Mémoire de Magistère

UTILISATION DES COURBES ELLIPTIQUES EN CRYPTOGRAPHIE

par Christophe Steiner
dirigé par Maurice Mignotte

Septembre 2007

Table des matières

1 Courbes elliptiques **4**
- 1.1 Définitions . . . 4
- 1.2 Loi de groupe . . . 5
- 1.3 Espace projectif et point à l'infini . . . 8
- 1.4 Points de torsion d'une courbe elliptique . . . 9
- 1.5 Couplage de Weil . . . 10
- 1.6 Courbes elliptiques définies sur un corps fini . . . 11

2 Calcul du nombre de points d'une courbe elliptique sur un corps fini **13**
- 2.1 L'algorithme de Schoof . . . 13
- 2.2 Calcul dans le cas général . . . 19
- 2.3 Exemple . . . 20

3 Le problème du logarithme discret **23**
- 3.1 La méthode Baby-Step Giant-Step . . . 23
- 3.2 L'algorithme MOV . . . 24
- 3.3 Courbes à anomalies . . . 28

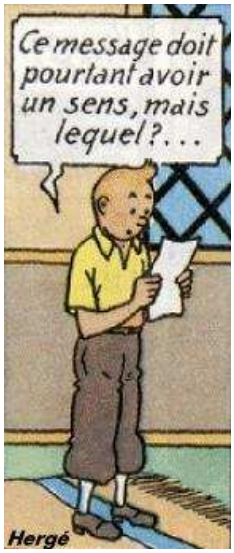
4 Algorithmes de cryptage **32**
- 4.1 Echange de clés . . . 32
- 4.2 Chiffrement asymétrique . . . 33
  - 4.2.1 L'algorithme de Massey-Omura . . . 33
  - 4.2.2 L'algorithme d'ElGamal . . . 36
- 4.3 Signature digitale . . . 37

Introduction

Depuis des millénaires, les rois, les reines et les généraux ont dû se doter de moyens de communication efficaces pour gouverner leur pays ou commander leurs armées. Dans le même temps, ils étaient conscients des risques encourus si leurs messages tombaient entre les mains de l'ennemi. La crainte de ces interceptions fut à l'origine du développement de la cryptographie, technique utilisée pour déguiser un message afin que seul son destinataire désigné puisse le lire. Bien que d'utilisation strictement militaire au début, la cryptographie fait aujourd'hui partie de notre vie quotidienne : les cartes à puce, les achats par internet et les envois de courrier electronique nécessitent d'être cryptés. Pour plus de détails sur l'histoire de la cryptographie, voir par exemple le livre de Simon Singh ([4]).

Dans ce mémoire, je vais m'intéresser aux algorithmes de codage utilisant les courbes elliptiques. L'usage des courbes elliptiques en cryptographie a été suggéré, de manière indépendante, par Neal Koblitz et Victor Miller en 1985.

Dans la première partie, je présenterai les courbes elliptiques et certaines de leurs propriétés. La seconde partie sera consacrée à la manière de calculer le nombre de points d'une courbe elliptique définie sur un corps fini. La troisième partie présentera le problème du logarithme discret, problème qui permet d'assurer la sécurité des algorithmes de cryptage qui seront présentés dans la quatrième et dernière partie.



Chapitre 1

Courbes elliptiques

Nous allons ici définir les courbes elliptiques et en donner certaines propriétés qui nous seront utiles dans les prochains chapitres.

1.1 Définitions

Définition 1.1.1 Soit $\mathbb{K}$ un corps, on appelle *équation de Weierstrass sur* $\mathbb{K}$ une équation de la forme :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \ , \quad a_i \in \mathbb{K}.$$

Définition 1.1.2 Soit $\mathbb{K}$ un corps. Une courbe donnée par une équation de Weierstrass sur $\mathbb{K}$ est dite *lisse* si les dérivées partielles en x et en y de

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$$

ne s'annulent pas en même temps.

Définition 1.1.3 Soit $\mathbb{K}$ un corps. Une *courbe elliptique* E *définie sur* $\mathbb{K}$ (notée $E(\mathbb{K})$) est une courbe lisse donnée par une équation de Weierstrass sur $\mathbb{K}$ à laquelle on rajoute un point à l'infini $\mathcal{O}$ dont nous discuterons la signification rigoureuse dans la partie 1.3.

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

Propriété 1.1.4 Si $\mathbb{K}$ est un corps de caractéristique différente de 2 ou 3, l'équation d'une courbe elliptique sur $\mathbb{K}$ peut s'écrire :

$$y^2 = x^3 + ax + b \ , \quad a, b \in \mathbb{K}$$

avec la condition : $4a^3 + 27b^2 \neq 0$.

Démonstration : Comme la caractéristique du corps est différente de 2, nous pouvons diviser par 2 et ainsi compléter le carré. L'équation

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

donne alors

$$\left(y + \frac{a_1x}{2} + \frac{a_3}{2}\right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + \left(a_4 + \frac{a_1a_3}{2}\right)x + \left(\frac{a_3^2}{4} + a_6\right).$$

En posant

$$\begin{cases} Y = y + \frac{a_1 x}{2} + \frac{a_3}{2} \\ A = a_2 + \frac{a_1^2}{4} \\ B = a_4 + \frac{a_1 a_3}{2} \\ C = \frac{a_3^2}{4} + a_6 \end{cases}$$

nous obtenons l'équation :

$$Y^2 = x^3 + Ax^2 + Bx + C.$$

Comme la caractéristique du corps est différente de 3, nous pouvons diviser par 3 :

$$Y^2 = \left(x + \frac{A}{3}\right)^3 + \left(B - \frac{A^2}{3}\right)\left(x + \frac{A}{3}\right) + \left(C - \frac{AB}{3} + \frac{A^3}{9}\right).$$

En posant

$$\begin{cases} X = x + \frac{A}{3} \\ a = B - \frac{A^2}{3} \\ b = C - \frac{AB}{3} + \frac{A^3}{9} \end{cases}$$

nous obtenons l'équation souhaitée :

$$Y^2 = X^3 + aX + b.$$

De plus, la courbe n'est pas lisse si

$$\begin{cases} 2Y = 0 \\ 3X^2 + a = 0 \end{cases}$$

d'où la relation

$$4a^3 + 27b^2 = 0.$$

La courbe est donc lisse si

$$4a^3 + 27b^2 \neq 0.$$

□

Pour des raisons de clarté, nous supposerons dans la suite du document que le corps est de caractéristique différente de 2 ou de 3 et nous considérerons donc l'équation :

$$y^2 = x^3 + ax + b \ , \quad a, b \in \mathbb{K}$$

où $4a^3 + 27b^2 \neq 0$ pour équation d'une courbe elliptique. Evidemment, tout ce qui suit pourrait être adapté aux cas des corps de caractéristique 2 ou 3.

1.2 Loi de groupe

Le fait central de ce chapitre est que l'ensemble des points d'une courbe elliptique définie sur un corps forme un groupe abélien. Pour expliquer visuellement la loi de groupe associée, considérons pour l'instant que $\mathbb{K} = \mathbb{R}$.

Définition 1.2.1 Soient E une courbe elliptique définie sur $\mathbb{R}$, P et Q deux points de $E(\mathbb{R})$. On définit l'opposé de P et la somme $P + Q$ conformément aux règles suivantes :

1. Si $P = \mathcal{O}$ alors $-P = \mathcal{O}$ et $P + Q = Q$. $\mathcal{O}$ est donc l'élément neutre du groupe. Dans la suite de cette définition, nous supposerons que ni P ni Q n'est égal à $\mathcal{O}$.

2. Si $P = (x, y)$ alors $-P = (x, -y)$. Il est clair que si P appartient à $E(\mathbb{R})$ alors $-P$ appartient également à $E(\mathbb{R})$.

3. Si P et Q ont des abscisses différentes, alors la droite $\Delta = \overline{PQ}$ intersecte la courbe en un troisième point R. Définissons alors $P + Q = -R$. Voici, dans ce cas, la construction géométrique de $P + Q$:

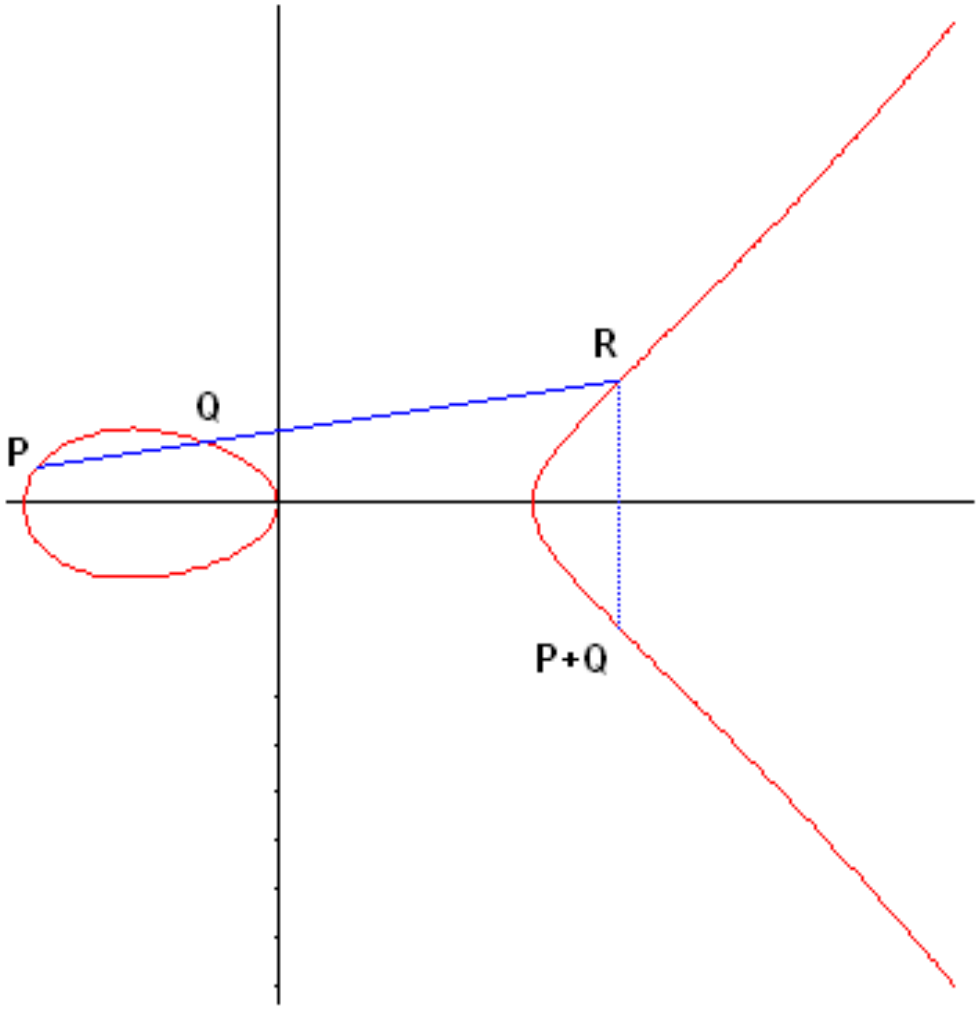


FIG. 1 - Addition sur la courbe elliptique d'équation $y^2 = x^3 - x$

4. Si $P = -Q$ alors $P + Q = \mathcal{O}$.

5. La dernière possibilité est $P = Q$. Dans ce cas, notons Δ la tangente à la courbe en P et soit R l'autre point d'intersection de la courbe avec Δ. On a alors $P + Q = -R$. Voici la

construction géométrique de $2P$:

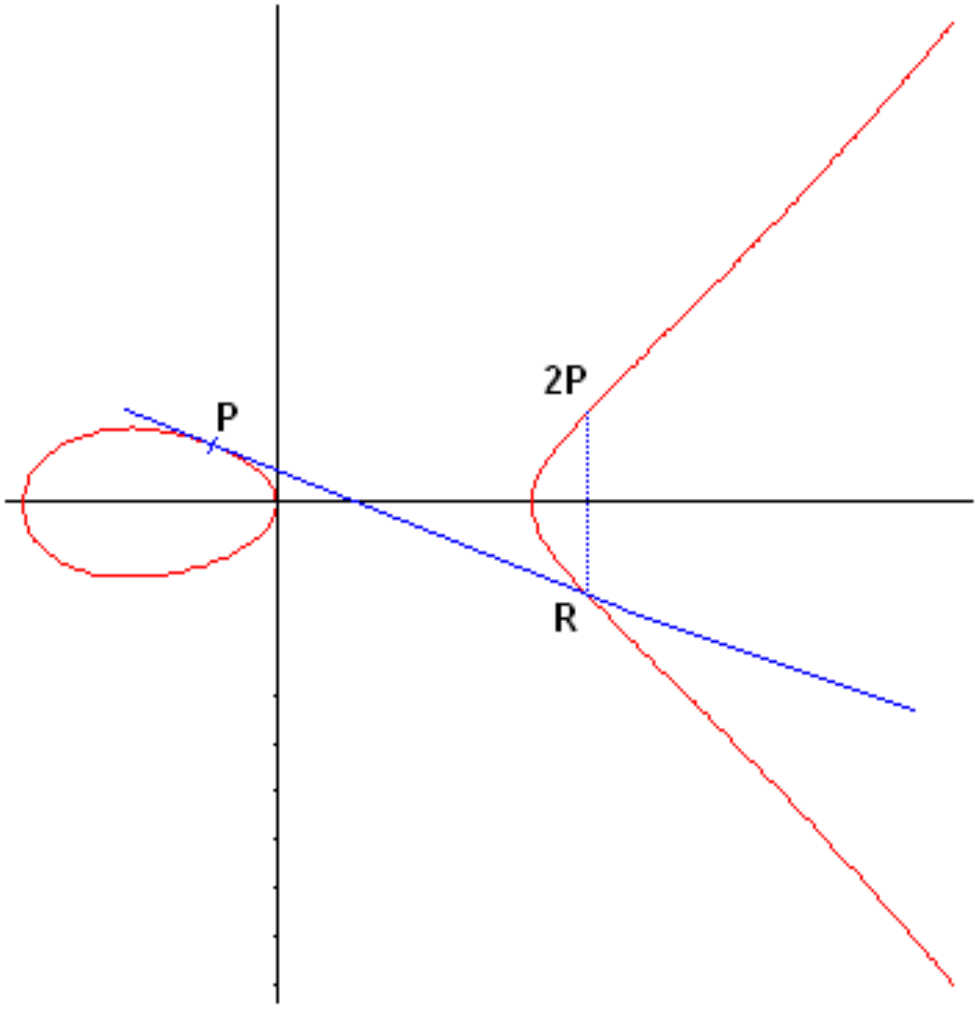


FIG. 2 - Addition sur la courbe elliptique d'équation $y^2 = x^3 - x$

Nous allons maintenant donner les formules explicites de $P+Q$ dans les cas 3 et 5 et ainsi prouver l'unicité du point d'intersection (noté R) entre Δ et la courbe elliptique dans ces 2 cas.

