, renvoie les k premières $\mathbb{F}_q$-coordonnées de l'abscisse du point P.

Définition 4.3.1. *Soit G un sous-groupe de $E(\mathbb{F}_{q^n})$ et soit k un entier positif plus petit que n. L'extracteur $\mathcal{D}_k$ est défini comme étant la fonction*

$$\begin{aligned} \mathcal{D}_k : G &\longrightarrow \mathbb{F}_q^k \\ P = (x, y) &\longmapsto (x_1, x_2, \ldots, x_k) \end{aligned}$$

où $x \in \mathbb{F}_{q^n}$ est écrit sous la forme $x = x_1\alpha_1 + x_2\alpha_2 + \ldots + x_n\alpha_n$, et $x_i \in \mathbb{F}_q$.

Theorème 4.3.2. *Soit E une courbe elliptique définie sur $\mathbb{F}_{q^n}$ et G un sous-groupe de $E(\mathbb{F}_{q^n})$. Alors,*

$$\Delta(\mathcal{D}_k(U_G), U_{\mathbb{F}_q^k}) \leq \frac{2\sqrt{q^{n+k}}}{|G|}$$

où U_G est une variable aléatoire uniformément distribuée sur G et $U_{\mathbb{F}_q^k}$ est la distribution uniforme sur $\mathbb{F}_q^k$.

Démonstration. Soit $f = x \in \mathbb{F}_{q^n}(E)$ et considérons les ensembles

$$M = \{(x_{k+1}\alpha_{k+1} + x_{k+2}\alpha_{k+2} + \ldots + x_n\alpha_n), x_i \in \mathbb{F}_q\} \subset \mathbb{F}_{q^n}$$

et

$$\mathbb{A} = \{(P, Q) \in G^2, \exists m \in M : f(P) - f(Q) = m\}.$$

Puisque

$$\frac{1}{q^n}\sum_{\psi\in\Psi}\psi(f(P)-f(Q)-m)=1_{(P,Q,m)},$$

où $1_{(P,Q,m)}$ est la fonction caractéristique qui est égale à 1 si $f(P)-f(Q)=m$ et à 0 sinon, on a

$$|\mathbb{A}|=\frac{1}{q^n}\sum_{P\in G}\sum_{Q\in G}\sum_{m\in M}\sum_{\psi\in\Psi}\psi(f(P)-f(Q)-m)$$

et

$$Col(\mathcal{D}_k(U_G))=\frac{1}{|G|^2}\,|\mathbb{A}|$$

$$\begin{aligned}
Col(\mathcal{D}_k(U_G)) &= \frac{1}{|G|^2\times q^n}\sum_{P\in G}\sum_{Q\in G}\sum_{m\in M}\sum_{\psi\in\Psi}\psi(f(P)-f(Q)-m)\\
&= \frac{1}{|G|^2q^n}q^{n-k}|G|^2+\frac{1}{|G|^2q^n}\sum_{P\in G}\sum_{Q\in G}\sum_{m\in M}\sum_{\psi\neq\psi_0}\psi(f(P)-f(Q)-m)\\
&= \frac{1}{q^k}+\frac{1}{|G|^2q^n}\sum_{\psi\neq\psi_0}\left(\sum_{P\in G}\psi(f(P))\right)\left(\sum_{Q\in G}\psi(-f(Q))\right)\left(\sum_{m\in M}\psi(-m)\right)\\
&= \frac{1}{q^k}+\frac{1}{|G|^2q^n}\sum_{\psi\neq\psi_0}S(\psi,f,G)S(\psi,-f,G)\left(\sum_{m\in M}\psi(-m)\right)\\
&\leq \frac{1}{q^k}+\frac{R^2}{|G|^2q^n}\sum_{\psi\neq\psi_0}\left|\sum_{m\in M}\psi(-m)\right|\\
&\leq \frac{1}{q^k}+\frac{R^2}{|G|^2},
\end{aligned}$$

où $R=\max_\psi(|S(\psi,f,G)|)$

D'après le Lemme 2.1.56, on a

$$\frac{1+4\Delta^2(\mathcal{D}_k(U_G),U_{\mathbb{F}_q^k})}{q^k}\leq Col(\mathcal{D}_k(U_G))\leq\frac{1}{q^k}+\frac{R^2}{|G|^2}$$

Puisque $R \leq 4\sqrt{q^n}$ d'après le Corollaire 4.2.3, on a

$$\Delta(\mathcal{D}_k(U_G), U_{\mathbb{F}_q^k}) \leq \frac{R\sqrt{q^k}}{2|G|} \leq \frac{2\sqrt{q^{n+k}}}{|G|}$$

□

Corollaire 4.3.3. *Soit $p > 2$ un nombre premier et E une courbe elliptique définie sur $\mathbb{F}_{p^n}$. Soit G un sous-groupe multiplicatif de $E(\mathbb{F}_{p^n})$ d'ordre r, avec $|r| = t$ et $|p| = m$. Soit U_G la distribution uniforme sur G. Si $e > 1$ et $k > 1$ sont des entiers tels que*

$$k \leq \frac{2t - 2e - nm - 4}{m},$$

alors $\mathcal{D}_k$ est un extracteur $(\mathbb{F}_{p^k}, 2^{-e})$-déterministe pour la courbe elliptic $E(\mathbb{F}_{p^n})$.

Démonstration. Puisque $k \leq \frac{2t - 2e - nm - 4}{m}$, on a $\frac{m(n+k)}{2} \leq t - e - 2$, c'est-à-dire

$$2^{\frac{m(n+k)}{2}} \leq 2^t 2^{-e} 2^{-2} = \frac{2^{t-1}}{2^{e+1}}.$$

Puisque $2^{m-1} \leq p < 2^m$, et $2^{t-1} \leq |G| < 2^t$, alors les inégalités ci-dessus entraînent que

$$p^{\frac{(n+k)}{2}} \leq \frac{|G|}{2^{e+1}} \Longleftrightarrow \Delta(\mathcal{D}_k(U_G), U_{\mathbb{F}_{p^k}}) \leq 2^{-e}.$$

□

Pour un corps de caractéristique 2, on a le corollaire suivant :

Corollaire 4.3.4. *Soit $E(\mathbb{F}_{2^n})$ une courbe elliptique et soit $G \subset E(\mathbb{F}_{2^n})$ un sous-groupe multiplicatif d'ordre r, avec $|r| = t$. Soit U_G la distribution uniforme sur G. Si $e > 1$ et $k > 1$ sont deux entiers tels que*

$$k \leq 2t - 2e - n - 4,$$

alors $\mathcal{D}_k$ est un extracteur $(\mathbb{F}_{2^k}, 2^{-e})$-déterministe pour la courbe elliptique $E(\mathbb{F}_{2^n})$.

