Courbes elliptiques et cryptographie

Robert Rolland

rolland@iml.univ-mrs.fr

C.N.R.S., Institut de Mathématiques de Luminy

F13288 Marseille cedex 9, France

II-1. Cryptographie elliptique

La **cryptographie elliptique** repose sur le problème de logarithme discret et problèmes connexes dans le groupe des points d'une courbe elliptique sur un corps fini. On va donc s'intéresser aux questions suivantes :

- **courbe elliptique sur un corps fini.**
- **la structure de groupe.**
- **cryptosystèmes basés sur les courbes elliptiques.**

II-1.1 Courbe elliptique

Une courbe elliptique sur un corps fini $\mathbb{F}_q$ est une courbe plane sans points singuliers sur $\overline{\mathbb{F}}_q$, d'équation affine

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

Si on se place dans le plan projectif l'équation devient

$$Y^2T + a_1XYT + a_3YT^2 = X^3 + a_2X^2T + a_4XT^2 + a_6T^3.$$

La courbe a donc un **point à l'infini**, le point

$$\mathcal{O} = (0 : 1 : 0).$$

II-1.1 Courbe elliptique (suite)

Après changement de variable rationnel, l'équation de la courbe est

- **Cas d'un corps de caractérisique 2 :**
  - **Cas non supersingulier :**

$$y^2 + xy = x^3 + ax^2 + b \quad (b \neq 0)$$

  - **Cas supersingulier :**

$$y^2 + cy = x^3 + ax + b \quad (c \neq 0)$$

II-1.1 Courbe elliptique (suite)

- **Cas d'un corps de caractérisique 3 :**
  - **Cas non supersingulier :**

$$y^2 = x^3 + ax^2 + b \quad (ab \neq 0)$$

  - **Cas supersingulier :**

$$y^2 = x^3 + ax + b \quad (a \neq 0)$$

- **Cas d'un corps de caractérisique** $\neq 2, 3$ **:**

$$y^2 = x^3 + ax + b \quad (4a^3 + 27b^2 \neq 0).$$

II-1.1 Courbe elliptique (suite)

Il y a deux quantités très importantes associées à une équation du type

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

- **Le discriminant :** il indique si la courbe est sans point singulier sur le corps $\overline{\mathbb{F}}_q$.
- **Le j-invariant :** qui définit des classes de courbes "isomorphes".

II-1.1.1 Le discriminant

Le discriminant est définit par

$$\Delta = -d_2^2 d_8 - 8d_4^3 - 27d_6^2 + 9d_2 d_4 d_6$$

où

$$d_2 = a_1^2 + 4a_2$$

$$d_4 = 2a_4 + a_1 a_3$$

$$d_6 = a_3^2 + 4a_6$$

$$d_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2$$

II-1.1.2 Le j-invariant

Le j-invariant est défini par

$$j = \frac{c_4^3}{\Delta}$$

où

$$c_4 = d_2^2 - 24d_4$$

II-1.2 La structure de groupe

Les points rationnels d'une courbe elliptique E (i.e. les points de la courbe à coordonnées dans $\mathbb{F}_q$) forment un **groupe commutatif**. On prend comme élément neutre le point à l'infini $\mathcal{O}$ (mais ça pourrait être n'importe quel point de la courbe). et on définit

$$P + Q = R$$

en construisant $R' = D(P, Q) \cap E$ puis $R = D(R', \mathcal{O}) \cap E$. (Lorsque $M = N$ la droite $D(M, N)$ est la tangente en M à la courbe E).

II-1.2 La structure de groupe (suite)

Avec cette définition l'opération est bien commutative, associative, ayant $\mathcal{O}$ pour élément neutre. Supposons que la courbe soit donnée par son équation générale de Weierstrass

$$y_2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Si $P = (x_1, y_1) \neq \mathcal{O}$ alors $-P = (x_1, -y_1 + a_1x_1 + a_3)$.
On se rend compte aussi que $P + Q = -R'$.
Posons $Q = (x_2, y_2) \neq -P$ et $R = (P + Q) = (x_3, y_3)$.