Cas 3 : Soient (x_1, y_1) et (x_2, y_2) les coordonnées de P et Q avec $x_1 \neq x_2$. Calculons les coordonnées (x_3, y_3) de $P+Q$. Soit $\Delta : y = \alpha x + \beta$ l'équation de la droite passant par P et Q. On obtient $\alpha = (y_2 - y_1)/(x_2 - x_1)$ et $\beta = y_1 - \alpha x_1$. Les points d'intersection entre la droite Δ et la courbe elliptique vérifient l'équation : $(\alpha x + \beta)^2 = x^3 + ax + b$. Ainsi les points d'intersection ont comme somme des abscisses le coefficient devant x^2 dans l'équation $x^3 - (\alpha x + \beta)^2 + ax + b = 0$ soit $x_1 + x_2 + x_3 = \alpha^2$ et $y_3 = -(\alpha x_3 + \beta)$ car $P+Q$ est le symétrique du troisième point par rapport à l'axe des abscisses. On obtient finalement :

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

$$y_3 = -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3).$$

Cas 5 : Ce cas est similaire au cas précédent à la différence près que α est ici égal à la dérivée dy/dx au point P : $\alpha = (3x_1^2 + a)/2y_1$. Ce qui donne :

$$\begin{aligned} x_3 &= \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 \\ y_3 &= -y_1 + \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3). \end{aligned}$$

Remarque : Dans le cas d'un corps $\mathbb{K}$ quelconque, les points 1, 2 et 4 de la définition de la loi de groupe ne changent pas. Pour les points 3 et 5, la construction géométrique n'est plus possible en général mais les formules algébriques restent valables.

Théorème 1.2.2 Soit E une courbe elliptique définie sur un corps $\mathbb{K}$ et soit $+$ la loi définie ci-dessus. Alors $(E(\mathbb{K}), +)$ est un groupe abélien.

Le seul point qui nécessite une démonstration est l'associativité de $+$: une démonstration complète (et assez longue) se trouve dans le livre de Lawrence Washington ([5] pp 20-32).

1.3 Espace projectif et point à l'infini

L'objectif de ce paragraphe est d'expliquer l'origine du point à l'infini $\mathcal{O}$.

Soit $\mathbb{K}$ un corps. Définissons la relation d'équivalente suivante : deux triplets (x_1, y_1, z_1) et (x_2, y_2, z_2) de $\mathbb{K}^3$ sont équivalents s'il existe un élément non nul λ de $\mathbb{K}$ tel que

$$(x_1, y_1, z_1) = (\lambda x_2, \lambda y_2, \lambda z_2).$$

L'espace projectif $\mathbb{P}^2_{\mathbb{K}}$ sur $\mathbb{K}$ est défini par la classe d'équivalence des triplets (x, y, z) notée $(x : y : z)$ où x, y, z ne sont pas tous nuls.

Soit $(x : y : z)$ un point de $\mathbb{P}^2_{\mathbb{K}}$ avec $z \neq 0$, alors $(x : y : z) = (x/z : y/z : 1)$: ce sont les *points finis* de $\mathbb{P}^2_{\mathbb{K}}$. Par contre, les points $(x : y : 0)$ sont appelés *points infinis* de $\mathbb{P}^2_{\mathbb{K}}$.

Le plan affine sur $\mathbb{K}$ est l'ensemble :

$$\mathbb{A}^2_{\mathbb{K}} = \{(x, y) \in \mathbb{K} \times \mathbb{K}\}.$$

L'inclusion

$$\begin{aligned} \mathbb{A}^2_{\mathbb{K}} &\hookrightarrow \mathbb{P}^2_{\mathbb{K}} \\ (x, y) &\mapsto (x : y : 1) \end{aligned}$$

permet d'identifier le plan affine avec les points finis de $\mathbb{P}^2_{\mathbb{K}}$.

Un polynôme est homogène de degré n s'il est la somme de termes de la forme $ax^i y^j z^k$ où $a \in \mathbb{K}$ et $i + j + k = n$. Si un polynôme F est homogène de degré n alors $F(\lambda x, \lambda y, \lambda z) = \lambda^n F(x, y, z)$ pour tout $\lambda \in \mathbb{K}$. Il s'en suit que si (x_1, y_1, z_1) et (x_2, y_2, z_2) sont équivalents alors $F(x_1, y_1, z_1) = 0$ si et seulement si $F(x_2, y_2, z_2) = 0$. Un zéro de F dans $\mathbb{P}^2_{\mathbb{K}}$ ne dépend donc pas du choix du représentant

de la classe d'équivalence, ainsi l'ensemble des zéros de F dans $\mathbb{P}^2_{\mathbb{K}}$ est bien défini. Par contre, si F n'est pas homogène, nous ne pouvons pas parler d'un point de $\mathbb{P}^2_{\mathbb{K}}$ lorsque $F(x, y, z) = 0$.

Par exemple, si $F(x, y, z) = x^2 + 2y - 3z$ alors $F(1, 1, 1) = 0$ et $F(2, 2, 2) = 2$ bien que $(1 : 1 : 1) = (2 : 2 : 2)$.

Pour contourner ce problème, nous devrons travailler avec des polynômes homogènes. Si $f(x, y)$ est un polynôme en x et en y, nous pouvons le rendre homogène en insérant des puissances de z.

Par exemple, si $f(x, y) = y^2 - x^3 - Ax - B$, nous pouvons obtenir le polynôme homogène $F(x, y, z) = y^2z - x^3 - Axz^2 - Bz^3$.

Regardons maintenant ce que cela signifie pour deux droites parallèles se rencontrant à l'infini. Soient

$$y = ax + b_1, \qquad y = ax + b_2$$

deux droites parallèles avec $b_1 \neq b_2$. Les formes homogènes sont

$$y = ax + b_1 z, \qquad y = ax + b_2 z.$$

En résolvant les deux équations pour déterminer leur intersection, nous trouvons

$$z = 0 \quad \text{et} \quad y = ax.$$

Les deux droites ont donc pour intersection $(1 : a : 0)$ qui est un point infini de $\mathbb{P}^2_{\mathbb{K}}$. De même, deux droites verticales $x = c_1$ et $x = c_2$ ont pour intersection le point infini $(0 : 1 : 0)$.

Intéressons-nous maintenant à une courbe elliptique d'équation $y^2 = x^3 + Ax + B$. Sa forme homogène est $y^2z = x^3 + Axz^2 + Bz^3$. Pour connaître les points de cette courbe se trouvant à l'infini, prennons $z = 0$. Il s'en suit $x^3 = 0$ soit $x = 0$. Comme y ne peut pas être nul (sinon x, y et z seraient nuls), le seul point infini de la courbe elliptique est $(0 : y : 0) = (0 : 1 : 0)$: c'est le point noté $\mathcal{O}$. Comme nous l'avons vu précédemment, le point $(0 : 1 : 0)$ appartient à chaque droite verticale donc chaque droite verticale intersecte la courbe elliptique en ce point.

1.4 Points de torsion d'une courbe elliptique

Définition 1.4.1 Soient E une courbe elliptique définie sur un corps $\mathbb{K}$ et n un entier positif non nul. On pose :

$$E[n] = \{P \in E(\overline{\mathbb{K}}) \mid nP = \mathcal{O}\}$$

où $\overline{\mathbb{K}}$ est la clotûre algébrique de $\mathbb{K}$.

Théorème 1.4.2 Soient E une courbe elliptique définie sur un corps $\mathbb{K}$ de caractéristique p et n un entier positif non nul. Si p est nul ou si p ne divise pas n alors

$$E[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}.$$

Si $p > 0$ divise n, écrivons $n = p^r n'$ où p ne divise pas n'. Alors

$$E[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n'\mathbb{Z} \quad \text{ou} \quad E[n] \simeq \mathbb{Z}/n'\mathbb{Z} \oplus \mathbb{Z}/n'\mathbb{Z}.$$

Démonstration : Voir [5] pp 76-82. □

Corollaire-Définition 1.4.3 Soit E une courbe elliptique définie sur un corps $\mathbb{K}$ de caractéristique p. Alors

$$E[p] \simeq \mathbb{Z}/p\mathbb{Z} \quad \text{ou} \quad E[p] = \{\mathcal{O}\}.$$

On dit que E est une courbe elliptique *supersingulière* si

$$E[p] = \{\mathcal{O}\}.$$

Dans le cas contraire, on dit que E est une courbe elliptique *ordinaire*.

1.5 Couplage de Weil

Définition 1.5.1 Soient $\mathbb{K}$ un corps de caractéristique p et n un entier positif non nul qui n'est pas divisible par p. On pose

$$\mu_n(\overline{\mathbb{K}}) = \{x \in \overline{\mathbb{K}} \mid x^n = 1\}.$$

Remarque : $\mu_n(\overline{\mathbb{K}})$ est le groupe des racines $n^{ième}$ de l'unité dans $\overline{\mathbb{K}}$. Puisque la caractéristique de $\mathbb{K}$ ne divise pas n, l'équation $x^n = 1$ n'a pas de racine multiple donc il y a n racines dans $\overline{\mathbb{K}}$. Ainsi, $\mu_n(\overline{\mathbb{K}})$ est un groupe cyclique d'ordre n. Chaque générateur ζ est appelé *racine primitive* $n^{ième}$ *de l'unité*. De plus, $\zeta^k = 1$ si et seulement si n divise k.

Théorème 1.5.2 Soient E une courbe elliptique définie sur un corps $\mathbb{K}$ de caractéristique p et n un entier positif non nul qui n'est pas divisible par p. Alors il existe une application

$$e_n : E[n] \times E[n] \longrightarrow \mu_n(\overline{\mathbb{K}})$$

appelée *couplage de Weil* qui possède les propriétés suivantes :

1. Pour tout $T \in E[n]$,
$$e_n(T, T) = 1.$$
2. Pour tout S, T appartenant à $E[n]$, on a
$$e_n(S, T) = e_n(T, S)^{-1}.$$
3. e_n est bilinéaire en chaque variable, c'est-à-dire que pour tout S_1, S_2, T_1, T_2 appartenant à $E[n]$, on a
$$\begin{cases} e_n(S_1 + S_2, T_1) = e_n(S_1, T_1) \cdot e_n(S_2, T_1) \\ e_n(S_1, T_1 + T_2) = e_n(S_1, T_1) \cdot e_n(S_1, T_2). \end{cases}$$
4. e_n est non dégénéré en chaque variable, c'est-à-dire que si pour tout T de $E[n]$, on a
$$e_n(S, T) = 1$$
alors $S = \mathcal{O}$ et de même si pour tout S de $E[n]$, on a
$$e_n(S, T) = 1$$
alors $T = \mathcal{O}$.

5. Pour tout automorphisme σ de $\overline{\mathbb{K}}$ tel que σ soit l'identité sur les coefficients de E, on a :

$$e_n(\sigma S, \sigma T) = \sigma(e_n(S,T))$$

où $S, T \in E[n]$.

Démonstration : Voir le chapitre 11 de [5]. □

Corollaire 1.5.3 Soit E une courbe elliptique définie sur un corps $\mathbb{K}$ et soit n un entier positif non nul non divisible par la caractéristique de $\mathbb{K}$. D'après le théorème 1.4.2, $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. Soit donc $\{T_1, T_2\}$ une base de $E[n]$. Alors $e_n(T_1, T_2)$ est une racine primitive $n^{ième}$ de l'unité.

Démonstration : Posons $\zeta = e_n(T_1, T_2)$ où $\zeta^d = 1$. Grâce aux propriétés du théorème 1.5.2, nous avons

$$e_n(T_1, dT_2) = e_n(T_1, T_2)^d = 1$$
$$e_n(T_2, dT_2) = e_n(T_2, T_2)^d = 1.$$

Soit $S \in E[n]$ alors il existe des entiers a, b tels que $S = aT_1 + bT_2$. Ainsi,

$$e_n(S, dT_2) = e_n(aT_1 + bT_2, dT_2) = e_n(T_1, dT_2)^a \cdot e_n(T_2, dT_2)^b = 1$$

pour tout $S \in E[n]$. Le point 4 du théorème 1.5.2 nous informe alors que $dT_2 = \mathcal{O}$. Or, $dT_2 = \mathcal{O}$ si et seulement si n divise d d'où ζ est une racine primitive $n^{ième}$ de l'unité.

