LE PROBLÈME DU LOGARITHME DISCRET ELLIPTIQUE : INDEX ET XEDNI

Abderrahmane Nitaj

April 2001

Abstract. Le but est de présenter le problème du logarithme discret elliptique.

1. Introduction-Un peu d'histoire.

• Le problème :

Soient G un groupe cyclique noté multiplcativement, engendré par un élément g. Soit a un élément de G. Le problème du logarithme discret est la détermination du plus petit entier $x = \log_g a$ vérifiant $a = g^x$.

Tout d'abord, une formule de 1984 due à Wells [7] donne : si $G = \mathbb{F}_p = \langle g \rangle$, alors pour tout $1 \leq a \leq p-1$,

$$\log_g a = \sum_{j=1}^{p-2} (1-g^j)^{-1} a^j \pmod{p}.$$

Il est évident que cette belle formule n'est pas pratique.

• Les méthodes :

- Pas de bébé, pas de géant de Shanks, temps exponentiel en $O\left(|G|^{1/2}\right)$.

- La méthode Rho de Pollard, $G = \mathbb{F}_q^*$, temps exponentiel en $O(\sqrt{q})$.

1991 *Mathematics Subject Classification.* 11G20, 11Y16.
Key words and phrases. Logarithme discret, Courbe elliptique, Cryptographie.

- La méthode de Silver-Pohling-Hellman, $G = \mathbb{F}_q^*$, temps exponentiel en $O(\sqrt{p})$ où p est le plus grand facteur premier de $q-1$. Cet algorithme est donc efficace si p est petit, ce qui oblige les cryptographes à regarder la composition de $q-1$.

- La méthode du calcul de l'index, $G = \mathbb{F}_p^*$. Le cas rigoureux, le temps est sous-exponentiel en

$$O\left(L_p\left[\frac{1}{2}, c_1\right]\right) = O\left(e^{(c_1+o(1))(\log p)^{1/2}(\log\log p)^{1/2}}\right)$$

Le cas heuristique (dépend de certaines conjectures), d'après Gordon, le temps est sous-exponentiel en

$$O\left(L_p\left[\frac{1}{3}, c_2\right]\right) = O\left(e^{(c+o(1))(\log p)^{1/3}(\log\log p)^{2/3}}\right)$$

pour des constantes positives c_1 et c_2. Ce dernier résultat a été obtenu par Gordon en 1992, en appliquant la méthode de factorisation du crible algébrique (the Number Filed Sieve). La méthode du calcul de l'index date de 1920 (Kraitchik) et a été redécouverte par Western, Miller, Adelman, Merckle, Pollard et bien d'autres.

document

2. La méthode du calcul de l'index.

Description : Soit p un nombre premier, g un générateur de $\mathbb{F}_p^*$ et a un élément de $\mathbb{F}_p^*$. Déterminer $x = \log_g a$ vérifiant $a = g^x$.

Etape 1.

- Choisir un entier r.
- Poser $F_r = \{2, 3, 5, 7, \cdots, p_r\}$ où p_r est le r-ème nombre premier. F_r est la base de facteurs.
- Poser $\langle F_r\rangle = \{z \in \mathbb{F}_p : z = \prod_{i=1}^r p_i^{e_i}\} \leq p_r\}$. L'ensemble $\langle F_r\rangle$ est composé des nombres entiers dont les facteurs premiers sont dans F_r. Il est appelé l'ensemble des entiers F_r-lisses.

Etape 2.

- Pour $j = 0, 1, 2, \cdots$, calculer $g_j = g^j \pmod{p}$.
- Si $g_j \in \langle F_r\rangle$,factoriser :

$$g_j = \prod_{i=1}^r p_i^{e_i(j)}.$$

Cette relation donne alors l'équation linéaire :

$$j \equiv \sum_{i=1}^r e_i(j)\log_g p_i \pmod{p-1},$$

dans laquelle les inconnues sont $\log_g p_i$, $1 \leq i \leq r$.

Le calcul des quantités g_j doit se poursuivre jusqu'à l'obtention de r équations linéaires. Ainsi, avec un système (r, r), on peut calculer $\log_g p_i$, $1 \leq i \leq r$.

Etape 3.

- Pour $j = 0, 1, 2, \cdots$, calculer $a_j = ag^j \pmod p$.
- Si pour un premier entier j on a $a_j \in \langle F_r \rangle$, factoriser :

$$a_j = \prod_{i=1}^{r} p_i^{f_i}.$$

Ceci donne alors l'égalité :

$$j + \log_g a \equiv \sum_{i=1}^{n} f_i \log_g p_i \pmod{p-1},$$

d'où la valeur de $\log_g a$.

Le choix de r.

• Si r est petit, l'étape 2 sera trop longue car il est peu probable qu'un $g_j = g^j$ soit dans $\langle F_r \rangle$.

• Si r est trog grand, l'étape 2 sera aussi longue car il faut factoriser chaque g_j, d'où l'importance du choix de la méthode de factorisation (le crible algébrique est certainement le plus adapté).

