Tores algébriques et jacobiennes généralisées en cryptographie

David R. Kohel

The University of Sydney
(et Université de Toulouse, le Mirail)

Institut de Mathématiques Luminy, 6 décembre 2005

Table des matières

Cryptographie

Le but d'un échange privé entre deux personnes est d'établir un secret commun S. Avec S ils peuvent appliquer une fonction hash h pour engendrer une clé privée commune $K = h(S)$.

Soit G un groupe cyclique d'ordre n et engendré par un élément P. Soit k un entier, $1 \leq k \leq n$ et $Q = kP$, le triplet (G, P, Q) forme une *clé publique* et k une *clé privée*.

Dans l'algorithme original de Diffie et Hellman (1976), le groupe G est un sous-groupe d'ordre premier du groupe multiplicatif $\mathbb{F}_q^*$. Néanmoins, pour un élément $P = \alpha \in \mathbb{F}_q^*$, on utilise la notation additive kP pour l'élément α^k.

Avec cette notation, on rappelle le protocole de Diffie et Hellman.

Le protocole Diffie–Hellman

Pour établir un secret commun Alice et Bob choisissent une paire (G, P) publique tel que $G = \langle P \rangle$.

- Alice prend un entier k_A et Bob un entier k_B.
- Alice calcule $Q = k_A P$ et Bob calcule $R = k_B P$.
- Ils rendent publiques leurs clés (G, P, Q) et (G, P, R).
- Alice calcule $S = k_A R$ et Bob calcule $S = k_B Q$.

Même si Eve intercepte l'information (G, P), Q, et R, on suppose que l'information dans $S = k_A k_B P$ est difficile à retrouver sans un effort calculatoire énorme.

La valeur d'un logarithme discret $k_A = \log_P(Q)$ ou $k_B = \log_P(R)$ donne une solution immédiate. Et donc notre supposition inclut la difficulté de calculer les logarithmes discrets dans G.

Groupes cryptographiques

Le protocole Diffie–Hellman se généralise à tout groupe G cyclique tel que :

- l'ordre n du groupe est un nombre premier ;
- il existe un algorithme efficace pour l'addition des éléments ; et
- il n'y a pas d'algorithme efficace *connu* pour le logarithme discret.

Les groupes standard pour la cryptographie sont :

- $G \subset \mathbb{G}_m(\mathbb{F}_q) = \mathbb{F}_q^*$, le groupe des points du groupe multiplicatif sur un corps fini [Diffie et Hellman (1976)]
- $G \subset E(\mathbb{F}_q)$, le groupe de points d'une courbe elliptique sur un corps fini [Koblitz, Miller (1985)]
- $G \subset J(\mathbb{F}_q)$, le groupe de points de la jacobienne d'une courbe hyperelliptique sur un corps fini [Koblitz (1989)]

Jacobiennes généralisées

Une *jacobienne généralisée* est un schéma en groupes J qui représente le groupe des classes de diviseurs équivalents sur un courbe. Ce sont des groupes naturels pour la cryptographie.

En effet, tous les exemples précédents sont des exemples de jacobiennes généralisées.

L'ensemble de points d'une courbe elliptique est un exemple bien connu en cryptographie.

Une courbe elliptique E elle-même est une varieté abélienne, donnée par une équation

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

Mais elle est aussi équivalente à son foncteur de Picard, qui représente les ensembles de classes de diviseurs.