Démonstration. Rappelons que $p = 2$. Puisque $k \leq 2t - 2e - n - 4$, on a $\frac{n+k}{2} \leq t - e - 2$. Par conséquent

$$2^{\frac{n+k}{2}} \leq 2^{t-1}2^{-(e+1)} \leq \frac{|G|}{2^{e+1}},$$

ce qui implique $\Delta(\mathcal{D}_k(U_G), U_{\mathbb{F}_{2^k}}) \leq 2^{-e}$. □

Le théorème suivant confirme la conjecture de Farashahi et *al.* dans [FPS08, FP07] dans le cas des courbes elliptiques.

Theorème 4.3.5. *Soit E une courbe elliptique définie sur $\mathbb{F}_{q^n}$, alors*

$$\Delta(\mathcal{D}_k(U_E), U_{\mathbb{F}_q^k}) \leq \frac{c}{\sqrt{q^{n-k}}},$$

où U_E est la distribution uniforme sur $E(\mathbb{F}_{q^n})$ et c est une constante dépendant de n.

Démonstration. En utilisant le fait que $\Big||E(\mathbb{F}_{q^n})| - (q^n + 1)\Big| \leq 2\sqrt{q^n}$, on a

$$\Delta(\mathcal{D}_k(U_E), U_{\mathbb{F}_q^k}) \leq \frac{2\sqrt{q^{n+k}}}{|E(\mathbb{F}_{q^n})|} \leq \frac{2\sqrt{q^{n+k}}}{q^n - 2\sqrt{q^n} + 1}.$$

Poser $c = \frac{2}{1-2q^{-n/2}+q^{-n}}$ pour obtenir le résultat souhaité.

□

Remarque 4.3.6. *Puisque pour des utilisations cryptographiques q^n est très grand, on a $c = 2 + o(1)$.*

Pour le cas binaire, comme établi par Farashahi et *al.* dans [FPS08], on a le théorème suivant

Theorème 4.3.7. *Si $q = 2$, alors*

$$\Delta(\mathcal{D}_k(U_E), U_{\mathbb{F}_2^k}) \leq \frac{3}{\sqrt{2^{n-k}}}$$

Démonstration. La preuve découle du théorème et des remarques précédents. □

Ce théorème confirme la seconde conjecture de Farashahi et *al.* dans [FPS08].

4.4 Applications au protocole d'échange de clés de Diffie-Hellman

Supposons que l'on veut dériver une clé symétrique de 256 bits à la suite du protocole de Diffie-Hellman dans un sous-groupe G d'une courbe elliptique $E(\mathbb{F}_{2^n})$ avec une borne de sécurité 2^{-80} comme dans le Leftover Hash Lemma. on peut alors considérer une courbe elliptique E définie sur le corps $\mathbb{F}_{2^{571}}$ et prendre G comme étant un sous-groupe d'ordre r avec $2^{492} \leq r < 2^{493}$. On peut ainsi voir que notre extracteur retourne à peu près le même nombre de bits que le Leftover Hash Lemma.

Comme application de notre extracteur, on a montré, sous l'hypothèse décisionnelle de Diffie-Hellman sur une courbe $E(\mathbb{F}_{2^n})$, que l'on peut dériver de façon déterministe une chaîne de bits uniformément aléatoire dans le modèle standard à partir d'un élément Diffie-Hellman. En pratique, on a montré, sous l'hypothèse DDH, que les k premiers coefficients dans $\mathbb{F}_2$ (resp. les k derniers bits) de l'abscisse d'un point aléatoire P d'un sous-groupe $G \subset E(\mathbb{F}_{p^n})$ sont indistinguables d'une chaîne de bits aléatoire de même longueur.

Conclusion

Nous avons construit un extracteur déterministe simple et efficace $\mathcal{D}_k$, où k est un entier positif, pour une courbe elliptique $\mathbb{F}_{q^n}$. L'extracteur $\mathcal{D}_k$, étant donné un point P sur E renvoie les k premiers $\mathbb{F}_q$-coordonnées de l'abscisse du point P. La partie principale de ce chapitre est l'analyse de l'extracteur qui montre que $\mathcal{D}_k$ est un bon extracteur d'aléa. Ainsi, $\mathcal{D}_k$ peut être utilisé dans n'importe quel protocole cryptographique.
Nous avons résolu du même coup deux conjectures différentes de Farashahi *et al.* posées dans [FP07] et [FPS08]. Comme travail future, notre but sera de généraliser cet extracteur aux courbes hyperelliptiques et aux autres familles de courbes comme celles d' Edwards, de Huff, etc.

Chapitre 5
COUPLAGES SUR LES COURBES DE HUFF

Dans ce chapitre, nous présentons le calcul du couplage de Tate sur les courbes elliptiques de Huff généralisées proposées par Wu et Feng dans [WF10]. Nous rappelons d'abord les techniques usuelles qui permettent de calculer le couplage sur la Jacobienne d'une courbe hyperelliptique et sur une courbe elliptique de façon générale avant de donner les formules du coulage de Tate sur les courbes elliptiques de Huff générales.

5.1 Rappels sur les couplages sur les variétés

Dans cette section, nous rappelons les couplages, particulièrement le couplage de Tate sur la Jacobienne d'une courbe hyperelliptique. Nous décrivons également les détails du calcul du couplage de Tate sur une courbe elliptique.
Les couplages utilisés en cryptographie sont des applications bilinéaires des sous groupes de torsion d'une courbe elliptique dans le groupe multiplicatif d'un corps fini. Notons que ces couplages sont très faciles à calculer.