• On pose

$$N(F_r) = \#\{z \in < F_r >: 1 \leq z \leq p\}.$$

Ceci donne avec $z = \prod_{i=1}^{r} p_i^{e_i}$:

$$N(F_r) = \#\{(e_1, \cdots, e_r) \in \mathbb{N}^r, \sum_{i=1}^{r} e_i \log p_i \leq \log p\}.$$

Ainsi $N(F_r)$ représente le nombre de r-uplets d'entiers positifs contenus dans le polhèdre de dimension r et de rayon $\log p$.

Soit $\Psi(x, y)$ le nombre d'éléments inférieurs à x et ayant un plus grand facteur jusquà y. Alors

$$N(F_r) = \Psi(p, p_r).$$

Il y a beaucoup de travaux qui concernent la fonction Ψ. On peut appliquer dans notre cas l'approximation suivante (Canfield, Erdös, Pomerance) :

$$\Psi(x, y) \approx x e^{-\frac{1}{2}\sqrt{\log x \log\log x}},$$

dans le cas $y \geq e^{\sqrt{\log x \log\log x}}$. En prenant $r \approx e^{\sqrt{\log p}}$, on obtient

$$r \log r \sim p_r \sim e^{\sqrt{\log p \log\log p}},$$

ce qui donne

$$N(F_r) \sim pp_r^{-\frac{1}{2}} > pe^{-\frac{1}{2}\sqrt{\log p}}.$$

La probabilité qu'un nombre $1 \leq z \leq p$ soit dans $\langle F_r \rangle$ est :

$$\frac{N(F_r)}{p-1} \approx e^{-\frac{1}{2}\sqrt{\log p}}.$$

Ainsi, le choix pour r de prendre $r \simeq e^{\sqrt{\log p}}$ représente une valeur sous-exponentielle pour r.

Les records

1. Avec Le Special Number Field Sieve (SNFS): Le record actuel est dû à D. Weber, en résolvant le challenge de Mc-Curley en 1998:

Déterminer x tel que $7^x \equiv b \pmod p$ avec b de 129 chiffres et $p = 793 \cdot \frac{7^{149}-1}{3} + 1$ de 129 chiffres aussi. Ici, les corps de nombres considérés sont très favorables au crible, d'où le terme "Special".

2. Avec Le General Number Field Sieve (GNFS): Lercier : $a^x \equiv b \pmod p$, avec $a = 2$ et $b = \lfloor 10^{119} e \rfloor$ et le 120 chiffres $p = \lfloor 10^{119}\pi \rfloor + 207819$. Ici, les corps de nombres considérés ne sont pas très favorables au crible, d'où le terme "General".

Autres méthode de factorisation : Il s'agit de factoriser un entier n. Le nombre premier p' est le plus grand facteur premier de $n-1$. Il y a cependant deux sortes d'algorithmes, les spéciaux (S) et les généraux (G). Les spéciaux exploitent la forme de n contrairement aux généraux.

Complexité des méthodes de factorisation		
Méthode	Autheur, Nature	Complexité
Rho de Pollard	$Pollard, 1975, S$	$O(\sqrt{n})$
p-1 de Pollard	$Pollard, 1974, S$	$O(sqrtp')$
Courbes elliptiques (ECM)	$Lenstra, 1985, S$	$O\left(e^{\sqrt{2\log n log\log n}}\right)$
Le crible algébrique (NFS)	$LLMP, 1989, G$	$O\left(e^{c(\log n)^{1/3}(\log\log n)^{2/3}}\right)$
Le crible quadratique (mpqs)	$Pomerance, 1984, G$	$\left(e^{\sqrt{\log n log\log n}}\right)$

LLMP=Lenstra, Lenstra, Manasse, Pollard,

L'algorithme de Gordon (Selon Weber):

Puisque $a = g^x \pmod p$, alors $1 \leq x \leq p-1$. Soit p' un grand diviseur premier de $p-1$. Si on trouve deux entiers s et t modulo $p-1$ avec $(t,q) = 1$ et si on trouve un entier w modulo p tels que

$$g^s a^t \equiv w^{p'} \pmod p,$$

alors $s + tx \equiv p' \pmod p - 1$, d'où $x = -st^{-1} \pmod{p'}$.

A développer plus tard ....

3. Le logartithme discret elliptique.

Soit G un groupe noté additivement et A et B deux éléments de G. Le problème du logarithme discret est la détermination d'un entier n (s'il existe) tel que $A = nB$.

Les algorithmes disponibles pour le cas des courbes elliptiques sont les analogues de la méthode de Shanks et celle de Pollard.

Les premiers shemas cryptographiques utilisant les courbes elliptiques furent introduits indépendament par V. Miller et N. Koblitz en 1985. L'intérêt des courbes elliptiques, est que les problèmes du logarithme discret y sont difficiles à résoudre, et aucun algorithme sous-exponentiel n'y est disponible. Un avantage évident dans ce domaine est de prendre des clées de longueur assez petites par rapport à celles requises pour RSA ou pour les corps finis (160 bits au lieu de 1024 bits).

