Mémoire

Courbes elliptiques et cryptographie

Bebba Yann-Arby

Mémoire rendu à
l'Université Picardie Jules Verne
dirigé par Mme R.Abdelatif

dans le cadre de la première année de
Master Mathématiques

Département de Mathématiques
LAMFA
CNRS 33 Rue Saint-Leu, 80000 Amiens, France
April 8, 2022

Table des matières

Chapitre 1

Les courbes elliptiques : histoire et liens avec la cryptographie

le cryptosystème RSA, inventé par Ronald **R**ivet, Adi **S**hamir et Leonard **A**dleman en 1977

1.1 Introduction

Dans ce mémoire, nous allons nous intéresser aux courbes elliptiques et plus particulièrement au groupe abélien des courbes elliptiques. Ce qui va nous permettre d'utiliser ce groupe en cryptographie et présenter une façon plus efficace d'utiliser l'algorithme d'El-Gamal (EG.) (date) et le protocol de Diffie-Hellman (D-H.) (date).

Dans un monde en constant évolution, notamment technique. Il est crucial de pouvoir améliorer, réinventer, ou même changer, des principes qui ont révolutionner à leur époque. C'est pourquoi, en (date) Klobnitz, à présenter une façon concrète d'utiliser les courbes elliptiques dans le cadre de la cryptographie. Ceci a permit d'apporter une nouvelle façon de faire de la cryptographie, tout en conservant des concepts eprouvé basé sur le problème du logarithme discret. Cette nouvelle approche, que l'on nommera version elliptique, contrairement à la version dite classique de chiffrement, qui est basé sur le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$ et sa commutativité, celle ci présente une diversité et complexité non négligeable.

En effet, que ce soit l'algorithme d'El Gamal ou le protocol de Diffie-Hellman, leur version classique est basé sur le générateur du groupe $(\mathbb{Z}/p\mathbb{Z})^*$, alors que leur version elliptique est basé sur les courbes elliptiques qui comme on le verra sont en grand nombre pour leur part. De plus, par construction du groupe des courbes elliptiques, plus abstrait, la résolution du logarithme discret est quasiment impossible sans l'aide d'ordinateur quantique extremement puissant (ref article Mme Abdelatif).

1.2 plan ?

- explication cryptographie
  - sym et asym
  - rsa
  - El Gamal et D-H
- histoire des fonctions elliptiques

1.3 La cryptographie

L'application première de notre construction étant la cryptographie, il me semble nécessaire de poser les bases de cette branche des mathématiques. Ceci nous permettra d'avoir une idée clair des différents concepts et enjeux qui la compose.

Tout d'abord, définition ce qu'est la cryptographie. Métaphysiquement, c'est le fait de vouloir communiquer des messages, entre diverses entités et ceci de façon à ce que seul ces dernières n'aient connaissances du contenue du message.

Cette définition personnel et trivial est basé sur comment dans l'histoire la cryptographie est apparu.

De nos jours, le concept c'est énormément diversifié. La transmission de message reste un élément majeur de ce qu'est la cryptographie mais

Chapitre 2

Définitions générales

Dans tout ce qui suit, je vais prendre pour fil rouge les cours de Mr Alain Kraus [Kra10b] et [Kra10a]. Dans cette optique, je vais essayer de completer ces cours, en y ajoutant soit des détails supplémentaires lors des différentes démonstration, soit en explicitant des concepts où je juge cela nécéssaire.

2.1 Définition

Dans cette partie, je vais définir le contexte autour duquel la théorie est construite.

Dans la totalité de ce qui suit la lettre K désignera un corps de caractéristique 0 ou un corps fini de caractéristique distincte de 2 et 3.

On désignera la clôture algébrique de K par la notation $\overline{K}$.

Tout d'abord, pour définition d'une courbe elliptique nous utiliserons la suivante :

Définition 2.1. Une courbe elliptique définie sur K est une courbe projective plane d'équation

$$y^2z = x^3 + axz^3 + bz^2. \tag{2.1}$$

où a et b sont des éléments de K vérifiant la condition

$$4a^3 + 27b^2 \neq 0. \tag{2.2}$$

Remarque. Il existe une autre définition plus général, mais dans notre cas cette dernière n'est pas nécéssaire pour construire le groupe des courbes elliptique.

Avec cette définition il est important d'expliquer ce qu'une courbe projective plane signifie.

Pour cela, il est important d'expliquer la notion de plan projectif.

2.1.1 Le plan projectif $\mathbb{P}^2(\overline{K})$

Notons dans un premier temps que le plan projectif $\mathbb{P}^2(\overline{K})$ peut également se noter $\mathbb{P}^2$ pour simplifier la notation.

Pour expliciter cette notion commençons par expliquer ce qu'est une droite projective, en prenant l'exemple de la droite projective $\mathbb{P}(\mathbb{R})$.

Il suffit de ce munir de l'espace vectoriel $\mathbb{R}^2$ et l'idée est de prendre l'ensemble de tous les droites vectorielles de cette espace.

Toutes ces droites s'intersectent alors en un unique point avec la droite affine d'équation $y = 1$. Sauf bien entendu la droite d'équation $y = 0$ qui elle est parallèle à la droite affine.

Ce qui nous permet d'introduire la notion de point à l'infini, que nous formaliserons par la suite. Son rôle étant essentiel pour la construction du groupe des courbes elliptiques.

En effet, on peut considérer que ces deux droites parallèle se coupe en un point à l'infini.

On peut alors définir la droite projective comme étant formé de l'ensemble des points qui intersectent la droite affine et de ce point à l'infini.

Plus formellement, on a

Définition 2.2. La droite projective $\mathbb{P}(\mathbb{R})$ est l'ensemble quotient

$$\mathbb{R}^2 - \{(0,0)\} \,/\, \sim,$$

où la relation d'équivalence est définie par

$$\forall (x,y),(x',y') \in (\mathbb{R}^2)^*,\ (x,y) \sim (x',y') \Leftrightarrow \exists \lambda \in \mathbb{R},\ (x,y) = (\lambda x', \lambda y').$$

En s'appuyant sur cette construction on peut aller un peu plus loin et construire le plan projectif $\mathbb{P}^2$ en prenant l'exemple de $\mathbb{P}^2(\mathbb{R})$.

Cette fois ci, à partir de l'espace vectoriel $\mathbb{R}^3$.

On prendre l'ensemble de tous les droites vectorielles qui s'intersectent avec le plan affine $z = 1$.