Définition 5.1.1. *Soit G_1 et G_2 deux groupes abéliens additifs finis et soit G_3 un groupe multiplicatif fini. Un couplage cryptographique est une application*

$$e : G_1 \times G_2 \longrightarrow G_3$$

qui satisfait les propriétés suivantes :

1. *elle est non dégénérée, c'est-à-dire, pour tout $0 \neq P \in G_2$, il existe $Q \in G_2$ tel que $e(P, Q) \neq 1$, et pour tout $0 \neq Q \in G_2$, il existe $P \in G_1$ tel que $e(P, Q) \neq 1$,*

2. *elle est bilinéaire, c'est-à-dire, pour tout* $P_1, P_2 \in G_1$ *et pour tout* $Q_1, Q_2 \in G_2$ *on a*

$$e(P_1 + P_2, Q_1) = e(P_1, Q_1)e(P_2, Q_1)e(P_1, Q_1 + Q_2) = e(P_1, Q_1)e(P_1, Q_2),$$

3. *elle est calculable de façon efficace.*

Une propriété importante qui est utilisée dans beaucoup d'applications et qui découle de la bilinéarité est le fait que

$$e([a]P, [b]Q) = e(P, Q)^{ab} = e([b]P, [a]Q),$$

pour tout $a, b \in \mathbb{Z}$ et pour tout $(P, Q) \in G_1 \times G_2$.

5.1.1 Couplage de Tate

Le couplage de Tate peut être défini sur une variété abélienne. C'est un couplage sur le sous-groupe de r-torsion d'une variété abélienne pour un nombre premier r donné.
Soit $\mathcal{C}$ une courbe hyperelliptique de genre g définie sur un corps fini $\mathbb{F}_q$ de caractéristique p. Soit $J_\mathcal{C}$ la Jacobienne de $\mathcal{C}$, $n = \#J_\mathcal{C}$, $r > 3$ un nombre premier et $r|n$.

Définition 5.1.2. *Le plus petit entier* k *tel que* $r|q^k - 1$ *est appelé* degré de plongement *de* $\mathcal{C}$ *relativement à* r.

Remarque 5.1.3. *Si* k *est le plus petit entier tel que* $r|q^k - 1$ *alors,* k *est l'ordre de* q *modulo* r. *Par conséquent, la plus petite extension de* $\mathbb{F}_q$ *qui contient le groupe* μ_r *de toutes les racines* $r^{ème}$ *de l'unité est* $\mathbb{F}_{q^k}$.

Définition 5.1.4. *Soit* $\mathcal{C}$ *une courbe hyperelliptique de genre* g *définie sur le corps* $\mathbb{F}_q$ *de caractéristique* p *et soit* $r \neq p$ *un nombre premier divisant* $\#J_\mathcal{C}(\mathbb{F}_q)$. *Soit* k *le degré de plongement de* $\mathcal{C}$ *par rapport à* r. *Le* couplage de Tate *est une application*

$$T_r : J_\mathcal{C}(\mathbb{F}_{q^k})[r] \times J_\mathcal{C}(\mathbb{F}_{q^k})/[r]J_\mathcal{C}(\mathbb{F}_{q^k}) \longrightarrow \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r$$

définie comme suit : soit $P \in J_{\mathcal{C}}(\mathbb{F}_{q^k})[r]$ *une classe de diviseurs* $\mathbb{F}_{q^k}$*-rationnels représentée par un diviseur* D_P *et soit* $Q \in J_{\mathcal{C}}(\mathbb{F}_{q^k})$ *une classe de diviseurs* $\mathbb{F}_{q^k}$*-rationnels représentée par un diviseur* D_Q *telle que son support et celui de* D_P *soient disjoints. Soit* $f_{r,P} \in \overline{\mathbb{F}_{q^k}}(C)$ *une fonction rationnelle sur* $\mathcal{C}$ *avec* $div(f_{r,P}) = rD_P$*. Alors,*

$$T_r(P, Q + [r]J_{\mathcal{C}}(\mathbb{F}_{q^k})) = f_{r,P}(D_Q)(\mathbb{F}_{q^k}^*)^r.$$

L'évaluation de $f_{r,P}$ *au diviseur* $D = \sum_{R \in \mathcal{C}} n_R(R)$ *est donnée par*

$$f_{r,P}(D) = \prod_{R \in C} f_{r,P}(R)^{n_R}$$

Proposition 5.1.5. *Le couplage de Tate, tel qu'il est décrit dans la définition ci-dessus, est bien défini, bilinéaire, non-dégénéré et peut être calculé en* $O(\log_2(r))$ *opérations sur* $\mathbb{F}_{q^k}$*.*

Démonstration. Voir [FR94], [DF05]. □

Le lemme suivant permet de représenter le groupe $J_{\mathcal{C}}(\mathbb{F}_{q^k})/[r]J_{\mathcal{C}}(\mathbb{F}_{q^k})$ avec les points de $J_{\mathcal{C}}(\mathbb{F}_{q^k})[r]$.

Lemme 5.1.6. *Soit* G *un groupe abélien additif fini,* r *un nombre premier divisant* $|G|$*. Soit* $G[r]$ *le sous-groupe de tous les points d'ordre un multiple de* r *et* rG *le sous-groupe de tous les éléments* $r\alpha$*,* $\alpha \in G$*. S'il n'existe aucun élément d'ordre* r^2 *dans* G *alors,*

$$G[r] \cong G/rG$$

Démonstration. Montrons que l'application $G[r] \longrightarrow G/[r]G$ est un isomorphisme de groupes.
Il est clair que c'est un morphisme de groupes. Supposons que $g_1 + rG = g_2 + rG$, avec $g_1, g_2 \in G[r]$. Il s'en suit alors que $g_1 - g_2 \in rG$, en d'autres termes $g_1 - g_2 = rg$, avec $g \in G$. Puisque $g_1, g_2 \in G[r]$, on a $0 = rg_1 - rg_2 = r^2 g$. Comme il n'y a pas d'élément d'ordre r^2 par hypothèse, on a $rg = 0$ et ainsi $g_1 = g_2$. Par

conséquent, l'application est injective.
Considérons maintenant l'homomorphisme de groupes

$$G \longrightarrow rG, \quad g \longmapsto rg.$$

Le noyau de cette application est $G[r]$ et il s'en suit que $G/rG \cong G[r]$. Par conséquent, $|G| = |G[r]|.|rG|$. Ce qui prouve le lemme. □

Corollaire 5.1.7. *S'il n'existe aucun point d'ordre r^2 dans $J_{\mathcal{C}}(\mathbb{F}_{q^k})$, alors on a*

$$J_{\mathcal{C}}(\mathbb{F}_{q^k})[r] \cong J_{\mathcal{C}}(\mathbb{F}_{q^k})/[r]J_{\mathcal{C}}(\mathbb{F}_{q^k}),$$

en d'autres termes, on peut prendre des points de r-torsion comme des représentants des classes de diviseurs.

