www.thalesgroup.com

Familles de courbes hyperelliptiques de genre 2 calcul de l'ordre de la jacobienne et constructions pour les couplages

Aurore Guillevic et Damien Vergnaud

Séminaire CARAMEL, Nancy

THALES

LETTRES SCIENCES ECOLE NORMALE SUPERIEURE

Plan

Plan

Cryptographie à clé publique

Dans un groupe cyclique $\mathbb{G}$ d'ordre $n = \prod {r_i}^{e_i}$, r_i premier

- Problème du log discret difficile
- Attaque générique de Pohlig-Hellman en $O(\sum e_i(\log n + \sqrt{r_i}))$
  - $O(\sqrt{r})$ avec $r = \max(r_i)$
- Si $\mathbb{G} = \mathbb{F}_p^*$, attaque par calcul d'indice
  - $n = p - 1$ de taille comparable aux tailles RSA
- Si G est une jacobienne de courbe de genre $g > 2$, attaque en $O(q^{2-2/g})$
  - $g = 1$ ou 2

Cryptographie à clé publique

Instanciations :

- 1977, Diffie-Hellman : groupe multiplicatif d'un corps fini $\mathbb{F}_p^*$, $n = p - 1$
  - Attaques génériques : n contient un grand facteur premier r.
  - Attaques sous-exponentielles : n très grand.
- 1985, Koblitz, Miller : groupe de points d'une courbe elliptique sur un corps fini
  - À ce jour, attaques sur les courbes de trace 1, supersingulières, définies sur $\mathbb{F}_{2^m}$, $\mathbb{F}_{3^m}$, $\mathbb{F}_{p^k}$.
- 1989, Koblitz : jacobienne de courbes de genre supérieur
  - 2000, Gaudry : attaque sous-exponentielle pour les genres à partir de 4.
  - Pour $g \geqslant 3$, attaque en $O(q^{2-2/g})$

$\rightarrow$ La plupart des courbes en genre 1 et 2.

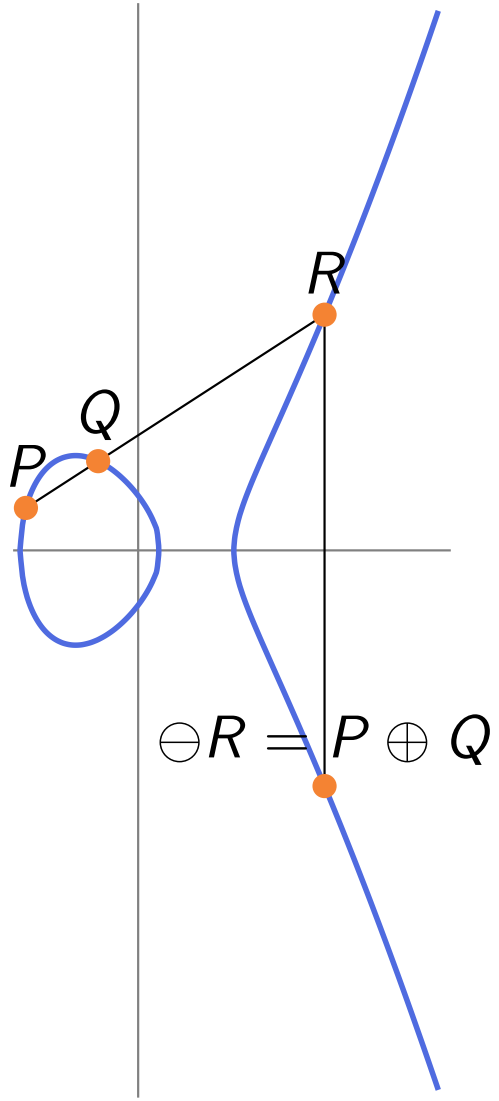
Courbes elliptiques

Formes réduites de Weierstraß sur $\mathbb{F}_q$, $q = p^n$, $p \geqslant 5$, $a, b, c \in \mathbb{F}_q$

$$E(\mathbb{F}_q) = \left\{ \begin{array}{l} (x, y) \in \mathbb{F}_q \times \mathbb{F}_q \text{ vérifant} \\ y^2 = x^3 + ax + b \end{array} \right\} \cup \{\mathcal{O}\}$$

est un groupe additif d'élément neutre $\mathcal{O}$ (noté aussi P_∞).

$$P \oplus Q \oplus R = \mathcal{O} \text{ d'où } P \oplus Q = \ominus R$$



Construction d'une courbe

$$E(\mathbb{F}_q) : y^2 = x^3 + ax + b, \qquad 4a^3 + 27b^2 \neq 0$$

Construire un groupe d'ordre r premier sur les points de la courbe.

