Université de Versailles

Projet d'étude

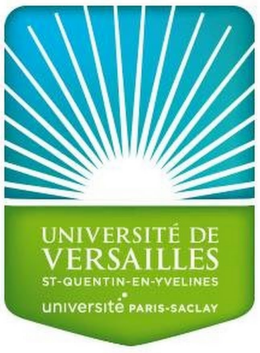
Master d'algèbre appliquée à la cryptographie

Algorithme de comptage de points de Schoof

Réalisé par:
Abdourahman Saleh Ibrahim
Abdessamad Fazzat

Supervisé par:
Prof. Luca De Feo

February 13, 2019



Contents

Abstract

Résumé du projet

1 Courbes elliptiques

1.1 Définitions

Définition 1 *(Silverman)*
Une courbe elliptique $\mathcal{E}$ est une variété projective lisse de genre 1.

C'est un ensemble de de couples (x, y) vérifiant une certaine équation, auquel on ajoute un point $\mathcal{O}$, ce point est considéré comme point à l'infini dans le plan projectif.

Définition 2 *(Blake, Seroussi)*
Une courbe elliptique $\mathcal{E}$ sur un corps $\mathbb{K}$ est définie par une équation de la forme:

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

où les $a_i \in \mathbb{K}$ sont des constantes.

Cette équation, dite de *Weierstrass*, peut être réduite selon la caractéristique du corps commutatif $\mathbb{K}$ dans lequel elle est définie.

Lemme 1 *(Washington) En caractéristique différente de 2 et 3, à l'aide d'un changement de variables, on peut se ramener à une équation de la forme:*

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

Définition 3 *Soit $\mathbb{K}$ un corps de caractéristique différente de 2 et 3. Une courbe elliptique est l'ensemble:*

$$\mathcal{E} = \{(x, y) \in \bar{\mathbb{K}} \times \bar{\mathbb{K}} | y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$

Avec $\Delta = 4a^3 + 27b^2 \neq 0$. son discriminant.

La condition $\Delta \neq 0$ signifie que le polynôme $x^3 + ax + b$ n'a pas de racine double et donc que la courbe est lisse.

Dans toute la suite, nous considérant le corps $\mathbb{K}$ de caractéristique differente de 2 et 3, pour pouvoir représenter une courbe elliptique avec une équation de *Weierstrass* réduite.

1.2 Loi de groupe

Proposition 1 *Soit $\mathcal{E}$ définie sur $\mathbb{K}$, P et Q deux points de $\mathcal{E}$, la droite (PQ)(ou la tangente à $\mathcal{E}$ si $P = Q$) et R le troisième point d'intersection de (PQ) avec la courbe. Le point $P + Q \in \mathcal{E}(\mathbb{K})$ est défini comme étant le deuxième point d'intersection de $\mathcal{E}$ avec la droite verticale passant par R.*

$\mathcal{E}(\mathbb{K})$ muni de cette loi de composition est un groupe commutatif, d'élément neutre $\mathcal{O}$.

On considère la courbe elliptique $\mathcal{E} : y^2 = x^3+ax+b$ et Soient $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$ et $R = (x_R, y_R)$ des point de $\mathcal{E}$ tels que P, $Q \neq \mathcal{O}$ et $P + Q = R$.
On distingue trois cas possibles:

1. Si $x_P = x_Q$ et $y_P \neq y_Q$: P et Q sont sur la même droite d'équation $x = c$ et $R = \mathcal{O}$;

2. Si $x_P = x_Q$ et $y_P = y_Q$: Si $y_P = 0$ alors $R = \mathcal{O}$, sinon $x_R = m^2 - 2x_P$, $y_R = m(x_P - x_R) - y_P$ où $m = (3x_P^2 + a)/2y_P$;

3. Si $x_P \neq x_Q$: $x_R = m^2 - x_P - x_Q$, $y_R = m(x_P - x_R) - y_P$ où $m = (y_Q - y_P)/(x_Q - x_P)$.

Remarque 1 *Si $P = (x_P, y_P) \in \mathcal{E}(\mathbb{K})$, $-P$ est le point d'intersection de la droite $x = x_P$ et $\mathcal{E}$.*

1.3 Points de n-torsion

Définition 4 *Soit $\mathcal{E}$ une courbe elliptique définie sur $\mathbb{K}$ et $n \in \mathbb{Z}$. Le groupe de n-torsion de $\mathcal{E}$ est l'ensemble:*

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

C'est le noyau de l'isogénie de multiplication par n. Comme le noyau d'une isogénie est toujours fini, $\mathcal{E}[n]$ contient un nombre fini de points pour tout n.