Courbes elliptiques et groupes de Picard

Soit E donnée par l'équation:

$$E : y^2 = x^3 + ax + b,$$

avec le point à l'infini O. Alors, on a l'équivalence entre les trois représentations:

$$E(k) \longrightarrow \mathrm{Pic}_k^0(E) \longrightarrow \mathrm{Pic}(\mathcal{O}),$$

$$(x_0, y_0) \longmapsto [(x_0, y_0) - O] \longmapsto [(x - x_0, y - y_0)]$$

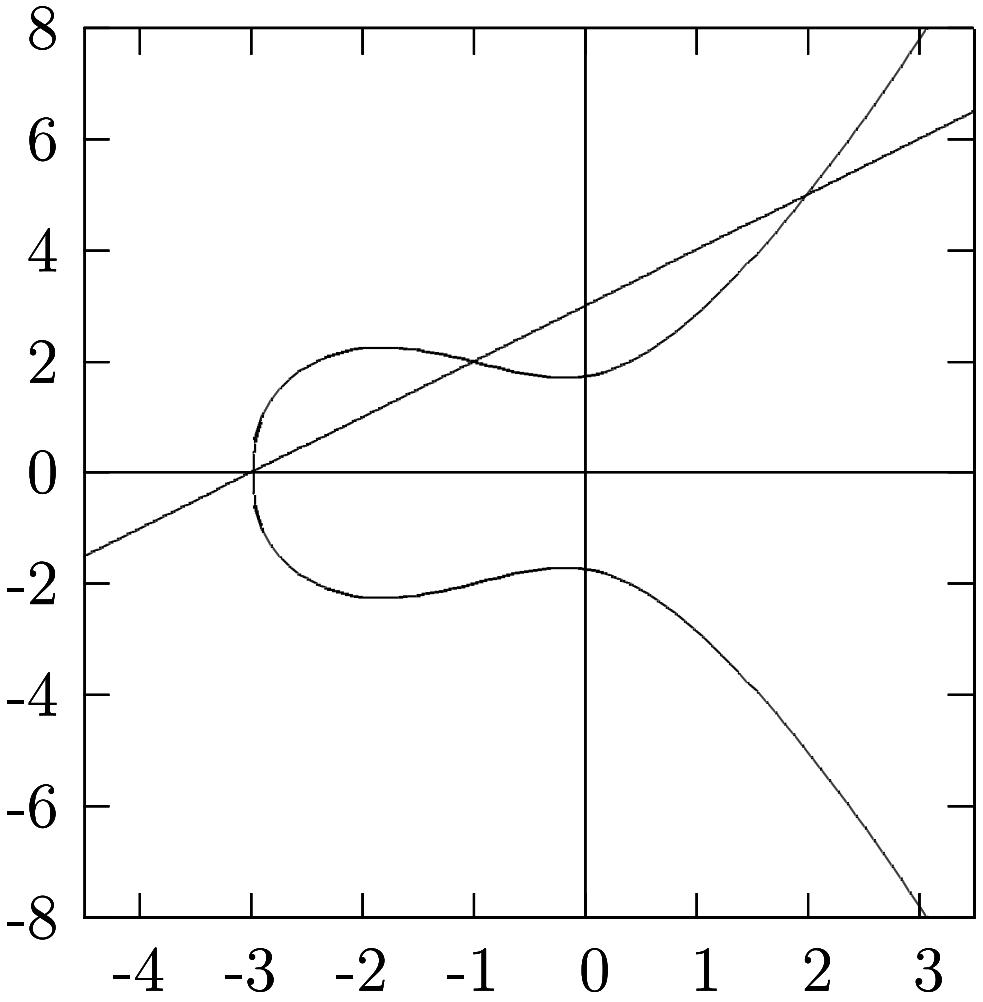
où

$$\mathcal{O} = \frac{k[x, y]}{(y^2 - x^3 - ax - b)}.$$

Pour les courbes générales, les représentations comme groupes de Picard $\mathrm{Pic}(\mathcal{O})$ sont les plus efficaces. Cette représentation se généralise aussi aux ordres non maximaux, qui définissent des courbes singulières.