□

Corollaire 1.5.4 Si $E[n] \subseteq E(\mathbb{K})$, alors $\mu_n(\overline{\mathbb{K}}) \subset \mathbb{K}$.

Remarque : Les points de $E[n]$ peuvent avoir leurs coordonnées dans $\overline{\mathbb{K}}$. L'hypothèse du corollaire contraint ces coordonnées à être dans $\mathbb{K}$.

Démonstration : Soit σ un automorphisme de $\overline{\mathbb{K}}$ tel que σ soit l'identité sur $\mathbb{K}$. Soit $\{T_1, T_2\}$ une base de $E[n]$. Puisque T_1, T_2 ont leurs coordonnées dans $\mathbb{K}$, on a $\sigma T_1 = T_1$ et $\sigma T_2 = T_2$. D'après le point 5 du théorème 1.5.2,

$$\zeta = e_n(T_1, T_2) = e_n(\sigma T_1, \sigma T_2) = \sigma(e_n(T_1, T_2)) = \sigma(\zeta).$$

ζ est alors un point fixe de σ et le théorème fondamental de la théorie de Galois permet alors de conclure que $\zeta \in \mathbb{K}$. De plus, par le corollaire 1.5.3, on sait que ζ est une racine primitive $n^{ième}$ de l'unité. Il en résulte que $\mu_n \subset \mathbb{K}$.

□

1.6 Courbes elliptiques définies sur un corps fini

En cryptographie, on s'intéresse surtout aux courbes elliptiques définies sur des corps finis.

Théorème 1.6.1 Soit E une courbe elliptique définie sur le corps fini $\mathbb{F}_q$. Alors

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/n\mathbb{Z} \quad \text{ou} \quad E(\mathbb{F}_q) \simeq \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z}$$

pour un certain entier $n \geq 1$, ou pour des entiers $n_1, n_2 \geq 1$ où n_1 divise n_2.

Démonstration : Un résultat de la théorie des groupes affirme qu'un groupe fini abélien est isomorphe à la somme directe de groupes cycliques

$$\mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus ... \oplus \mathbb{Z}/n_r\mathbb{Z}$$

où n_i divise n_{i+1} pour $i \geq 1$. Puisque, pour chaque i, le groupe $\mathbb{Z}/n_i\mathbb{Z}$ a n_1 éléments d'ordre divisant n_1, nous obtenons que $E(\mathbb{F}_q)$ a n_1^r éléments d'ordre divisant n_1. Or, par le théorème 1.4.2, nous savons qu'il existe au plus n_1^2 points d'ordre divisant n_1. Ainsi $r \leq 2$, ce qui est le résultat escompté.

□

Définition 1.6.2 Soient $\mathbb{F}_q$ un corps fini et $\overline{\mathbb{F}}_q$ la clôture algébrique de $\mathbb{F}_q$. On définit l'*endomorphisme de Frobenius* sur $\overline{\mathbb{F}}_q$ ainsi :

$$\begin{array}{rcl} \phi_q : \overline{\mathbb{F}}_q & \longrightarrow & \overline{\mathbb{F}}_q \\ x & \longmapsto & x^q. \end{array}$$

On peut étendre cette définition sur les coordonnées des points de $E(\overline{\mathbb{F}}_q)$:

$$\begin{array}{rcl} \phi_q : E(\overline{\mathbb{F}}_q) & \longrightarrow & E(\overline{\mathbb{F}}_q) \\ (x, y) & \longmapsto & (x^q, y^q) \\ \mathcal{O} & \longmapsto & \mathcal{O}. \end{array}$$

Propriété 1.6.3

1. Si $(x, y) \in E(\overline{\mathbb{F}}_q)$ alors $\phi_q(x, y) \in E(\overline{\mathbb{F}}_q)$.

2. $(x, y) \in E(\mathbb{F}_q)$ si et seulement si $\phi_q(x, y) = (x, y)$.

3. ϕ_q est un endomorphisme.

Démonstration : Voir [5] p. 93 □

Théorème 1.6.4 (Hasse) Soit E une courbe elliptique définie sur $\mathbb{F}_q$. Le cardinal du groupe $E(\mathbb{F}_q)$ est noté $\#E(\mathbb{F}_q)$. Alors

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

Démonstration : Voir [5] pp 91-94. □

Dans la suite de cette partie, nous noterons $a = q + 1 - \#E(\mathbb{F}_q)$.

Théorème 1.6.5 Soit E une courbe elliptique définie sur $\mathbb{F}_q$. Alors

$$\phi_q^2 - a\phi_q + q = 0$$

en tant qu'endomorphisme de $E(\mathbb{F}_q)$. Autrement dit, nous avons

$$(x^{q^2}, y^{q^2}) - a \cdot (x^q, y^q) + q \cdot (x, y) = \mathcal{O}$$

pour tout $(x, y) \in E(\overline{\mathbb{F}}_q)$. De plus, a est le seul entier qui vérifie cette relation.

Démonstration : Voir [5] pp 95-96. □

Chapitre 2

Calcul du nombre de points d'une courbe elliptique sur un corps fini

Intéressons-nous maintenant au calcul du nombre de points d'une courbe elliptique E sur un corps fini $\mathbb{F}_q$, c'est à dire le cardinal du groupe $E(\mathbb{F}_q)$ où $q = p^r$.

Il est clair que $E(\mathbb{F}_q)$ a au maximum $2q+1$ points, *i.e.* le point à l'infini plus $2q$ paires $(x, y) \in \mathbb{F}_q^2$ vérifiant $E : y^2 = x^3 + Ax + B$. Ainsi,

$$1 \leq \#E(\mathbb{F}_q) \leq 2q + 1.$$

Le théorème de Hasse (théorème 1.6.4) donne un meilleur encadrement :

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

Nous allons, dans ce chapitre, présenter un algorithme qui permet de calculer exactement $\#E(\mathbb{F}_q)$.

Nous nous intéressons à cette question car il sera indispensable de connaître ce cardinal dans la mise en oeuvre de l'algorithme de Massey-Omura (partie 4.2.1) et pour assurer la sécurité des algorithmes de cryptage (voir chapitre 3).

2.1 L'algorithme de Schoof

René Schoof a publié en 1985 (voir [3]) un algorithme permettant de calculer le cardinal du groupe $E(\mathbb{F}_p)$ où p est un nombre premier impair (Dans le cas $p = 2$, ce cardinal se calcule très rapidement à la main).

Le théorème de Hasse (théorème 1.6.4) nous informe que :

$$\#E(\mathbb{F}_p) = p + 1 - a, \qquad \text{où } \mid a \mid \leq \ 2\sqrt{p}.$$

Notons S le plus petit ensemble des premiers nombres premiers $\{2, 3, 5, ..., \ell_k\}$ vérifiant

$$\prod_{i=1}^{k} \ell_i > 4\sqrt{p}.$$

Pour calculer a, il suffit de déterminer $a \ mod \ \ell_i$ pour tous les i entre 1 et k. En effet, le théorème des restes chinois nous donnera

$$a \ \ mod \prod_{i=1}^{k} \ell_i$$

et l'encadrement $\mid a \mid \leq 2\sqrt{p}$ permettra alors de déterminer a.

Premier cas : calcul de $a \ mod \ 2$.

Comme p est impair et que $\#E(\mathbb{F}_p) = p + 1 - a$, on a :

$$a \equiv \#E(\mathbb{F}_p) \pmod 2.$$

Si $a \equiv 0 \ (mod \ 2)$, cela signifie que $E(\mathbb{F}_p)$ est d'ordre pair et donc qu'il existe un élément d'ordre 2. Nous savons que les seuls éléments d'ordre 2 de $E(\mathbb{F}_p)$ sont de la forme $(e, 0)$ avec $e \in \mathbb{F}_p$, c'est-à-dire que e est racine de $x^3 + Ax + B$.

Par contre, si $x^3 + Ax + B$ n'a pas de racine dans $\mathbb{F}_p$ alors $\#E(\mathbb{F}_p) \equiv 1 \ (mod \ 2)$ donc $a \equiv 1 \ (mod \ 2)$.

Rappelons que les éléments de $\mathbb{F}_p$ sont exactement les racines de $x^p - x$. Ainsi, il nous suffit de calculer

$$PGCD(x^3 + Ax + B, x^p - x)$$

par l'algorithme d'Euclide.

Si ce $PGCD$ est égal à 1, alors les polynômes $x^3 + Ax + B$ et $x^p - x$ n'ont pas de racine commune et donc $x^3 + Ax + B$ n'a pas de racine dans $\mathbb{F}_p$ d'où $a \equiv 1 \ (mod \ 2)$.

Par contre, si ce $PGCD$ est différent de 1, alors $x^3 + Ax + B$ a une racine dans $\mathbb{F}_p$ et donc $a \equiv 0 \ (mod \ 2)$.

Remarque : Si p est très grand, le polynôme x^p est de très grand degré. Il est alors préférable de calculer

$$x_p \equiv x^p \ (mod \ x^3 + Ax + B)$$

puis d'utiliser le fait que :

$$PGCD(x_p - x, x^3 + Ax + B) = PGCD(x^p - x, x^3 + Ax + B).$$

Second cas : calcul de $a \ mod \ \ell$ (où $\ell \neq 2$).

D'après le théorème 1.6.5, pour déterminer $a \ mod \ \ell$, il suffit de trouver quelle relation du type

$$\phi_p^2 - k\phi_p + p = 0$$

peut avoir lieu sur $E[\ell]$. On aura alors $k \equiv a \ (mod \ \ell)$.

Dans ce qui suit, nous allons avoir besoin des polynômes de division. En voici une définition :

Définition 2.1.1 Soient A et B des variables. Les *polynômes de division* $\psi_\ell \in \mathbb{Z}[x, y, A, B]$ sont définis ainsi :

$$\begin{aligned} \psi_0 &= 0 \\ \psi_1 &= 1 \\ \psi_2 &= 2y \end{aligned}$$

$$\begin{aligned}
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2 \\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) \\
\psi_{2m} &= (2y)^{-1}(\psi_m)(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \quad \text{pour } m \geq 3 \\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \quad \text{pour } m \geq 2.
\end{aligned}$$

Voici quelques propriétés des polynômes de division qui nous seront utiles pour la suite :

Propriété 2.1.2 Si n est impair alors ψ_n est un polynôme de $\mathbb{Z}[x, y^2, A, B]$. Par contre, si n est pair, alors ψ_n est dans $2y\mathbb{Z}[x, y^2, A, B]$.

Démonstration : La preuve se fait par récurrence. La propriété est vraie pour $n \leq 4$. Supposons qu'elle est vraie pour tout $n < 2m$. Nous pouvons supposer que $2m > 4$, soit $m > 2$. Alors $2m > m + 2$ donc les polynômes apparaissant dans la définition de ψ_{2m} satisfont l'hypothèse de récurrence. Si m est pair, alors ψ_m, ψ_{m+2} et ψ_{m-2} sont dans $2y\mathbb{Z}[x, y^2, A, B]$ donc ψ_{2m} est dans $2y\mathbb{Z}[x, y^2, A, B]$. Si m est impair, alors ψ_{m-1} et ψ_{m+1} sont dans $2y\mathbb{Z}[x, y^2, A, B]$, nous trouvons donc de nouveau que ψ_{2m} est dans $2y\mathbb{Z}[x, y^2, A, B]$. La propriété est donc vraie pour $n = 2m$. De même, on montre qu'elle est vraie pour $n = 2m + 1$.

□

Plaçons-nous maintenant sur une courbe elliptique

$$E: \quad y^2 = x^3 + Ax + B, \quad 4A^3 + 27B^2 \neq 0.$$

Nous pouvons alors voir les polynômes de $\mathbb{Z}[x, y^2, A, B]$ comme polynômes de $\mathbb{Z}[x, A, B]$ en remplaçant y^2 par $x^3 + Ax + B$. De même, nous pouvons voir les polynômes de $2y\mathbb{Z}[x, y^2, A, B]$ comme polynômes de $2y\mathbb{Z}[x, A, B]$. La proposition suivante précise un peu les choses.

Propriété 2.1.3

$$\psi_n = \begin{cases} y(nx^{(n^2-4)/2} + \text{termes en } x \text{ de degré plus petit}) & \text{si n est pair.} \\ nx^{(n^2-1)/2} + \text{termes en } x \text{ de degré plus petit} & \text{si n est impair.} \end{cases}$$

Démonstration : La preuve se fait de nouveau par récurrence. Par exemple, si $n = 2m + 1$ où m est pair, alors le terme dominant de $\psi_{m+2}\psi_m^3$ est

$$(m + 2)m^3 y^4 x^{\frac{(m+2)^2-4}{2} + \frac{3m^2-12}{2}}.$$

En remplaçant y^4 par $(x^3 + Ax + B)^2$, on obtient :

$$(m + 2)m^3 x^{\frac{(2m+1)^2-1}{2}}.$$

De même, le terme dominant de $\psi_{m-1}\psi_{m+1}^3$ est

$$(m - 1)(m + 1)^3 x^{\frac{(2m+1)^2-1}{2}}.$$

En utilisant la relation de récurrence définissant ψ_{2m+1}, on obtient bien le terme dominant énoncé dans la proposition. Les autres cas se traitent de la même manière.