Remarque 5.1.8. *Puisque $r|\#J_{\mathcal{C}}(\mathbb{F}_q)$, il existe des points de r-torsion dans $J_{\mathcal{C}}(\mathbb{F}_q)$ et on peut prendre le premier argument du couplage de Tate dans $J_{\mathcal{C}}(\mathbb{F}_q)[r]$. On peut ainsi définir le couplage de Tate comme une fonction*

$$T_r : J_{\mathcal{C}}(\mathbb{F}_q)[r] \times J_{\mathcal{C}}(\mathbb{F}_{q^k})/[r]J_{\mathcal{C}}(\mathbb{F}_{q^k}) \longrightarrow \mathbb{F}^*_{q^k}/(\mathbb{F}^*_{q^k})^r$$

On suppose dans tout ce qui suit que $J_{\mathcal{C}}(\mathbb{F}_{q^k})$ ne contient pas de points d'ordre r^2. Dans ce cas, le couplage de Tate peut être donné par

$$T_r : J_{\mathcal{C}}(\mathbb{F}_q)[r] \times J_{\mathcal{C}}(\mathbb{F}_{q^k})[r] \longrightarrow \mathbb{F}^*_{q^k}/(\mathbb{F}^*_{q^k})^r,$$

d'après le Corollaire 5.1.7.
Les valeurs du couplage de Tate sont des classes dans $\mathbb{F}^*_{q^k}/(\mathbb{F}^*_{q^k})^r$. En applicant la version multiplicative du Lemme 5.1.6, on voit que $\mathbb{F}^*_{q^k}/(\mathbb{F}^*_{q^k})^r \cong \mu_r$, le sous-groupe des racines $r^{\text{ème}}$ de l'unité dans $\mathbb{F}^*_{q^k}$. L'isomorphisme est donné par

$$\mathbb{F}^*_{q^k}/(\mathbb{F}^*_{q^k})^r \longrightarrow \mu_r, \quad a(\mathbb{F}^*_{q^k})^r \longrightarrow a^{(q^k-1)/r}$$

En tenant compte des modifications faites dans la remarque précédentes on peut définir une version simplifiée du couplage de Tate, convenable pour une implémentation [DFO5b].

Définition 5.1.9. *Le* couplage de Tate réduit *est l'application*

$$e_r : J_{\mathcal{C}}(\mathbb{F}_q)[r] \times J_{\mathcal{C}}(\mathbb{F}_{q^k})[r] \longrightarrow \mu_r \subseteq \mathbb{F}_{q^k}$$
$$(P, Q) \longmapsto Tr(P, Q)^{(q^k-1)/r} = f_{r,P}(D_Q)^{(q^k-1)/r}$$

induit par le couplage de Tate

5.1.2 Calcul du couplage de Tate sur les courbes elliptiques

Dans [Mil04], Miller donne un algorithme pour calculer le couplage de Tate sur une courbe elliptique. Cet algorithme est connu sous le nom d'*algorithme de Miller*. Il décrit comment calculer la fonction $f_{r,P}(D_Q)$ utilisée dans le couplage de Tate.
Soit E une courbe elliptique définie sur le corps $\mathbb{F}_q$ de caractéristique $p > 3$, donnée par une équation de Weierstrass

$$E : y^2 = x^3 + ax + b \quad a, b \in \mathbb{F}_q.$$

Soit $r \neq p$ un nombre premier tel que $r|n = \#E(\mathbb{F}_q)$ et soit $k > 1$ le degré de plongement de E relativement à r.

Theorème 5.1.10. *Soit* $D = \sum_{P \in E} n_P(P) \in Div(E)$. *Alors* D *est un diviseur principal si et seulement si* $\deg(D) = 0$ *et* $\sum_{P \in E} [n_P](P) = 0$, *où la dernière somme décrit l'addition sur* E

Démonstration. Voir [Sil86], [Mil04]. □

En remplaçant les classes de diviseurs par des points, on définit le couplage de Tate réduit sur une courbe elliptique par l'application

$$e_r : E(\mathbb{F}_q)[r] \times E(\mathbb{F}_{q^k})[r] \longrightarrow \mu_r \subseteq \mathbb{F}_{q^k}$$
$$(P, Q) \longmapsto f_{r,P}(D_Q)^{(q^k-1)/r}.$$

Lorsqu'on calcule $f_{r,P}(Q)$, c'est-à-dire lorsque rD_p est supposé être le diviseur de la fonction $f_{r,P}$, on peut choisir $D_p = (P) - (O)$. Le diviseur $D_Q \sim (Q) - (O)$ doit avoir un support disjoint de O et de P. Pour se faire, on peut choisir un point convenable $S \in E(\mathbb{F}_{q^k})$ et prendre D_Q comme étant $(Q + S) - (S)$.

La fonction $f_{r,P}$ a pour diviseur $\mathrm{div}(f_{r,P}) = r(P) - r(O)$. Le Théorème 5.1.10 montre que, pour tout $m \in \mathbb{Z}$, le diviseur $m(P) - ([m]P) - (m-1)(O)$ est principal et qu'il existe une fonction rationnelle $f_{m,P} \in \overline{\mathbb{F}_q}(E)$ telle que $\mathrm{div}(f_{m,P}) = m(P) - ([m]P) - (m-1)(O)$. Puisque P est un point de r-torsion, on a $\mathrm{div}(f_{r,P}) = r(P) - r(O)$, et $f_{r,P}$ est bien la fonction que nous recherchons. Ce qui justifie les notations.

Définition 5.1.11. *Soit $m \in \mathbb{Z}$ et $P \in E(\mathbb{F}_{q^k})[r]$, une fonction $f_{m,P} \in \overline{\mathbb{F}_{q^k}}(E)$ avec* $\mathrm{div}(f_{m,P}) = m(P) - ([m]P) - (m-1)(O)$ *est appelée* fonction de Miller.

Le calcul de $f_{r,P}$ requiert la définition des droites passant par les points sur la courbe elliptique lorsque ces points sont additionnés.