- $\#E(\mathbb{F}_q) = q + 1 - t$ avec $|t| \leqslant 2\sqrt{q} \rightarrow \#E(\mathbb{F}_q) \sim q$
- Tirer $a, b \in \mathbb{F}_q$, calculer la trace t avec SEA (Schoof-Elkies-Atkin)
  - Vérifier que $t \not\equiv 0 \mod p$ avec $q = p^n$ (courbe supersingulière, attaque avec un couplage)
  - vérifier que $t \neq 1$ (courbe anomale)
- Calculer $\#E(\mathbb{F}_q) = q + 1 - t$,
- Jusqu'à ce qu'il soit rugueux, i.e. quasiment premier ($r \cdot h$ avec r premier et h très petit).

Cryptographie avec couplage

Pairing : $\begin{array}{ccc} \mathbb{G}_1 \times \mathbb{G}_2 & \to & \mathbb{G}_T \\ (P_1, P_2) & \mapsto & e(P_1, P_2) \end{array}$

- bilinéaire
- non dégénéré
- calculable efficacement

- Chiffrement basé sur l'identité
- Diffusion chiffrée
- Signatures courtes
- Traçage de traîtres
- Proxy re-encryption

Instanciation

- couplages de Weil ou Tate et leurs variantes
- sur des courbes elliptiques appropriées

Instanciation d'un couplage sur une courbe

$$\begin{array}{rccc} \text{Pairing :} & \mathbb{G}_1 \times \mathbb{G}_2 & \rightarrow & \mathbb{G}_T \\ & (P_1, P_2) & \mapsto & e(P_1, P_2) \end{array}$$

- $\mathbb{G}_1, \mathbb{G}_2$ sous-groupes distincts d'ordre r
- r^2 points d'ordre r sur la courbe elliptique: $\#E[r] = r^2$
- $\mathbb{G}_1 \subset E(\mathbb{F}_q)$, $\mathbb{G}_2 \not\subset E(\mathbb{F}_q)$ ($r \mid \#E(\mathbb{F}_q)$, $r^2 \nmid \#E(\mathbb{F}_q)$)
- soit k le plus petit entier tel que $r \mid q^k - 1$
  - $\mathbb{G}_1 \subset E(\mathbb{F}_q)$: la 1re dim de $E[r]$ est sur $\mathbb{F}_q$
  - $\mathbb{G}_2 \subset E(\mathbb{F}_{q^k})$: la 2e dim de $E[r]$ est sur $\mathbb{F}_{q^k}$
  - $\mathbb{G}_T \subset \mathbb{F}^*_{q^k}$

Considérations de sécurité

Niveau de sécurité par rapport à un calcul de log discret :

- Sur le sous-groupe d'ordre r premier de $E(\mathbb{F}_p)$:
  - Attaque générique en $O(\sqrt{r})$
  - Pour n bits de sécurité, prendre $\log_2 r = 2n$
- Sur $\mathbb{F}_{p^k}^*$:
  - Attaques sous-exponentielles
    $O(\exp(1.923(\log N)^{1/3}(\log\log N)^{2/3}))$ avec $N = p^k - 1$
  - Considéré comme équivalent à une taille RSA

Recommandations NIST 2007

Niveau de sécurité (bits)	Taille $\log_2 r$ du sous-groupe de $E(\mathbb{F}_p)$	Taille de $\mathbb{F}_{p^k}^*$ $k \log p$
112	224 – 255	2048
128	256 – 383	3072
256	512 +	15360

j-invariant, isomorphisme et isogénie

j-invariant

$$j_E = 1728\frac{4a^3}{4a^3 + 27b^2}$$

Théorème

- $E(\mathbb{F}_q)$ et $E'(\mathbb{F}_q)$ sont isomorphes $\Rightarrow$ elles ont le même j-invariant.
- $E(\mathbb{F}_q)$ et $E'(\mathbb{F}_q)$ ont le même j-invariant $\Rightarrow$ elles sont isomorphes sur $\overline{\mathbb{F}_q}$.
  - $p \geqslant 5$, $q = p^n$: sur $\mathbb{F}_q, \mathbb{F}_{q^2}, \mathbb{F}_{q^4}, \mathbb{F}_{q^3}$ ou $\mathbb{F}_{q^6}$.
  - $E'(\mathbb{F}_q) : y^2 = x^3 + a\omega^4 x + b\omega^6$, $(x, y) \mapsto (\omega^2 x, \omega^3 y)$

j-invariant, isomorphisme et isogénie

Isogénie

une isogénie entre deux courbes est un morphisme de courbes (qui préserve l'élément neutre de la loi de groupe).