□

Propriété 2.1.4 Soient $(x, y) \in E(\overline{\mathbb{F}}_q)$ et n un entier positif impair. Alors

$$(x, y) \in E[n] \Longleftrightarrow \psi_n(x) = 0.$$

Démonstration : Voir le chapitre 9.5 de [5]. □

On se donne $\ell \in S$ où $\ell \neq 2$ et $(x, y) \in E(\mathbb{F}_p) \cap E[\ell]$. Alors on a

$$\begin{cases} \left(x^{p^2}, y^{p^2}\right) + p(x, y) = a(x^p, y^p) \\ \psi_\ell(x) = 0. \end{cases}$$

La dernière équation permet de travailler modulo ψ_l dans tout ce qui suit afin de réduire le degré des polynômes. Soit $p_\ell \in]-\ell/2, \ell/2[$ tel que $p_\ell \equiv p \ (mod\ \ell)$. Comme $p_\ell \equiv p \ (mod\ \ell)$, nous avons $p(x, y) = p_\ell(x, y)$ d'où

$$\left(x^{p^2}, y^{p^2}\right) + p_\ell(x, y) = a(x^p, y^p).$$

Ceci nous permet de travailler avec de plus petites valeurs. Puisque (x^p, y^p) est aussi d'ordre ℓ (se rappeler que ϕ_p est un endomorphisme), la relation ci-dessus détermine $a \ mod\ \ell$. L'idée est de calculer tous les termes de cette équation excepté a. Notons que si cette relation est vérifiée pour un point de $(x, y) \in E[\ell]$, alors nous pourrons déterminer $a \ mod\ \ell$ et cette relation sera vraie pour tout $(x, y) \in E[\ell]$.

<u>*Premier cas :*</u> Supposons qu'il existe $(x, y) \in E[\ell]$ tel que $(x^{p^2}, y^{p^2}) \neq \pm p_\ell(x, y)$.

Posons alors :

$$(x', y') \stackrel{def}{=} (x^{p^2}, y^{p^2}) + p_\ell(x, y) \neq \mathcal{O}$$

donc $a \not\equiv 0 \ (mod\ \ell)$. Dans ce cas, les premières coordonnées de (x^{p^2}, y^{p^2}) et $p_\ell(x, y)$ sont distinctes.

Nous allons utiliser la formule d'addition décrite dans la partie 1.2.

Posons d'abord :

$$(x_j, y_j) \stackrel{def}{=} j(x, y)$$

pour tout entier j. On s'aperçoit en regardant la loi d'addition que x_j est une fraction rationnelle en x. Notons donc $x_j = r_{1,j}(x)$ où $r_{1,j}(x)$ est une fraction rationnelle en x. De même, y_j peut être mis sous la forme $y_j = r_{2,j}(x)y$ où $r_{2,j}(x)$ est également une fraction rationnelle en x.

La formule d'addition donne alors :

$$x' = \left(\frac{y^{p^2} - y_{p_\ell}}{x^{p^2} - x_{p_\ell}}\right)^2 - x^{p^2} - x_{p_\ell}.$$

Nous pouvons exprimer $(y^{p^2} - y_{p_\ell})^2$ en fonction de x :

$$\begin{aligned} \left(y^{p^2} - y_{p_\ell}\right)^2 &= y^2 \left(y^{p^2-1} - r_{2,p_\ell}(x)\right)^2 \\ &= (x^3 + Ax + B)\left((x^3 + Ax + B)^{(p^2-1)/2} - r_{2,p_\ell}(x)\right)^2. \end{aligned}$$

Il en va de même avec $(x^{p^2} - x_{p_\ell})^2$. Ainsi, x' est une fraction rationnelle en x.

Nous cherchons j tel que

$$(x', y') = (x_j^p, y_j^p).$$

Regardons d'abord la première coordonnée. Soit $(x, y) \in E[\ell]$, alors $(x', y') = \pm(x_j^p, y_j^p)$ si et seulement si $x' = x_j^p$. Nous avons vu plus haut que si cette relation est vraie pour un point de $E[\ell]$, alors elle est vraie pour tous les points de $E[\ell]$. Puisque les racines de ψ_ℓ sont les premières coordonnées des points de $E[\ell]$, ceci implique que

$$x' - x_j^p \equiv 0 \pmod{\psi_\ell}.$$

(Ceci signifie que le numérateur de $x' - x_j^p$ est un multiple de ψ_ℓ). Nous utilisons en fait que les racines de ψ_ℓ sont simples (sinon nous pourrions uniquement conclure que ψ_ℓ divise une puissance de $x' - x_j^q$). Ceci se prouve en remarquant qu'il y a $\ell^2 - 1$ points distincts d'ordre ℓ (théorème 1.4.2). Il y a donc $(\ell^2 - 1)/2$ premières coordonnées différentes (car si $(x, y) \in E[\ell]$ alors $-(x, y) = (x, -y) \in E[\ell]$) et ce sont toutes des racines de ψ_ℓ (ψ_ℓ est de degré $(\ell^2 - 1)/2$ d'après la propriété 2.1.3). Ainsi, les racines de ψ_ℓ sont simples.

Supposons maintenant que nous ayons trouvé j tel que

$$x' - x_j^q \equiv 0 \pmod{\psi_\ell}.$$

Alors

$$(x', y') = \pm(x_j^p, y_j^p) = (x_j^p, \pm y_j^p)$$

Pour déterminer le signe, nous avons besoin de regarder les secondes coordonnées. y'/y et y_j^p/y peuvent toutes les deux être exprimées comme fonctions de x. Si

$$(y' - y_j^p)/y \equiv 0 \pmod{\psi_\ell}$$

alors $a \equiv j \pmod{\ell}$. Sinon $a \equiv -j \pmod{\ell}$.

<u>*Second cas*</u> : Supposons que $(x^{p^2}, y^{p^2}) = \pm p_\ell(x, y)$ pour tout $(x, y) \in E[\ell]$.

Si

$$\phi_p^2(x, y) = (x^{p^2}, y^{p^2}) = -p_\ell(x, y)$$

alors

$$aP = (\phi_p^2 + p)P = \mathcal{O}$$

pour tout $P \in E[l]$. Il en résulte que

$$a \equiv 0 \pmod{\ell}.$$

Si

$$\phi_p^2(x, y) = (x^{p^2}, y^{p^2}) = p_\ell(x, y)$$

alors

$$a\phi_p(x, y) = \phi_p^2(x, y) + p(x, y) = 2p(x, y)$$

d'où

$$a^2 p(x, y) = a^2 \phi_p^2(x, y) = (2p)^2(x, y).$$

Ainsi $a^2 q \equiv 4q^2 \pmod{\ell}$, p est donc un carré modulo ℓ. Notons alors $w^2 \equiv p \pmod{\ell}$. Il vient

$$(\phi_p + w)(\phi_p - w)(x, y) = (\phi_p^2 - p)(x, y) = \mathcal{O}$$

pour tout $(x, y) \in E[l]$. Soit P un point de $E[\ell]$. Nous avons deux possibilités : soit $(\phi_p - w)P = \mathcal{O}$, c'est-à-dire $\phi_p P = wP$, soit $P' = (\phi_p - w)P$ est un point fini qui vérifie $(\phi_p + w)P' = \mathcal{O}$. Dans les

deux cas, il existe un point $P \in E[\ell]$ tel que $\phi_p P = \pm wP$.

Supposons qu'il existe un point $P \in E[\ell]$ tel que $\phi_p P = wP$. Alors

$$\mathcal{O} = (\phi_p^2 - a\phi_p + p)P = (p - aw + p)P$$

d'où $aw \equiv 2p \equiv 2w^2 \ (mod\ \ell)$. Ainsi, $a \equiv 2w \ (mod\ \ell)$. De même, s'il existe $P \in E[\ell]$ tel que $\phi_p P = -wP$, alors $a \equiv -2w \ (mod\ \ell)$.

Nous pouvons savoir dans quel cas nous nous trouvons par la méthode qui suit. En fait, nous voulons savoir s'il existe $(x, y) \in E[\ell]$ tel que

$$\phi_p(x, y) = (x^p, y^p) = \pm w(x, y) = \pm(x_w, y_w) = (x_w, \pm y_w).$$

Pour cela, nous calculons $x^p - x_w$ qui est une fraction rationnelle en x. Si

$$PGCD(numérateur(x^p - x_w), \psi_\ell) \neq 1$$

alors il existe $(x, y) \in E[\ell]$ tel que $\phi_p(x, y) = \pm w(x, y)$. Dans ce cas, nous utiliserons la seconde coordonnée pour déterminer le signe. Par contre, si

$$PGCD(numérateur(x^p - x_w), \psi_\ell) = 1$$

nous ne pouvons pas être dans le cas

$$(x^{p^2}, y^{p^2}) = p(x, y).$$

Nous sommes alors dans le cas

$$(x^{p^2}, y^{p^2}) = -p(x, y)$$

qui a été traité plus haut.

Résumé de l'algorithme de Schoof

Nous démarrons avec une courbe elliptique E définie sur $\mathbb{F}_p$ donnée par $y^2 = x^3 + Ax + B$. Nous cherchons à calculer $\#E(\mathbb{F}_p) = p + 1 + a$. L'algorithme se déroule ainsi :

1. On se donne l'ensemble $S = \{2, 3, 5, ..., \ell_i\}$ défini plus haut.
2. Si $\ell = 2$, alors $a \equiv 0 \ (mod\ 2)$ si et seulement si
$$PGCD(x^3 + Ax + B, x^p - x) \neq 1.$$
3. Pour chaque nombre premier impair $\ell \in S$, faire ce qui suit :
   (a) Soit $p_\ell \equiv p \ (mod\ \ell)$ tel que $\mid p_\ell \mid < \ \ell/2$.
   (b) Calculer x', la première coordonnée de
   $$(x', y') = (x^{p^2}, y^{p^2}) + p_\ell(x, y) \quad (mod\ \psi_\ell).$$
   (c) Pour $j = 1, 2, ..., (\ell - 1)/2$, faire ce qui suit :
      i. Calculer x_j, la première coordonnée de
      $$(x_j, y_j) = j(x, y).$$

ii. Si $x' - x_j^p \equiv 0 \ (mod\ \psi_\ell)$, aller à l'étape (iii). Sinon retourner en (i) avec l'entier j suivant. Si toutes les valeurs $1 \leq j \leq (\ell-1)/2$ ont été essayées, aller à l'étape (d).

iii. Calculer y' et y_j. Si

$$(y' - y_j^p)/y \equiv 0 \quad (mod\ \psi_\ell)$$

alors $a \equiv j \ (mod\ \ell)$, sinon $a \equiv -j \ (mod\ \ell)$.

(d) Si toutes les valeurs $1 \leq j \leq (\ell-1)/2$ ont été essayées sans succès, posons

$$w^2 \equiv p \ (mod\ \ell).$$

Dans le cas où w n'existerait pas, alors $a \equiv 0 \ (mod\ \ell)$.

(e) Si

$$PGCD(numérateur(x^p - x_w), \psi_\ell) = 1$$

alors $a \equiv 0 \ (mod\ \ell)$. Sinon calculer

$$PGCD(numérateur((y^p - y_w)/y), \psi_\ell).$$

Si ce $PGCD$ est différent de 1 alors $a \equiv 2w \ (mod\ \ell)$, sinon $a \equiv -2w \ (mod\ \ell)$.

4. Puisque nous connaissons $a\ mod\ \ell$ pour tout $\ell \in S$, nous pouvons calculer

$$a\ mod \prod_{\ell \in S} \ell$$

grâce au théorème des restes chinois. Choisir ensuite la valeur de a qui satisfait cette congruence et telle que $\mid a \mid \leq 2\sqrt{p}$. Le nombre de points dans $E(\mathbb{F}_p)$ est alors

$$\#E(\mathbb{F}_p) = p + 1 - a.$$

Un exemple sera donné dans la partie 2.3.

2.2 Calcul dans le cas général

Nous connaissons le cardinal de $E(\mathbb{F}_p)$ grâce à l'algorithme précédent. Dans cette partie, nous allons voir comment calculer $\#E(\mathbb{F}_q)$ où $q = p^r$ en connaissant $\#E(\mathbb{F}_p)$.

Théorème 2.2.1 Soit $\#E(\mathbb{F}_p) = p + 1 - a$. Ecrivons $X^2 - aX + p = (X - \alpha)(X - \beta)$, alors

$$\#E(\mathbb{F}_{p^r}) = p^r + 1 - (\alpha^r + \beta^r)$$

pour tout $r \geq 1$.

Démonstration : Montrons d'abord que $\alpha^r + \beta^r$ est un entier.
Considérons la suite

$$s_n = \alpha^n + \beta^n$$

Nous avons $s_0 = 2$ et $s_1 = a$. Montrons que

$$s_{n+1} = as_n - ps_{n-1}$$

pour tout $n \geq 1$, ce qui justifiera que $\alpha^r + \beta^r$ est un entier.

En multipliant la relation $\alpha^2 - a\alpha + p = 0$ par α^{n-1}, nous obtenons

$$\alpha^{n+1} = a\alpha^n - p\alpha^{n-1}.$$

De même, en multipliant la relation $\beta^2 - a\beta + p = 0$ par β^{n-1}, nous obtenons

$$\beta^{n+1} = a\beta^n - p\beta^{n-1}.$$

En additionnant les deux égalités précédentes, nous avons l'égalité souhaitée :

$$s_{n+1} = as_n - ps_{n-1}.$$

Posons

$$f(X) = (X^r - \alpha^r)(X^r - \beta^r) = X^{2r} - (\alpha^r + \beta^r)X^r + p^r.$$

α et β sont des racines de f donc $(X - \alpha)(X - \beta) = X^2 - aX + p$ divise $f(X)$. Il existe donc un polynôme Q tel que

$$f(X) = Q(X)(X^2 - aX + p).$$

Remarquons que f et $X^2 - aX + p$ ont des coefficients entiers (se rappeler que $\alpha^n + \beta^n$ est un entier) et que le coefficient dominant de $X^2 - aX + p$ est 1, on peut donc affirmer que Q a également des coefficients entiers.