Tous ces droites s'intersectent donc en un unique point avec ce plan affine.

De nouveau, il reste une partie des droites vectorielles qui sont parallèles à ce plan. Ce sont tous les droites dans le plan $(\mathcal{O}, \overrightarrow{x}, \overrightarrow{y})$, où $\mathcal{O}$ est l'origine.

On peut donc une nouvelle fois s'entendre sur le fait que ces deux plan s'intersectent en un point à l'infini.

Ainsi, on peut définir le plan projectif comme étant formé du plan affine et du point à l'inifini.

Algébriquement, on a pour définition

Définition 2.3. Le plan projectif $\mathbb{P}^2(\mathbb{R})$ est l'ensemble quotient

$$\mathbb{R}^3 - \{(0,0,0)\} / \sim,$$

où $\sim$ est une relation d'équivalence définie par

$$\forall x,\ y \in (\mathbb{R}^3)^*,\ x \sim y \Leftrightarrow \exists \lambda \in \mathbb{R},\ x = \lambda y.$$

Finalement, on peut énoncer la définition du plan projectif $\mathbb{P}^2(\overline{K})$.

Définition 2.4. Le plan projectif $\mathbb{P}^2(\overline{K})$ est l'ensemble quotitent

$$\overline{K}^3 - \{(0,0,0)\} / \sim,$$

où $\sim$ est la relation d'équivalence qui pour tous (x_1, y_1, z_1) et (x_2, y_2, z_2), non nuls de $\overline{K}^3$ on a

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

Pour tous $(x, y, z) \in \overline{K}^3$, non nul, on notera alors $[x, y, z]$ sa classe d'équivalence.

Comme l'on raisonne dans la clotûre algébrique de K, il est donc intéréssant de raisonner en termes de polynôme pour pouvoir ce servir de la définition 2.1.

C'est pourquoi, dans l'anneau des polynômes $K[X, Y, Z]$, posons

$$F = Y^2 Z - \left(X^3 + aXZ^2 + bZ^3\right).$$

C'est un polynôme homogène de degrè 3. Autrement dit, tous ses monômes non nuls sont de même degré total.

Si (x, y, z) est un élément non nul de $\overline{K}^3$, la condition $F(x, y, z) = 0$, ne dépend que de sa classe dans $\mathbb{P}^2(\overline{K})$.

Remarque. Dans la définition, on signifie par courbe projective plane d'équation (2.1), l'ensemble des zéros de F dans $\overline{K}$. Dit de façon plus terre à terre cela signifie qu'une courbe elliptique est l'intersection de la courbe dans l'espace avec le plan $z = 1$.

Un point $P = [x, y, z]$ de $\mathbb{P}^2(\overline{K})$ est un zéro de F dans $\overline{K}$, ou plus simplement un zéro de F, si l'on a $F(x, y, z) = 0$.

La condition (2.2) signifie que les racines dans $\overline{K}$ du polynôme

$$f = X^3 + aX + b$$

sont simples.

Ce que nous prouvons dans le lemme suivant :

Lemme 2.5. Soit $\Delta = -(4a^3 + 27b^2)$ le discriminant $f : x^3 + ax + b$. Les racines de f sont simples, si et seulement si $\Delta \neq 0$.

Démonstration. Montrons tout d'abord que le discriminant de f est $\Delta = -(4a^3 + 27b^2)$.

Soit Δ le discriminant de f. Soient α, β, γ les racines de f dans $\overline{K}$ et f' le polynôme dérivé de f.

Tout d'abord montrons que :

$$\begin{aligned}\Delta &= (-1)(\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2 \\ &= -f(\alpha)'f(\beta)'f(\gamma)'.\end{aligned}$$

D'après le théorème de d'Alembert on peut écrire f sous la forme :

$$f = (X-\alpha)(X-\beta)(X-\gamma).$$

En dérivant f sous cette forme on obtient :

$$\begin{aligned}f &= (X-\alpha)\left((X-\beta)(X-\gamma)\right)' + (X-\beta)(X-\gamma) \\ &= (X-\alpha)\left((X-\beta)+(X-\gamma)\right) + (X-\beta)(X-\gamma).\end{aligned}$$

Donc

$$f' = (X-\alpha)(X-\beta) + (X-\alpha)(X-\gamma) + (X-\beta)(X-\gamma).$$

On a alors successivement :

$$f(\alpha)' = (\alpha-\beta)(\alpha-\gamma),$$

$$f(\beta)' = (\beta-\alpha)(\beta-\gamma),$$

et

$$f(\gamma)' = (\gamma-\alpha)(\gamma-\beta).$$

En multipliant ces trois expressions, on obtient :

$$\begin{aligned}f(\alpha)'f(\beta)'f(\gamma)' &= (\alpha-\beta)(\alpha-\gamma)(\beta-\alpha)(\beta-\gamma)(\gamma-\alpha)(\gamma-\beta) \\ &= (X-\alpha)(\alpha-\gamma)(-1)(\alpha-\beta)(\beta-\gamma)(-1)(\alpha-\gamma)(-1)(\beta-\gamma) \\ &= (-1)^3(\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2 \\ &= -\Delta.\end{aligned}$$

Et donc

$$\Delta = -f'(\alpha)f'(\beta)f'(\gamma).$$

En partant de la forme $f : x^3 + ax + b$, on remarque que $f' : 3x^2 + a$. Par suite on obtient,

$$\begin{aligned}\Delta &= -f'(\alpha)f'(\beta)f'(\gamma) \\ &= -\left(3\alpha^2+a\right)\left(3\beta^2+a\right)\left(3\gamma^2+a\right).\end{aligned}$$

Ce qui donne :

$$\begin{aligned}\Delta &= -\left((9\alpha^2\beta^2 + 3a(\alpha^2+\beta^2) + a^2)(3\gamma^2 + a)\right) \\ &= -\left(27\left(\alpha\beta\gamma\right)^2 + 9a\left(\alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2\right) + 3a^2\left(\alpha^2+\beta^2+\gamma^2\right) + a^3\right).\end{aligned}$$

On peut écrire

$$\alpha^2 + \beta^2 + \gamma^2 = \left(\alpha+\beta+\gamma\right)^2 - 2\left(\alpha\beta + \alpha\gamma + \beta\gamma\right),$$

$$\alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2 = \left(\alpha\beta + \alpha\gamma + \beta\gamma\right)^2 - 2\alpha\beta\gamma\left(\alpha+\beta+\gamma\right).$$

Donc d'après les relations entre coefficients et racine (i.e relation de Viète), pour un polynôme de la forme $ax^3 + bx^2 + cx + d$, on a :

$$\alpha + \beta + \gamma = -\frac{b}{a},$$

$$\alpha\beta + \alpha\gamma + \beta\gamma = \frac{c}{a},$$

$$\alpha\beta\gamma = -\frac{d}{a}.$$

Donc pour f on a $a = 1$, $b = 0$, $c = a$ et $d = b$.