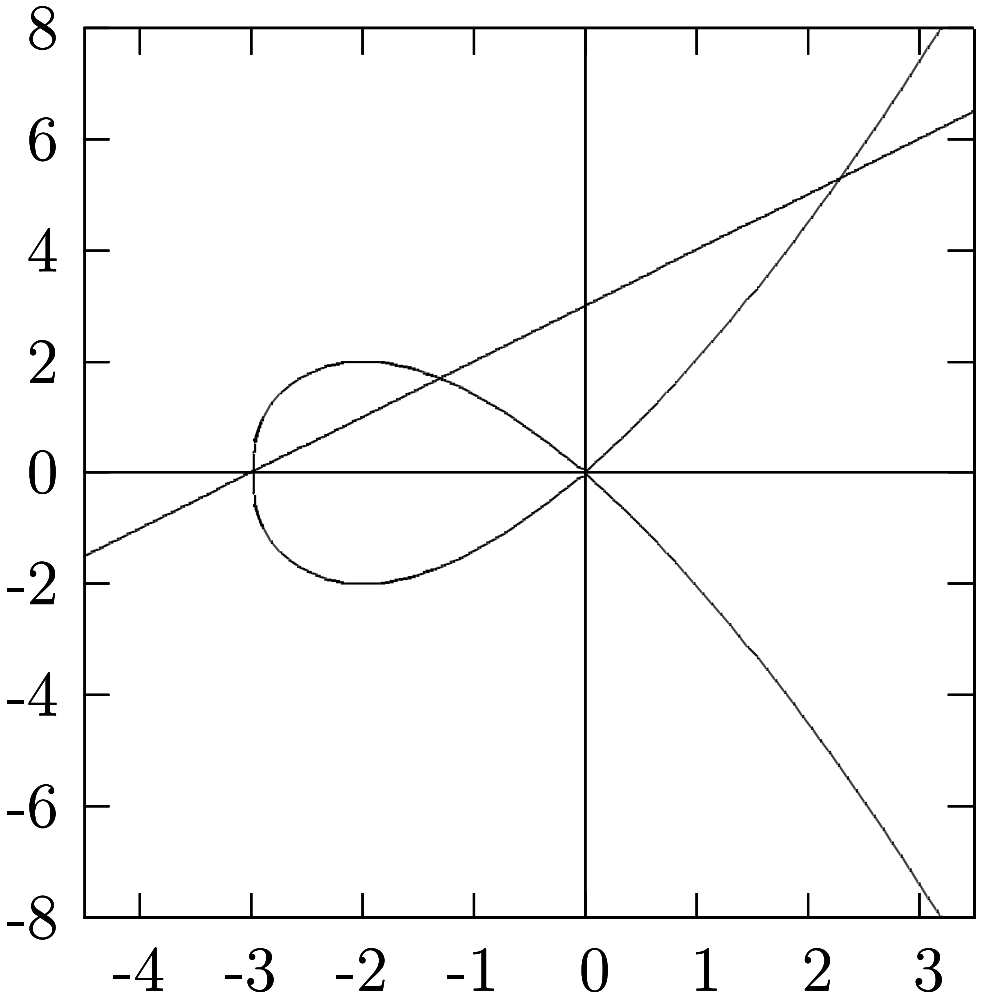
La loi de groupe d'une courbe elliptique

$$y^2 = (x^2 + 1)(x + 3)$$



La loi de groupe d'une courbe elliptique dégénérée

$$y^2 = x^2(x+3)$$



Tores algébriques

Un *tore algébrique* est un schéma en groupes $\mathbb{T}$ de dimension d sur un corps k, tel que

$$\mathbb{T} \times_k \bar{k} \cong \mathbb{G}_m \times \cdots \times \mathbb{G}_m = (\mathbb{G}_m)^d,$$

où $\mathbb{G}_m$ est le groupe multiplicatif. Si L/k est une extension telle que $\mathbb{T} \times_k L \cong (\mathbb{G}_m)^d$, on dit que L déploie $\mathbb{T}$. On s'intéresse au cas où k est un corps fini ; on dit alors que $n = [L : k]$ est le degré déployant de $\mathbb{T}$.