Exemple : doublement d'un point, Frobénius $(x, y) \mapsto (x^p, y^p)$.

Théorème

E et E' ont même nombre de points sur $\mathbb{F}_q \Leftrightarrow$ elles sont isogènes sur $\mathbb{F}_q$.

Il existe un morphisme de E vers E' et un morphisme (dual) de E' vers E définis sur $\mathbb{F}_q$ qui ne sont a priori pas des isomorphismes et les courbes n'ont a priori pas le même j-invariant.

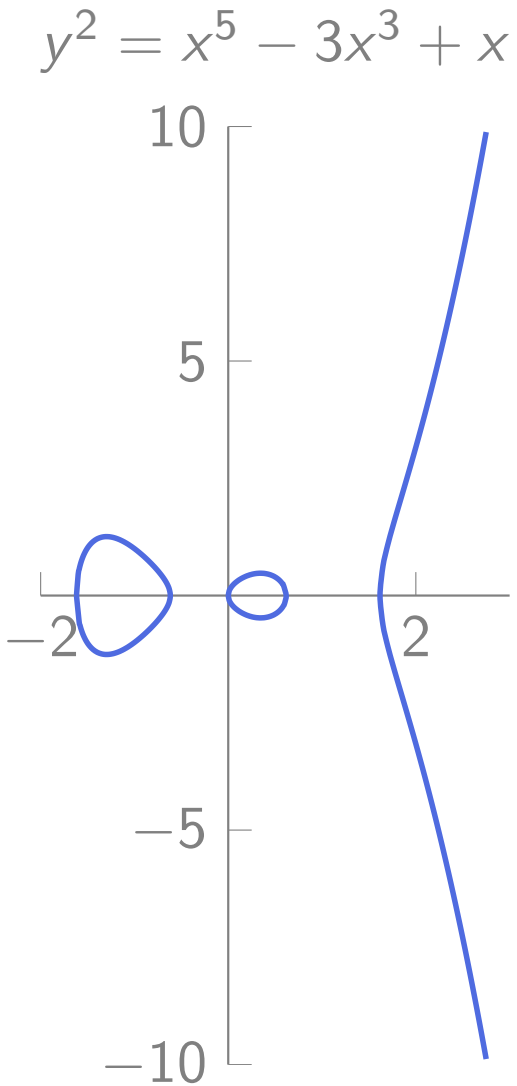
Jacobienne en genre 2

Courbes hyperelliptiques de genre g :

$$\mathcal{C} : y^2 + h(x)y = f(x)$$

- $g = \lfloor \frac{\deg(f)-1}{2} \rfloor$ et $\deg(h) \leqslant g$
- f unitaire
- $\forall (x, y) \in \mathbb{F}_q \times \mathbb{F}_q, 2y + h(x) \neq 0$ et $f'(x) - h'(x)y \neq 0$

Ce n'est pas un groupe : on construit la **jacobienne**. Au lieu de manipuler des points, on manipule des couples de points.