Lemme 5.1.12. *Soit $P_1, P_2 \in E$ et soit l_{P_1,P_2} le polynôme homogène définissant la droite passant par P_1 et P_2, et la tangente à la courbe si $P_1 = P_2$. La fonction $L_{P_1,P_2} = l_{P_1,P_2}(X, Y, Z)/Z$ a pour diviseur*

$$\mathrm{div}(L_{P_1,P_2}) = (P_1) + (P_2) + (-(P_1 + P_2)) - 3(O).$$

On donne maintenant les polynômes affines définissant ces droites décrites dans le lemme ci-dessus.

Lemme 5.1.13. *Soit $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, $Q = (x_Q, y_Q) \in E$. Pour $P_1 \neq -P_2$ définissons*

$$\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1) & \text{si } P_1 \neq P_2, \\ (3x_1^2 + a)/(2y_1) & \text{si } P_1 = P_2. \end{cases}$$

Alors, le deshomogénéisé $(l_{P_1,P_2})_*$ de l_{P_1,P_2} évalué en Q est donné par

$$(l_{P_1,P_2})_*(Q) = \lambda(x_Q - x_1) + (y_1 - y_Q).$$

Si $P_1 = -P_2$, alors $(l_{P_1,P_2})_*(Q) = x_Q - x_1$.

Démonstration. La preuve de ce lemme découle de la loi de groupe sur la courbe elliptique et de son interprétation géométrique. □

Lemme 5.1.14. *Soit $P_1, P_2 \in E$. Alors, la fonction $g_{P_1,P_2} := L_{P_1,P_2}/L_{P_1+P_2,-(P_1+P_2)}$ a pour diviseur*

$$\mathrm{div}(g_{P_1,P_2}) = (P_1) + (P_2) - (P_1 + P_2) - (O).$$

Démonstration. La preuve découle du Lemme 5.1.12 □

La fonction g du Lemme 5.1.14 peut être utilisée pour calculer la fonction de Miller de façon recursive comme le montre le lemme suivant.

Lemme 5.1.15. *La fonction de Miller $f_{r,P}$ peut être choisie telle que $f_{1,P} = 1$ et pour tout $m_1, m_2 \in \mathbb{Z}$,*

$$f_{m_1+m_2,P} = f_{m_1,P} f_{m_2,P} g_{[m_1]P,[m_2]P},$$

$$f_{m_1 m_2,P} = f_{m_1,P}^{m_2} f_{m_2,[m_1]P} = f_{m_2,P}^{m_1} f_{m_1,[m_2]P}$$

Démonstration. [Mil04] et [Gal05]. □

Remarque 5.1.16. *On peut établir les cas spéciaux suivant découlant du lemme précédent. Soit $m \in \mathbb{Z}$ alors,*

1. $f_{m+1,P} = f_{m,P} g_{[m]P,P}$,
2. $f_{2m,P} = f_{m,P}^2 g_{[m]P,[m]P}$,
3. $f_{-m,P} = (f_{m,P} g_{[m]P}, -[m]P)^{-1}$.

Notons que $f_{0,P} = 1$ pour tout $P \in E$ et $g_{P_1,P_2} = 1$ si $P_1 = O$ ou $P_2 = O$. Ces formules montrent que toute fonction $f_{m,P}$ peut être calculée de façon recursive comme un produit de droites. Les fonctions sont définies dans le corps de définition de P.

Algorithm 1 Algorithme de Miller

1: $R \leftarrow P$, $f \leftarrow 1$
2: **for** $(i = l - 1\,;\, i \geq 0\,;\, i - -)$ **do**
3: $\quad f \leftarrow f^2.g_{R,R}(Q)$
4: $\quad R \leftarrow 2R$
5: $\quad$ **if** $(r_i = 1)$ **then**
6: $\quad\quad f \leftarrow f.g_{R,P}(Q)$
7: $\quad\quad R \leftarrow R + P$
8: $\quad$ **end if**
9: **end for**
10: **return** $f^{(q^k-1)/r}$

Ces formules seront utilisées dans l'algorithme de Miller pour calculer $[r]P$. L'évaluation de $f_{r,P}$ en D_Q peut être remplacée par $f_{r,P}(Q)$.

Lemme 5.1.17. *Soit $P \in E(\mathbb{F}_q)[r]$ et $Q \in E(\mathbb{F}_{q^k})[r]$, $\notin E(\mathbb{F}_q)$. Alors, le couplage de Tate réduit peut être calculé comme $e_r(P,Q) = f_{r,P}(Q)^{(q^k-1)/r}$.*

Démonstration. Voir [BLS04]. □

L'algorithme ci-dessus, connu sous le nom d'*algorithme de Miller* permet de calculer $f_{r,P}(Q)$ pour $P \in E(\mathbb{F}_q)[r]$, $Q \in E(\mathbb{F}_{q^k})[r]$ et $r = (r_l, r_{l-1}, \ldots, r_0)_2$ en représentation binaire.

Remarque 5.1.18. *Notons que les fonctions $g_{R,R}$ et $g_{R,P}$ dans les étapes 3 et 6 de l'Algorithme 1 sont des fractions et que les inversions dans chaque étape de la boucle peuvent être différées jusqu'à la fin de la boucle en gardant la trace des numérateurs et des dénominateurs séparément.*

Pour compléter le calcul du couplage, on applique l'exponentiation finale au résultat de l'algorithme de Miller. Pour cela, on peut utiliser une méthode d'exponentiation rapide sur le corps $\mathbb{F}_{q^k}$ (voir [Doc05a] et [Doc05b]). Des améliorations récentes pour le calcul de l'exponentiation finale ont été apportées dans [SBC+09].

Lorsque le degré de plongement est pair, on peut encore améliorer l'algorithme de Miller en utilisant le twist de la courbe elliptique considérée.

Proposition 5.1.19. *Soit $\delta = 2$ si $j(E) \notin \{0, 1728\}$, $\delta = 4$ si $j(E) = 1728$ et $\delta = 6$ si $j(E) = 0$. Si $\delta | k$ alors, il existe un unique twist E' de E de degré δ avec $r | \#E'(\mathbb{F}_{q^k})$.*

Démonstration. Voir [HSV06]. □

Lemme 5.1.20. *Soit E' le twist de la Proposition 5.1.19 et soit $\sigma_\varsigma : E' \longrightarrow E$ l'isomorphisme correspondant, étant donné $\varsigma \in \mathbb{F}_{q^k}$. La restriction de σ_ς à $E'(\mathbb{F}_{q^k})[r]$ est un isomorphisme*

$$\sigma_\varsigma : E'(\mathbb{F}_{q^k})[r] \longrightarrow G_2$$

de groupes cycliques d'ordre r.
Si $Q \in G_2$ alors, l'abscisse x de Q appartient à un sous-groupe propre de $\mathbb{F}_{q^k}$.