D'où,

$$\alpha + \beta + \gamma = 0,\ \alpha\beta + \alpha\gamma + \beta\gamma = a \text{ et } \alpha\beta\gamma = -b.$$

Ce qui donne :

$$\begin{aligned}\alpha^2 + \beta^2 + \gamma^2 &= 0^2 - 2a = -2a \\ \alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2 &= a^2 + 2b \times 0.\end{aligned}$$

Donc le discriminant vaut :

$$\begin{aligned}\Delta &= -\left(27b^2 + 9a^3 - 6a^3 + a^3\right) \\ &= -\left(4a^3 + 27b^2\right).\end{aligned}$$

Maintenant, supposons que $\Delta = 0$. On a alors :

$$\begin{aligned}-\left(4a^3 + 27^2\right) = 0 &\Leftrightarrow -f(\alpha)'f(\beta)'f(\gamma)' = 0 \\ &\Leftrightarrow (f(\alpha)' = 0) \vee (f(\beta)' = 0) \vee (f(\gamma)' = 0) \\ &\Leftrightarrow \alpha \text{ ou } \beta \text{ ou } \gamma \text{ est une racine multiple.}\end{aligned}$$

D'où le résultat. □

Remarque. Si (X, Y, Z) un point de $\overline{K}$ avec $Z \neq 0$ vérifie $F(X, Y, Z) = 0$ alors de façon équivalente (x, y) un point de $\overline{K}$ vérifie $f(x, y) = 0$.

En effet, il suffit dans l'équation $y^2 = x^3 + ax + b$ de remplacer x par $\frac{X}{Z}$ et y par $\frac{Y}{Z}$ et de multiplier par la puissance de Z qu'il faut pour obtenir l'équation polynômiale en terme de (X, Y, Z).

2.2 Partie affine et point à l'infini

Posons

$$U = \left\{ [x, y, z] \in \mathbb{P}^2(\overline{K}) | z \neq 0 \right\}.$$

On dispose de l'application $\varphi : U \to \overline{K}^2$ définie par

$$\varphi([x, y, z]) = \left(\frac{x}{z}, \frac{y}{z} \right).$$

C'est une bijection, dont l'application réciproque est donnée par la formule

$$\varphi^{-1}(x, y) = [x, y, 1].$$

Considérons des éléments a et b de K tels que $4a^3 + 27b^2 \neq 0$. Soit E la courbe elliptique définie sur K d'équation

$$y^2 z = x^3 + axz^2 + bz^3.$$

L'ensemble des points $[x.y.z] \in E$ tels que $z = 0$ est réduit au singleton $\{O\}$ où

$$O = [0, 1, 0].$$

Par ailleurs, $E \cap U$ s'identifie via φ à l'ensemble des éléments (x, y) de $\overline{K}^2$ vérifiant l'égalité

.

$$y^2 = x^3 + ax + b. \tag{2.3}$$

On dira que $E \cap U$ est la partie affine de E et que O est le point à la l'infinie de E.

Dans toute la suite, on identifira $E \cap U$ et le sous-ensemble de $\overline{K}^2$ formé des éléments (x, y) vérifiant (2.3). Avec cette identification, on a

$$E = \left\{ (x, y) \in \overline{K} \times \overline{K} \mid y^2 = x^3 + ax + b \right\} \cup \{O\}.$$

Ainsi, E est la courbe affine d'équation (2.3) à laquelle on adjoint le point à l'infini O. C'est pourquoi on définira souvent une courbe elliptique par sa partie affine, sans préciser le point O. Cela étant, il ne faudra pas perdre de vue l'importance du point à l'infini, comme on s'en rendra compte notamment dans la définition de la loi de groupe sur E que l'on verra plus loin.

Remarque. On retiendra qu'une courbe affine d'équation de la forme (2.3) est une courbe elliptique si et seulement si, par définition, la condition (**??**) est satisfaite.

2.3 Points rationnels d'une courbe elliptique

Soit L une extension de K dans $\overline{K}$.

Définition 2.6. Soit $P = [x, y, z]$ un point de $\mathbb{P}^2$. On dit que P est rationnel sur L s'il existe $\lambda \in \overline{K}^*$ tel que λx, λy et λz soient dans L. On note $\mathbb{P}^2(L)$ l'ensemble des points de $\mathbb{P}^2$ rationnels sur L.

Cela justifie la notation $\mathbb{P}^2 = \mathbb{P}^2(\overline{K})$.

Remarque. Étant donné un point $[x_1, x_2, x_3] \in \mathbb{P}^2$, le fait qu'il soit rationnel sur L n'implique pas que les x_i soient dans L. Cela signifie qu'il existe i tel que x_i soit non nul, et que chaque $\frac{x_j}{x_i}$ appartienne à L.

Soit E une courbe elliptique définie sur K d'équation (2.1).

Définition 2.7. Un point de E est dit rationnel sur L s'il appartient à $E \cap \mathbb{P}^2(L)$. On note $E(L)$ l'ensemble des points de E rationnels sur L.

Par définition, on a donc

$$E = E(\overline{K}).$$

Le point $O = [0, 1, 0]$ appartient à $E(K)$. Soit $(x, y) \in \overline{K}^2$ un point de la partie affine de E. Par définition, il est rationnel sur L si et seulement si x et y sont dans L. Il en résulte que l'on a

$$E = \left\{(x, y) \in L \times L \mid y^2 = x^3 + ax + b\right\} \cup \{O\}.$$

Exemple. mettre l'exemple avec la courbe et le corps fini pour les exemples des cryptosystèmes ◇

Chapitre 3

Loi de groupe

Soit E une courbe elliptique définie sur K. Pour toute extension L de K dans $\overline{K}$, on va munir $E(L)$ d'une structure naturelle de groupe abélien, d'élément neutre le point à l'infini.