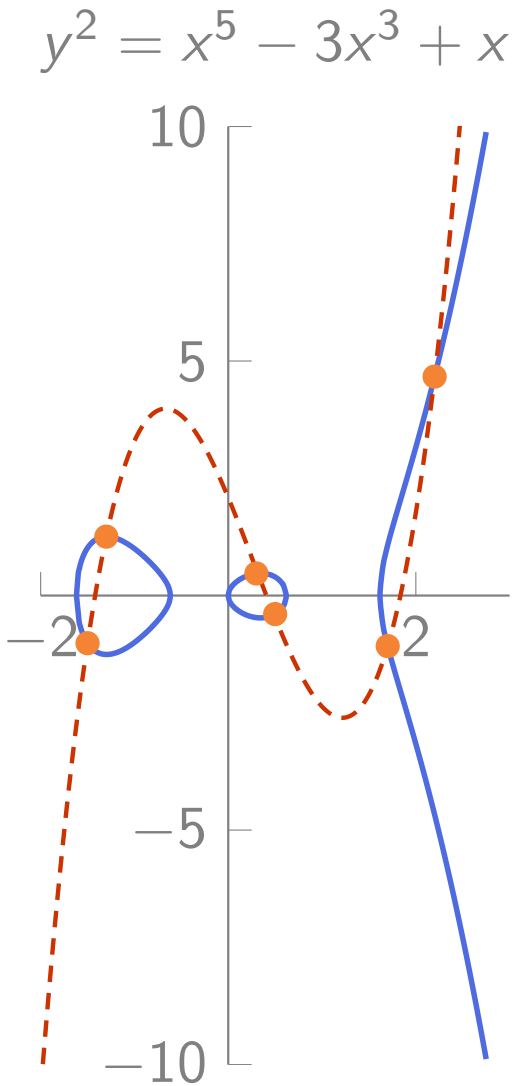


Jacobienne en genre 2 : loi de groupe

- On additionne 2 couples de points $(P_1, P_2) \oplus (Q_1, Q_2)$
- Géométriquement : on trace la cubique qui passe par ces 4 points
- $\rightarrow$ elle coupe $\mathcal{C}$ en 2 autres points (R_1, R_2).
- $(P_1, P_2) \oplus (Q_1, Q_2) \oplus (R_1, R_2) = \mathcal{O}$ d'où

$$(P_1, P_2) \oplus (Q_1, Q_2) = (-R_1, -R_2)$$

La **jacobienne** est notée $J_{\mathcal{C}}$.



Jacobienne en genre 2 : Comptage de points

$$\begin{aligned} \#J_C(\mathbb{F}_q) &= q^2 + 1 - (1+q)a_q + b_q \\ &\sim q^2 \end{aligned}$$

- Pour avoir un groupe d'ordre $\#J_C(\mathbb{F}_q)$ de 256 bits : prendre $\log q \approx 128$
- Coordonnées (x, y) d'un point de taille deux fois plus petite
- Mais on calcule avec des couples de points :
  - Même coût en bande passante que pour les courbes elliptiques

Points limitants :

- Pas encore d'algorithme aussi efficace que SEA pour calculer l'ordre de la jacobienne *[GaudryKohelSmith11]*, *[GaudrySchost11]*
- Arithmétique très complexe sur la jacobienne

Jacobienne en genre 2

$\rightarrow$ on va étudier deux cas particuliers :

$$\mathcal{C}_5(\mathbb{F}_q) : Y^2 = X^5 + aX^3 + bX, \text{ avec } a, b \neq 0 \in \mathbb{F}_q$$

$$\mathcal{C}_6(\mathbb{F}_q) : Y^2 = X^6 + aX^3 + b, \text{ avec } a, b \neq 0 \in \mathbb{F}_q$$

d'après *[Satoh09]* et *[FreemanSatoh11]*,

- puis construire une extension de $\mathbb{F}_q$ où la jacobienne se sépare en deux courbes elliptiques;
- compter le nombre de points de chaque courbe;
- en déduire le nombre de points de la jacobienne sur l'extension;
- redescendre au nombre de points de la jacobienne sur $\mathbb{F}_q$.

Plan

Décomposition en deux courbes elliptiques

$$\mathcal{C}_5(\mathbb{F}_q) : Y^2 = X^5 + aX^3 + bX, \text{ avec } a, b \neq 0 \in \mathbb{F}_q$$

L'isogénie est à coefficients en $\sqrt{b}$ et $\sqrt[4]{b}$.
Si $\sqrt{b}, \sqrt[4]{b} \in \mathbb{F}_q$: immédiat

$$J_{\mathcal{C}_5}(\mathbb{F}_q) \overset{\text{isogénie}}{\longleftrightarrow} E_1(\mathbb{F}_q) \times E_2(\mathbb{F}_q)$$

$$E_1(\mathbb{F}_q) : Y^2 = \delta(X-1)(X^2 - \gamma X + 1)$$
$$E_2(\mathbb{F}_q) : Y^2 = -\delta(X-1)(X^2 - \gamma X + 1)$$

Décomposition en deux courbes elliptiques

$$\mathcal{C}_5(\mathbb{F}_q) : Y^2 = X^5 + aX^3 + bX, \text{ avec } a, b \neq 0 \in \mathbb{F}_q$$