Exemple 1

- $\mathcal{E}[1]$ *est le sous-groupe réduit à $\mathcal{O}$;*
- $\mathcal{E}[2]$ *est constitué des points d'ordre 2, i.e. les points spéciaux de la courbe.*

$$\mathcal{E}[2] = \{P_{\alpha_1}, P_{\alpha_2}, P_{\alpha_3}, \mathcal{O}\}$$

où $P_{\alpha_i} = (\alpha_i, 0)$.

Soit $\mathbb{K}$ un corps de caractéristique p.

Théorème 1 *Pour tout entier n non multiple de p,*

$$Card(\mathcal{E}[n]) = n^2$$

Proposition 2 *Pour tout entier n non multiple de p, le groupe $\mathcal{E}[n]$ est isomorphe au produit direct $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.*

En particulier, $\mathcal{E}[p]$ est soit isomorphe à $\mathbb{Z}/p\mathbb{Z}$, soit égale à $\mathcal{O}$.
Si $\mathcal{E}[p] = \mathcal{O}$, on dit que la courbe est supersingulière.

2 Courbles elliptiques sur un corps fini

Soit $\mathbb{F}_q$ le corps à $q = p^d$ éléments et $\bar{\mathbb{F}}_q$ sa clôture algébrique.

Théorème 2 *(Cassel)*
Soit $\mathcal{E}$ une courbe elliptique sur $\mathbb{F}_q$. Alors:

- *soit $\mathcal{E}(\mathbb{F}_q)$ est un groupe cyclique;*
- *soit il est isomotphe à $\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$ avec $d_1|d_2$.*

2.1 Endomorphisme de Frobenius

Soit $\mathcal{E} : y^2 = x^3 + ax + b$ une courbe elliptique sur $\mathbb{F}_q$.

Définition 5 *Pour un point $P = (x_P, y_P)$ de $\mathcal{E}$, le point $(x_P^q, y_P^q) \in \mathcal{E}$, donc l'application $\phi_q : (x, y) \mapsto (x^q, y^q)$ et $\mathcal{O} \mapsto \mathcal{O}$ est un morphisme de $\mathcal{E}$ dans $\mathcal{E}$.*

L'ensemble des points de $\mathcal{E}(\mathbb{F}_q)$ fixés par ϕ_q est exactement $\mathcal{E}(\mathbb{F}_q)$, formellement:

$$\ker(\phi_q - [1]) = \mathcal{E}(\mathbb{F}_q)$$

Remarque 2 *Comme $y^2 = x^3 + ax + b$, on a $y^q = y^{q-1} = y(x^3 + ax + b)^{(q-1)/2}$, on peut donc exprimer $\phi_q(x, y)$ sous sa forme réduite:*

$$\phi_q(x, y) = (x^q, y(x^3 + ax + b)^{(q-1)/2})$$

Propriétés 1

- *ϕ_q est une isogénie inséparable;*
- $\phi_q(x, y) = (x, y) \iff (x, y) \in \mathcal{E}(\mathbb{F}_q)$;
- $\phi_q^n(x, y) = (x, y) \iff (x, y) \in \mathcal{E}(\mathbb{F}_{q^n})$ *où* $\phi_q^n(x, y) = (x^{q^n}, y^{q^n})$;
- $\#\ker(\phi_q - [1]) = deg(\phi_q - [1])$.

$\phi_q - [1]$ est une isogénie séparable de $\mathcal{E}$, de degré égale à l'ordre du groupe $\mathcal{E}(\mathbb{F}_q)$

2.2 Trace et théorème de Hasse

La trace t d'une courbe elliptique $\mathcal{E}$ est un paramètre lié à l'ordre du groupe $\mathcal{E}(\mathbb{F}_q)$.