D'après le théorème 1.6.5, $\phi_p^2 - a\phi_p + p = 0$ donc

$$f(\phi_p) = (\phi_p^r)^2 - (\alpha^r + \beta^r)\phi_p^r + p^r = Q(\phi_p)(\phi_p^2 - a\phi_p + p) = 0$$

comme endomorphisme de E. Remarquons que $\phi_p^r = \phi_{p^r}$, ainsi

$$\phi_{p^r}^2 - (\alpha^r + \beta^r)\phi_{p^r} + p^r = 0$$

et par le théorème 1.6.5, nous obtenons

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

□

Un exemple sera donné dans le paragraphe suivant.

2.3 Exemple

Considérons la courbe elliptique $E : y^2 = x^3 + 2x + 1$ définie sur $E(\mathbb{F}_{19^9})$.

Première partie : Calcul de $\#E(\mathbb{F}_{19})$

Nous avons donc :

$$\#E(F_{19}) = 19 + 1 - a$$

et nous cherchons à déterminer a. Comme $p = 19$, nous avons $S = \{2, 3, 5\}$.

Nous allons montrer que

$$a \equiv \begin{cases} 1 \ (mod\ 2) \\ 2 \ (mod\ 3) \\ 3 \ (mod\ 5) \end{cases}$$

d'où on en déduit que

$$a \equiv \ 23 \ (mod\ 30)$$

et comme $|a| < 2\sqrt{19} < 9$, on aura finalement $a = -7$.

Calcul de $a \ mod \ 2$

Nous réduisons d'abord x^{19} modulo $x^3 + 2x + 1$:

$$x^{19} \equiv x^2 + 13x + 14 \quad (mod\ x^3 + 2x + 1).$$

Ensuite, calculons le $PGCD$ suivant :

$$PGCD(x^{19} - x, x^3 + 2x + 1) = PGCD(x^2 + 12x + 14, x^3 + 2x + 1) = 1.$$

Ainsi, $x^3 + 2x + 1$ n'a pas de racine dans $\mathbb{F}_{19}$ et donc

$$a \equiv\ 1\ (mod\ 2).$$

Calcul de $a \ mod \ 3$

Nous avons $p = 19 \equiv 1\ (mod\ 3)$ donc $p_\ell = 1$. Nous voulons savoir si

$$(x^{361}, y^{361}) + (x, y) = \pm(x^{19}, y^{19}).$$

Il nous faut encore connaître $p^2 = 361$. Le troisième polynôme de division est :

$$\psi_3 = 3x^4 + 12x^2 + 12x - 4.$$

Ensuite calculons la première coordonnée de $(x^{361}, y^{361}) + (x, y)$:

$$\left(\frac{y^{361} - y}{x^{361} - x}\right)^2 - x^{361} - x = (x^3 + 2x + 1)\left(\frac{(x^3 + 2x + 1)^{180} - 1}{x^{361} - x}\right)^2 - x^{361} - x$$

où nous avons utilisé la relation $y^2 = x^3 + 2x + 1$. Nous avons besoin de réduire cette relation modulo ψ_3. Une idée serait d'utiliser l'algorithme d'Euclide généralisé pour trouver l'inverse de $x^{361} - x\ (mod\ \psi_3)$. Cependant,

$$PGCD(x^{361} - x, \psi_3) = x - 8 \neq 1$$

donc cet inverse n'existe pas. Nous pourrions simplifier la fraction

$$\frac{(x^3 + 2x + 1)^{180} - 1}{x^{361} - x}$$

par $x - 8$ mais cela n'est pas nécessaire. En effet, comme $x = 8$ est une racine de ψ_3, le point $(8, 4) \in E(\mathbb{F}_{19})$ est d'ordre 3 et donc

$$\#E(\mathbb{F}_{19}) = 19 + 1 - a \equiv 0\ (mod\ 3)$$

d'où

$$a \equiv\ 2\ (mod\ 3).$$

Calcul de $a \ mod \ 5$

Nous avons $p = 19 \equiv -1 \ (mod\ 5)$ donc $p_\ell = -1$. De plus,

$$19(x,y) = -(x,y) = (x,-y) \text{ pour tout } (x,y) \in E[5].$$

Nous voulons savoir si

$$(x',y') \stackrel{def}{=} (x^{361},y^{361}) + (x,-y) \stackrel{?}{=} \pm 2(x^{19},y^{19}) \stackrel{def}{=} \pm(x'',y'')$$

pour tout $(x,y) \in E[5]$. Le cinquième polynôme de division est :

$$\psi_5 = 5x^{12} + 10x^{10} + 17x^8 + 5x^7 + x^6 + 9x^5 + 12x^4 + 2x^3 + 5x^2 + 8x + 8.$$

Le calcul des premières coordonnées x' et x'' donne

$$x' = \left(\frac{y^{361}+y}{x^{361}-x}\right)^2 - x^{361} - x \stackrel{?}{\equiv} \left(\frac{3x^{38}+2}{2y^{19}}\right)^2 - 2x^{19} = x'' \pmod{\psi_5}.$$

En remplaçant y^2 par $x^3 + 2x + 1$, nous obtenons une relation polynomiale en x et après calculs, on s'aperçoit que la relation ci-dessus est vérifiée. Ainsi,

$$a \equiv \pm 2 \pmod 5.$$

Pour déterminer le signe, nous allons regarder les secondes coordonnées. La seconde coordonnée de $(x',y') = (x^{361},y^{361}) + (x,-y)$ est (après calculs) :

$$y(9x^{11} + 13x^{10} + 15x^9 + 15x^7 + 18x^6 + 17x^5 + 8x^4 + 12x^3 + 8x + 6) \pmod{\psi_5}.$$

La seconde coordonnée de $(x_2,y_2) = 2(x,y)$ est

$$y(13x^{10} + 15x^9 + 16x^8 + 13x^7 + 8x^6 + 6x^5 + 17x^4 + 18x^3 + 8x + 18) \pmod{\psi_5}.$$

Après calculs,

$$(y' + y_2^{19})/y \equiv 0 \pmod{\psi_5}.$$

Cela signifie que

$$(x',y') \equiv (x_2^{19}, -y_2^{19}) = -2(x^p,y^p) \pmod{\psi_5}$$

et donc

$$a \equiv -2 \ (mod\ 5)$$

ce qui termine le cas $\ell = 5$.

Comme nous l'avons vu précédemment, $a = -7$ d'où :

$$\#E(F_{19}) = 19 + 1 - a = 27.$$

Seconde partie : Calcul de $\#E(\mathbb{F}_{19^9})$

Nous savons que $a = -7$, nous avons ainsi le polynôme :

$$X^2 - aX + p = X^2 + 7X + 19 = \left(X - \frac{-7-i\sqrt{7}}{2}\right)\left(X - \frac{-7+i\sqrt{7}}{2}\right).$$

Le cardinal recherché vaut donc :

$$\begin{aligned} \#E(\mathbb{F}_{19^9}) &= 19^9 + 1 - \left(\frac{-7-i\sqrt{7}}{2}\right)^9 - \left(\frac{-7+i\sqrt{7}}{2}\right)^9 \\ &= 387134771. \end{aligned}$$

Il est donc assez rapide de calculer le cardinal d'un groupe $E(\mathbb{F}_q)$ par cet algorithme.

Chapitre 3

Le problème du logarithme discret

Dans ce chapitre, nous allons traiter du problème du logarithme discret sur une courbe elliptique. En voici une définition : étant donné une courbe elliptique E définie sur un corps fini $\mathbb{F}_q$ et deux points $P, Q \in E(\mathbb{F}_q)$ tel qu'il existe un entier k vérifiant $Q = kP$, le problème du logarithme discret consiste à déterminer k en connaissant uniquement les points P et Q.

Les algorithmes de cryptage utilisant les courbes elliptiques se basent sur la difficulté de résoudre le problème du logarithme discret en un temps raisonnable (voir chapitre 4). Ainsi, il est important de savoir s'il existe des courbes elliptiques particulières où le problème du logarithme discret se résout facilement afin d'éviter ces cas là.

Dans la première partie, j'exposerai l'algorithme *Baby-Step Giant-Step* qui permet de résoudre le problème du logarithme discret sur une courbe elliptique quelconque. La seconde et la troisième partie présenteront des algorithmes spécifiques pour certaines catégories de courbes elliptiques : les courbes elliptiques supersingulières (partie 2) et les courbes elliptiques à anomalies (partie 3).

3.1 La méthode Baby-Step Giant-Step

Cette méthode, développée par D. Shanks, permet de résoudre le problème du logarithme discret dans un groupe fini quelconque. Nous allons exposer la méthode pour un groupe de la forme $E(\mathbb{F}_q)$ où E est une courbe elliptique définie sur un corps fini $\mathbb{F}_q$. Notons N l'ordre du groupe $E(\mathbb{F}_q)$. Nous supposerons qu'il existe un entier k tel que $Q = kP$ où $P, Q \in E(\mathbb{F}_q)$. L'algorithme se déroule ainsi :

1. Choisir un entier $m > \sqrt{N}$.

2. Calculer et stocker la liste des iP pour $0 \leq i \leq m-1$.

3. Calculer les points $Q - jmP$ où $j = 0, 1, 2, ..., m-1$ jusqu'à ce qu'un de ces éléments corresponde à un iP de la liste précédente.

4. Si $iP = Q - jmP$, nous avons $Q = kP$ avec $k \equiv i + jm \ (mod\ N)$.

Pourquoi cet algorithme fonctionne t-il ? Comme $m^2 > N$, nous savons que $0 \leq k < m^2$. La division

euclidienne de k par m donne $k = k_1 m + k_0$ où

$$\begin{cases} 0 \leq k_0 \leq m-1 \\ 0 \leq k_1 \leq m-1. \end{cases}$$

Posons $i = k_0$ et $j = k_1$, nous obtenons donc

$$Q - k_1 mP = kP - k_1 mP = k_0 P$$

ce qui est la relation souhaitée.

Remarque 1 : Nous n'avons pas besoin de connaître l'ordre exact de $E(\mathbb{F}_q)$ et de mettre en oeuvre l'algorithme décrit dans le chapitre 2. Nous devons juste connaître une borne supérieure de N. Une telle borne nous est donnée par le théorème de Hasse (théorème 1.6.4) :

$$q + 1 + 2\sqrt{q} > N.$$

Remarque 2 : Cette méthode nécessite environ $\sqrt{N}$ étapes donc elle n'est plus utilisable en pratique une fois que N devient très grand.

Exemple : Considérons la courbe elliptique $E : y^2 = x^3 + 2x + 1$ définie sur $\mathbb{F}_{41}$. Soient $P = (0, 1)$ et $Q = (30, 40)$. Par le théorème de Hasse, nous avons :

$$55 > 41 + 1 + 2\sqrt{41} > N.$$

Ensuite, nous devons choisir un naturel m tel que $m^2 > 55$, posons donc $m = 8$. Les points iP pour $1 \leq i \leq 7$ sont :

$$(0, 1), (1, 39), (8, 23), (38, 38), (23, 23), (20, 28), (26, 9).$$

Nous calculons maintenant $Q - jmP$ pour $j \geq 0$:

$$(30, 40), (9, 25), (26, 9).$$

Nous nous arrêtons au rang $j = 2$ car le point $Q - 2mP$ correspond au point $7P$. Nous obtenons donc :

$$Q = (7 + 2 \cdot 8)P = 23P.$$

3.2 L'algorithme MOV

L'algorithme MOV, développé par Menezes, Okamoto et Vanstone, utilise le couplage de Weil pour transformer le problème du logarithme discret dans $E(\mathbb{F}_q)$ en un problème du logarithme discret dans $\mathbb{F}_{q^m}^{\times}$. Le problème du logarithme discret dans $\mathbb{F}_{q^m}^{\times}$ peut alors être résolu par des méthodes classiques (voir par exemple la méthode du calcul d'index décrite dans [5] pp. 134-136). Ces méthodes de résolution sur $\mathbb{F}_{q^m}^{\times}$ sont généralement plus rapides que les algorithmes sur $E(\mathbb{F}_q)$ tant que l'entier m reste assez petit.

Faisons maintenant quelques rappels du chapitre 1. Pour une courbe elliptique E définie sur $\mathbb{F}_q$, $E[N]$ désigne l'ensemble des points d'ordre divisant N dont les coordonnées sont dans la clotûre algébrique de $\mathbb{F}_q$. Si $PGCD(q, N) = 1$ et si $S, T \in E[N]$, alors le couplage de Weil $e_N(S, T)$ est une racine $N^{ième}$ de l'unité. Le couplage de Weil est bilinéaire, et si $\{S, T\}$ est une base de $E[N]$, alors $e_N(S, T)$ est une racine primitive $N^{ième}$ de l'unité. De plus, pour tout S, $e_N(S, S) = 1$.

Soit E une courbe elliptique définie sur $\mathbb{F}_q$. Soient $P, Q \in E(\mathbb{F}_q)$ et N l'ordre de P. Supposons que

$$PGCD(N, q) = 1.$$

Nous souhaitons trouver k tel que $Q = kP$. Le lemme suivant nous permet de savoir si un tel k existe.

