Tores algébriques sur les corps finis
(un survol)

David A. Madore
TELECOM ParisTech
david.madore@enst.fr
http://perso.enst.fr/~madore/

2010-03-12

Le problème

Pour des systèmes basés sur le DLP (Diffie-Hellman, elGamal...) dans $\mathbb{F}_{q^n}^\times$:

- Isoler la partie « cryptographiquement significative » de $\mathbb{F}_{q^n}^\times$.
  I.e., celle qui résiste « le mieux » aux attaques sous-exponentielles.
- La représenter de façon compacte.
  I.e., en moins de $n \log q$ bits.
- Lui donner une structure algébrique.
  I.e., de groupe algébrique (pas juste de groupe).

Structure de $\mathbb{F}_{q^n}^\times$

Pour chaque $d|n$, on a une flèche de norme $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}} : \mathbb{F}_{q^n}^\times \to \mathbb{F}_{q^d}^\times$ (donnée par $x \mapsto x^{(q^n-1)/(q^d-1)}$), surjective (car $\mathrm{N}(g) \in \mathbb{F}_{q^d}^\times$ est primitif si $g \in \mathbb{F}_{q^n}^\times$ l'est).

$$1 \to \ker \mathrm{N} \to \mathbb{F}_{q^n}^\times \xrightarrow{\mathrm{N}} \mathbb{F}_{q^d}^\times \to 1$$

Le DLP au milieu se ramène au DLP aux deux extrémités :
Pour trouver a tel que $g^a = x$ dans $\mathbb{F}_{q^n}^\times$, on peut d'abord trouver b tel que $\mathrm{N}(g)^b = \mathrm{N}(x)$ dans $\mathbb{F}_{q^d}^\times$, puis c tel que $x/g^b = g'^c$ avec $g' = g^{q^d-1}$ par exemple. (Alors $a = b + c(q^d-1)$ convient.)

Sous-groupe de norme 1

On veut donc définir le sous-groupe :

$$T_{n,q} = \bigcap_{\substack{d|n \\ d<n}} \ker(\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}) \subseteq \mathbb{F}_{q^n}^\times$$

Bien sûr, il suffit de considérer les $d = n/\ell$ avec $\ell|n$ premier.

On a $\#T_{n,q} = \Phi_n(q)$ où Φ_n désigne le n-ième polynôme cyclotomique.

(En effet, $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}(g^a) = 1$ ssi $(q^d - 1)|a$, et on a $\mathrm{ppcm}(\{(q^d - 1) : d|n \wedge d < n\}) = (q^n - 1)/\Phi_n(q)$).

En particulier, $\#T_{n,q} \approx q^{\varphi(n)}$.

Représentation compacte ?

On a, $\#T_{n,q} \approx q^{\varphi(n)}$:
peut-on représenter un élément de $T_{n,q}$ en environ $\varphi(n) \log q$ bits ?

On a $\liminf_{n\to+\infty} \varphi(n)/n = 0$.
Cas intéressant : $n = \ell_1 \cdots \ell_t$ avec ℓ_i premiers distincts.
On gagnerait ainsi un facteur $\frac{\varphi(n)}{n} = \prod \frac{\ell_i - 1}{\ell_i}$.

En pratique :
$n = 2 \Longrightarrow \varphi(n) = 1$ (« LUC »)
$n = 6 \Longrightarrow \varphi(n) = 2$ (« XTR », « CEILIDH »)
$n = 30 \Longrightarrow \varphi(n) = 8$ (van Dijk & Woodruff)
$n = 210 \Longrightarrow \varphi(n) = 48$?

On veut voudrait paramétrer $T_{n,q}$ par $\varphi(n)$ paramètres.

Restriction des scalaires : définition

Comment voir $\mathbb{F}_{q^n}^\times$ comme une variété sur $\mathbb{F}_q$?

Vision « à la Grothendieck » :

- « Groupe multiplicatif » : $\mathbb{G}_{\mathrm{m},\mathbb{F}_{q^n}} = GL_{1,\mathbb{F}_{q^n}} : A \mapsto A^\times$

où A est une $\mathbb{F}_{q^n}$-algèbre, $A^\times$ son groupe des inversibles.

- « Restriction à la Weil » de $\mathbb{F}_{q^n}$ à $\mathbb{F}_q$ de celui-ci :

$\mathfrak{R}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\mathbb{G}_{\mathrm{m},\mathbb{F}_{q^n}}) : A \mapsto (A \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n})^\times$

Alors $\mathfrak{R}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\mathbb{G}_{\mathrm{m},\mathbb{F}_{q^n}})$ est une variété sur $\mathbb{F}_q$, de dimension n :

- ses points sur $A = \mathbb{F}_q$ sont : $\mathbb{F}_{q^n}^\times$,
- ses points sur $A = \mathbb{F}_{q^n}$ sont $(\mathbb{F}_{q^n}^\times)^n$
  (car $\mathbb{F}_{q^n} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n} \cong (\mathbb{F}_{q^n})^n$ par $u \otimes v \mapsto (\mathrm{Frob}_q^i(u)\, v)_{i=0}^{n-1}$).

Restriction des scalaires : équations

Vision plus concrète : si $b_0, \ldots, b_{n-1}$ est une $\mathbb{F}_q$-base de $\mathbb{F}_{q^n}$:

$$\mathfrak{R}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\mathbb{G}_{\mathrm{m},\mathbb{F}_{q^n}}) = \{(x_0, \ldots, x_{n-1}) : \mathrm{N}(\Sigma x_i b_i) \neq 0\}$$

où $\mathrm{N}(\Sigma x_i b_i)$ est le polynôme norme, homogène de degré n en $x_0, \ldots, x_{n-1}$.