L'isogénie est à coefficients en $\sqrt{b}$ et $\sqrt[4]{b}$.
Si $\sqrt{b}, \sqrt[4]{b} \in \mathbb{F}_{q^2}$, il faut redescendre sur $\mathbb{F}_q$

$$\begin{array}{ccc} J_{\mathcal{C}_5}(\mathbb{F}_{q^2}) & \overset{\text{isogénie}}{\longleftrightarrow} & E_1(\mathbb{F}_{q^2}) \times E_2(\mathbb{F}_{q^2}) \\ \downarrow & & \\ J_{\mathcal{C}_5}(\mathbb{F}_q) & & \end{array}$$

$$E_1(\mathbb{F}_{q^2}) : Y^2 = \delta(X-1)(X^2 - \gamma X + 1)$$
$$E_2(\mathbb{F}_{q^2}) : Y^2 = -\delta(X-1)(X^2 - \gamma X + 1)$$

Décomposition en deux courbes elliptiques

$$\mathcal{C}_5(\mathbb{F}_q) : Y^2 = X^5 + aX^3 + bX, \text{ avec } a, b \neq 0 \in \mathbb{F}_q$$

L'isogénie est à coefficients en $\sqrt{b}$ et $\sqrt[4]{b}$.
Si $\sqrt{b}, \sqrt[4]{b} \in \mathbb{F}_{q^4}$, il faut redescendre sur $\mathbb{F}_q$ en deux étapes

$$\begin{array}{ccc} J_{\mathcal{C}_5}(\mathbb{F}_{q^4}) & \overset{\text{isogénie}}{\longleftrightarrow} & E_1(\mathbb{F}_{q^4}) \times E_2(\mathbb{F}_{q^4}) \\ \downarrow & & \\ J_{\mathcal{C}_5}(\mathbb{F}_{q^2}) & & \\ \downarrow & & \\ J_{\mathcal{C}_5}(\mathbb{F}_q) & & \end{array}$$

$$E_1(\mathbb{F}_{q^4}) : Y^2 = \delta(X-1)(X^2 - \gamma X + 1)$$
$$E_2(\mathbb{F}_{q^4}) : Y^2 = -\delta(X-1)(X^2 - \gamma X + 1)$$

Fonction Zêta

$$\begin{aligned} \#J_{\mathcal{C}_5}(\mathbb{F}_{q^2}) &= q^4 + 1 - (1+q^2)a_2 + b_2 \\ \#J_{\mathcal{C}_5}(\mathbb{F}_q) &= q^2 + 1 - (1+q)a_1 + b_1 \end{aligned}$$

Le calcul explicite est fait en fassant par les fonctions zêta. On obtient un système facile à résoudre

$$\begin{cases} a_2 &= (a_1)^2 - 2b_1 \\ b_2 &= (b_1)^2 - 4qb_1 + 2q^2 - 2qa_2 \end{cases}$$

On déduit les coeffs a_2, b_2 en fonction de la trace d'une courbe elliptique grâce à l'isognie.

- si l'isogénie est défninie sur $\mathbb{F}_{q^2}$, $(a_2, b_2) = (2t_2, (t_2)^2 + 2q^2)$ avec t_2 la trace de E_1et E_2 sur $(\mathbb{F}_{q^2})$.

Fonction Zêta

$$\begin{cases} (a_1)^2 - 2b_1 - 2t_2 &= 0 \quad (2) \\ (b_1)^2 - 4qb_1 - 4qt_2 - (t_2)^2 &= 0 \quad (1) \end{cases}$$

(1) $b_1 = 4q + t_2$, $a_1 = \pm 2\sqrt{2q + t_2}$

(2) $b_1 = -t_2$, $a_1 = 0$

- si $2q + t_2$ n'est pas un carré, $b_1 = -t_2$, $a_1 = 0$ et $\#J_{\mathcal{C}_5}(\mathbb{F}_q) = q^2 + 1 - t_2$.
- cas spécial : si $2q + t_2 = y^2$, il y a deux solutions supplémentaires (détails dans l'article).