Définition 6 *La trace de $\mathcal{E}(\mathbb{F}_q)$ est l'unique entier*

$$t = q + 1 - \#\mathcal{E}(\mathbb{F}_q)$$

Proposition 3 *Soit t la trace de $\mathcal{E}$. Pour tout entier n non multiple de p, la restriction de*

$$\phi_q^2 - [t] \circ \phi_q + [q]$$

au groupe $\mathcal{E}[n]$ est l'isogénie nulle $P \mapsto \mathcal{O}$.

Appliqué à un point $P = (x, y) \in \mathcal{E}(\mathbb{F}_q)$, on a $(x^{q^2}, y^{q^2}) - t(x^q, y^q) + q(x, y) = \mathcal{O}$.
On définit le polynôme caractéristique de Frobinius par $X^2 - tX + q$ en écrivant la matrice associée à ϕ_q dans une base de $\mathcal{E}[n]$,

$$\Phi_q = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$$

de polynôme caractéristique $X^2 - (a+d)X + \det(\Phi_q)$ avec $a + d = t$ modulo n et $\det(\Phi_q) = q$ modulo n

Théorème 3 *(Hasse)*
La trace t de $\mathcal{E}(\mathbb{F}_q)$ est telle que:

$$-2\sqrt{q} \leq t \leq 2\sqrt{q}$$

Autrement dit, le nombre de points de la courbe vérifie:

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

2.3 Polynômes de division

Définition 7 *Pour tout entier n non nul, le polynôme de division $\psi_n \in \mathbb{F}_q(\mathcal{E})$ est défini par son coefficient dominant n et diviseur $div(\psi_n) = (\mathcal{E}[n] - n^2(\mathcal{O})$.*

D'après ce qui précède, $\#\mathcal{E}[n] = n^2$ et comme $(\mathcal{E}[n] - n^2(\mathcal{O})$ est principal, on peu affirmer que c'est le diviseur d'une fonction sans pôles(autres que $\mathcal{O}$), cette fonction est donc un polynôme.
On définie les premiers polynômes de division comme suit:

- $\psi_0 = 0$ car $\mathcal{E}[0] = \mathcal{E}$;
- $\psi_1 = 1$ car $\mathcal{E}[1] = \mathcal{O}$;
- $\psi_2 = 2y$ (c.f. Exemple 1);
- $\psi_3 = 3x^4 + 6ax^2 + 12bx - a^2$;
- $\psi_4 = 4y(x^6 + 5ax^4 + 20bx^3 - 5ax^2 - 4abx - 8b^2 - a^3$.

Le reste est construit par récurrence sur n.

- $\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3$ Pour $n \geq 2$;
- $\psi_{2n} = \frac{\psi_n}{2y}(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2)$ Pour $n \geq 3$

Avec la convention $\psi_{-n} = -\psi_n$ pour tout n.
Si n est impair:

$$\psi_n(x,\, y) = n \prod_{P \in \mathcal{E}} (x - x_P)$$

$\psi_n(x,\, y)$ peut être réduit sous la forme d'un polynôme $f_n(x) \in \mathbb{F}_q[x]$, de degré $(n^2-1)/2$
Si n est pair: impair:

$$\psi_n(x,\, y) = ny \prod_{P \in \mathcal{E}} (x - x_P)$$

et on peut écrire $\psi_n(x,\, y) = y f_n(x)$ avec f_n de degré $(n^2-4)/2$
En reprenant les deux relations de récurrence et en distinguant les cas n pair et impair, on obtient:

- Cas n pair: $f_{2n+1} = y^4 f_{n+2} f_n^3 - f_{n-1} f_{n+1}^3$.
  De même, en divisant par y: $f_{2n} = \frac{f_n}{2}(f_{n+2} f_{n-1}^2 - f_{n-2} f_{n+1}^2)$
- Cas n impair: $f_{2n+1} = f_{n+2} f_n^3 - y^4 f_{n-1} f_{n+1}^3$.
  Et $f_{2n} = \frac{f_n}{2}(f_{n+2} f_{n-1}^2 - f_{n-2} f_{n+1}^2)$

Puis on remplace y^2 par $x^3 + ax + b$.

Proposition 4 *(Caractérisation des points de n-torsion)*
Soit $P = (x,\, y)$ un point ordinaire($y \neq 0$) de $\mathcal{E}(\mathbb{F}_q)$, on dit que P est un point de n-torsion si et seulement si $\psi_n(P) = 0$. Autrement dit, si et seulement si $f_n(x) = 0$.