3.1 Droites de $\mathbb{P}^2$

Définition 3.1. Une droite de $\mathbb{P}^2$ est une partie de $\mathbb{P}^2$ formée des points $[x, y, z]$ tels que

$$ux + vy + wz = 0,$$

où u, v et w sont des éléments non tous nuls de $\overline{K}$.

On parle alors de la droite d'équation $ux + vy + wz = 0$. Une droite d'équation $x = \lambda z$, où λ est dans $\overline{K}$, est dite verticale. Une telle droite passe par le point $O = [0, 1, 0]$. En fait, toute droite passant par O a une équation de la forme $ux + wz = 0$. On dit souvent que la droite d'équation $z = 0$ est la droite à l'infini. En identifiant la partie de $\mathbb{P}^2$ formée des points $[x, y, z]$ tels que $z \neq 0$ avec $\overline{K}^2$, le plan projectif s'interprète comme la reunion de $\overline{K}^2$ avec la droite à l'infini.

Lemme 3.2. Soient $P = [a_1, a_2, a_3]$ et $Q = [b_1, b_2, b_3]$ deux points distincts de $\mathbb{P}^2$.

Il existe une unique droite de $\mathbb{P}^2$ passant par P et Q. C'est la droite D d'équation $ux + vy + wz = 0$ avec $[x, y, z] \in \mathbb{P}^2$ et

$$u = a_2b_3 - a_3b_2,\ v = a_3b_1 - a_1b_3,\ w = a_1b_2 - a_2b_2.$$

Énoncé originel :

Soient $P = [a_1, a_2, a_3]$ et $Q = [b_1, b_2, b_3]$ deux points distincs de $\mathbb{P}^2$. Il existe une unique droite de $\mathbb{P}^2$ passant par P et Q. C'est l'ensemble des points $[x, y, z] \in \mathbb{P}^2$

tels que le déterminant de la matrice

$$M = \begin{pmatrix} a_1 & b_1 & x \\ a_2 & b_2 & y \\ a_3 & b_3 & z \end{pmatrix}$$

soit nul. Autrement dit, c'est la droite d'équation $ux + vy + wz = 0$, avec

$$u = a_2b_3 - a_3b_2,\ v = a_3b_1 - a_1b_3,\ w = a_1b_2 - a_2b_2.$$

Démonstration. Montrons qu'il existe une droite D passant par P et Q.

Les éléments $u,\ v$ et w ne sont pas tous nuls car P et Q sont distincts.

En effet, si $P = Q$ alors $a_1 = b_1,\ a_2 = b_2$ et $a_3 = b_3$ donc $u = v = w = 0$ or $P \neq Q$ donc il existe $x \in \{u, v, w\}$ tel que $x \neq 0$.

□

3.2 Tangente à E en un point

Soit

$$y^2z = x^3 + axz^2 + bz^3,$$

l'équation de E, où $a, b \in K$.

Notons

$$F = Y^2Z - \left(X^3 + aXZ^2 + bZ^3\right) \in K[X, Y, Z],$$

$$F_X = \frac{\partial F}{\partial X}, \quad F_Y = \frac{\partial F}{\partial Y}, \quad F_Z = \frac{\partial F}{\partial Z},$$

c'est-à-dire,

$$F_X = -\left(3X^2 + aZ^2\right), \quad F_Y = 2YZ, \quad F_Z = Y^2 - \left(2aXZ + 3bZ^2\right).$$

Lemme 3.3. Il n'existe pas de point $P \in E$ tel que

$$F_X(P) = F_Y(P) = F_Z(P) = 0.$$

Démonstration. Supposons par l'absurde, qu'il existe un tel point $P \in E$. Remarquons que $F_Z(O) = 1 \neq 0 = F_Z(P)$ donc par hypothèse P est disctinct de O.

Pour fixer les idées posons $P = [x, y, 1]$.

Puisque $\mathrm{Car}(K) \neq 2$, on a

$$(F_Y = 0) \Leftrightarrow (2YZ = 0) \Leftrightarrow (Y = 0),$$

donc $y = 0$.

Donc P serait de la forme $[x, 0, 1]$.

On obtient alors

$$F_X = -\left(3X^2 + a\right) = 0 \text{ et } F_Z = -\left(2aX + 3b\right) = 0.$$

— Supposons $a \neq 0$, on alors à partir de F_Z

$$X = -\frac{3b}{2a}.$$

Donc par F_X

$$-\left(3(-\frac{3b}{2a})^2 + a\right) = 0$$
$$-\left(27b^2 + 4a^3\right) = 0.$$

Ce qui est absurde car F est elliptique. D'après le lemme 2.5

— Supposons que $a = 0$, alors

$$(3b = 0) \underbrace{\Rightarrow}_{\text{Car}(K)\neq 3} (b = 0).$$

Donc on $a = b = 0$ donc $-\left(27b^2 + 4a^3\right) = 0$ absurde car F est elliptique. (lem 2.5)
D'où le résultat.

□

Lemme 3.4. 1) L'équation de la tangente à E au point O est z = 0.

2) Soit $P = [x_0, y_0, 1]$ un point de E distinct de O. L'équation de la tangente à E en P est

$$F_X(P)\left(x - x_0 z\right) + F_Y(P)\left(y - y_0 z\right) = 0.$$

Démonstration. 1) Soit $O \in E$ le point à l'infini. D'après l'équation de la tangente à E au point O. On a successivement

$$F_X(O) = 0,\ F_Y(O) = 0 \text{ et } F_Z(O) = 1.$$

Ainsi on retrouve bien $z = 0$.

2) Soit P un tel point, d'après l'équation (cite ? set up snippet -nommé + cité) de la tangente et de l'égalité $y_0^2 = x_0^3 + ax_0 + b$ on a,

$$\begin{aligned}
F_X(P)x + F_Y(P)y + F_Z(P)z &= 0\\
-\left(3x_0^2 + a\right)x + \left(2y_0\right)y + \left(y_0^2 - \left(2ax_0 + 3b\right)\right)z &= 0\\
-3x_0^2 x - ax + 2y_0 y + y_0^2 z - 2ax_0 z - 3bz &= 0\\
-3x_0^2 x - ax + 2y_0 y + y_0^2 z - 2ax_0 z - 3z\left(y_0^2 - x_0^3 - ax_0\right) &= 0 \left(\text{i.e } b = y_0^2 - \left(x_0^3 + ax_0\right)\right)\\
-3x_0^2 x - ax + 2y_0 y + y_0^2 z - 2ax_0 z - 3y_0^2 z + 3x_0^3 z + 3ax_0 z &= 0\\
-\left(3x_0^2 + a\right)x + 2y_0 y - 2y_0^2 z + \left(3x_0^2 + a\right)x_0 z &= 0\\
-\left(3x_0^2 + a\right)\left(x - x_0\right) + 2y_0\left(y - y_0 z\right) &= 0.
\end{aligned}$$

D'où le résultat.