Résultats

$\mathcal{C}_5(\mathbb{F}_q) : Y^2 = X^5 + aX^3 + bX$ avec $a, b \neq 0 \in \mathbb{F}_q$
$E_1, E_2(\mathbb{F}_q[\sqrt[4]{b}]) : Y^2 = \pm\delta(X-1)(X^2 - \gamma X + 1)$
$E_1', E_2'(\mathbb{F}_q[\sqrt{b}]) : Y^2 = \pm(X-1)(X^2 - \gamma X + 1)$

Nombre de points de la jacobienne de $\mathcal{C}_5(\mathbb{F}_q)$

1. Isogénie sur $\mathbb{F}_q$: $\#J_{\mathcal{C}_5}(\mathbb{F}_q) = (q + 1 - t_1)(q + 1 \pm t_1)$.
2. Isogénie sur $\mathbb{F}_{q^2}$, $\sqrt{b} \notin \mathbb{F}_q$: $\#J_{\mathcal{C}_5}(\mathbb{F}_q) = q^2 + 1 - t_2$.
3. Isogénie sur $\mathbb{F}_{q^2}$, $\sqrt{b} \in \mathbb{F}_q$: $\#J_{\mathcal{C}_5}(\mathbb{F}_q) = q^2 + 1 - 2q + (t_1')^2$.
4. Isogénie sur $\mathbb{F}_{q^4}$: $\#J_{\mathcal{C}_5}(\mathbb{F}_q) = q^2 + 1 - 2n(q+1) + 2n^2$, avec $n \in \mathbb{Z}$ t.q. $2q \pm t_2' = 2n^2$.
5. $+$ cas spéciaux détaillés dans l'article.

Courbe $\mathcal{C}_5$, exemple

- p premier, $p \equiv 1 \mod 4$
- On cherche une courbe $\mathcal{C}_5(\mathbb{F}_p) : Y^2 = X^5 + aX^3 + bX$ dont la jacobienne admet un grand sous-groupe d'ordre r premier $\#J_{\mathcal{C}_5}(\mathbb{F}_p) = rh = p^2 + 1 - 2n(p+1) + 2n^2$ avec $2p - t_2 = 2n^2$.
- Tant que l'ordre trouvé n'est pas satisfaisant :
  1. On tire $a \in \mathbb{F}_p$, $b \in \mathbb{F}_p$ non carré;
  2. soit $\gamma = \frac{2a-12\sqrt{b}}{a+2\sqrt{b}}$, on construit $E_1^{'}(\mathbb{F}_{p^2}) : Y^2 = (X-1)(X^2 - \gamma X + 1)$ et on calcule sa trace $t_2^{'}$ avec SEA;
  3. il existe $n \in \mathbb{Z}$ tel que $2p \pm t_2^{'} = 2n^2$, puis on calcule $\#J_{\mathcal{C}_5}(\mathbb{F}_p) = p^2 + 1 - 2n(p+1) + 2n^2$

Courbe $\mathcal{C}_5$, exemple

$p =$ 0x84c4f7a6b9aee8c6b46b34fa2a2bae69 $= 1 \mod 8$.
Le 17e essai donne $b = -38$,
$t_2' =$ 0x702461acf6a929e295786868f846ab40 $= 0 \mod 2$,
$b_1 = 2p - t_2' = 2n^2$ comme prévu avec
$n =$ − 0x8c1fc81b9542ce23.
On trouve $\#J_{\mathcal{C}_5}(\mathbb{F}_p) = 2^5 r$ avec r premier de 250 bits, pour une taille cryptographique proche de 128 bits de sécurité.
$r =$ 0x226ddb780b2ded62d1d70138d9c7361794679a609fbe5ae85918c88f5b6ea7d.

Courbe $\mathcal{C}_6$

$$\mathcal{C}_6(\mathbb{F}_q) : Y^2 = X^6 + aX^3 + b, \text{ avec } a, b \neq 0 \in \mathbb{F}_q$$

Soit $c = a/\sqrt{b}$ tel que $c \neq \pm 2$.

