Chiffrement El Gamal sur une courbe de Weierstrass

Marie Virat *

26 novembre 2004

Le but de cet exposé est d'introduire un nouveau cryptosystème aussi sûr que la version elliptique du système El Gamal.

La sécurité de ce nouveau système repose, elle aussi, sur la difficulté de calculer un logarithme discret. Il s'agit donc d'exhiber un groupe sur lequel le problème du calcul de logarithme discret est aussi difficile que le calcul de logarithme discret sur une courbe elliptique.

Considérons un corps fini $\mathbb{F}_q$ de caractéristique p différent de 2 et 3, ainsi que l'anneau artinien $\mathbb{F}_q[X]/(X^2)$. Usuellement, on note cet anneau $\mathbb{F}_q[\varepsilon]$ où ε vérifie $\varepsilon^2 = 0$. Son idéal maximal est alors $M = \mathbb{F}_q.\varepsilon$. De plus, cet anneau se projette canoniquement dans $\mathbb{F}_q$. On note π cette projection : pour a_0, a_1 dans $\mathbb{F}_q$, $\pi(a_0 + a_1\varepsilon) = a_0$.

Une équation de Weierstrass sur $\mathbb{F}_q[\varepsilon]$ est une équation homogène de degré 3 du type $Y^2Z = X^3 + aXZ^2 + bZ^3$ avec a et b dans $\mathbb{F}_q[\varepsilon]$. La réduction sur $\mathbb{F}_q$ d'une telle équation est alors $Y^2Z = X^3 + \pi(a)XZ^2 + \pi(b)Z^3$.

Considérons une équation de Weierstrass sur $\mathbb{F}_q[\varepsilon]$. Si la cubique définie par cette équation est lisse sur $\mathbb{F}_q[\varepsilon]$, on dit qu'elle est de Weierstrass. Il est alors équivalent de dire que l'équation de Weierstrass associée vérifie que $4a^3 + 27b^2$ est inversible dans $\mathbb{F}_q[\varepsilon]$ ou bien encore que sa réduction à $\mathbb{F}_q$ définit une courbe elliptique sur $\mathbb{F}_q$.

Considérons maintenant l'action de $\mathbb{F}_q[\varepsilon]^*$ sur $\mathbb{F}_q[\varepsilon]^3 \setminus M^3$ définie par :

$$u \bullet (X, Y, Z) = (uX, uY, uZ).$$

On note $\mathbf{P}$ l'ensemble des orbites de cette action et $[X : Y : Z]$ l'orbite de (X, Y, Z). On appelle élément d'une cubique de Weierstrass sur $\mathbb{F}_q[\varepsilon]$ tout point $[X : Y : Z]$ de $\mathbf{P}$ vérifiant l'équation de Weierstrass associée. On note $\mathcal{E}_{a,b}(\mathbb{F}_q[\varepsilon])$ l'ensemble de ces éléments.

*Laboratoire J.A. Dieudonné, U.M.R. C.N.R.S. N°6621, Université de Nice Sophia-Antipolis

On peut alors étendre la construction de corde et tangente, usuelle sur les courbes elliptiques, à l'ensemble des éléments d'une cubique de Weierstrass sur $\mathbb{F}_q[\varepsilon]$ et le munir ainsi d'une loi de groupe (cf. [**?**]).

Fixons donc une cubique de Weierstrass $\mathcal{E}_{a,b}$ sur $\mathbb{F}_q[\varepsilon]$ d'équation $Y^2Z = X^3+aXZ^2+bZ^3$. Notons alors $E_{a,b}$ sa réduction à $\mathbb{F}_q$ et N le cardinal de l'ensemble des points $\mathbb{F}_q$-rationnels de $E_{a,b}$ (noté $E_{a,b}(\mathbb{F}_q)$). L'ensemble des éléments de $\mathcal{E}_{a,b}$ est alors de cardinal $q \times N$.

En particulier, pour k dans $\mathbb{F}_q$, les éléments du type $\Theta_k = [k\varepsilon : 1 : 0]$ appartiennent à $\mathcal{E}_{a,b}(\mathbb{F}_q[\varepsilon])$. L'ensemble de ces éléments à l'infini est isomorphe à $\mathbb{F}_q$ et on obtient la suite exacte courte :

$$\begin{array}{ccccccccc} & & & \overset{\Theta}{} & & \overset{\pi}{} & & & \\ 0 & \longrightarrow & \mathbb{F}_q & \longrightarrow & \mathcal{E}_{a,b}(\mathbb{F}_q[\varepsilon]) & \longrightarrow & E_{a,b}(\mathbb{F}_q) & \longrightarrow & 0 \\ & & k & \mapsto & \Theta_k & & & & \\ & & & & [X:Y:Z] & \mapsto & [\pi(X):\pi(Y):\pi(Z)] & & \end{array}$$

Quand p ne divise pas N, cette suite exacte est scindée et $\mathcal{E}_{a,b}(\mathbb{F}_q[\varepsilon])$ est isomorphe à $\mathbb{F}_q \times E_{a,b}(\mathbb{F}_q)$. Par contre, nous verrons sur un exemple que ce n'est pas toujours le cas.

Nous donnerons des algorithmes polynomiaux en la taille de q calculant un isomorphisme entre ces deux groupes. Ainsi, les problèmes du calcul de logarithme discret sur $\mathcal{E}_{a,b}(\mathbb{F}_q[\varepsilon])$ et $\mathbb{F}_q \times E_{a,b}(\mathbb{F}_q)$ sont équivalents.

Nous montrerons ensuite qu'il y a également équivalence entre les problèmes du calcul de logarithme discret sur $\mathcal{E}_{a,b}(\mathbb{F}_q[\varepsilon])$ et $E_{a,b}(\mathbb{F}_q)$.

Enfin, nous présenterons une adaptation du système El Gamal (cf. [**?**]) dont les paramètres appartiennent à $\mathbb{F}_q[\varepsilon]$. Celle-ci aura l'avantage de simplifier les problèmes de codage.