Soit E une courbe elliptique définie sur $\mathbb{F}_p$ par l'équation :

$$E: \qquad Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \tag{1}$$

avec a_1, a_2, a_3, a_4 et $a_6 \in \mathbb{F}_p$. On pose $N_p = \#E(\mathbb{F}_p)$. Une combinaison des des algorithmes de Schoof, Elkies et Atkin (SEA) permet de calculer N_p en un temps polynômial en

$$O(\log^6 p).$$

Le problème du logarithme discret elliptique est le suivant :

Etant donné deux points S et T de $E(\mathbb{F}_p)$ vérifiant $S \in \langle T \rangle$, déterminer un entier x tel que $S = xT$. On pose alors $x = \log_T S$.

Les méthodes connues sont les suivantes :

- La méthode exhaustive. Cette méthode consiste à calculer T, $2T$, $3T$, $\cdots$ jusquà obtenir S. Ceci peut prendre N_p étapes.

- La méthode de Shanks (Baby Step, Giant Step). Cette méthode requiert $\sqrt{N_p}$ étapes.

- La méthode Rho de Pollard. Cette méthode requiert $\sqrt{\pi N_p/2}$ étapes.

- La méthode Western-Pohling-Hellman. Cette méthode requiert $\sqrt{n}$ étapes, où n est le plus grand facteur premier de N_p.

Il existe des cas de courbes elliptiques pour lesquelles le problème du logarithme discret peut être plongé dans des corps finis, et donc peuvent être considérées comme triviales pour la cryptographie.

- Les courbes supersingulières. (Menezes, Okamoto, Vanstone) Ce sont les courbes pour lesquelles $N_p = p + 1$. Le probléme du logarithme discret sur ces courbes peut être réduit au groupe multiplicatif $\mathbb{F}_p^*$.

- Les courbes elliptiques anomales "anomalous". (Samaev, Araki, Satoh, Smart) Ce sont les courbes pour lesquelles $N_p = p$. Le probléme du logarithme discret sur ces courbes peut être réduit au groupe additif $\mathbb{F}_p$.

- Les courbes spéciales. Ce sont les courbes pour lesquelles N_p n'admet que des facteurs premiers petits. Dans ce cas, la méthode de Pollard et celle de Western-Pohling-Hellman peuvent être efficacement utilisées.

4. La méthode du calcul de l'index pour les courbes elliptiques.

Soit $E/\mathbb{F}_p$ une courbe elliptique et deux points S et T de $E(\mathbb{F}_p)$ vérifiant $S \in \langle T \rangle$. On veut déterminer un entier x tel que $S = xT$. On pose alors $x = \log_T S$.

Pour appliquer la méthode du calcul de l'index dans le cas elliptique, voici comment on pourrait procéder :

Etape 1.

- Choisir une courbe elliptique $\mathcal{E}/\mathbb{Q}$ qui se réduit à $E/\mathbb{F}_p$.

Etape 2.

- Choisir un entier r.
- Choisir r points indépendants Q_1, Q_2, $\cdots$, Q_r de $\mathcal{E}/\mathbb{Q}$.
- Pour $i = 1, \cdots, r$, poser $P_i \equiv Q_i \pmod p$.

Le but est de déterminer r entiers $\log_T(P_i) \pmod{N_p}$ vérifiant $P_i = (\log_T(P_i))T$.

Etape 3.

- Pour $j = 1, 2, \cdots.$, calculer les points T, $2T$, $\cdots$, jT, $\cdots$ dans $E(\mathbb{F}_p)$, et pour chaque j, essayer de plonger jT dans un point T_j de $\mathcal{E}(\mathbb{Q})$. Ainsi, $T_j \equiv jT \pmod p$. Si le plongement estpossible, essayer d'écrire dans $\mathcal{E}(\mathbb{Q})$:

$$T_j = \sum_{i=1}^{r} n_i Q_i.$$

sinon reprendre un autre j.

Cette étape doit être poursuivie jusqu'à l'obtention de r combinaison de la forme ci-dessus.

La combinaison ci-dessus donne

$$j \equiv \sum_{i=1}^{r} n_i \log_T(P_i) \pmod{N_p},$$

avec $\log_T(P_i)$ vérifiant $P_i = (\log_T(P_i))T$, et le système de r équations aux r inconnues $\log_T(P_j)$ peut être donc résolu.

Etape 4.

- Pour $j = 0, 1, \cdots$, essayer de plonger $S + jT$ dans un point T'_j de $\mathcal{E}(\mathbb{Q})$. On doit poursuivre cette opération jusqu'à obtenir un entier j pour lequel T'_j est dans $\mathcal{E}(\mathbb{Q})$.
- Essayer décrire dans $\mathcal{E}(\mathbb{Q})$:

$$T'_j = \sum_{i=1}^{r} f_i Q_i.$$

Si cette opération réussi, alors

$$\log_T(S) + j = \sum_{i=1}^{r} f_i \log_T(P_i),$$

et donc finalement $\log_T(S)$, ce qui résoud le problème du logarithme discret.

Cette méthode ne peut être utilisée efficacement à cause des trois problèmes suivants :

Problème 1. *Il est très difficile de déterminer des courbes elliptiques définis sur $\mathbb{Q}$ ayant un grand rang.*

Le record actuellement est de 24.