Remarque 3 *Les points spéciaux $(\alpha,\, 0)$ sont des points de n-torsion dans le cas n pair.*

3 Algorithme de Schoof

3.1 Principes de l'algorithme

Le théorème de Hasse nous donne que la trace t dont dépend le cardinal de la courbe est inférieure en valeur absolue à $2\sqrt{q}$. C'est donc un élément de $\mathbb{Z}/M\mathbb{Z}$ où M est un entier supérieur à $4\sqrt{q}$ et premier à la caractéristique.

Pour le calculer éfficacement, on commence par déterminer sa valeur modulo les premiers l divisant M, puis on le reconstitue modulo M à l'aide du théorème des restes chinois. Tavailler modulo l revient à se restreindre aux points de l-torsion car dans ce cas on a $(l+1)P = P$ c'est à dire $lP = \mathcal{O}$.

La trace est l'entier t unique modulo M vérifiant

$$\forall P \in \mathcal{E}(\mathbb{F}_q),\ \phi_q^2(P) + qP = t\phi_q(P).$$

Dans le cas particulier $\mathbf{l = 2}$, on a $\#\mathcal{E}(\mathbb{F}_q) = q + 1 - t = t \ mod\ 2$ car q est impair.
Donc $t = 0$ modulo 2 est équivalent à $\#\mathcal{E}(\mathbb{F}_q) = 0 \ mod\ 2$ c'est à dire que $\mathcal{E}(\mathbb{F}_q)$ possède un point d'ordre 2 (donc) de la forme $(x, 0)$. Du coup $t = 0$ modulo 2 si et seulement si $x^3 + ax + b$ s'annule sur $\mathbb{F}_q$. Ce qui se teste en calculant le $pgcd(x^3 + ax + b, x^q - x)$. S'il est différent de 1,
$t = 0$ modulo 2 sinon, $t = 1$ modulo 2.

On note k le représentant de q modulo l et on remarque que $\psi_l(x, y) = f_l(x)$. Pour un point $P = (x, y)$ de l-torsion sur $\mathcal{E}(\mathbb{F}_q)$, $\phi^2(P) = (x^{q^2}, y^{q^2})$ et

$$kP = \left(x - \frac{\psi_{k-1}\psi_{k+1}}{\psi_k^2}, \frac{\psi_{k+2}\psi_{k-1}^2 - \psi_{k-2}\psi_{k+1}^2}{4y\psi_k^3} \right)$$

1er cas: il existe un point P tel que $\phi^2(P) = \pm kP$
Cela est vrai si les deux points ont le même abscisse c'est à dire

$$x^{q^2} = x - \frac{\psi_{k-1}\psi_{k+1}}{\psi_k^2} \ mod\ f_l \Leftrightarrow (x^{q^2} - x)\psi_k^2 + \psi_{k-1}\psi_{k+1} = 0 \ mod\ f_l$$

Si k est pair, on a $\psi_k = y f_k$, alors:

$$(x^{q^2} - x)\psi_k^2 + \psi_{k-1}\psi_{k+1} = (x^{q^2} - x)y^2 f_k^2 + f_{k-1}f_{k+1} = (x^{q^2} - x)(x^3 + ax + b)f_k^2 + f_{k-1}f_{k+1} \ (1)$$

Et si k est impair, on a:

$$(x^{q^2} - x)\psi_k^2 + \psi_{k-1}\psi_{k+1} = (x^{q^2} - x)f_k^2 + y^2 f_{k-1}f_{k+1} = (x^{q^2} - x)f_k^2 + (x^3 + ax + b)f_{k-1}f_{k+1} \ (2)$$

Si le pgcd de ce polynôme avec f_l n'est pas 1, on est dans le cas présent sinon on passe au 2ème cas.

Si $\phi^2(P) = -kP$, alors $\phi^2(P) + kP = \mathcal{O}$ donc t=0 mod l et réciproquement.