□

3.3 Loi de composition des cordes-tangentes

Dans cette proposition à l'aide du comportement de deux points du plan E et de la droite qui les intersectent. On veut construit une loi de composition interne

$$\begin{aligned} \top : E \times E &\longrightarrow E \\ (P, Q) &\longmapsto P \top Q \end{aligned}$$

Cette loi, comme on va le voir, n'est pas une loi de groupe. C'est ce qui va nous permettre cependant de donner, par la suite, de donner une structure de groupe au plan E à l'aide d'une symétrie bien choisie.

Proposition 3.5. Soient P et Q des points de E. Soit D la droite de $\mathbb{P}^2$ passant par P et Q si $P \neq Q$, ou bien la tangente à E en P si $P = Q$. On a

$$D \cap E = \{P, Q, f(P, Q)\},$$

où $f(P, Q)$ désigne le point de E défini par les conditions suivantes.

1) Supposons $P \neq Q,\ P \neq O$ et $Q \neq O$.

i) Supposons $x_P \neq x_Q$. Posons

$$\lambda = \frac{y_P - y_Q}{x_P - x_Q} \text{ et } \nu = \frac{x_P y_Q - x_Q y_P}{x_P - x_Q}.$$

On a

$$f(P, Q) = \left[\lambda - x_P - x_Q, \lambda\left(\lambda^2 - x_P - x_Q\right) + \nu, 1\right]. \tag{3.1}$$

ii) Si $x_P = x_Q$, on a $f(P, Q) = O$.

2) Supposons $P \neq O$ et $Q = O$. On a

$$f(P, O) = [x_P, -y_P, 1]. \tag{3.2}$$

De même, si $P = O$ et $Q \neq O$, on a $f(O, Q) = [x_Q, -y_Q, 1]$

3) Si $P = Q = O$, on a $f(O, O) = O$.

4) Supposons $P = Q$ et $P \neq O$.

i) Si $y_P = 0$, on a $f(P, P) = O$.

ii) Supposons $y_P \neq 0$. Posons

$$\lambda = \frac{3x_P^3 + a}{2y_P} \text{ et } \nu = \frac{-x_P^3 + ax_P + 2b}{2y_P}.$$

On a

$$f(P, P) = \left[\lambda^2 - 2x_P, \lambda\left(\lambda^2 - 2x_P\right) + \nu, 1\right]. \tag{3.3}$$

Dans cette démonstration, on étudie le comportement des points P et Q selon qu'ils soient distincts ou égaux. Que ce soit pour la droite ou la tangente tous les deux vont éventuellement, soit recouper la courbe elliptique et rester dans le plan E, soit "couper" le point à l'infini O. C'est ce qu'on veut découvrir à l'aide du point que l'on a nommé $f(P,Q)$ qui désigne le comportement par rapport à P et Q de ce troisième point.

Démonstration. Soient $P = [x_P, y_P, 1]$ et $Q = [x_Q, y_Q, 1]$ des points de E tels qu'ils sont distincts. Alors il existe une droite $D \in \mathbb{P}^2$ qui passe par P et Q.

1) Supposons $P \neq Q$, $P \neq O$ et $Q \neq O$. Donc comme D existe, il existe un point $M \in D \cap E$ et on cherche donc à connaitre son comportement dans le plan E.

i) Supposons $x_P \neq x_Q$. Comme $P, Q \neq O$, le point à l'infini n'appartient pas à D. Comme $M \in D$, il est de la même forme que P et Q. Posons $M = [x_0, y_0, 1]$ avec x_0, y_0 des coordonnées sur $\overline{K}$.
Comme $M \in E$, on a la première égalité

$$y_0^2 = x_0^3 + ax_0 + b. \tag{3.4}$$

Ensuite avec $M \in D$ d'après le lemme 3.2 on a la matrice suivante

$$\begin{pmatrix} x_P & x_Q & x_0 \\ y_P & y_Q & y_0 \\ 1 & 1 & 1 \end{pmatrix},$$

qui nous permet d'obtenir une seconde égalité.

$$\begin{aligned} (y_P - y_Q)\, x_0 - (x_P - x_Q)\, y_0 + (x_P y_Q - x_Q y_P) &= 0 \\ y_0 = \frac{y_P - y_Q}{x_P - x_Q} x_0 + \frac{x_P y_Q - x_Q y_P}{x_P - x_Q}&. \end{aligned}$$

Posons

$$\lambda = \frac{y_P - y_Q}{x_P - x_Q} \quad \text{et} \quad \nu = \frac{x_P y_Q - x_Q y_P}{x_P - x_Q}.$$

Donc l'équation de D est de la forme

$$y = \lambda x + \nu z,$$

c'est-à-dire dans notre cas on a

$$y_0 = \lambda x_0 + \nu.$$

En remplacent dans (3.4), il vient

$$\begin{aligned} (\lambda x_0 + \nu)^2 &= x_0^3 + ax_0 + b \\ \lambda^2 x_0^2 + 2\lambda\nu x_0 + \nu^2 &= x_0^3 + ax_0 + b \\ x_0^3 - \lambda^2 x_0^2 + (a - 2\lambda\nu)\, x_0 + b - \nu^2 &= 0. \end{aligned}$$

Donc x_0 est une racine du polynôme

$$H = X^3 - \lambda X^2 + (a - 2\lambda\nu)\, X + b - \nu^2.$$

On remarque que $H(x_P) = H(x_Q) = 0$ donc x_p et x_q sont aussi des racines de H. Par les relations coefficients racines obtient la valeur de x_0

$$\begin{aligned} x_0 + x_P + x_Q &= -\left(-\lambda^2\right) \\ x_0 &= \lambda^2 - x_P - x_Q. \end{aligned}$$

Ainsi les racines de H sont

$$x_P, \quad x_Q \quad \text{et} \quad \lambda^2 - x_P - x_Q.$$

Il en résulte que $D \cap E$ est formé de P, et du point $M = f(P, Q)$. Donc

$$\begin{aligned} f(P,Q) &= [x_0, y_0, 1] \\ &= \left[\lambda^2 - x_P - x_Q, \lambda x_0 + \nu, 1\right] \\ &= \left[\lambda^2 - x_P - x_Q, \lambda\left(\lambda^2 - x_P - x_Q\right), 1\right]. \end{aligned}$$