$$\begin{array}{ccccc}
J_{\mathcal{C}_6}(\mathbb{F}_q[\sqrt[6]{b}]) & \overset{\text{isogénie}}{\longleftrightarrow} & J_{\mathcal{C}_6'}(\mathbb{F}_q[\sqrt[6]{b}]) & & \\
\vert & & \vert & & \\
J_{\mathcal{C}_6}(\mathbb{F}_q[\sqrt{b}]) & & J_{\mathcal{C}_6'}(\mathbb{F}_q[\sqrt{b}]) & \overset{\text{isogénie}}{\longleftrightarrow} & E_c(\mathbb{F}_q[\sqrt{b}]) \times E_{-c}(\mathbb{F}_q[\sqrt{b}]) \\
\vert & & & & \\
J_{\mathcal{C}_6}(\mathbb{F}_q) & & & &
\end{array}$$

$$E_c^{\text{red}}(\mathbb{F}_q[\sqrt{b}]) : Y^2 = X^3 + 3(2c-5)X + c^2 - 14c + 22$$
$$E_{-c}^{\text{red}}(\mathbb{F}_q[\sqrt{b}]) : Y^2 = X^3 - 3(2c+5)X + c^2 + 14c + 22$$

Courbe $\mathcal{C}_6$, Résultats

$\mathcal{C}_6(\mathbb{F}_q) : Y^2 = X^6 + aX^3 + b$, avec $a, b \neq 0 \in \mathbb{F}_q$
$E^{\text{red}}_{\pm c}(\mathbb{F}_q[\sqrt{b}]) : Y^2 = X^3 + 3(\pm 2c - 5)X + c^2 \mp 14c + 22$,
$c = a/\sqrt{b}$

Nombre de points de la jacobienne de $\mathcal{C}_6(\mathbb{F}_q)$

1. Isogénie sur $\mathbb{F}_q$: $\#J_{\mathcal{C}_6}(\mathbb{F}_q) = (q + 1 - t_1)(q + 1 \pm t_1)$.
2. Isogénie sur $\mathbb{F}_{q^2}$: $\#J_{\mathcal{C}_6}(\mathbb{F}_q) = q^2 + 1 - t_2$.
3. Isogénie sur $\mathbb{F}_{q^3}$: $\#J_{\mathcal{C}_6}(\mathbb{F}_q) = q^2 - q + 1 + (1 + q + t_1)t_1$.
4. Isogénie sur $\mathbb{F}_{q^6}$: $\#J_{\mathcal{C}_6}(\mathbb{F}_q) = q^2 + q + 1 + (q + 1 + n)3n$, avec $n \in \mathbb{Z}$ tel que $2q - t_2 = 3n^2$.
5. $+$ cas spéciaux détaillés dans l'article.

Plan

Cryptographie avec couplage

Pairing : $\begin{array}{ccc} \mathbb{G}_1 \times \mathbb{G}_2 & \to & \mathbb{G}_T \\ (P_1, P_2) & \mapsto & e(P_1, P_2) \end{array}$

- bilinéaire
- non dégénéré
- calculable efficacement

- $(\mathbb{G}_1, +), (\mathbb{G}_2, +)$ et $(\mathbb{G}_T, \times)$ 3 groupes cycliques d'ordre r premier (≈ 256 bits)
- $\mathbb{G}_1 =$ sous-groupe des points sur $\mathbb{F}_p$ d'ordre r, $r \mid \#E(\mathbb{F}_p) = p + 1 - t$
- *Degré de plongement* : soit k le plus petit entier tel que $r \mid p^k - 1$.
- théorème [Balasubramanian, Koblitz] $r \mid p^k - 1 \Leftrightarrow E[r] \subset E(\mathbb{F}_{p^k})$
- $E(\mathbb{F}_{p^k})[r] \simeq \mathbb{Z}_r \times \mathbb{Z}_r$ et on prend $\mathbb{G}_1 \times \mathbb{G}_2 = E(\mathbb{F}_{p^k})[r]$
- $\mathbb{G}_T \subset \mathbb{F}_{p^k}^*$, $\mathbb{G}_T \simeq \mu_r = \left\{ x \in \mathbb{F}_{p^k}^*, x^r = 1 \right\}$

Cryptographie avec couplage : contraintes

$\#E(\mathbb{F}_p) = p + 1 - t = h \cdot r$ avec r premier,
$\Delta = (t)^2 - 4p = -Dy^2$

- k choisi suivant le niveau de sécurité, $6 \leqslant k \leqslant 36$
  - k est le plus petit entier tel que $r \mid p^k - 1$, $k \sim r$ dans le cas général
- $|t| < 2\sqrt{p}$
- $\Delta = (t)^2 - 4p = -Dy^2$ avec D petit pour que la méthode CM aboutisse, $D < 10^9$.
- r grand, i.e. le cofacteur h petit. $1 \leqslant \rho = \frac{\log p}{\log r} \leqslant 2$.