Lemme 3.2.1 Il existe k tel que $Q = kP$ si et seulement si $NQ = \mathcal{O}$ et le couplage de Weil donne $e_N(P, Q) = 1$.

Démonstration : Si $Q = kP$, alors $NQ = kNP = \mathcal{O}$. Ainsi,

$$e_N(P, Q) = e_N(P, P)^k = 1^k = 1.$$

Réciproquement, si $NQ = \mathcal{O}$, alors $Q \in E[N]$. Comme $PGCD(N, q) = 1$, nous avons

$$E[N] \simeq \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z},$$

d'après le théorème 1.4.2. Choisissons un point R tel que $\{P, R\}$ soit une base de $E[N]$. Alors il existe des entiers a et b tels que

$$Q = aP + bR.$$

D'après le corollaire 1.5.3, $e_N(P, R) = \zeta$ est une racine $N^{ième}$ primitive de l'unité. Ainsi, si $e_N(P, Q) = 1$, alors

$$1 = e_N(P, Q) = e_N(P, P)^a e_N(P, R)^b = \zeta^b.$$

Ceci implique que $b \equiv 0 \ (mod\ N)$ donc $bR = \mathcal{O}$. Ainsi, $Q = aP$ ce qui est le résultat recherché.

□

Puisque tous les points de $E[N]$ ont leurs coordonnées dans $\overline{\mathbb{F}}_q = \cup_{j \geq 1} \mathbb{F}_{q^j}$, il existe un entier m tel que

$$E[N] \subseteq E(\mathbb{F}_{q^m}).$$

D'après le corollaire 1.5.4, le groupe μ_N des racines $N^{ième}$ de l'unité est contenu dans $\mathbb{F}_{q^m}$. Tous nos calculs se feront donc dans $\mathbb{F}_{q^m}$.

L'algorithme se déroule ainsi :

1. Choisir aléatoirement un point $T \in E(\mathbb{F}_{q^m})$.

2. Calculer M, l'ordre de T.

3. Soit $d = PGCD(M, N)$. Posons $T_1 = (M/d)T$, l'ordre de T_1 est alors d. Comme d divise N, $T_1 \in E[N]$.

4. Calculer $\zeta_1 = e_N(P, T_1)$ et $\zeta_2 = e_N(Q, T_1)$. ζ_1 et ζ_2 sont alors dans $\mu_d \subseteq \mu_N \subseteq \mathbb{F}_{q^m}^{\times}$ car

   $$\zeta_1^d = e_N(P, T_1)^d = e_N(P, dT_1) = e_N(P, \mathcal{O}) = 1.$$

   Idem pour ζ_2.

5. Résoudre le problème du logarithme discret $\zeta_2 = \zeta_1^k$ dans $\mathbb{F}_{q^m}^\times$. Nous obtenons alors $k \ (mod\ d)$.

6. Recommencer avec des points aléatoires T jusqu'à ce que le $PPCM$ des d obtenus soit égal à N. Ceci détermine $k \ (mod\ N)$.

Remarque : A priori, on pourrait penser que le cas $d = 1$ apparaisse fréquemment. Cependant, ce n'est pas le cas à cause de la structure de $E(\mathbb{F}_q)$. Rappelons nous (théorème 1.6.1) que

$$E(\mathbb{F}_{q^m}) \simeq \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z}$$

pour des entiers n_1, n_2 où n_1 divise n_2. Alors N divise n_2 car n_2 est le plus grand ordre possible d'un élément du groupe. Soient B_1 et B_2 des points d'ordre respectif n_1 et n_2 tels qu'ils engendrent $E(\mathbb{F}_{q^m})$. Nous pouvons donc écrire

$$T = a_1 B_1 + a_2 B_2.$$

Soient ℓ un nombre premier et e un entier naturel tels que ℓ^e divise N. Soit f un entier naturel $f \geq e$ tel que ℓ^f divise n_2. Si ℓ ne divise pas a_2, alors ℓ^f divise l'ordre de T que l'on notera M. De ce fait, ℓ^e divise $PGCD(M, N)$. La probabilité que ℓ ne divise pas a_2 est de $1 - 1/\ell$, donc la probabilité que $PGCD(M, N) \neq 1$ est au moins de $1 - 1/\ell$. Ainsi, après quelques choix de T, nous devrions trouver le cas $PGCD(M, N) \neq 1$ et après quelques itérations de l'algorithme, nous devrions trouver k.

Il se peut que l'entier m soit grand, auquel cas le problème du logarithme discret dans le groupe $\mathbb{F}_{q^m}^\times$, qui est d'ordre $q^m - 1$, sera aussi difficile à résoudre que le problème du logarithme discret sur $E(\mathbb{F})$ qui est environ d'ordre q. Cependant, dans le cas des courbes elliptiques supersingulières, nous pouvons prendre $m = 2$ comme le montre la proposition 3.2.4.

Nous avons défini les courbes elliptiques supersingulières dans le premier chapitre (Corollaire-Définition 1.4.3). En voici maintenant deux caractérisations :

Propriété 3.2.2 Soit E une courbe elliptique définie sur $\mathbb{F}_q$ où q est une puissance du nombre premier p. Posons $a = q + 1 - \#E(\mathbb{F}_q)$. Alors E est supersingulière si et seulement si

$$\#E(\mathbb{F}_q) \equiv 1 \ (mod\ p),$$

c'est-à-dire si et seulement si $a \equiv 0 \ (mod\ p)$.

Démonstration : Ecrivons $X^2 - aX + q = (X - \alpha)(X - \beta)$. Le théorème 2.2.1 implique que

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

Dans la démonstration du théorème 2.2.1, nous avons montré que la suite $s_n = \alpha^n + \beta^n$ satisfait la relation de récurrence

$$s_0 = 2, \quad s_1 = a, \quad s_{n+1} = as_n - qs_{n-1}.$$

Supposons que $a \equiv 0 \ (mod\ p)$. Alors $s_1 = a \equiv 0 \ (mod\ p)$ et par récurrence, $s_{n+1} \equiv 0 \ (mod\ p)$ pour tout $n \geq 1$. Ainsi,

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - s_n \equiv 1 \pmod{p},$$

donc il n'y a pas de points d'ordre p dans $E(\mathbb{F}_{q^n})$ pour tout $n \geq 1$. Comme $\overline{\mathbb{F}}_q = \cup_{n \geq 1} \mathbb{F}_{q^n}$, il n'y a pas de points d'ordre p dans $E(\overline{\mathbb{F}}_q)$ donc E est supersingulière.

Supposons maintenant que $a \not\equiv 0 \ (mod\ p)$. La récurrence implique que $s_{n+1} \equiv as_n \ (mod\ p)$ pour tout $n \geq 1$. Comme $s_1 = a$, nous avons $s_n \equiv a^n \ (mod\ p)$ pour tout $n \geq 1$. Ainsi,

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - s_n \equiv 1 - a^n \pmod{p}.$$

D'après le petit théorème de Fermat, $a^{p-1} \equiv 1 \ (mod\ p)$. $E(\mathbb{F}_{q^{p-1}})$ est donc d'ordre divisible par p donc contient un point d'ordre p. Ceci signifie que E n'est pas supersingulière.

Pour la dernière partie de la propriété, notons que

$$\#E(\mathbb{F}_q) \equiv 1 - a \pmod{p},$$

donc $\#E(\mathbb{F}_q) \equiv 1 \ (mod\ p)$ si et seulement si $a \equiv 0 \ (mod\ p)$.

□

Corollaire 3.2.3 Soient $p \geq 5$ un nombre premier et E une courbe elliptique définie sur $\mathbb{F}_p$. Alors E est supersingulière si et seulement si

$$\#E(\mathbb{F}_p) = p + 1,$$

c'est-à-dire si et seulement si $a = 0$.

Démonstration : Si $a = 0$ alors E est supersingulière d'après la proposition 3.2.2. Inversement, supposons que E soit supersingulière mais que $a \neq 0$. Alors $a \equiv 0 \ (mod\ p)$ implique que $\mid a \mid \geq \ p$. D'après le théorème de Hasse, $\mid a \mid \leq \ 2\sqrt{p}$, donc $p \leq 2\sqrt{p}$. Ceci signifie que $p \leq 4$, d'où la contradiction.

□

Voici la proposition principale de cette partie :

Propriété 3.2.4 Soit E une courbe elliptique sur $\mathbb{F}_q$ et supposons que $a = 0$, *i.e.* E est supersingulière. Soit N un entier positif. S'il existe un point $P \in E(\mathbb{F}_q)$ d'ordre N, alors $E[N] \subseteq E(\mathbb{F}_{q^2})$.

Démonstration : L'endomorphisme ϕ_q satisfait la relation

$$\phi_q^2 - a\phi_q + q = 0$$

d'après le théorème 1.6.5. Par hypothèse $a = 0$ donc

$$\phi_q^2 = -q$$

Soit $S \in E[N]$. Sachant que $\#E(\mathbb{F}_q) = q+1$ et qu'il existe un point d'ordre N, nous avons $N|(q+1)$ donc $-q \equiv 1 \ (mod\ N)$. Ainsi,

$$\phi_q^2(S) = -qS = 1 \cdot S.$$

Donc $S \in E(\mathbb{F}_{q^2})$ par la propriété 1.6.3.

□

En conclusion, l'algorithme MOV est très efficace lorsque $E(\mathbb{F}_q)$ est une courbe elliptique supersingulière puisque nous pouvons nous ramener à un problème du logarithme discret sur $\mathbb{F}_{q^2}^{\times}$.

3.3 Courbes à anomalies

Le problème du logarithme discret peut également être facilement résolu sur une autre classe de courbes elliptiques : les courbes à anomalies.

Définition 3.3.1 Une courbe elliptique E définie sur $\mathbb{F}_q$ est appellée *courbe à anomalies* si

$$\#E(\mathbb{F}_q) = q.$$

Remarque : Le fait d'être à anomalies dépend du corps sur lequel la courbe est définie. Si E est à anomalies sur $\mathbb{F}_q$, elle ne l'est pas forcément sur $\mathbb{F}_{q^r}$ où $r \geq 2$. Ceci contraste avec le fait d'être supersingulière qui est une propriété de la courbe elliptique définie sur une clôture algébrique.

Exemple : Rappelons (théorème 2.2.1) que pour une courbe elliptique E définie sur $\mathbb{F}_{p^r}$, nous avons :

$$\#E(\mathbb{F}_{p^r}) = p^r + 1 - (\alpha^r + \beta^r)$$

où α et β sont les racines du polynôme :

$$X^2 - aX + p$$

avec

$$a = p + 1 - \#E(\mathbb{F}_p).$$

Soit E une courbe elliptique à anomalies définie sur $\mathbb{F}_2$ donc par définition $\#E(\mathbb{F}_2) = 2$. Nous avons donc :

$$a = p + 1 - \#E(\mathbb{F}_p) = 2 + 1 - 2 = 1.$$

Il s'en suit :

$$X^2 - aX + p = X^2 - X + 2 = \left(X - \frac{1 - i\sqrt{7}}{2}\right)\left(X - \frac{1 + i\sqrt{7}}{2}\right).$$

Ainsi $\alpha = \frac{1-i\sqrt{7}}{2}$, $\beta = \frac{1+i\sqrt{7}}{2}$ et donc :

$$\begin{aligned} \#E(\mathbb{F}_{2^4}) &= 2^4 + 1 - \left(\left(\frac{1 - i\sqrt{7}}{2}\right)^4 + \left(\frac{1 + i\sqrt{7}}{2}\right)^4\right) \\ &= 16 = 2^4 \end{aligned}$$

mais

$$\begin{aligned} \#E(\mathbb{F}_{2^2}) &= 2^2 + 1 - \left(\left(\frac{1 - i\sqrt{7}}{2}\right)^2 + \left(\frac{1 + i\sqrt{7}}{2}\right)^2\right) \\ &= 8 \neq 2^2. \end{aligned}$$

E est donc à anomalies sur $\mathbb{F}_{2^4}$ mais pas sur $\mathbb{F}_{2^2}$.

Nous allons maintenant voir comment résoudre le problème du logarithme discret dans le cas d'une courbe à anomalies. Nous ne traiterons ici que le cas où q est premier, nous noterons donc $q = p$.

Nous allons d'abord relever la courbe elliptique E définie sur $\mathbb{F}_p$ en une courbe elliptique $\tilde{E}$ définie sur $\mathbb{Z}$ à l'aide de la propriété suivante :

Propriété 3.3.2 Soient E une courbe elliptique définie sur $\mathbb{F}_p$ et $P, Q \in E(\mathbb{F}_p)$. Supposons que E soit de la forme : $y^2 = x^3 + Ax + B$. Alors il existe des entiers $\tilde{A}, \tilde{B}, x_1, x_2, y_1, y_2$ et une courbe elliptique donnée par

$$y^2 = x^3 + \tilde{A}x + \tilde{B}$$

telle que $\tilde{P} = (x_1, y_1)$, $\tilde{Q} = (x_2, y_2) \in \tilde{E}(\mathbb{Z})$ et telle que

$$A \equiv \tilde{A},\ B \equiv \tilde{B},\ P \equiv \tilde{P},\ Q \equiv \tilde{Q} \quad (mod\ p).$$

Démonstration : Choisissons des entiers x_1 et x_2 tels que $x_1\ mod\ p$ (resp. $x_2\ mod\ p$) corresponde à la première coordonnée de P (resp. de Q).

Cas 1 : Supposons que $x_1 \not\equiv x_2\ (mod\ p)$.