Problème 2. *Il est très difficile de déterminer des courbes elliptiques définis sur $\mathbb{Q}$ engendrés par des points ayant des petites hauteurs.*

Problème 3. *Il est très dificle de plonger un point de $E(\mathbb{F}_p)$ dans un point de $\mathcal{E}(\mathbb{Q})$.*

Analyse des difficultés.

La hauteur d'un rationnel r/s est :

$$H\left(\frac{r}{s}\right) = \max(|r|, |s|).$$

La hauteur canonique d'un point $P \in \mathcal{E}(\mathbb{Q})$ est :

$$\hat{h}(P) = \frac{1}{2}\lim_{n\to\infty}\frac{1}{n^2}\log H(x(nP)),$$

ce qui défini le produit :

$$\langle P, Q\rangle = \frac{1}{2}(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)).$$

Le régulateur d'un ensemble de points $P_1, \cdots, P_r$ de $\mathcal{E}(\mathbb{Q})$ est alors :

$$R(\mathcal{E}) = \det(\langle P_i, P_j\rangle)_{1\le i,j\le r}.$$

Soit B une borne fixée. On pose

$$N(\mathcal{E}, B) = \#\{P \in \mathcal{E}(\mathbb{Q}) : H(x(P)) \le B\}.$$

Alors, on démontre que :

$$N(\mathcal{E}, B) \simeq 16\frac{1}{\sqrt{\pi r}}\left(\frac{\pi e \log B}{rR(\mathcal{E})^{1/r}}\right)^{r/2}.$$

Pour que $N(\mathcal{E}, B)$ soit assez grand, on doit donc avoir

$$\log B \ge \frac{r}{\pi e}R(\mathcal{E})^{1/r}.$$

D'autre part, on a le résultat classique suivant :

$$R(\mathcal{E})^{1/r} \ge \left(\frac{\sqrt{3}}{2}\right)^{r-1}\min_{P\in\mathcal{E}(\mathbb{Q}),\hat{h}(P)\neq 0}\hat{h}(P).$$

Une conjecture de Lang dit :

$$\hat{h}(P) \geq c_1 \log|\Delta(\mathcal{E})|,$$

où c_1 est une constante indépendante de $\mathcal{E}$ et $\Delta(\mathcal{E})$ est le discriminant de $\mathcal{E}$. On obtient ainsi

$$\log B \geq c_2 r \log|\Delta(\mathcal{E})|,$$

où c_2 est une constante. Enfin, une conjecture de Mestre donne

$$\log|\Delta(\mathcal{E}| \geq c_3 r \log r,$$

où c_3 est une constante. On obtient finalement :

$$\log B \geq c_4 r^2 \log r,$$

où c_4 est une constante.

Ainsi, si r (le rang de $\mathcal{E}$) est grand, B est très grand. Cela veut dire que même si le problème 1 est résolu, en démontrant l'existence de r (grand) générateurs de $\mathcal{E}$), le problème 2 se pose pour déterminer explicitement ces générateurs.

la probablité pour qu'un point P de $E(\mathbb{F}_p)$ soit plongé dans un point Q de $\mathcal{E}(\mathbb{Q})$ avec une hauteur inférieur à B est :

$$\frac{N(\mathcal{E}, B)}{N_p} \sim \frac{N(\mathcal{E}, B)}{p},$$

puisque, d'après le théorème de Hasse $N_p = p + 1 - t$ avec $|t| \leq 2\sqrt{p}$. Pour maximiser cette probabilité, on doit prendre $N(\mathcal{E}, B)$ proche de p. On peut prendre par exemple une constante c_5 et imposer $N(\mathcal{E}, B) \geq p/c_5$. On obtient alors :

$$\log B \geq \left(\frac{p\sqrt{\pi r}}{16c_5}\right)^{2/r} \frac{rR(\mathcal{E})^{\frac{1}{r}}}{\pi e},$$

et en utilisant l'estimation $R(\mathcal{E})^{1/r} \geq c_6 r \log r$, on obtient

$$\log B \geq \left(\frac{p\sqrt{\pi r}}{16c_5}\right)^{2/r} \frac{c_6 r^2 \log r}{\pi e}.$$

Expérimentalement, en reprenant des exemples de courbes elliptiques définies sur $\mathbb{Q}$ de grands rangs (inérieurs à 14) déterminées par Mestre, et heuristiquement, en admettant des conjectures optimistes de Lang et Mestre, Silverman et Suzuki ont explicité les constantes ci-dessus avec $p = 173$ et on obtenu la minoration suivante :

$$\log B \geq \frac{r \log(p^{11.93} r^{0.26r})}{20\pi e} \left(\frac{p\sqrt{\pi r}}{2^{10}}\right)^{2/r},$$

ce qui permet d'établir le tableau suivant

Table minimum de B		
p	r	B
2^{20}	15	$p^{3.63}$
2^{40}	40	$p^{9.95}$
2^{80}	87	$p^{22.79}$
2^{120}	134	$p^{35.81}$
2^{160}	180	$p^{48.94}$

Pour avoir une sécurité suffisante, il faut prendre $p \geq 2^{80}$, ce qui veut dire avoir une courbe elliptique de rang au moins 87 (à comparer avec le record actuel).