Si $\phi^2(P) = kP$, alors par le polynôme caractéristique de ϕ: $2kP = t\phi(P)$.

$$\phi(P) = \frac{2k}{t}P \Rightarrow \phi^2(P) = kP = \frac{4k^2}{t^2} \Rightarrow (t^2 - 4k)P = \mathcal{O} \Rightarrow t^2 - 4k = 0 \ mod\ l$$

Alors $k = (\frac{t}{2})^2 := w^2 \ mod\ l$ et $\phi(P) = \pm wP$.
On teste l'abscisse:

$$(x^q - x)(x^3 + ax + b)f_w^2 + f_{w-1}f_{w+1}, \ si\ w\ est\ pair \quad (3)$$

$$(x^q - x)f_w^2 + (x^3 + ax + b)f_{w-1}f_{w+1}, \ sinon \quad (4)$$

S'il est premier avec f_l alors t=0 mod l.
Sinon on passe l'ordonnée pour départager les deux racines carrées.
Si w est pair:

$$4y^{q+1}\psi_w^3 - \psi_{w+2}\psi_{w-1}^2 + \psi_{w-2}\psi_{w+1}^2 = 4y^{q+1}y^3 f_w^3 - y f_{w+2}f_{w-1}^2 + y f_{w-2}f_{w+1}^2$$

$$= y(4y^{q+3}f_w^3 - f_{w+2}f_{w-1}^2 + f_{w-2}f_{w+1}^2)$$
$$= y(4(x^3+ax+b)^{(q+3)/2}f_w^3 - f_{w+2}f_{w-1}^2 + f_{w-2}f_{w+1}^2)$$

Il suffit de tester $4(x^3+ax+b)^{(q+3)/2}f_w^3 - f_{w+2}f_{w-1}^2 + f_{w-2}f_{w+1}^2$ (5), car l'ordonnée des points des l-torsion est non nulle (puisque l n'est pas 2).
Si w est impair:

$$4y^{q+1}\psi_w^3 - \psi_{w+2}\psi_{w-1}^2 + \psi_{w-2}\psi_{w+1}^2 = 4y^{q+1}f_w^3 - y^2 f_{w+2}f_{w-1}^2 + y^2 f_{w-2}f_{w+1}^2$$
$$= y^2(4y^{q-1}f_w^3 - f_{w+2}f_{w-1}^2 + f_{w-2}f_{w+1}^2)$$
$$= y^2(4(x^3+ax+b)^{(q-1)/2}f_w^3 - f_{w+2}f_{w-1}^2 + f_{w-2}f_{w+1}^2)$$

Il suffit de tester $4(x^3+ax+b)^{(q-1)/2}f_w^3 - f_{w+2}f_{w-1}^2 + f_{w-2}f_{w+1}^2$ (6).
Si le pgcd avec f_l est 1, alors $t = -2w \ mod \ l$ sinon $t = 2w \ mod \ l$.

2ème cas: Pour tout point P $\phi^2(P) \neq \pm kP$
On calcule $\phi^2(P) + kP$ avec la formule de la somme de deux points d'abscisses différentes.

$$\phi^2(P) + kP = \left(-x^{q^2} - x + \frac{\psi_{k-1}\psi_{k+1}}{\psi_k^2} + \mu^2, \left(2x^{q^2} + x - \frac{\psi_{k-1}\psi_{k+1}}{\psi_k^2} - \mu^2\right)\mu - y^{q^2}\right)$$

$$avec \ \mu = \frac{\psi_{k+2}\psi_{k-1}^2 - \psi_{k-2}\psi_{k+1}^2 - 4y^{q^2+1}\psi_k^3}{4y\psi_k((x-x^{q^2})\psi_k^2 - \psi_{k-1}\psi_{k+1})} := \frac{\alpha}{\beta}$$

Pour tout $1 \leq j \leq \frac{l-1}{2}$, on calcule:

$$j\phi(P) = \phi(jP) = \left(\left(x - \frac{\psi_{j-1}\psi_{j+1}}{\psi_j^2}\right)^q, \left(\frac{\psi_{j+2}\psi_{j-1}^2 - \psi_{j-2}\psi_{j+1}^2}{4y\psi_j^3}\right)^q\right)$$

Comme la caractéristique divise q, on obtient

$$j\phi(P) = \left(x^q - \frac{(\psi_{j-1}\psi_{j+1})^q}{\psi_j^{2q}}, \frac{(\psi_{j+2}\psi_{j-1}^2 - \psi_{j-2}\psi_{j+1}^2)^q}{4y\psi_j^{3q}}\right)$$

$\phi^2(P) + kP$ aura à fortiori la même abscisse qu'un des $j\phi(P)$. A ce moment-là, on compare les ordonnées si elles sont aussi les mêmes modulo f_l alors j est notre trace sinon c'est $-j$. Ainsi tous les j de $\mathbb{Z}/l\mathbb{Z}$ sont testés.