Démonstration. Voir [HSV06]. □

Le lemme suivant montre qu'on peut définir un couplage $G_1 \times E'(\mathbb{F}_{q^k})[r] \longrightarrow G_3$ en envoyant simplement les éléments de $E'(\mathbb{F}_{q^k})[r]$ dans G_2 à travers σ_ς.

Définition 5.1.21. *Soit $G_2' = E'(\mathbb{F}_{q^k})[r]$. Le couplage*

$$e_r' : G_1 \times G_2' \longrightarrow G_3, \quad (P, Q') \longmapsto e_r(P, \sigma_\varsigma(Q'))$$

est appelé twist du couplage de Tate.

Lorsque k est pair, il est très facile d'utiliser un twist quadratique, c'est-à-dire un twist de degré 2. Dans ce cas, les abscisses de tous les points de G_2 et de G_2' appartiennent à un sous-corps propre de $\mathbb{F}_{q^k}$. Les dénominateurs des fonctions $g_{R,R}$ et $g_{R,P}$ dans l'algorithme de Miller sont des droites verticales de la formes $x - x_{[2]R}$ ou $x - x_{R+P}$. Puisque les points R et P sont finis sur $\mathbb{F}_q$, les valeurs de $g_{R,P}(Q)$ et de $g_{R,R}(Q)$ appartiennent à un sous-corps propre de $\mathbb{F}_{q^k}$, par conséquent, elles sont réduites à 1 par l'exponentiation finale.

Proposition 5.1.22. *Supposons que k est pair. Alors, les dénominateurs des fonctions $g_{R,R}$ et $g_{R,P}$ peuvent être éliminés dans les étapes 3 et 6 de l'algorithme de Miller sans changer la valeur finale du couplage de Tate réduit.*

Démonstration. Voir [BLS04]. □

5.2 Couplage sur les courbes de Huff $X(aY^2-Z^2) = Y(bX^2-Z^2)$

Le couplage sur les courbes de Huff classiques a été donné par Joye *et al.* dans [JTV10]. La contribution dans ce chapitre consiste à donner une version du couplage sur les courbes de Huff généralisées proposées par Wu et Feng dans [WF10].

Les courbes de Huff sont représentées comme des cubiques planes. Ce qui fait que l'on peut appliquer directement l'algorithme de Miller pour calculer les couplages sur ces courbes.

On représente très souvent le point $Q \in E(\mathbb{F}_{q^k})\backslash E(\mathbb{F}_q)$ en coordonnées affine puisque, dans l'algorithme de Miller, la fonction est toujours évaluée au même point Q. On peut choisir les coordonnées de Q comme $Q = (y, z) = (1 : y : z)$. Supposons que le degré de plongement k soit pair, alors Q peut être représenté sous la forme $Q = (y_Q, z_Q\alpha)$, avec $y_Q, z_Q \in \mathbb{F}_{q^{k/2}}$, $\mathbb{F}_{q^k} = \mathbb{F}_{q^{k/2}}(\alpha)$ où α n'est pas un résidu quadratique dans $\mathbb{F}_{q^{k/2}}$.

Soit $P, R \in E(\mathbb{F}_q)$ et soit $l_{R,P}$ la fonction rationnelle s'annulant à la droite passant par P et R. On a

$$l_{R,P}(Q) = \frac{(zX_p - Z_p) - \lambda(yX_p - Y_P)}{X_P}$$

où λ est la pente, suivant (y, z), de la droite passant par P et R. Alors, le diviseur de $l_{R,P}$ est donné par

$$div(l_{R,P}) = R + P + T - (1 : 0 : 0) - (0 : 1 : 0) - (a : b : 0)$$

où T est le troisième point d'intersection de la droite passant par P et R avec la courbe. Si U est l'élément neutre pour la lois de groupe $\oplus$, la fonction $g_{R,P}$ peut être exprimée par

$$g_{R,P} = \frac{l_{R,P}}{l_{R\oplus P,U}}$$

Soit $U = O = (0 : 0 : 1)$ l'élément neutre de la l'addition. Alors, pout tout $Q = (y_Q, z_Q\alpha)$,

$$l_{R\oplus P,O} = y_Q - \frac{Y_{R\oplus P}}{X_{R\oplus P}} \in \mathbb{F}_{q^{k/2}}$$

Cette quantité est égale à 1 après l'exponentiation finale dans l'algorithme de Miller puisqu'elle appartient à un sous-corps propre de $\mathbb{F}_{q^k}$. Ce qui veut dire donc qu'on peut ne pas la considérer dans les calculs. De même, les divisions par X_P peuvent être omises, et le dénominateur dans l'expression de λ peut être omis. En d'autres termes, si $\lambda = \frac{A}{B}$, alors la fonction $g_{R,P}$ peut être évaluée comme

$$g_{R,P}(Q) = (z_Q\alpha.X_p - Z_p)B - (yX_p - Y_P)A$$

On peut maintenant donner des formules précises pour l'addition et le doublement dans la boucle de Miller.

Étape d'addition. Dans le cas de l'addition, la pente suivant (y, z) de la droite passant par les points $P = (X_P : Y_P : Z_P)$ et $R = (X_R : Y_R : Z_R)$ est donnée par

$$\lambda = \frac{Z_R X_P - Z_P X_R}{Y_R X_P - Y_P X_R}.$$

Par conséquent, la fonction à évaluer est de la forme

$$g_{R,P}(Q) = (z_Q\alpha.X_P - Z_P)(Y_R X_P - Y_P X_R) - (y_Q.X_P - Y_P)(Z_R X_P - Z_P X_R).$$