Conclusion et moralité : La méthode du calcul de l'index pour les courbes elliptiques aboutit a des problèmes encore plus difficiles que le problème original.

Comparaison des tailles des éléments des bases de facteurs

Dans le cas de $\mathbb{F}_p$, le plus grand facteur premier p_r vérifie $p_r \simeq r \log r$.

Dans le cas des courbes elliptiques, on a pour chaque i, $\hat{h}(Q_i) \geq c_7 r \log r$. De plus, un résultat de Silverman donne :

$$\hat{h}(Q_i) = \frac{1}{2} \log H(x(Q_i)) + c_8,$$

où c_8 est une constante positive dépendant de $\mathcal{E}$. Ainsi

$$H(x(Q_i)) \geq c_9 r^{2c_7 r}.$$

Ceci montre que la taille des générateurs dans le cas elliptique est exponentiel relativement au cas entiers.

Description des étapes

Etape 1. On veut plonger plonger $E/\mathbb{F}_p$ dans $\mathcal{E}/\mathbb{Q}$. Si E est définie par l'équation :

$$E : \qquad Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6,$$

avec a_1, a_2, a_3, a_4 et $a_6 \in \mathbb{F}_p$. Alors, si t_i, $1 \leq i \leq 7$ sont des nombres rationnels de dénominateurs premiers avec p, la courbe $\mathcal{E}/\mathbb{Q}$ définie par :

$$\begin{aligned} \mathcal{E} : \qquad & (1 + pt_1)Y^2 + (a_1 + pt_2)XY + (a_3 + pt_3)Y \\ & = (1 + pt_4)X^3 + (a_2 + pt_5)X^2 + (a_4 + pt_6)X + (a_6 + pt_7), \end{aligned}$$

vérifie $\mathcal{E} \equiv E \pmod{p}$. Le choix de valeurs t_i, $1 \leq t_i \leq 7$ est celui qui donne une courbe elliptique $\mathcal{E}/\mathbb{Q}$ de grand rang.

Etape 2.

La construction de courbes elliptiques de grand rang est un problème difficile. Ce fut Mestre qui commeça la recherche dans ce domaine.

Ancienne méthode, 1982. Cette méthode est à la base de la plupart des calculs qui ont produit des courbes elliptiques de grand rang. Soit $p[X]$ un polynôme de degré 12 à coefficients dans Q. Il existe un unique triplet $g[X]$, $r_1[X]$ et $r_2[X]$ tels que $\deg(g) = 4$, $\deg r_1, \deg r_2 \leq 3$ et $p = g^3 + r_1 g + r_2$. Soit la courbe $y^3 + r_1(x)y + r_2(x)$. Cette courbe contient 12 points $(x_i, g(x_i))$ où x_i sont les racines de p. Si $\deg r_2 \leq 2$, alors on obtient une courbe elliptique de rang au moins 11.

Nouvelle méthode, 1984. Cette méthode consiste à considérer une courbe elliptique $\mathcal{E}$ sous la forme de Weierstrass et de déterminer les coefficients a_i de telle sorte que, modulo des nombres premiers $l = 2, 3, \cdots, l_0$, $\#E(\mathbb{F}_l)$ est maximal pour la relation de Hasse. En utilisant le théorème Chinois, on peut déterminer des entiers a_i, avec la condition supplémentaire que $|\Delta(\mathcal{E})|$ soit assèz petit. Alors, en admettant la conjecture de Birch-Swinnerton-Dyer, on peut espérer un grand rang. La conjecture BSD étant la suivante :

$$\lim_{s\to 1} \frac{L(s)}{(s-1)^r} = \frac{1}{r!} L^{(r)}(1) = \frac{\Omega RC|\text{Shaf}|}{|T|^2}.$$

avec les quantités habituelles.

Etapes 3 et 4.

On veut plonger un point $P(u, v)$ de $E(\mathbb{F}_p)$ dans un point $Q(U, V)$ de $\mathcal{E}(\mathbb{Q})$. On se place alors dans le cas projectif $Q(r, s, t)$ avec des entiers r, s et t et prendre

$$r = u + pu', \qquad s = v + pv', \qquad t = 1 + pt',$$

et déterminer des entiers u', v' et t' de telle sorte que $Q(r, s, t)$ soit un point de $\mathcal{E}(\mathbb{Q})$. Cette opération conduit à la recherche de points rationnels sur une courbe elliptique.

Etant donné une base $\{Q_1, \cdots, Q_r\}$ de $\mathcal{E}(\mathbb{Q})$, il y a deux façon de déterminer les entiers $n_1, \cdots, n_r, f_1, \cdots, f_r$ dans ces étapes : la méthode de la 2-descente et la méthode du régulateur (voir partie 5).

5. La méthode du xedni

En 1998, Silverman d'une part, Kim, Cheon et Hahn d'autre part annoncèrent une méthode pour résoudre le problème du logarithme discret elliptique. Un des nombreux problèmes qui se posent dans l'application de la mathode du calcul de l'index elliptique est la détermination d'une courbe elliptique $\mathcal{E}/\mathbb{Q}$ de grand rang qui se réduit à $E/\mathbb{F}_p$ modulo p et qui contient tous les points plongés de $E(\mathbb{F}_p)$. L'idée de la méthode du xedni est inverse.