Soit L une extension d'un corps fini $k = \mathbb{F}_q$ de degré n. Alors la restriction des scalaires $\mathrm{Res}_{L/k}(\mathbb{G}_m)$ est un tore qui contient un tore $\mathbb{T}_n$ tel que

$$\mathbb{T}_n(F) = \bigcap_{K \subset L} \ker\left((F \times_k L)^* \to (F \times_k K)^*\right)$$

pour toute extension F/k. Remarquons que sa dimension est $d = \varphi(n)$.

XTR, LUC, et CEILIDH

Rubin et Silverberg ont introduit l'utilisation systématique des tores algébriques dans la cryptographie en 2003. En particulier, ils ont donné :

- Une démonstration que l'ensemble de XTR (système cryptographique proposé par Lenstra et Verheul) vient d'un isomorphisme
$$\mathbb{A}^2 \cong \mathbb{T}_6/S_3,$$
i.e. que XTR $= \mathbb{T}_6/S_3(\mathbb{F}_q)$.
- Une démonstration que l'ensemble de LUC vient d'un isomorphisme $\mathbb{A}^1 \cong \mathbb{T}_2/S_3$.
- Une paramétrisation birationelle $\mathbb{A}^2 \cong \mathbb{T}_6$ et son utilisation dans le protocole de Diffie et Hellmann (système appelé CEILIDH).

Pour les systèmes plus efficaces en mémoire, on demande une représentation $\mathbb{A}^d \cong \mathbb{T}_n$ *rationelle* du tore $\mathbb{T}_n$ où $d = \varphi(n)$.

Tores algébriques et courbes singulières

La courbe $E : y^2 = x^2(x + a)$ représente soit le tore $\mathbb{G}_m = \mathbb{T}_1$ soit le tore $\mathbb{T}_2$. Cette construction se généralise aux courbes superelliptiques :

$$C_m : y^m = xg(x)^m,$$

sur un corps fini de q elements, on obtient le théorème suivant :

Theorem 1. *Pour $g(x)$ un polynôme primitif de degré n premier à m, tel que $q^n \equiv 1 \bmod m$, la jacobienne généralisée contient un facteur isomorphe à $\mathbb{T}_{mn}$.*

Pour les courbes hyperelliptiques, *i.e.* $m = 2$, ou superelliptiques avec $m = 3$, il existe des algorithmes efficaces pour calculer dans les groupes de Picard de ces courbes.

Morphismes vers les groupes multiplicatifs

Soit $C : y^m = xg(x)^m$ une courbe singulière superelliptique, et soit J_C sa jacobienne généralisée, qui représente le foncteur de Picard, *i.e.* pour tout extension K/k :

$$J_C(K) = \mathrm{Pic}(K \otimes_k \mathcal{O}) = \mathrm{Pic}\Big(\frac{K[x,y]}{(y^m - xg(x)^m)}\Big).$$

Soit $z = y/g(x)$ dans le corps de fonctions de C, et α et β tel que $g(\alpha) = 0$ et $\beta^m = \alpha$. Alors pour tout m-ième racine de l'unité ζ, il existe des morphismes fonctoriels :

$$J_C(K) \to \big(K \otimes_k k[\beta]\big)^* / \big(K \otimes_k k[\alpha]\big)^*$$

qui envoie la classe d'un élément $(x - x_0, y - y_0)$ de $J_C(K)$ sur $(z_0 - \zeta\beta)/(z_0 - \beta)$, où $z_0 = y_0/g(x_0)$.

Morphismes vers les groupes multiplicatifs (suite)

Pour un diviseur général on note que

$$x = z^m \text{ et } y = zg(x) = zg(z^m).$$

Donc la classe $(a(x), y - b(x))$ de $J_C(K)$ définit l'idéal :

$$\big(a(z^m), zg(z^m) - b(z^m)\big) = (D(z))$$

dans l'anneau principal $K[z]$.

Avec la notation ci-dessus, l'image du diviseur est alors :

$$\frac{D(\zeta\beta)}{D(\beta)} = \prod_{i=1}^{r} \frac{(z_i - \zeta\beta)}{(z_i - \beta)},$$

où $D(z) = (z - z_1) \cdots (z - z_r)$.