Choisissons un entier y_1 tel que $\tilde{P} = (x_1, y_1)$ soit une réduction de P modulo p. Maintenant choisissons un entier y_2 tel que

$$y_2^2 \equiv y_1^2\ (mod\ x_2 - x_1) \quad \text{et} \quad (x_2, y_2) \equiv Q\ (mod\ p).$$

Choisir un tel y_2 est possible d'après le théorème des restes chinois car p et $x_2 - x_1$ sont premiers entre eux par hypothèse.

Considérons les équations :

$$\begin{aligned} y_1^2 &= x_1^3 + \tilde{A}x_1 + \tilde{B} \\ y_2^2 &= x_2^3 + \tilde{A}x_2 + \tilde{B} \end{aligned}$$

où nous pouvons en déduire les valeurs de $\tilde{A}$ et de $\tilde{B}$:

$$\tilde{A} = \frac{y_2^2 - y_1^2}{x_2 - x_1} - \frac{x_2^3 - x_1^3}{y_2 - y_1}, \quad \tilde{B} = y_1^2 - x_1^3 - \tilde{A}x_1.$$

Comme $y_2^2 - y_1^2$ est divisible par $x_2 - x_1$ et que x_1, x_2, y_1, y_2 sont entiers, il s'en suit que $\tilde{A}$ et $\tilde{B}$ sont des entiers. Les points P, Q sont sur la courbe $\tilde{E}$ que nous avons obtenue.

Cas 2 : Supposons que $x_1 \equiv x_2\ (mod\ p)$.

Dans ce cas nous avons $P = \pm Q$ et nous choisissons $x_2 = x_1$. Ensuite choisissons un entier y_1 tel que $\tilde{P} = (x_1, y_1)$ soit une réduction de P modulo p. De plus, choisissons un entier $\tilde{A} \equiv A\ (mod\ p)$ et posons $\tilde{B} = y_1^2 - x_1^3 - \tilde{A}x_1$. Alors $\tilde{P} = (x_1, y_1)$ se trouve sur $\tilde{E}$. Posons $\tilde{Q} = \pm\tilde{P}$. Ainsi $\tilde{Q}$ est une réduction de $\pm P = Q\ (mod\ p)$. Finalement

$$4\tilde{A}^3 + 27\tilde{B}^2 \equiv 4A^3 + 27B^2 \not\equiv 0\ (mod\ p)$$

car E est une courbe elliptique. Ainsi $4\tilde{A}^3 + 27\tilde{B}^2 \neq 0$ et donc $\tilde{E}$ est une courbe elliptique.

□

Remarque : Si nous avons la relation $Q = kP$ pour un certain entier k, nous n'avons pas, en général, $\tilde{Q} = k\tilde{P}$. Mais dans le cas des courbes à anomalies, nous pouvons obtenir assez d'informations pour déterminer k.

Définition 3.3.3 Soient $a/b \neq 0$ un nombre rationnel, où a,b sont des entiers premiers entre eux et p un nombre premier. Ecrivons $a/b = p^r(a_1/a_2)$ où p ne divise ni a_1 ni a_2. On définit la *valuation p-adique* comme suit :

$$v_p(a/b) = r.$$

Par convention, $v_p(0) = +\infty$.

Exemple :

$$v_2(7/40) = -3,\ v_3(9/2) = 2,\ v_{13}(8/5) = 0.$$

Soient $\tilde{E}$ une courbe elliptique sur $\mathbb{Z}$ donnée par $y^2 = x^3 + \tilde{A}x + \tilde{B}$ et $r \geq 1$ un entier. On pose :

$$\tilde{E}_r = \{(x,y) \in \tilde{E}(\mathbb{Q}) \mid v_p(x) \leq -2r,\ v_p(y) \leq -3r\} \cup \{\mathcal{O}\}.$$

C'est l'ensemble des points tels que x a au moins le facteur p^{2r} au dénominateur et y au moins le facteur p^{3r} au dénominateur.

Théorème 3.3.4 Soit $\tilde{E} : y^2 = x^3 + \tilde{A}x + \tilde{B}$, où $\tilde{A}, \tilde{B} \in \mathbb{Z}$. Soient encore p un nombre premier et r un entier positif. Alors :

1. $\tilde{E}_r$ est un sous-groupe de $\tilde{E}(\mathbb{Q})$.

2. Si $(x,y) \in \tilde{E}(\mathbb{Q})$, alors $v_p(x) < 0$ si et seulement si $v_p(y) < 0$. Dans ce cas, il existe un entier $r \geq 1$ tel que $v_p(x) = -2r$, $v_p(y) = -3r$.

3. L'application

$$\begin{array}{rcl} \lambda_r : \tilde{E}_r/\tilde{E}_{5r} & \longrightarrow & \mathbb{Z}/p^{4r}\mathbb{Z} \\ (x,y) & \longmapsto & p^{-r}x/y \pmod{p^{4r}} \\ \mathcal{O} & \longmapsto & 0 \end{array}$$

   est un homomorphisme injectif.

4. Si $(x,y) \in \tilde{E}_r$ et $(x,y) \notin \tilde{E}_{r+1}$, alors $\lambda_r(x,y) \not\equiv 0 \pmod{p}$.

Démonstration : Voir [5] pp 189-197. □

Il nous faut encore énoncer une proposition :

Propriété 3.3.5 Soit p un nombre premier. On défini l'*application de réduction modulo p* ainsi :

$$\begin{array}{rcl} red_p : \tilde{E}(\mathbb{Q}) & \longrightarrow & \tilde{E} \pmod{p} \\ (x,y) & \longmapsto & (x,y) \pmod{p} \quad si\ (x,y) \notin \tilde{E}_1 \\ \tilde{E}_1 & \longmapsto & \mathcal{O}. \end{array}$$

L'application red_p est alors un homomorphisme dont le noyau est $\tilde{E}_1$.

Démonstration : Voir [5] p 66. □

Nous allons maintenant exposer l'algorithme pour résoudre le problème du logarithme discret. Donnons-nous une courbe elliptique à anomalies E définie sur un corps fini $\mathbb{F}_p$ et deux points P et Q de $E(\mathbb{F}_p)$. Nous cherchons un entier k tel que $Q = kP$ (supposons que $k \neq 0$). Puisque E est à anomalies, $\#E(\mathbb{F}_p) = p$. L'algorithme se déroule ainsi :

1. Relever E, P et Q dans $\mathbb{Z}$ pour obtenir $\tilde{E}, \tilde{P}$ et $\tilde{Q}$ comme décrit dans la démonstration de la propriété 3.3.2.

2. Soient $\tilde{P}_1 = p\tilde{P}$ et $\tilde{Q}_1 = p\tilde{Q}$. On remarque que $\tilde{P}_1, \tilde{Q}_1 \in \tilde{E}_1$ car

$$red_p(\tilde{P}_1) = red_p(p\tilde{P}) = p \cdot red_p(\tilde{P}) = \mathcal{O}$$

   (se rappeler que $\#E(\mathbb{F}_p) = p$).

3. Si $\tilde{P}_1 \in \tilde{E}_2$, choisir des nouveaux $\tilde{E}, \tilde{P}, \tilde{Q}$ et réessayer. Sinon, posons $\ell_1 = \lambda_1(\tilde{P}_1)$ et $\ell_2 = \lambda_1(\tilde{Q}_1)$. Nous avons alors :

$$k \equiv \ell_2 \ell_1^{-1} \ (mod\ p).$$

Pourquoi est-ce que ça marche ? Posons $\tilde{K} = k\tilde{P} - \tilde{Q}$. Nous avons :

$$\mathcal{O} = kP - Q = red_p(k\tilde{P} - \tilde{Q}) = red_p(\tilde{K}).$$

Ainsi $\tilde{K} \in \tilde{E}_1$, donc $\lambda_1(\tilde{K})$ est bien défini et

$$\lambda_1(p\tilde{K}) = p\lambda_1(\tilde{K}) \equiv 0 \quad (mod\ p).$$

Ainsi,

$$k\ell_1 - \ell_2 \equiv \lambda_1(k\tilde{P}_1 - \tilde{Q}_1) \equiv \lambda_1(kp\tilde{P} - p\tilde{Q}) \equiv \lambda_1(p\tilde{K}) \equiv 0 \quad (mod\ p).$$

d'où $k \equiv \ell_2 \ell_1^{-1} \ (mod\ p)$.

Notons que le fait que E soit à anomalies est crucial. En effet, si $E(\mathbb{F}_p)$ est d'ordre N, nous devons multiplier $\tilde{P}$ et $\tilde{Q}$ par N pour les amener dans $\tilde{E}_1$ où λ_1 est définie. La différence $\tilde{K} = k\tilde{P} - \tilde{Q}$ est alors multipliée par N. Si N est un multiple de p, nous avons $\lambda_1(N\tilde{K}) \equiv 0 \ (mod\ p)$ donc la contribution de $\tilde{K}$ disparaît de nos calculs.

Remarque : Si p est très grand nombre premier, nous pouvons rencontrer des difficultés lors de l'implémentation de l'algorithme décrit ci-dessus. Il faudra alors utiliser un autre algorithme (voir [5] pp 150-153).

Chapitre 4

Algorithmes de cryptage

Plaçons-nous dans la situation suivante : Alice souhaite envoyer un message secret à Bob sans que l'espionne nommée Eve puisse connaître le contenu du message. Il existe alors deux types de chiffrement : le chiffrement symétrique et asymétrique.

Le **chiffrement symétrique** consiste à ce qu'Alice et Bob partagent une même clé secrète pour crypter et décrypter les messages. En voici un exemple : *Le chiffre de César*. Ce chiffre est une des méthodes de chiffrement symétrique les plus célèbres. Cette méthode consiste à décaler toutes les lettres d'un message de 3 crans dans l'alphabet pour crypter le message. Pour le décrypter, on décale alors toutes les lettres de -3 crans dans l'alphabet. Ici, la clé secrète qu'Alice et Bob se partagent est le nombre de crans de décalage.

L'autre type de chiffrement est le **chiffrement asymétrique**. Dans ce cas, Alice et Bob n'ont plus besoin d'avoir un contact préalable pour échanger une clé commune : chacun dispose d'une clé privée et d'une clé publique. Ainsi, pour crypter un message, Alice peut utiliser sa clé privée et la clé publique de Bob, ce dernier pourra utiliser sa clé privée et la clé publique d'Alice pour décrypter le message. RSA (voir par exemple [1]) est l'algorithme de chiffrement asymétrique le plus connu.

Le chiffrement symétrique a un avantage de poids : il est généralement plus rapide, ce qui n'est pas négligeable lorsque de nombreuses données sont échangées. Ainsi une méthode souvent utilisée consiste à échanger une clé par un chiffrement asymétrique puis d'utiliser cette clé dans un chiffrement symétrique. Un algorithme d'échange de clés sera présenté dans la première partie. Dans la seconde partie, nous exposerons deux algorithmes de chiffrement asymétrique. Enfin dans la dernière partie, nous donnerons un algorithme de signature digitale, algorithme qui permettra d'identifier l'expéditeur d'un message.

4.1 Echange de clés

Imaginons qu'Alice et Bob soient des banques s'échangeant un flot important de données cryptées. Ces banques vont utiliser un chiffrement symétrique car ce type de chiffrement est le plus rapide. Cependant, elles doivent s'échanger une clé pour faire fonctionner leur chiffrement symétrique. Une méthode efficace consiste à s'échanger la clé grâce à un chiffrement asymétrique. Ici est exposé un algorithme d'échange de clés dû aux mathématiciens Diffie et Hellman.

L'algorithme se déroule ainsi :

1. Alice et Bob choisissent une courbe elliptique E sur un corps fini $\mathbb{F}_q$ sur laquelle le problème du logarithme discret est difficile à résoudre. Ils choisissent également un point $P \in E(\mathbb{F}_q)$ tel que l'ordre du sous-groupe engendré par P soit un grand nombre premier.

2. Alice choisit un entier secret a, calcule aP et envoie le résultat à Bob.

3. Bob choisit un entier secret b, calcule bP et envoie le résultat à Alice.

4. Alice calcule $a(bP)$.

5. Bob calcule $b(aP)$.

6. Alice et Bob se mettent d'accord sur le moyen d'extraire la clé de abP. Par exemple, ils peuvent prendre les 256 derniers bits de la première coordonnée de abP.

Si Eve a espionné les échanges d'Alice et de Bob, elle connaît E, $\mathbb{F}_q$ ainsi que les points P, aP et bP. Elle doit donc résoudre le problème suivant :

Problème de Diffie-Hellman : Etant donné P, aP et bP dans $E(\mathbb{F}_q)$, calculer abP.

Il est clair que si l'on sait résoudre le problème du logarithme discret sur $E(\mathbb{F}_q)$, alors on sait résoudre le problème de Diffie-Hellman sur $E(\mathbb{F}_q)$. En effet, en connaissant P et aP on peut déterminer a puis $abP = a(bP)$.

La réciproque (*i.e.* l'assertion selon laquelle le problème de Diffie-Hellman est équivalent au problème du logarithme discret) reste une conjecture.

4.2 Chiffrement asymétrique

Je vais exposer ici deux algorithmes de chiffrement asymétrique utilisant les courbes elliptiques : l'algorithme de Massey-Omura et l'algorithme de ElGamal.

4.2.1 L'algorithme de Massey-Omura

L'algorithme de Massey-Omura est un algorithme de chiffrement asymétrique. Voici son principe d'une manière imagée : Alice envoie un coffre contenant son message à Bob, coffre-fort qui est vérouillé par un cadenas. A sa réception, Bob place également un cadenas sur le coffre puis le renvoit à Alice. Ensuite, Alice retire son cadenas et envoie le coffre à Bob. Il ne reste plus à Bob qu'à retirer son propre cadenas pour pouvoir lire le message d'Alice.