Partant de $E/\mathbb{F}_p$, choisir $2 \leq r \leq 9$ points $P_1, \cdots, P_r$ de $E(\mathbb{F}_p)$. Les transformer en points $Q_1, \cdots, Q_r$ à coefficients entiers. Déterminer une courbe elliptique $\mathcal{E}/\mathbb{Q}$ passant par ces points. Tester si les points $Q_1, \cdots, Q_r$ sont dépendants dans $\mathcal{E}(\mathbb{Q})$. Si oui, le problème du logarithme discret est résolu.

Le problème qui se pose ici donc est de trouver une courbe elliptique de rang inférieur à r.

Rappel: p est un nombre premier, $E/\mathbb{F}_p$ est une courbe elliptique, S et T sont deux points de $E(\mathbb{F}_p)$ tels que $S \in \langle T \rangle$. Déterminer un entier x tel que $S = xT$.

L'algorithme du xedni (Version très simplifiée):

Etape 1.

- Choisir un entier r, $2 \leq r \leq 9$.
- Choisir des couples d'entiers (s_i, t_i), $1 \leq i \leq r$.
- Poser dans $E(\mathbb{F}_p)$, $P_i = s_i S - t_i T$, $1 \leq i \leq r$.

Etape 2.

- Plonger les points P_i dans des points Q_i à coordonnées entières.
- Déterminer une courbe elliptique $\mathcal{E}/\mathbb{Q}$ passant par les points Q_i, $1 \leq i \leq r$.

Etape 3.

- Déterminer si les points $Q_1, \cdots, Q_r$ sont indépendants, si oui, retourner à l'étape 1.
- Déterminer des entiers $\alpha_1, \cdots, \alpha_r$ tels que, dans $\mathcal{E}(\mathbb{Q})$

$$\alpha_1 Q_1 + \cdots + \alpha_r Q_r = 0.$$

Etape 4.

- Calculer

$$s = \sum_{i=1}^{r} \alpha_i s_i, \qquad \text{et} \qquad t = \sum_{i=1}^{r} \alpha_i t_i.$$

- Si $(s, N_p) > 1$, aller à l'étape 1.
- Calculer $x = ts^{-1} \pmod{N_p}$.

Alors $\log_T(S) = x$ et le problème du logarithme discret est résolu.

Commentaires sur les étapes:

Etape 1. Le choix $2 \leq r \leq 9$ est basé sur le fait que la détermination d'une cubique (et par la suite une courbe elliptique) nécessite au plus 9 points de passage.

Etape 2. Dans cette étape, on détermine d'abord l'équation d'une cubique avec 10 coefficients :

$$u_1X^3 + u_2X^2Y + u_3XY^2 + u_4X^3 + u_5X^2Z \\ + u_6XYZ + u_7Y^2Z + u_8XZ^2 + u_9YZ^2 + u_{10}Z^3 = 0.$$

On peut alors la transformer en une équation de Weierstrass par l'algorithme de Nagell.

Etape 3. Il y a deux façon de déterminer les entiers $\alpha_1, \cdots, \alpha_r$ en question : la méthode de la 2-descente et la méthode du régulateur.

La méthode de la 2-descente. On veut déterminer des entiers $\alpha_1, \cdots, \alpha_r$ tels que $\alpha_1 Q_1 + \cdots + \alpha_r Q_r = 0$.

Etape a. Déterminer des entiers $\varepsilon_i \in \{0, 1\}$, $1 \le i \le r$ tels que

$$\varepsilon_1 Q_1 + \cdots + \varepsilon_r Q_r = 0 \pmod{2\mathcal{E}(\mathbb{Q})},$$

Si tous les coefficients ε_i sont nuls, alors, les points Q_i sont linéairement indépendants dans $\mathcal{E}(\mathbb{Q})/2\mathcal{E}(\mathbb{Q})$, et par conséquent dans $\mathcal{E}(\mathbb{Q})$.

Etape b. Déterminer un point R de $\mathcal{E}(\mathbb{Q})$ tel que $2R = \varepsilon_1 Q_1 + \cdots + \varepsilon_r Q_r$. Si les racines du polynôme de 2-division ne sont pas rationnelles, alors R est unique. En effet, si V est un point de 2-torsion, on peut utiliser la relation $2V = 0$ si et seulement si $\psi_2(V) = 0$ avec $\psi_2^2(X) = 4X^3 + b_2X^2 + 2b_4X + b_6$.

Etape c. Si R n'est pas un point de torsion, soit j un entier tel que $\varepsilon_j \neq 0$. On remplace le point Q_j par R et on recommence à l'étape a.

Cette étape peut durer assez longtemps, dans ce cas on peut tester si les points R n'apparaissent pas deux fois, ou bien on arrête carrément les calculs.

Etape d. Si R est un point de torsion, alors en multipliant par son ordre, et en remplaçant tous les points R de l'étape b, on obtient une relation entre les points Q_i, ce qui donne les valeurs des α_i.

Cette méthode est maintenant classique et est implémentée dans de nombreux systèmes de calculs (Mwrank, Simath, Lidia,...). Cette méthode donne une solution en un temps polynômial en $\max_i(\hat{h}(Q_i))$.