Courbes superelliptiques singulières

Soit $C_m : y^m = xg(x)^m$ une courbe singulière superelliptique. Pour $g(x)$ un polynôme primitif de degré n premier à m, tel que $q^n \equiv 1 \bmod m$, sa jacobienne généralisée contient un facteur d'isogénie isomorphe à $\mathbb{T}_{mn}$. La table ci-dessous donne les informations sur J_{C_m} et $\mathbb{T}_{nm}$.

$\dim(J_{C_2})$	$\deg(g(x))$	$\dim(\mathbb{T}_{2n})$	$\dim(J_{C_3})$	$\deg(g(x))$	$\dim(\mathbb{T}_{3n})$
1	1	1	3	1	2
3	3	2	6	2	2
5	5	4	12	4	4
7	7	6	15	5	8
11	11	10	21	7	12
15	15	6	33	11	20

On note que la dimension de J_{C_3} est la même que la dimension du corps déployant de $\mathbb{T}_{3n}$.

Lien avec les logarithmes discrets

On note que les groupes $\mathbb{F}_{q^n}^*$ et aussi les groupes J_C de grande dimension admettent des diviseurs lisses indépendants.

D'autre part, il y a des isogénies de petits degrés qui envoient ces groupes l'un dans l'autre.

Ainsi les tores algébriques dans les deux représentations ont des logarithmes discrets aussi difficiles (ou faciles) à calculer.

G-ensembles cryptographiques

Soit H un groupe fini d'automorphismes (de schéma en groupes) d'une jacobienne généralisée J_C. Le quotient $X = J_C/H$ est une variété algébrique, qui admet une action de semi-groupe :

$$\mathbb{Z} \times X \longrightarrow X.$$

L'action est bien définie parce que les éléments de H sont des morphismes de schémas en groupes.

Attention: la multiplication scalaire $n(mP) = (nm)P$ est bien défini mais pas l'addition ; et donc $(n+m)P$ existe mais on ne peut pas calculer $nP + mP$ avec nP et mP.

Si $J_C(\mathbb{F}_q)$ est un groupe cyclique d'ordre n, alors son image dans $X(\mathbb{F}_q)$ admet un action de $\mathbb{Z}/n\mathbb{Z}^*$. L'image S des éléments primitifs de $J_C(\mathbb{F}_q)$ admet une action transitive de $\mathbb{Z}/n\mathbb{Z}^*$.

Les système XTR et LUC sont des exemples de cette construction.

Surfaces de Kummer et leurs dégénérescences

Les quotients de variétés abéliennes par le groupe $\{\pm 1\}$ donnent des exemples classiques de cette construction.

Soit $C : y^2 = x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5$ une courbe hyperelliptiques de genre 2. Sa jacobienne J_C est une variété de dimension 2 qui a un modèle non-singulier dans $\mathbb{P}^8$ (ce qui n'est pas très efficace pour le calcul).

Par contre, son quotient $K = J_C/\{\pm 1\}$ est une hypersurface quartique dans $\mathbb{P}^3$ (qui s'appelle une surface de Kummer). Les surfaces de Kummer et leurs dégénérescences donnent des G-ensembles naturels pour la cryptographie.

En résumé

- Il existe des représentations du tore $\mathbb{T}_n/\mathbb{F}_q$ comme facteurs des jacobiennes généralisées J.
- Il existe des algorithmes efficaces pour la loi du groupe $J(\mathbb{F}_q)$ (déjà connus et développés pour les jacobiennes).
- Il existe des constructions naturelles de G-ensembles dans le contexte de la géométrie arithmétique.
- Cette représentation donne un système de diviseurs *lisses* distincts de ceux du corps déployant $\mathbb{F}_{q^n}$.
- Il existe des isogénies de degré n vers $J/L \to \mathbb{G}_m/L$ avec n petit, et qui induisent des homomorphismes de $J(k)$ vers $\mathbb{G}_m(L) = L^*$ de petits noyaux.