II-1.2 La structure de groupe (suite)

$$\begin{cases} x_3 &= -a_2 + \lambda^2 + a_1\lambda - x_1 - x_2, \\ y_3 &= -(\lambda x_3 + \gamma) - a_1 x_3 - a_3; \end{cases}$$

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \; si \; P \neq Q \\ \\ \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} \; si \; P = Q \end{cases}$$

$$\gamma = y_1 - \lambda x_1$$

II-1.2.1 Caractéristique $\neq 2, 3$

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

Si $P = (x_1, y_1)$ et $Q = (x_2, y_2)$ alors $-P = (x_1, -y_1)$, si $Q = -P$ alors $P + Q = \mathcal{O}$, sinon $P + Q = (x_3, y_3)$ où

$$x_3 = \lambda^2 - x_1 - x_2 \quad y_3 = \lambda(x_1 - x_3) - y_1$$

avec

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \text{ si } P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1} \text{ si } P = Q \end{cases}$$

II-1.2.2 Caractéristique 2

1) Cas non-supersingulier

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

Si $P = (x_1, y_1)$ et $Q = (x_2, y_2)$ alors $-P = (x_1, x_1 + y_1)$, si $Q = -P$ alors $P + Q = \mathcal{O}$, sinon $P + Q = (x_3, y_3)$ où

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a \quad y_3 = \lambda(x_1 + x_3) + x_3 + y_1$$

avec $\lambda = \frac{y_1 + y_2}{x_1 + x_2}$ si $P \neq Q$.

II-1.2.2 Caractéristique 2 (suite)

et

$$x_3 = \lambda^2 + \lambda + a$$

$$y_3 = x_1^2 + \lambda x_3 + x_3$$

avec

$$\lambda = x_1 + \frac{y_1}{x_1}$$

si $P = Q$.

II-1.2.3 Caractéristique 3

1) Cas non-supersingulier

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

$$\begin{cases} x_3 &= -a + \lambda^2 - x_1 - x_2, \\ y_3 &= -\lambda(x_1 - x_3) - y_1; \end{cases}$$

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \; si \; P \neq Q \\ \\ \dfrac{ax_1}{y_1} \; si \; P = Q \end{cases}$$

II-1.2.3 Caractéristique 3 (suite)

1) Cas supersingulier

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

$$\begin{cases} x_3 &= \lambda^2 - x_1 - x_2, \\ y_3 &= -\lambda(x_1 - x_3) - y_1; \end{cases}$$

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \; si \; P \neq Q \\ \\ \dfrac{a}{2y_1} \; si \; P = Q \end{cases}$$

II-1.3 Ordre du groupe

Soit E une courbe elliptique sur $\mathbb{F}_q$. Notons $\#E(q)$ son nombre de points sur $\mathbb{F}_q$. On dispose de la borne de Hasse

$$q + 1 - 2\sqrt{q} \leq \#E \leq q + 1 + 2\sqrt{q}.$$

Écrivons que

$$\#E(q) = q + 1 - t$$

avec $|t| \leq 2\sqrt{q}$.

Quels sont les ordres possibles?

II-1.3.1 Existence

Si $q = p^m$, il existe une courbe elliptique vérifiant $\#E(q) = q + 1 - t$ si et seulement si l'une des conditions suivantes est satisfaite

1) $t \not\equiv 0 \mod p$ et $t^2 \leq 4q$
2) m est impair et
   a) ou bien $t = 0$
   b) ou bien $t^2 = 2q$ et $p = 2$
   c) ou bien $t^2 = 3q$ et $p = 3$
3) m est pair et
   a) ou bien $t^2 = 4q$
   b) ou bien $t^2 = q$ et $p \not\equiv 1 \mod 3$
   c) ou bien $t = 0$ et $p \not\equiv 1 \mod 4$

II-1.3.2 Calcul de l'ordre

Si on connaît $\#E(q) = q + 1 - t$ alors on peut calculer par récurrence $\#E(q^n) = q + 1 - t_n$ en posant $t_0 = 2$, $t_1 = t$, $t_n = t_1 t_{n-1} - q t_{n-2}$ (pour $n \geq 2$).

Ceci arrivera en particulier si la courbe utilisée a ses coefficients dans un petit corps.

Sinon, on dispose de l'algorithme de Schoof et de ses variantes, ou alors des constructions de Morain pour obtenir une courbe ayant un nombre de points donné.

II-1.4 Courbes supersingulières

Soit E une courbe sur $\mathbb{F}_q$ ayant $\#E(q) = q + 1 - t$ points sur $\mathbb{F}_q$ ($q = p^m$).

Nous dirons que E est **supersingulière** si p divise t.