D'où l'assertion.

ii) Supposons $x_P = x_Q$. Comme P et Q sont distinct, on a alors $y_P = -y_Q$. D'après le lemme 3.2 , la matrice suivante

$$\begin{pmatrix} x_P & x_Q & x \\ y_P & -y_Q & y \\ 1 & 1 & z \end{pmatrix}.$$

D'où l'équation de la droite suivante

$$\begin{aligned} 2y_P x - 2y_P x_P z &= 0 \\ x &= x_P z. \end{aligned}$$

Donc le point O est aussi un point de la droite D donc de $D \cap E$. Soit $M \in D \cap E$ distincts de O. Si $M = [0, 1, 0]$, d'après la situation on a $x_0 = x_P$ et $y_0 = \pm y_P$, donc $M = P$ ou $M = Q$. Or on a $P, Q \neq O$. Donc on a nécessairement $M = O$. Ainsi on a bien $D \cap E = \{P, Q, f(P, Q) = O\}$, d'où l'assertion dans ce cas ci.

2) Supposons $P \neq O$ et $Q = O$. Donc d'après lemme 3.2 , on a

$$\begin{pmatrix} x_P & 0 & x \\ y_P & 1 & y \\ 1 & 0 & z \end{pmatrix}.$$

À partir de la deuxième ligne on obtient l'équation de la droite suivante

$$\begin{aligned} x_P z - x &= 0 \\ x &= x_P z. \end{aligned}$$

Si $M = [x_0, y_0, 1]$ est un point de $D \cap E$, on a donc $x_0 = x_P$ d'où $y_0 = \pm y_P$. On a ainsi $D \cap E = \{P, O, f(P, O)\}$, où $f(P, O) = [x_P, -y_P, 1]$.

3) Supposons $P = Q = O$, par le lemme 3.4 la tangente D à E au point O à pour $z = 0$. Par suite, O est le seul point de $D \cap E$, d'où $f(O, O) = O$.

4) Supposons $P = Q$ et $P \neq O$. L'équation de la tangente D à E en P a donc pour équation

$$F_X(P)\,(x - x_P z) + F_Y(P)\,(y - y_P z) = 0.$$

i) Si $y_P = 0$, on a

$$x_P^3 + a x_P + b = 0.$$

Donc x_P est racine simple de ce polynôme. De plus, $F_X(P) \neq 0$. En effet, si $F_X(P) = 0$ on a

$$\begin{aligned} -\left(3x_P^2 + a\right) &= 0 \\ x_P^2 &= -\frac{a}{3}, \end{aligned}$$

ce qui est absurde.

Ainsi à partir de l'équation de la tangente D on a

$$\begin{aligned} F_X(P)\,(x - x_P z) = 0 &\Rightarrow (F_X(P)) = 0 \vee (x - x_P z) = 0 \\ &\Rightarrow x - x_P z = 0. \end{aligned}$$

Donc pour D on a

$$D : x = x_P z.$$

Le seul point de $D \cap E$ distinct de P est donc le point O, d'où $D \cap E = (P, O)$, d'où l'assertion.

ii) Supposons $y_P \neq 0$. Du lemme 3.4 et de l'équation $b = y_P^2 - x_P^3 - a x_P$ on obtient

$$\begin{aligned} -\left(3x_P^2 + a\right)(x - x_P z) + 2y_P\,(y - y_P z) &= 0 \\ -3x_P^2 x + 3x_P^3 z - ax + a x_P z + 2y_P y - 2y_P^2 z &= 0 \\ 2y_P y = 3x_P^2 x - 3x_P^3 z + ax - a x_P z + 2y_P^2 z & \\ 2y_P y - a x_P z = 3x_P^2 x + ax - x_P^3 z + 2b & \\ y = \frac{3x_P^2 + a}{2y_P} x + \frac{-x_P^3 + a x_P + 2b}{2y_P} z. & \end{aligned}$$

On pose $\lambda = \frac{3x_P^2 + a}{2y_P}$ et $\nu = \frac{-x_P^3 + a x_P + 2b}{2y_P}$ et on obtient l'équation de D, c'est-à-dire

$$y = \lambda x + \nu z.$$

Le point O n'est donc pas sur D. Soit $M = [x_0, y_0, 1]$ un point de $E \cap D$. On a par le même raisonnement que dans le cas (1-i) (utilise ref ?) les deux équations suivantes

$$y_0^2 = x_0^3 + a x_0 + b \quad \text{et} \quad y_0 = \lambda x_0 + \nu.$$

Par suite x_0 est une racine du polynôme

$$G = X^3 - \lambda^2 X^2 + (a - 2\lambda\nu)\,X + b - \nu^2.$$

Le polynôme dérivé de G est

$$G' = 3X^2 - 2\lambda^2 X + a - 2\lambda\nu.$$

On a

$$\begin{cases} G(x_P) = (0) \Leftrightarrow x_P^3 - \lambda^2 x_P^2 + (a - 2\lambda\nu)\, X + b - nu^2 = 0 \\ y_P^2 = x_P^3 + a x_P + b \Rightarrow b = y_P^2 - x_P^3 - a x_P \quad \text{et} \quad y_P = \lambda x_P + \nu \Rightarrow \nu = y_P - \lambda x_P \end{cases}.$$

Donc,

$$\begin{aligned} G(x_P) &= x_P^3 - \lambda^2 x_P^2 + (a - 2\lambda\,(y_p - \lambda x_P))\, x_P + y_P^2 - x_P^3 - a x_P - (y_P - \lambda x_P)^2 \\ &= x_P^3 - \lambda^2 x_P^2 + a x_P - 2\lambda x_P y_P + 2\lambda^2 x_P^2 + y_P^2 - x_P^3 - a x_P - y_P^2 + 2\lambda x_P y_P - \lambda^2 x_P^2 \\ &= 2\lambda^2 x_p^2. \end{aligned}$$

Par suite,

$$\begin{aligned} G'(x_P) = 0 &\Leftrightarrow 3x_P^2 - G(x_P) + a - 2\lambda\nu = 0 \\ &\Leftrightarrow G(x_P) = 3x_P^2 + a - 2\lambda\nu \\ &\Leftrightarrow G(x_P) = 0 \\ &\Leftrightarrow x_P \text{ racine de G.} \end{aligned}$$

Ainsi, x_P est une racine d'ordre au moins 2 de G. Les racines de G sont donc

$$x_P \quad \text{et} \quad \lambda^2 - 2x_P.$$

On obtient donc par le même raisonnement que (1-i) la formule annoncé.