On note *absc* le polynôme numérateur de la différence des abscisses et *ordo* celui des ordonnées.

$$absc = \gamma_1\psi_j^{2q} + \delta_1(\psi_{j-1}\psi_{j+1})^q, \ avec$$
$$\gamma_1 = (\psi_{k-1}\psi_{k+1} - \psi_k^2(x^{q^2} + x^q + x))\beta^2 + \psi_k^2\alpha^2, \ et \ \delta_1 = \psi_k^2\beta^2.$$
$$ordo = \gamma_2\psi_j^{3q} - \delta_2(\psi_{j+2}\psi_{j-1}^2 - \psi_{j-2}\psi_{j+1}^2)^q, \ avec$$
$$\gamma_2 = 4y^q(\alpha\beta^2(\psi_k^2(2x^{q^2} + x) - \psi_{k-1}\psi_{k+1}) - \psi_k^2(\alpha^3 + \beta^3 y^{q^2})), \ et \ \delta_2 = \beta^3\psi_k^2$$

Pour continuer à manipuler des polynômes univariés, on distingue des plusieurs cas selon la parité de k et j.

Si k est pair:

$$\alpha = \psi_{k+2}\psi_{k-1}^2 - \psi_{k-2}\psi_{k+1}^2 - 4y^{q^2+1}\psi_k^3 = yf_{k+2}f_{k-1}^2 - yf_{k-2}f_{k+1}^2 - 4y^{q^2+1}y^3f_k^3$$

$$= y(f_{k+2}f_{k-1}^2 - f_{k-2}f_{k+1}^2 - 4y^{q^2+3}f_k^3) = y(f_{k+2}f_{k-1}^2 - f_{k-2}f_{k+1}^2 - 4(x^3+ax+b)^{(q^2+3)/2}f_k^3) = y\alpha_x$$

$$\beta = 4y\psi_k((x-x^{q^2})\psi_k^2 - \psi_{k-1}\psi_{k+1}) = 4yyf_k((x-x^{q^2})y^2f_k^2 - f_{k-1}f_{k+1})$$
$$= 4(x^3+ax+b)f_k((x-x^{q^2})(x^3+ax+b)f_k^2 - f_{k-1}f_{k+1}).$$

$$\gamma_1 = (\psi_{k-1}\psi_{k+1} - \psi_k^2(x^{q^2}+x^q+x))\beta^2 + \psi_k^2\alpha^2 = (f_{k-1}f_{k+1} - y^2f_k^2(x^{q^2}+x^q+x))\beta^2 + y^2f_k^2y^2\alpha_x^2$$
$$= (f_{k-1}f_{k+1} - (x^3+ax+b)f_k^2(x^{q^2}+x^q+x))\beta^2 + (x^3+ax+b)^2f_k^2\alpha_x^2$$

$$\delta_1 = \psi_k^2\beta^2 = y^2f_k^2\beta^2 = (x^3+ax+b)f_k^2\beta^2.$$

$$\gamma_2 = 4y^q(\alpha\beta^2(\psi_k^2(2x^{q^2}+x) - \psi_{k-1}\psi_{k+1}) - \psi_k^2(\alpha^3+\beta^3y^{q^2}))$$
$$= 4y^q(y\alpha_x\beta^2(y^2f_k^2(2x^{q^2}+x) - f_{k-1}f_{k+1}) - y^2f_k^2(y^3\alpha_x^3+\beta^3y^{q^2}))$$
$$= 4y^{q+1}(\alpha_x\beta^2(y^2f_k^2(2x^{q^2}+x) - f_{k-1}f_{k+1}) - y^2f_k^2(y^2\alpha_x^3+\beta^3y^{q^2-1}))$$
$$= 4(x^3+ax+b)^{(q+1)/2}(\alpha_x\beta^2((x^3+ax+b)f_k^2(2x^{q^2}+x) - f_{k-1}f_{k+1}) - (x^3+ax+b)f_k^2((x^3+ax+b)\alpha_x^3$$
$$+\beta^3(x^3+ax+b)^{(q^2-1)/2}))$$