La méthode du régulateur. Cette méthode consiste à calculer le régulateur $\langle Q_i, Q_j\rangle_{1\le i,j\le r}$, et si ce déterminant est proche de 0, on utilise l'algorithme LLL pour déterminer une relation linéaire sur les colonnes du déterminant, ce qui donne la réponse voulue.

Etape 4. Si dans $\mathcal{E}(\mathbb{Q})$ on a $\alpha_1 Q_1 + \cdots + \alpha_r Q_r = 0$, alors dans $E(\mathbb{F}_p)$ on a $\alpha_1 P1 + \cdots + \alpha_r P_r = 0$ et puisque $Q_i = s_i S - t_i T$, alors

$$\left(\sum_{i=1}^{r} \alpha_i s_i\right) S - \left(\sum_{i=1}^{r} \alpha_i t_i\right) T = sS - tT = 0,$$

et donc $(sx - t)T = 0$, où x vérifie $S = xT$. Comme dans $E(\mathbb{F}_p)$ on a $N_pT = 0$, alors $sx - t \equiv 0 \pmod{N_p}$, ce qui justifie le test $(s, N_p) > 1$.

Théorème (Jacobson, Koblitz, Silverman, Stein, Teske). *La probalité pour que de la méthode du xedni résolve le problème du logarithme discret est inférieure à C_0/p, où C_0 est une constante qui ne dépend que de certaines conjectures.*

On suppose que les points Q_i, $1 \le i \le r$ sont linéairement dépendants. Soit $E' = \langle Q_1, \cdots, Q_r\rangle$. Soit r' le rang de E'. Alors $r' \le r - 1$. Ainsi E'/E'_{tors} est engendré par r' points $Q'_1, \cdots, Q'_{r'}$. Soit T' le nombre de points de torsion de E'. Alors le théorème de Mazur donne $T' \le 16$. Soit R' le régulateur de E', i.e. $R' = \det(\langle < Q_i, Q_j\rangle)_{1\le i,j\le r'}$. Pour $B > 0$, on pose

$$N(B) = \#\{Q \in E' : \hat{h}(Q) \le B\}.$$

Alors, on a :

$$N(B) = T' \frac{V(r')}{\sqrt{R'}} B^{r'/2} + O\left(B^{(r'-1)/2}\right),$$

où $V(r')$ est le volume de la sphère de dimension r' et de rayon 1.

Pour r' assez grand, on peut utliser la formule de Stirling qui donne :

$$V(r') \approx \frac{1}{\sqrt{\pi r}} \left(\frac{2\pi e}{r}\right)^{r/2}.$$

D'autre part, si on pose $m = \min_{Q\in\mathcal{E}(\mathbb{Q}),\hat{h}(Q)\neq 0} \hat{h}(Q)$, alors

$$R' \geq \left(\frac{\sqrt{3}}{2}\right)^{r'(r-1)} m^{r'}.$$

Ceci donne alors

$$N(B) < T'V(r') \left(\frac{\sqrt{3}}{2}\right)^{-r'(r'-1)/2} \left(\frac{B}{m}\right)^{r'/2} + O\left(B^{(r'-1)/2}\right),$$

D'autre part, puisque $\sqrt{\hat{h}}$ est est une distance, alors :

$$\sqrt{\hat{h}}\left(\sum_{i=1}^{r} n_i Q_i\right) \leq \sum_{i=1}^{r} \sqrt{\hat{h}}(n_i Q_i) \leq r \max_{1\leq i\leq r} n_i \max_{1\leq i\leq r} \sqrt{\hat{h}}(Q_i).$$

En posant $\mathcal{M} = \max_{1\leq i\leq r} \hat{h}(Q_i)$ et $C = \max_{1\leq i\leq r} n_i$, on obtient :

$$\hat{h}\left(\sum_{i=1}^{r} n_i Q_i\right) \leq (r^2 C^2)\mathcal{M}.$$

On peut donc prendre $B = (r^2C^2)\mathcal{M}$, ce qui donne :

$$N(B) < T'V(r') \left(\frac{\sqrt{3}}{2}\right)^{-r'(r'-1)/2} (rC)^{r'} \left(\frac{\mathcal{M}}{m}\right)^{r'/2}.$$

Comme il y a $(2C)^r$ points de la forme $\sum_{i=1}^{r} n_i Q_i$ avec $|n_i| \leq C$, si on a

$$(2C)^r > T'V(r') \left(\frac{\sqrt{3}}{2}\right)^{-r'(r'-1)/2} (rC)^{r'} \left(\frac{\mathcal{M}}{m}\right)^{r'/2},$$

alors il y a deux points identiques avec des coefficients non tous égaux, ce qui signifie certifie que les points Q_i, $1 \leq i \leq r$ sont linéairement dépendants, en explicitant les quantités α_i. On pose

$$C' = \frac{\log|\Delta|}{\mathcal{M}},$$

où Δ est le dsicriminant de la courbe $\mathcal{E}$. La conjecture de Lang donne alors

$$m = \min_{Q\in\mathcal{E}(\mathbb{Q}),\hat{h}(Q)\neq 0} \hat{h}(Q) \geq C_L \log|D| \geq C'C_L\mathcal{M},$$

et on obtient ainsi la condition suffisante :

$$(2C)^r > T'V(r')\left(\frac{\sqrt{3}}{2}\right)^{-r'(r'-1)/2}(rC)^{r'}(C'C_L)^{-r'/2}.$$