Cette procédure peut être implémentée de la manière suivante.

1. Alice et Bob choisissent une courbe elliptique E sur un corps fini $\mathbb{F}_q$ tel que le problème du logarithme discret soit difficile à résoudre sur $E(\mathbb{F}_q)$.

2. Alice et Bob calculent $N = \#E(\mathbb{F}_q)$ par la méthode présentée dans le second chapitre.

3. Alice représente son message comme un point $M \in E(\mathbb{F}_q)$. (*Remarque :* nous verrons plus bas comment faire ceci concrètement.)

4. Alice choisit secrètement un entier m_A premier avec N, calcule $M_1 = m_A M$ et envoie le résultat à Bob.

5. Bob choisit secrètement un entier m_B premier avec N, calcule $M_2 = m_B M_1$ et envoie le résultat à Alice.

6. Alice calcule $m_A^{-1} \in \mathbb{Z}/N\mathbb{Z}$ puis $M_3 = m_A^{-1} M_2$ et envoie le résultat à Bob.

7. Bob calcule $m_B^{-1} \in \mathbb{Z}/N\mathbb{Z}$ puis $M_4 = m_B^{-1} M_3$. Alors M_4 est le message initial M.

Montrons pourquoi M_4 est le message initial M. Nous avons formellement

$$M_4 = m_B^{-1} m_A^{-1} m_B m_A M = M,$$

mais nous devons encore justifier pourquoi m_A^{-1} et m_A s'annulent. Nous avons $m_A^{-1} m_A \equiv 1 \ (mod\ N)$ donc $m_A^{-1} m_A = 1 + kN$ pour un certain entier k. Le groupe $E(\mathbb{F}_q)$ est d'ordre N donc d'après le théorème de Lagrange, $NR = \mathcal{O}$ pour tout $R \in E(\mathbb{F}_q)$. Ainsi,

$$m_A^{-1} m_A R = (1 + kN)R = R + k\mathcal{O} = R.$$

En appliquant ceci avec $R = m_B M$, on obtient

$$M_3 = m_A^{-1} m_B m_A = m_B M.$$

De même, m_B^{-1} et m_B s'annulent, donc

$$M_4 = m_B^{-1} M_3 = m_B^{-1} m_B M = M.$$

Si Eve a surveillé leurs échanges, elle connaît $E(\mathbb{F}_q)$ ainsi que les points $m_A M$, $m_B m_A M$ et $m_B M$. Posons $a = m_A^{-1}$, $b = m_B^{-1}$ et $P = m_A m_B M$. Alors nous remarquons qu'Alice connaît P, aP, bP et veut trouver abP. Ceci est le problème de Diffie-Hellman (voir partie 4.1).

Il nous reste à montrer comment représenter un message comme point d'une courbe elliptique. Nous allons utiliser une méthode présentée par Neil Koblitz dans [2]. Supposons que E soit une courbe elliptique donnée par $y^2 = x^3 + Ax + B$ sur $\mathbb{F}_q$ (où q est impair vu l'équation de la courbe elliptique). Soit m le message à envoyer exprimé sous la forme d'un entier $0 \leq m < q/100$. Posons $x_j = 100m + j$ où $0 \leq j < 100$. Ensuite calculons

$$s_j = x_j^3 + Ax_j + B$$

pour $j = 0, 1, 2, ..., 99$ jusque

$$s_j^{(q-1)/2} \equiv 1 \ (mod\ q).$$

Dans ce cas s_j est un carré modulo q, nous n'avons donc plus besoin d'essayer d'autres valeurs de j. Il faut maintenant trouver une racine carrée de s_j, nous allons pour cela distinguer deux cas.

Premier cas : $q \equiv 3 \ (mod\ 4)$.

Dans ce cas, une racine carrée de s_j est donnée par

$$y_j \equiv s_j^{(q+1)/4} \ (mod\ q).$$

En effet,

$$y_j^2 \equiv s_j \cdot s_j^{(q-1)/2} \equiv s_j \ (mod\ q).$$

Second cas : $q \equiv 1 \ (mod\ 4)$.

Ce cas est un peu plus long. Posons $q - 1 = 2^s t$ où t est un entier impair et $s \geq 2$. Soit u un élément de $\mathbb{F}_q^\times$ qui n'est pas un carré, un tel u peut être trouvé en choisissant des éléments aléatoires de $\mathbb{F}_q^\times$ et en s'arrêtant lorsque

$$u^{(q-1)/2} \equiv -1 \ (mod\ q).$$

Posons $v \equiv u^t \ (mod\ q)$. Alors

$$v^{2^s} \equiv u^{2^s t} \equiv u^{q-1} \equiv 1 \ (mod\ q).$$

Ainsi v est une racine 2^s-*ième* de l'unité dans $\mathbb{F}_q^\times$. Nous obtenons une solution "approximative" y'_j de l'équation $y_j^2 \equiv x_j \ (mod\ q)$ en posant $y'_j \equiv s_j^{(t+1)/2} \ (mod\ q)$. Nous avons alors

$$(y'_j)^2 \equiv s_j \cdot s_j^t \ (mod\ q).$$

Puisque s_j^t est une racine (2^{s-1})-*ième* de l'unité, il existe une puissance v^ℓ telle que

$$y_j \equiv y'_j \cdot v^{-\ell} \ (mod\ q)$$

soit une racine carrée de s_j. Cette dernière équation est équivalent à :

$$v^{2\ell} \equiv (y'_j)^2 / s_j \equiv s_j^t \ (mod\ q). \tag{4.1}$$

La valeur v^ℓ est le "terme correctif" dont nous avons besoin pour convertir y'_j en une racine carrée y_j de s_j. Il nous faut maintenant déterminer ℓ. Décomposons ℓ en base 2 :

$$\ell = \ell_0 + \ell_1 \cdot 2 + \ell_2 \cdot 2^2 + ... + \ell_{s-2} \cdot 2^{s-2}.$$

Recherchons les valeurs $\ell_0, \ell_1, ..., \ell_{s-2}$. En élevant les deux côtés de l'équation (4.1) à la puissance 2^{s-2}, nous voyons que $\ell_0 = 0$ si et seulement si nous obtenons 1 dans le membre de droite. Ensuite élevons les deux côtés de l'équation (4.1) à la puissance 2^{s-3} pour déterminer si ℓ_1 est égal à 0 ou à 1. En continuant ainsi, nous pourrons déterminer les valeurs $\ell_0, \ell_1, ..., \ell_{s-2}$, calculer ℓ, puis déterminer y_j.

Ceci termine ce second cas.

Nous obtenons ainsi un point $(x_j, y_j) \in E(\mathbb{F}_q)$. Pour retrouver m à partir de (x_j, y_j), il suffit simplement de calculer la partie entière

$$m = \lfloor x_j / 100 \rfloor.$$

Remarque : Comme s_j est un élément aléatoire de $\mathbb{F}_q^\times$ (qui est d'ordre pair), la probabilité que s_j soit un carré est environ $1/2$. Ainsi, la probabilité de ne pas trouver de carré après avoir testé les 100 valeurs de j est approximativement 2^{-100}.

4.2.2 L'algorithme d'ElGamal

L'algorithme de ElGamal est un algorithme de chiffrement asymétrique. Voici son principe d'une manière imagée : Bob envoye un cadenas ouvert à Alice. Alice place le message dans un coffre et le ferme à l'aide du cadenas de Bob. Ensuite, elle envoie ce coffre à Bob qui n'a plus qu'à ouvrir son propre cadenas pour pouvoir lire le message.

Concrètement, Bob choisit une courbe elliptique E sur un corps fini $\mathbb{F}_q$ tel que le problème du logarithme discret soit difficile à résoudre sur $E(\mathbb{F}_q)$. Il choisit également un point $P \in E(\mathbb{F}_q)$ tel que l'ordre de P soit un grand nombre premier. Ensuite, il choisit un entier secret s et calcule $B = sP$. Bob rend les informations suivantes publiques :

$$E, \quad \mathbb{F}_q, \quad P, \quad B.$$

Sa clé secrète est l'entier s.

Pour envoyer un message à Bob, Alice procède ainsi :

1. Télécharger la clé publique (P, B) de Bob.

2. Représenter le message comme un point $M \in E(\mathbb{F}_q)$ (voir partie 4.2.1).

3. Choisir un entier secret k et calculer $M_1 = kP$.

4. Calculer $M_2 = M + kB$.

5. Envoyer M_1 et M_2 à Bob.

Bob décrypte le message en calculant

$$M = M_2 - sM_1.$$

Le résultat est le bon car

$$M_2 - sM_1 = (M + kB) - s(kP) = M + k(sP) - skP = M.$$

Si Eve a espionné leurs échanges, elle connaît les informations publiques de Bob ainsi que M_1 et M_2. Si elle peut résoudre le problème du logarithme discret, elle peut utiliser P et B pour trouver s, qui pourra alors être utilisé pour calculer $M = M_2 - sM_1$. Par contre, si elle ne peut pas résoudre le problème du logarithme discret, alors il n'y a pas de méthode pour déterminer M.

Par ailleurs, il est important pour Alice d'utiliser à chaque fois un entier k différent. Supposons qu'Alice utilise le même k pour deux messages M et M'. Alors Eve le remarquera car dans ce cas, $M_1 = M_1'$. Supposons également que le message M soit rendu public peu de temps après son envoi, alors Eve pourra déterminer $M' = M - M_2 + M_2'$. Dans ce cas où Alice utilise le même k, la connaissance d'un message M permet donc à Eve de décrypter l'autre message M'.

4.3 Signature digitale

Il reste un problème à règler : l'authenticité du message. En effet, comment prouver à Bob que le message provient bien d'Alice ? Un imposteur pourrait très bien se faire passer pour Alice en créant lui-même une clé publique et une clé privée. L'idée est de joindre au message une signature électronique qui certifie au destinataire l'identité de l'expéditeur. Cette signature digitale est l'équivalent de la signature que l'on appose à la fin d'un document dans le monde physique.

Nous allons évoquer ici l'algorithme ECDSA (Elliptic Curves Digital Signature Algorithme).

Alice souhaite signer un document m (où m est un entier). Elle choisit alors une courbe elliptique E sur un corps fini $\mathbb{F}_q$ tel que

$$\#E(\mathbb{F}_q) = fr$$

où r est un grand nombre premier et f un petit entier (en général, f est égal à 1, 2 ou 4). Alice choisit ensuite un point $G \in E(\mathbb{F}_q)$ d'ordre r. Finalement, elle choisit un entier secret a et calcule $Q = aG$. Alice rend les informations suivantes publiques :

$$\mathbb{F}_q, \quad E, \quad r, \quad G, \quad Q.$$

(Il n'est pas besoin de garder f secret car il peut être déduit en calculant $\#E(\mathbb{F}_q)$ par la méthode indiquée dans le second chapitre). Pour signer le message, Alice procède ainsi :

1. Choisir un entier aléatoire k tel que $1 \leq k < r$ et calculer $R = kG = (x, y)$.

2. Calculer $s = k^{-1}(m + ax) \ (mod\ r)$.

Le document signé est alors :

$$(m, R, s).$$

Pour vérifier la signature, Bob suit ces étapes :

1. Calculer $u_1 = s^{-1}m \ (mod\ r)$ et $u_2 = s^{-1}x \ (mod\ r)$.

2. Calculer $V = u_1G + u_2Q$.

3. Déclarer la signature valide si $V = R$.

Si la signature est valide, nous avons bien :

$$V = u_1G + u_2Q = s^{-1}mG + s^{-1}xQ = s^{-1}(mG + xaG) = kG = R.$$

Remarquons qu'Alice doit choisir une courbe elliptique sur laquelle le problème du logarithme discret soit difficile à résoudre sur cette courbe.

Eve connaît G et P mais elle ne peut pas trouver a, ne peut pas calculer s et ne peut pas se faire passer pour Alice.

Conclusion

Nous avons étudié différents algorithmes reposant sur les courbes elliptiques : les protocoles d'échange de clés, les algorithmes asymétriques et les signatures digitales. L'usage des courbes elliptiques en cryptographie permet alors une grande souplesse dans le choix des groupes utilisés.

La résistance des algorithmes de cryptage repose sur le problème du logarithme discret. Pour assurer cette sécurité, il faut choisir une courbe elliptique sur un corps fini vérifiant certains critères : le cardinal du corps doit être suffisamment grand, la courbe elliptique ne doit être ni supersingulière ni à anomalies...

Le chiffrement par courbe elliptique présente des avantages par rapport aux autres méthodes de chiffrement : le niveau de sécurité est plus important et les clés employées sont plus courtes. Cependant, comme les développements théoriques sur les courbes elliptiques sont relativement récents, des trapes pour résoudre le problème du logarithme discret peuvent encore être découvertes. De plus, le grand nombre de brevets déposés peut rendre l'utilisation de ces algorithmes très couteuse.

Bibliographie

[1] N. Koblitz. *A Course in Number Theory and Cryptography,* Springer-Verlag, 1987.

[2] N. Koblitz. *Algebraic Aspects of Cryptography,* Springer, 1998.

[3] R. Schoof. *Elliptic Curves over Finite Fields and the Computation of Square Roots.* pp. 483-494, Mathematics of Computation, Vol. 44, avril 1985.

[4] S. Singh. *Histoire des Codes Secrets.* Lattès, 1999.

[5] L.C. Washington. *Elliptic Curves Number Theory and Cryptography.* Chapman & Hall/CRC, 2003.