$$\delta_2 = \beta^3\psi_k^2 = \beta^3y^2f_k^2 = \beta^3(x^3+ax+b)f_k^2$$

Si de plus j est pair:

$$absc = \gamma_1\psi_j^{2q} + \delta_1(\psi_{j-1}\psi_{j+1})^q = \gamma_{1y^{2q}}f_j^{2q} + \delta_1(f_{j-1}f_{j+1})^q = \gamma_1(x^3+ax+b)^qf_j^{2q} + \delta_1(f_{j-1}f_{j+1})^q$$

$$ordo = \gamma_2\psi_j^{3q} - \delta_2(\psi_{j+2}\psi_{j-1}^2 - \psi_{j-2}\psi_{j+1}^2)^q = \gamma_2y^{3q}f_j^{3q} - \delta_2y^q(f_{j+2}f_{j-1}^2 - f_{j-2}f_{j+1}^2)^q$$
$$= y(\gamma_2y^{3q-1}f_j^{3q} - \delta_2y^{q-1}(f_{j+2}f_{j-1}^2 - f_{j-2}f_{j+1}^2)^q)$$
$$= y(\gamma_2(x^3+ax+b)^{(3q-1)/2}f_j^{3q} - \delta_2(x^3+ax+b)^{(q-1)/2}(f_{j+2}f_{j-1}^2 - f_{j-2}f_{j+1}^2)^q)$$

et si j est impair:

$$absc = \gamma_1\psi_j^{2q} + \delta_1(\psi_{j-1}\psi_{j+1})^q = \gamma_1f_j^{2q} + \delta_1(x^3+ax+b)^q(f_{j-1}f_{j+1})^q$$

$$ordo = \gamma_2f_j^{3q} - \delta_2(x^3+ax+b)^q(f_{j+2}f_{j-1}^2 - f_{j-2}f_{j+1}^2)^q$$

Si k est impair:

$$\alpha = \psi_{k+2}\psi_{k-1}^2 - \psi_{k-2}\psi_{k+1}^2 - 4y^{q^2+1}\psi_k^3 = (x^3+ax+b)(f_{k+2}f_{k-1}^2 - f_{k-2}f_{k+1}^2) - 4(x^3+ax+b)^{(q^2+1)/2}f_k^3$$

$$\beta = 4y\psi_k((x-x^{q^2})\psi_k^2 - \psi_{k-1}\psi_{k+1}) = 4yf_k((x-x^{q^2})f_k^2 - (x^3+ax+b)f_{k-1}f_{k+1}) = y\beta_x$$

$$\gamma_1 = (\psi_{k-1}\psi_{k+1} - \psi_k^2(x^{q^2}+x^q+x))\beta^2 + \psi_k^2\alpha^2$$
$$= ((x^3+ax+b)f_{k-1}f_{k+1} - f_k^2(x^{q^2}+x^q+x))(x^3+ax+b)\beta_x^2 + \psi_k^2\alpha^2$$

$$\delta_1 = \psi_k^2\beta^2 = f_k^2(x^3+ax+b)\beta_x^2$$

$$\gamma_2 = 4y^q(\alpha\beta^2(\psi_k^2(2x^{q^2}+x) - \psi_{k-1}\psi_{k+1}) - \psi_k^2(\alpha^3+\beta^3y^{q^2}))$$
$$= 4y(x^3+ax+b)^{(q-1)/2}(\alpha(x^3+ax+b)\beta_x^2(f_k^2(2x^{q^2}+x) - (x^3+ax+b)f_{k-1}f_{k+1}) - f_k^2(\alpha^3+\beta_x^3(x^3+ax+b)^{(q^2+3)/2}))$$
$$= y\gamma_{2,x}$$

$$\delta_2 = \beta^3\psi_k^2 = y(x^3+ax+b)\beta_x^3f_k^2 = y\delta_{2,x}$$

Si de plus j est pair:

$$absc = \gamma_1(x^3+ax+b)^qf_j^{2q} + \delta_1(f_{j-1}f_{j+1})^q$$

$$ordo = (x^3+ax+b)(\gamma_{2,x}(x^3+ax+b)^{(3q-1)/2}f_j^{3q} - \delta_{2,x}(x^3+ax+b)^{(q-1)/2}(f_{j+2}f_{j-1}^2 - f_{j-2}f_{j+1}^2)^q)$$

et si j est impair:

$$absc = \gamma_1f_j^{2q} + \delta_1(x^3+ax+b)^q(f_{j-1}f_{j+1})^q$$
$$ordo = y(\gamma_{2,x}f_j^{3q} - \delta_{2,x}(x^3+ax+b)^q(f_{j+2}f_{j-1}^2 - f_{j-2}f_{j+1}^2)^q)$$

Dans les cas où $ordo$ possède un y en facteur(pair-pair, impair-impair), on l'identifie à $\frac{ordo}{y}$.

3.2 Pseudo-code

1. Si $pgcd(x^3 + ax + b, x^q - x) = 1$ alors $t \leftarrow 1 \ mod \ 2$ sinon $t \leftarrow 0 \ mod \ 2$
2. $M \leftarrow 2$ et $l \leftarrow 3$
3. Tant que $M \leq 4\sqrt{q}$
   a. Si $pgcd(\ (1) \ ou \ (2), f_l) \neq 1$
      a'. Si q n'est pas un résidu quadratique alors $t \leftarrow 0 \ mod \ l$
      b'. Sinon si $pgcd(\ (3) \ ou \ (4), f_l) \neq 1$,
         a". Si $pgcd(\ (5) \ ou \ (6), f_l) \neq 1$ alors $t \leftarrow 2w \ mod \ l$
         b". Sinon $t \leftarrow -2w \ mod \ l$
   b. Pour j allant de 1 à $(l-1)/2$
      a'. Si $pgcd(absc, f_l) \neq 1$,
         a". Si $pgcd(ordo, f_l) \neq 1$, alors $t \leftarrow j \ mod \ l$
         b". Sinon $t \leftarrow -j \ mod \ l$
   c. $M \leftarrow M \times l$
   d. $l \leftarrow$ le premier suivant différent de p
4. Calcul de t avec le TRC
5. $\#\mathcal{E}(\mathbb{F}_q) = q + 1 - t$

Schoof's algorithm [1] Schoof$a, b, q \ pgcd(x^3 + ax + b, x^q - x) = 1 \ t = 1 \ mod \ l \ \ t = 0 \ mod \ l$ $M \leftarrow 2, \ l \leftarrow 3 \ M \leq 4\sqrt{q} \ pgcd(\ (1) \ ou \ (2), f_l) \neq 1 \ q$ n'est pas un résidu quadratique $t \leftarrow 0 \ mod \ l \ \ pgcd(\ (3) \ ou \ (4), f_l) \neq 1 \ pgcd(\ (5) \ ou \ (6), f_l) \neq 1 \ t \leftarrow 2w \ mod \ l \ \ t \leftarrow -2w \ mod \ l$ j allant de 1 à $(l-1)/2 \ pgcd(absc, f_l) \neq 1 \ pgcd(ordo, f_l) \neq 1 \ t \leftarrow j \ mod \ l \ \ t \leftarrow -j \ mod \ l$ $j \leftarrow j + 1 \ M \leftarrow M \times l \ l \leftarrow$ le premier suivant différent de p Calculer $t \mod M$ avec le TRC $\#\mathcal{E}(\mathbb{F}_q) = q + 1 - t$ avec $|t| \leq 2\sqrt{q}$

4 Implémentation de l'algorithme de Schoof

4.1 Architecture du programme

4.2 Complexité

5 Cryptographie sur les courbes elliptiques

5.1 Problème du logarithme discret

References

[1] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. Mathematics of computation 44.170 (1985):483-494.

[2] R. Crandall, C. Pomerance. Prime numbers: a computational perspective. Vol. 182. Springer Science and Business Media, 2006. Côte 512.7 CRA. §7.5.2.

[3] I. F. Blake, G. Seroussi, N. Smart. Elliptic curves in cryptography. Vol. 265. Cambridge university press, 1999. Côte 005.82 BLA. Chapitre VII.

[4] P. Guillot: Introduction aux courbes elliptiques pour la cryptographie.