Comme $r' \leq r-1$, alors il suffit d'avoir

$$C \geq T'V(r-1)\left(\frac{\sqrt{3}}{2}\right)^{-(r-1)(r-2)/2}\left(\frac{r}{2}\right)^{r-1}(C'C_L)^{-(r-1)/2}.$$

Ainsi, on peut donc avoir des coefficients n_i de magnitude C. On a alors pour les points P_i, $1 \leq i \leq r$ de la courbe $E/\mathbb{F}_p$,

$$\#\{P = \sum_{i=1}^{r} n_iP_i : \max|n_i| \leq C\} \approx (2C)^r,$$

et la probabilité pour qu'une combinaison soit nulle est donc

$$\frac{(2C)^r}{p} = \frac{C_0}{p},$$

ce qui prouve le théorème puisque $2 \leq r \leq 9$.

Numériquement, On prend les hypothèses suivantes :
- pour le nombre de points de torsion, $T' = 1$,
- pour la constante de Lang : $C_L \geq 0.00005$,
- Pour la constante $C' = \log|D|/\max_{1\leq i\leq r}\hat{h}(Q_i)$, on prend

$$C' = \begin{cases} 12(1+3r/(7-r)) & \text{si } 2 \leq r \leq 6, \\ 110(1+3r/(10-r)) & \text{si } 7 \leq r \leq 9, \end{cases}$$

On obtient ainsi une valeur explicite pour C, puis pour C_0, qui ne dépend que r, ce qui donne le tableau suivant :

C **et** C_0		
r	$C \approx$	$C_0 \approx$
2	$10^{1.8}$	10^{4}
3	$10^{3.8}$	10^{12}
4	$10^{5.6}$	10^{23}
5	$10^{7.5}$	10^{38}
6	$10^{8.9}$	10^{54}
7	$10^{9.2}$	10^{65}
8	$10^{10.4}$	10^{84}
9	10^{11}	10^{100}

Expérimentalement, Jacobson et al. on testé l'algorithme du Xedni avec $r = 2, 3, 4$ pour des petites valeurs de p ($p = 17$, 67, 5167), et on dressé le tableaux suivant :

Expériences		
r	*#courbes*	*#courbes positives*
2	200000	2895
3	200000	21165
4	200000	10698

Conclusion : En considérant l'application de $\mathbb{Z}^r$ dans $E(\mathbb{F}_p)$ définie par :

$$(n_1, \cdots, n_r) \to n_1P_1 + \cdots + n_rP_r,$$

avec $|n_i| \leq C$ pour une constante C, les points $n_1P_1 + \cdots + n_rP_r$ sont équirépartis. La probabilité pour que qu'un point vérifie $n_1P_1 + \cdots + n_rP_r = 0$ est $(2C)^r/p$. Il suffit donc de prendre C vérifiant $(2C)^r \approx p$ et donc $C = O\left(p^{1/r}\right)$ avec $2 \leq r \leq 9$. Deux possibilités se posent alors :

• Si les points Q_i de $\mathcal{E}(\mathbb{Q})$, images des points P_i de $E(\mathbb{F}_p)$ par le plongement, sont linéirement dépendants, l'algorithme du xedni donne la réponse avec des coefficients n_i de magnitude $C = O(p^{1/r})$.

• Si les points Q_i sont indépendants, alors il faut changer de paramètres à l'étape 1 ou 2.

Ainsi, l'algorithme du xedni est en $O(p)$, ce qui n'est pas pratique pour les valeurs prises pour p en cryptographie.

References

1. Kim, Hwan Joon; Cheon, Jung Hee; Hahn, Sang Geun, *Elliptic curve lifting problem and its applications.*, Proc. Japan Acad. Ser. A Math. Sci. **75** (1999), 166-169..
2. ———, *On remarks of lifting problems for elliptic curves.*, Adv. Stud. Contemp. Math. (Pusan) 2 (2000), **2** (2000), 21-36..
4. Jacobson, Michael J.; Koblitz, Neal; Silverman, Joseph H.; Stein, Andreas; Teske, Edlyn, *Analysis of the xedni calculus attack*, Des. Codes Cryptogr. 20 (2000), no. 1, **20** (2000), 41-64..
5. Silverman, Joseph H., *The xedni calculus and the elliptic curve discrete logarithm problem*, Des. Codes Cryptogr. **20** (2000), 5–40..
6. Silverman, Joseph H.; Suzuki, Joe, *Elliptic curve discrete logarithms and the index calculus*, In Advances in cryptology - ASIACRYPT '98. Proceedings. Berlin: Springer. Lect. Notes Comput. Sci. **1514** (1998), 5–40..
7. Wells, Albert L.jun., *A polynomial form for logarithms modulo a prime*, IEEE Trans. Inf. Theory **30** (1984), 845-846.