Puisque les points P et Q restent constants durant l'exécution de la boucle, les valeurs dépendant de P et de Q, c'est-à-dire $y'_Q = y_Q.X_P - Y_P$ et $z'_Q = z_Q\alpha.X_P$, peuvent être précalculées. Ainsi, chaque étape d'addition dans l'algorithme de Miller requiert le calcul de $R \oplus P$ (une addition sur $E(\mathbb{F}_q)$), l'évaluation de $g_{R,P}(Q)$, et le calcul de $f.g_{R,P}(Q)$ (une multiplication dans $\mathbb{F}_{q^k}$.
Le calcul de $R\oplus P$ peut être effectué en 12m+2c en incluant toutes les résultats des étapes intermédiaires $M_1, M_2, \ldots, M_7$. Calculons aussi $M_8 = (X_R+Y_R)(X_P-Y_P)$ et $M_9 = (X_P + Z_P)(Z_R - X_R)$. Alors,

$$g_{R,P}(Q) = (z'_Q - Z_P)(M_8 - M_1 + M_2) - y'_Q(M_9 + M_1 - M_3),$$

où le premier terme requiert $(\frac{k}{2}+1)\mathbf{m}$, et le second $\frac{k}{2}\mathbf{m}$. Avec la multiplication finale sur $\mathbb{F}_{q^k}$, le coût total de l'étape d'addition est de $1\mathbf{M}+(k+15)\mathbf{m}+2\mathbf{c}$.

Étape de doublement. Dans le cas du doublement, la pente de la tangente à la courbe au point $R=(X_R:Y_R:Z_R)$ est donnée par

$$\lambda=\frac{aZ_R^2-2bY_RZ_R-X_R^2}{bY_R^2-2aY_RZ_R-X_R^2}=\frac{A}{B}.$$

Par conséquent,

$$g_{R,R}(Q)=z_Q\alpha.X_RB-Z_RB-y_Q.X_RA+Y_RA.$$

Dans l'algorithme de Miller, on a besoin de calculer le point $2R$. Ce calcul peut être effectué en $7\mathbf{m}+5\mathbf{s}+2\mathbf{c}$. Les quotients A et B peuvent être évalués en $1\mathbf{m}$, à savoir Y_RZ_R puisque les autres termes ont été déjà calculés avec l'opération de doublement. La fonction $g_{R,R}$ peut être évaluée en $4\mathbf{m}$ (X_RB, Z_RB, X_RA et Y_RA), $\frac{k}{2}\mathbf{m}$ pour $z_Q\alpha.X_RB$ et $\frac{k}{2}\mathbf{m}$ pour $y_Q.X_RA$. Ce qui fait un coût total de $1\mathbf{M}+1\mathbf{S}+(k+12)\mathbf{m}+5\mathbf{s}+2\mathbf{c}$, en tenant compte de la multiplication, de l'élévation au carré pour compléter l'étape de doublement.

Conclusion

Nous avons introduit avec succès une nouvelle généralisation du couplage de Tate sur les courbes elliptiques de Huff. Ce couplage est aussi efficace que celui proposé par Joye, Tibouchi et Vergnaud pour le modèle de Huff standard et peut être utilisé pour mettre en œuvre des protocoles cryptographiques comme ceux basés sur l'identité.

BIBLIOGRAPHIE

[BK98] R. Balasubramanian and Neal Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the menezes - okamoto - vanstone algorithm. *J. Cryptology*, 11 :141–145, 1998.

[BLS04] Paulo S. L. M. Barreto, Ben Lynn, and Michael Scott. Efficient implementation of pairing-based cryptosystems. *J. Cryptol.*, 17 :321–334, September 2004.

[Bon98] Dan Boneh. The decision diffie-hellman problem. In *Proceedings of the Third International Symposium on Algorithmic Number Theory*, pages 48–63, London, UK, 1998. Springer-Verlag.

[BR93] Mihir Bellare and Phillip Rogaway. Random oracles are practical : a paradigm for designing efficient protocols. In *Proceedings of the 1st ACM conference on Computer and communications security*, CCS '93, pages 62–73, New York, NY, USA, 1993. ACM.

[BSSC05] I. Blake, G. Seroussi, N. Smart, and J. W. S. Cassels. *Advances in Elliptic Curve Cryptography (London Mathematical Society Lecture Note Series)*. Cambridge University Press, New York, NY, USA, 2005.

[BV96] Dan Boneh and Ramarathnam Venkatesan. Hardness of computing the most significant bits of secret keys in diffie-hellman and related schemes. In *Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '96, pages 129–142, London, UK, 1996. Springer-Verlag.

[Can87] David G. Cantor. Computing in the jacobian of a hyperelliptic curve. *Mathematics of Computation*, 48(177) :pp. 95–101, 1987.

[CF05] Henri Cohen and Gerhard Frey, editors. *Handbook of elliptic and hyperelliptic curve cryptography*. CRC Press, 2005.

[CFK+00] R. Carneti, J. Friedlander, S. Koyagin, M. Larsen, D. Lieman, and I. Shparlinski. On the statistical properties of diffie-hellman distributions. *Israel Journal of Mathematic*, 120 :23–46, 2000.

[CFPZ09] Céline Chevalier, Pierre-Alain Fouque, David Pointcheval, and Sébastien Zimmer. Optimal randomness extraction from a diffie-hellman element. In *Proceedings of the 28th Annual International Conference on Advances in Cryptology : the Theory and Applications of Cryptographic Techniques*, EUROCRYPT '09, pages 572–589, Berlin, Heidelberg, 2009. Springer-Verlag.

[CS11] Abdoul Aziz Ciss and Djiby Sow. On randomness extraction in elliptic curves. In *Proceedings of the 4th international conference on Progress in cryptology in Africa*, AFRICACRYPT'11, pages 290–297, Berlin, Heidelberg, 2011. Springer-Verlag.

[DF05] Silvain Duquesne and Gerhard Frey. Background on pairings. In *chapter 6 in [CF05]*, pages 115–124. CRC press, 2005.

[DGKR04] Yevgeniy Dodis, Rosario Gennaro, Hugo Krawczyk, and Tal Rabin. Randomness extraction and key derivation using the cbc, cascade and hmac modes. In *In Crypto '04, LNCS*, pages 494–510. Springer-Verlag, 2004.

[DH76] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(5) :644–654, 1976.

[DJ11] Julien Devigne and Marc Joye. Binary huff curves. In *Proceedings of the 11th international conference on Topics in cryptology : CT-RSA 2011*, CT-RSA'11, pages 340–355, Berlin, Heidelberg, 2011. Springer-Verlag.

[DL05] Silvain Duquesne and Tanja Lange. Arithmetic of hyperelliptic curves. In *chapter 14 in [CF05]*, pages 303–354. CRC press, 2005.