□

3.4 Loi de groupe sur E

Considérons comme précédemment a et b des éléments de K tels que $4a^3+27b^2 \neq 0$ et E la courbe elliptique définie sur K d'équation

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

Notons $+$ la loi de composition interne sur E, définie pour tous P et Q dans E par l'égalité

$$P + Q = f(f(P, Q), O). \tag{3.5}$$

Géométriquement, $P+Q$ s'obtient à partir de $f(P, Q)$ par symétrie par rapport à l'axe des abscisses. Cette loi de composition est une loi de groupe sur E.

Théorème 3.6. Le couple $(E, +)$ est un groupe abélien, d'élément neutre O. La loi interne $+$ est décrite explicitement par les formules suivantes.

Soient P et Q des points de E distincts de O. Posons $P = (x_P, y_P)$ et $Q = (x_Q, y_Q)$.

1) Supposons x_{PQ}. Posons

$$\lambda = \frac{y_P - y_Q}{x_P - x_Q} \quad \text{et} \quad \nu = \frac{x_P y_Q = x_Q y_P}{x_P - x_Q}.$$

On a

$$P + Q = \left(\lambda^2 - x_P - x_Q, -\lambda\left(\lambda^2 - x_P - x_Q\right) - \nu\right). \tag{3.6}$$

2) Si $x_P = x_Q$ et P, on a $P + Q = O$.

3) Supposons $P = Q$ et $y_P \neq 0$. Posons

$$\lambda = \frac{3x_P^2 + a}{2y_P} \quad \text{et} \quad \nu = \frac{-x_P^3 + ax_P + b}{2y_P}.$$

On a

$$2P = \left(\lambda^2 - 2x_P, \lambda\left(-\lambda^2 - 2x_P\right) - \nu\right). \tag{3.7}$$

4) Si $P = Q$ et $y_P = 0$, on a $2P = O$.

5) L'opposé de P est le point

$$-P = (x_P, -y_P). \tag{3.8}$$

Démonstration. 1) Supposons x_{PQ}, compte tenu de (3.5), (3.1) et (3.2) on a

$$\begin{cases} (3.1) \Leftrightarrow f(\left[\lambda^2 - x_P - x_Q, \lambda\left(\lambda^2 - x_P - x_Q\right) + \nu, 1\right], [0,1,0]) \\ (3.2) \Leftrightarrow f(P,O) = [x_P, -y_P, 1] \end{cases}.$$

On retrouve bien la formule (3.6).

2) Supposons $x_P = x_Q$ et $P \neq Q$ c'est à dire y_{PQ}.
D'après la proposition 3.5 (1-i), on a $f(P,Q) = O$ donc $f(f(P,Q),O) = f(O,O) = O$. D'où la formule énoncé.

3) Supposons $P = Q$ et $y_P \neq 0$, en prenant compte (3.5) , (3.2) et (3.3) on obtient

$$\begin{cases} (3.3) \Leftrightarrow f(\left[\lambda^2 - 2_{xP}, \lambda\left(\lambda^2 - 2x_P\right) + \nu, 1\right], [0,1,0]) \\ (3.2) \Leftrightarrow f(P,O) = [x_P, -y_P, 1] \end{cases}.$$

Ce qui permet de retrouver la formule (3.7).

4) Supposons $P = Q$ et $y_P = 0$, d'après l'assertion (4-i) de la proposition 3.5 , on a $f(P,P) = O$ d'où $2P = f(f(P,P),O) = f(O,O) = O$.

5) Pour l'opposer on cherche un point $M \in E$ tel que $P \neq M$ et $P, Q \neq O$ d'après le théorème énoncé assertion 2) on a donc $x_P = x_M$ et donc nécessairement $y_M = -y_P$ donc le point recherché est $M = (x_M, y_M) = (x_P, -y_P) = -P$. (j'avais invoqué avant notre rendez vous la prop 7.1 assertion 2 et procédé par analyse synthèse, i.e je trouve ce que je cherche et je montre que j'ai bien trouvé ce que je cherchais mais ici je ne pense pas que cela soit nécessaire puisque l'assertion 2 rempli ce rôle en fournissant un contexte suffisamment restreint pour trouver l'opposé)

□

Exemple. mettre exemple de calcul de $2P$ pour la suite ◇

3.5 Morphisme de groupes de $E(\overline{K})$

Considérons un morphisme de groupes $f : E(\overline{K}) \to E(\overline{K})$. Soit n un entier ≥ 2 non divisible par $\mathrm{Car}(K)$. Le groupe $E[n]$ est un $\mathbb{Z}/n\mathbb{Z}$-module libre de rang 2. L'image par f de $E[n]$ est contenue dans $E[n]$. Par suite, f induit un endomorphisme du $\mathbb{Z}/n\mathbb{Z}$-module $E[n$. Dans toute base (P_1, P_2) de $E[n]$ sur $\mathbb{Z}/n\mathbb{Z}$, il est donc représenté par une matrice

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

qui décrit l'action de f sur $E[n]$.

Exemple. mettre l'exemple 1 de morphisme de groupe ◇

Chapitre 4

Cryptosystèmes

4.1 context

En cryptographie parmis les deux types de cryptosystème à notre disposition. À savoir les cryptosytèmes symétriques (i.e. à clé secrète) et les cryptosystèmes asymétriques (i.e. à clé publique). On peut à l'aide de la théorie des courbes elliptique adapter les cryptosystèmes asymétriques dit classique à leur équivivalents, c'est-à-dire, les cryptosystèmes asymétriques dit elliptique.

La force des cryptosytèmes asymétrique réside dans la difficulté, voir l'impossibilité actuel dans le cas elliptique, de résoudre le problème du logarithme discret que nous énoncerons par la suite.

Dans le cas des cryptosystèmes à clé publique classique, on s'appuie sur le groupe multiplicatif d'un corps fini et de son groupe des inversibles. Ce qui réduit grandement notre choix comparé aux versions elliptique des algorithmes équivalent.