On cherche à construire des courbes très rares.

Méthode de Cocks-Pinch appliquée à $\mathcal{C}_5$

$\#J_{\mathcal{C}_5}(\mathbb{F}_p) = p^2 + 1 - 2n(p+1) + 2n^2$ avec $2p - t_2^{'} = 2n^2$.

Soit $\Delta(E^{'}(\mathbb{F}_{p^2})) = (t_2^{'})^2 - 4p^2 = -4n^2Dy^2$. $p = \frac{2n^2+2Dy^2}{4}$

Input: D, $\log_2 r$, k (sachant que $\log r \approx \frac{1}{4}\log p$).

Output: r, p premiers; parametres $a, b \in \mathbb{F}_p$ t.q. la Jacobienne $J_{\mathcal{C}_5}$ de $\mathcal{C}_5(\mathbb{F}_p) : Y^2 = X^5 + aX^3 + bX$ vérifie $r \mid \#J_{\mathcal{C}_5}(\mathbb{F}_p)$ et ait un degré de plongement k par rapport à r.

Repeat

1. Choisir r premier de taille voulue avec $i, \sqrt{D}, \zeta_k \in \mathbb{F}_r$.
2. Soient $n = (\zeta_k + i)(1-i)/2$ et $y = \pm(\zeta_k - i)(1+i)/(2\sqrt{D}) \in \mathbb{F}_r$.
3. Relever n et y de $\mathbb{F}_r$ sur $\mathbb{Z}$, soit $p = (n^2 + Dy^2)/2$.

Until $p \equiv 1 \mod 4$ et p premier.

Méthode de Cocks-Pinch appliquée à $\mathcal{C}_5$, fin

4. Avec la méthode CM, calculer le j-invariant d'une courbe elliptique $E'(\mathbb{F}_{p^2})$ de trace $\pm t_2'$ avec $\Delta = -4D(ny)^2$.
5. Résoudre $j(E') = 2^6 \frac{(3c-10)^3}{(c-2)(c+2)^2}$ dans $\mathbb{F}_{p^2}$ et retenir la solution t.q. $c^2 \in \mathbb{F}_p$.
6. Choisir $a, b \in \mathbb{F}_p$ t.q. $a \neq 0$ et $b = (a/c)^2$ (b est un carré dans $\mathbb{F}_{p^2}$ mais pas dans $\mathbb{F}_p$).

Return r, p premiers, $a, b \in \mathbb{F}_p$

Pour calculer le j-invariant de la courbe, on a modifié `cm.cpp` de la librairie MIRACL d'après *[Konstantinou et al. J. Crypto 23, 2010]*.

Plan

- Comptage de points :
  - améliorations d'une méthode efficace pour deux familles particulières de courbes hyperelliptiques de genre 2.
  - Il faut calculer une trace de courbe elliptique puis choisir entre quelques formules explicites.
- Constructions pour les couplages :
  - On peut choisir n'importe quel degré de plongement (avant : $4 \mid k$ pour $\mathcal{C}_5$ et $3 \mid k$ pour $\mathcal{C}_6$).
  - On trouve toujours les coefficients a, b de la courbe de genre 2 à condition de vérifier quelques congruences sur p, r et la trace de E.
  - le j-invariant de la courbe elliptique peut être dans $\mathbb{F}_p$ ou $\mathbb{F}_{p^2}$.
  - Variante de Cocks-Pinch : $\rho \approx 4$, variante de Brezing-Weng : $\rho \approx 3$.

Perspectives d'améliorations

- Lorsque $D = 1$ ou 3, la Jacobienne se scinde en deux, $\rho = 2$ peut être atteint mais c'est un cas trivial.
- Autres possibilités lorsque $D = 2$

$\Rightarrow$ Restrictions aux scalaires de Weil d'ordre 8 lorsque $D = 1$ ou 2 et d'ordre 12 lorsque $D = 3$

- $\rho < 2$ semble inatteignable avec ces méthodes
- MIRACL est devenu un produit commercial de CertiVox Ltd. en novembre 2011 et son principal contributeur Dr Michael Scott chef de CertiVox Labs. Il serait intéressant d'utiliser par exemple la librairie multiprécision développée par Andreas Enge pour la calcul de j-invariant.

Pour plus de détails

`http://eprint.iacr.org/2011/604`
et à paraître dans les actes de Pairing 2012.

`aurore.guillevic@ens.fr`