[Doc05a] Christophe Doche. Exponentiation. In *chapter 9 in [CF05]*, pages 303–354. CRC press, 2005.

[Doc05b] Christophe Doche. Finite field arithmetic. In *chapter 6 in [CF05]*, pages 201–237. CRC press, 2005.

[FL05] Gerhard Frey and Tanja Lange. Background on curves and jacobians. In *chapter 4 in [CF05]*, pages 45–85. CRC press, 2005.

[FP07] Reza Rezaeian Farashahi and Ruud Pellikaan. The quadratic extension extractor for (hyper)elliptic curves in odd characteristic. In *Proceedings of the 1st international workshop on Arithmetic of Finite Fields*, WAIFI '07, pages 219–236, Berlin, Heidelberg, 2007. Springer-Verlag.

[FPS08] Reza Rezaeian Farashahi, Ruud Pellikaan, and Andrey Sidorenko. Extractors for binary elliptic curves. *Des. Codes Cryptography*, 49 :171–186, December 2008.

[FPSZ06] P.-A. Fouque, D. Pointcheval, J. Stern, and S. Zimmer. Hardness of distinguishing the msb or lsb of secret keys in diffie-hellman schemes. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *ICALP '06, Part II*, volume 4052 of *LNCS*, pages 240–251. Springer, jul 2006.

[FPZ08] Pierre-Alain Fouque, David Pointcheval, and Sébastien Zimmer. Hmac is a randomness extractor and applications to tls. In *Proceedings of the 2008 ACM symposium on Information, computer and communications security*, ASIACCS '08, pages 21–32, New York, NY, USA, 2008. ACM.

[FR94] Gerhard Frey and Hans-Georg Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Mathematics of Computation*, 62(206) :865–874, 1994.

[Ful69] William Fulton. *Algebraic curves*. Advanced Book Classics. W. A. Benjamin, Inc, 1969.

[GÖ5] Nicolas Gürel. Extracting bits from coordinates of a point of an elliptic curve. Cryptology ePrint Archive, Report 2005/324, 2005. `http://eprint.iacr.org/`.

[Gal05] Steven D. Galbraith. Pairings. In *chapter IX in [BSSC05]*, pages 183–214. Cambridge University Press, 2005.

[GKR04] Rosario Gennaro, Hugo Krawczyk, and Tal Rabin. Secure hashed diffie-hellman over non-ddh groups. In *Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings*, pages 361–381, 2004.

[Har77] R. Hartshorne. *Algebraic geometry*. Graduate texts in mathematics. Springer-Verlag, 1977.

[HILL99] Johan Hastad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM J. Comput.*, 28 :1364–1396, March 1999.

[HSV06] F. Hess, N. Smart, and F. Vercauteren. The eta pairing revisited. *IEEE Transactions on Information Theory*, 52 :4595–4602, 2006.

[Huf48] Gerald B. Huff. Diophantine problems in geometry and elliptic ternary forms. *Duke Math. J.*, 15 :443–453, 1948.

[JTV10] Marc Joye, Mehdi Tibouchi, and Damien Vergnaud. Huff's Model for Elliptic Curves. In Guillaume Hanrot, François Morain, and Emmanuel Thomé, editors, *Algorithmic Number Theory, 9th International*

Symposium, ANTS-IX, volume 6197 of *Lecture Notes in Computer Science*, pages 234–250, Nancy, France, 2010. Springer. The original publication is available at www.springerlink.com.

[Kob87] Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177) :pp. 203–209, 1987.

[Kob89] Neal Koblitz. Hyperelliptic cryptosystems. *J. Cryptol.*, 1 :139–150, January 1989.

[KS99] S.V. Koyagin and I.E. Shparlinski. *Character sums with exponential functions and their applications*. Cambridge tracts in mathematics. Cambridge University Press, 1999.

[KS00] David R. Kohel and Igor Shparlinski. On exponential sums and group generators for elliptic curves over finite fields. In *Proceedings of the 4th International Symposium on Algorithmic Number Theory*, pages 395–404, London, UK, 2000. Springer-Verlag.

[LN83] R. Lidl and H. Niederreiter. *Finite fields*. Encyclopedia of mathematics and its applications. Addison-Wesley Pub. Co., Advanced Book Program/World Science Division, 1983.

[Lor96] D. Lorenzini. *An invitation to arithmetic geometry*. Graduate studies in mathematics. American Mathematical Society, 1996.

[Men94] Alfred J. Menezes. *Elliptic Curve Public Key Cryptosystems*. Kluwer Academic Publishers, Norwell, MA, USA, 1994.

[Mil86] Victor S. Miller. Use of elliptic curves in cryptography. In *Advances in Cryptology*, CRYPTO '85, pages 417–426, London, UK, UK, 1986. Springer-Verlag.

[Mil04] Victor S. Miller. The weil pairing, and its efficient calculation. *J. Cryptol.*, 17 :235–261, September 2004.

[SBC+09] Michael Scott, Naomi Benger, Manuel Charlemagne, Luis J. Perez Dominguez, and Ezekiel J. Kachisa. On the final exponentiation for calculating pairings on ordinary elliptic curves. In *Pairing*, pages 78–88, 2009.

[Sha02] Ronen Shaltiel. Recent developments in explicit constructions of extractors. *Bulletin of the EATCS*, 77 :67–95, 2002.

[Sho05] Victor Shoup. *A computational introduction to number theory and algebra*. Cambridge University Press, New York, NY, USA, 2005.

[Shp04] Igor E. Shparlinski. Bounds of gauss sums in finite fields. *Proceedings of the American Mathematical Society*, 132(10) :pp. 2817–2824, 2004.

[Sil86] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, 1986.

[Sti93] Henning Stichtenoth. *Algebraic function fields and codes*. Springer-Verlag, 1993.

[TV00] L. Trevisan and S. Vadhan. Extracting randomness from samplable distributions. In *Proceedings of the 41st Annual Symposium on Foundations of Computer Science*, pages 32–, Washington, DC, USA, 2000. IEEE Computer Society.

[WF10] Hongfeng Wu and Rongquan Feng. Elliptic curves in huff 's model. *IACR Cryptology ePrint Archive*, 2010 :390, 2010.

[Win01] Arne Winterhof. *Incomplete additive character sums and applications.*, pages 462–474. Berlin : Springer, 2001.