En effet, dans le cas elliptique, on remplace le groupe multiplicatif sur un corps fini par le groupe des points rationnels d'une courbe elliptique. L'avantage de cette méthode est que pour un corps fini K donné, on dispose généralement de nombreux choix de courbes elliptiques E sur K. Autrement dit, on a de nombreux groupes $E(K)$, pour utiliser efficacement un cryptosystème asymétrique élliptique contrairement aux versions classique comme énoncé plus haut où l'on ne dispose que du groupe des inversible K^*.

Dans ce qui suit Alice et Bob sont deux personnes qui souhaite s'échanger soit un message, soit une clef secrète. Cependant, il faut bien comprendre qu'il peuvent également représenter deux entité qui souhaitent communiqué via des messages chiffrés ou bien s'échanger une clef secréte via cannaux publique. Par entité, j'entends soit des banques, des entreprises ou tout ce qui serait suceptible de vouloir communiqué secretement entre eux.

De plus le choix des clés secret s'effectue de façon aléatoire dans le respect des conditions de chaque cas.

4.2 Cryptosystème version classique

4.2.1 Algorithme d'El Gamal

Une personne Alice, souhaite envoyer à quiconque des messages confidentiels. Pour ce faire, elle choisit au départ un couple qui sera public (i.e. accessible à tout le monde). Ce couple est (K, g) où K est un corps fini et g un générateur du groupe des inversibles de ce corps à savoir K^*.

Soit q le cardinal de K.

L'algorithme d'El Gamal est alors le suivant :

1) Alice choisit un entier a tel que $1 < a < q - 1$, qui sera sa clé secrète.
Elle calcul alors g^a qu'elle rend public, et qui sera considéré comme sa clé publique.
On a donc au départ le triplet (K, g, g^a) qui est connue de tous.

2) Pour qu'une personne Bob puisse envoyer un message $m \in K$ à Alice, il choisit un entier b qui lui aussi est tel que $1 < b < q - 1$. Bob transmet alors à Alice le couple :

$$(g^b, mg^{ab}),$$

où g^b représente la clé publique de Bob. C'est ce qu'on appelle la phase d'encryptage du message m.

3) Pour que Alice puisse déchiffrer le message reçu, elle passe par la phase dite de décryptage. C'est-à-dire, connaissant son entier secret a et la clé publique de Bob, à savoir g^b, elle doit alors déterminer l'inverse de $(g^b)^a$ dans K. C'est-à-dire l'entier g^{-ab}.
Il lui suffit alors d'effectuer la multiplication de g^{-ab} par mg^{ab}, qui nous donne alors :

$$g^{-ab}\left(mg^{ab}\right) = m.$$

Ce qui permet donc à Alice de retrouver le message clair m et Alice et Bob on donc pu communiquer de façon publique en toute discrétion.

4.2.2 Protocole de Diffie-Hellman

À la différence de l'agorithme d'El Gammal, ici deux personnes Alice et Bob souhaite se construire une clé secrete commune via cannaux public donc à la vue de tous, qui seront donc les seuls à connaître. Ceci leur permettra donc de pouvoir communiqué sur un canal non sûr en utilisant cette clé pour déchiffrer leur correspondance.

Comme pour l'algorithme d'El Gamal, on se donne un corps fini K, ainsi qu'un générateur $g \in K^*$, qui seront tout deux public. Donc (K, g) est connu de tous.

Le procédé de construction de leur clé secret est ainsi le suivant :

1) Alice choisit sa clé secret qui est un entier a tel que $1 < a < q - 1$, elle transmet ensuite publiquement à Bob l'entier g^a.

2) Bob choisit de la même manière un entier b, et il transmet lui aussi publiquement l'élément g^b à Alice.

3) Alice pour sa part élève g^b à la puissance a, ce qui lui permet d'obtenir l'élément $(g^b)^a$.

4) Bob d'autre part, élève g^a à la puissance b, et il obtient donc l'élément $(g^a)^b$. Ainsi Alice et Bob on pu se construire de façon public une clé secret commun qui est l'entier g^{ab}.

4.3 Cryptosystème version elliptique

4.3.1 Algorithme d'El Gamal

Alice souhaite envoyer un message chiffré à Bob. Pour se faire elle choisit un corps fini K, une courbe elliptique E définie sur K de sorte que le problème du logarithme discret soit difficile à résoudre dans le groupe $E(K)$. Elle choisit ensuite un point $P \in E(K)$. Enfin elle choisit sont entier naturel secret, non nul, s et calcul et calcul le point $A = sP$.

Elle rend ainsi public le quadruplet

$$(K, E, P, A).$$

C'est la base de ce qui va permettre à Alice et Bob de pouvoir communiquer de façon confidentiel entre eux.

Ainsi, pour que Bob puisse envoyer un message chiffré $M \in E(K)$ à Alice, il choisit secrétement un entier non nul k et calcules les points

$$M_1 = kP \quad \text{et} \quad M_2 = M + kA.$$

Il transmet alors publiquement à Alice le couple (M_1, M_2). C'est donc la phase d'encryptage du message M.

Pour qu'Alice puisse déchiffrer le message M, elle doit calculer le point

$$M_2 - sM_1.$$

Ce qui lui permet grâce au calcul suivant de retrouver M :

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

4.3.2 Protocol Diffie-Hellman

Alice et Bob souhaite s'échanger publiquement une clé secrète commune. Pour cela ils se mettent d'accord pour la construire selon le procédé suivant :

1) Ils choisissent un corps fini K et une courbe elliptique E définie sur K, pour que le problème du logaritme discret soit difficile à résoudre dans le groupe $E(K)$. Ils choisissent un point $P \in E(K)$. Ils rendent alors publique le triplet (K, E, P).

2) Alice choisit un entier naturel secret non nun a et calcul le point $P_a = aP$, qu'elle transmet publiquement à Bob.

3) Bob procède de la même façon en choisissant un entier naturel secret, non nul, b, et il calcul de son côté le point $P_b = bP$, qu'il transmet publiquement à Alice.

4) Alice calcul le point $aP_b = a(bP)$.

5) Bob calcul le point $bP_a = b(aP)$.

Ils ont ainsi construit leur clé secret commun qui est le point abP.

Chapitre 5

Exemples

Références

[Kra10a] Alian Kraus. *Courbes elliptiques*. 2009/10. URL : https://www.math.univ-paris13.fr/~boyer/enseignement/crypto/Chap7.pdf.

[Kra10b] Alian Kraus. *Cryptosystèmes à clés publiques*. 2009/10. URL : https://www.math.univ-paris13.fr/~boyer/enseignement/crypto/Chap4.pdf.