Si $b_i = \alpha^i$ pour α un élément de degré n et de polynôme minimal P, c'est plus simplement

$$\{x_0 1_{n\times n} + x_1 C_P + x_2 C_P^2 + \cdots + x_{n-1} C_P^{n-1} \in GL_{n,\mathbb{F}_q}\}$$

où C_P est la matrice compagnon du polynôme P
(et $\mathrm{N}(\sum x_i \alpha^i)$ est le déterminant de $\sum x_i C_P^i$).

Multiplication = multiplication des matrices.

Tore de norme 1

Pour chaque $d|n$, l'application $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}$ donne un morphisme de groupes algébriques sur $\mathbb{F}_q$:

$$\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}} : \mathfrak{R}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\mathbb{G}_{\mathrm{m},\mathbb{F}_{q^n}}) \to \mathfrak{R}_{\mathbb{F}_{q^d}/\mathbb{F}_q}(\mathbb{G}_{\mathrm{m},\mathbb{F}_{q^d}})$$

On définit :

$$\mathbb{T}_{n,\mathbb{F}_q} = \bigcap_{\substack{d|n\\d<n}} \ker(\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}) \subseteq \mathfrak{R}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\mathbb{G}_{\mathrm{m},\mathbb{F}_{q^n}})$$

- Ses points sur $\mathbb{F}_q$ sont : $\mathbb{T}_{n,\mathbb{F}_q}(\mathbb{F}_q) = T_{n,q}$,
- ses points sur $\mathbb{F}_{q^n}$ ($n = \ell$ premier) sont $\mathbb{T}_{n,\mathbb{F}_q}(\mathbb{F}_{q^n}) = \{(\lambda_0, \dots, \lambda_{n-1}) \in (\mathbb{F}_{q^n}^\times)^n : \prod_i \lambda_i = 1\}$
  (et pour $n = \ell_1 \cdots \ell_t$ avec ℓ_i premiers, ce sont les tableaux $\ell_1 \times \cdots \times \ell_t$ dont le produit de chaque ligne/colonne/... vaut 1).

Qu'est-ce qu'un tore algébrique ?

Un *tore algébrique* (de dimension r) sur un corps k est un groupe algébrique S qui devient $S_{k^{\mathrm{sép}}} \cong (\mathbb{G}_{\mathrm{m},k^{\mathrm{sép}}})^r$ après extension des scalaires à la clôture algébrique[1] $k^{\mathrm{sép}}$.
Si $S \times_k L \cong (\mathbb{G}_{\mathrm{m},L})^r$, on dit que l'extension L/k *déploie* S.

Les tores algébriques sont classifiés par le *réseau des caractères* $\hat{S} = \mathrm{Hom}(S_{k^{\mathrm{sép}}}, \mathbb{G}_{\mathrm{m},k^{\mathrm{sép}}}) \cong \mathbb{Z}^r$ du tore + l'action du groupe de Galois $\mathrm{Gal}(k^{\mathrm{sép}}/k)$ dessus (= module galoisien).
(De façon savante : $H^1(k, GL_r(\mathbb{Z}))$.)

Les morphismes $S \to T$ de tores sont classifiés par les morphismes de modules galoisiens de sens opposé $\hat{T} \to \hat{S}$.

[1] (séparable suffit)

Tores sur les corps finis

Un tore S de dimension r sur $\mathbb{F}_q$ (déployé par $\mathbb{F}_{q^n}$) est la donnée d'un $\mathbb{Z}$-module $\hat{S}$ de rang r + un automorphisme ϕ d'ordre n fini (ou, si on veut, d'un $\phi \in GL_r(\mathbb{Z})$ d'ordre n, à simil. près).

- Tore trivial $(\mathbb{G}_{\mathrm{m},\mathbb{F}_q})^r$: c'est $\phi = \mathrm{id}_{\mathbb{Z}^r}$.
- Tore $\mathfrak{R}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\mathbb{G}_{\mathrm{m},\mathbb{F}_{q^n}})$: permutation cyclique ϕ de $\mathbb{Z}^n$.
- Tore $\mathbb{T}_n$: son réseau des caractères est $\mathbb{Z}[\zeta_n] = \mathbb{Z}[X]/\Phi_n(X)$ (de rang $r = \varphi(n)$) avec ζ_n racine primitive n-ième de l'unité, et ϕ opère par multiplication par ζ_n.

Tout tore sur $\mathbb{F}_q$ est *isogène* à un produit de $\mathbb{T}_n$ pour différents n (théorie de la représentation de $\mathbb{Z}/n\mathbb{Z}$).

Le cas de $\mathbb{T}_2$

Si $\mathbb{F}_{q^2} = \mathbb{F}_q(\sqrt{D})$ (cas q impair), où $D \in \mathbb{F}_q^\times \setminus \mathbb{F}_q^{\times 2}$, on a

$$\mathbb{T}_{2,\mathbb{F}_q} = \{(x,y) : x^2 - Dy^2 = 1\}$$

Multiplication $(x,y) * (x',y') = (xx' + Dyy', xy' + x'y)$.

Cette conique admet un paramétrage rationnel par la pente de la droite reliant $(-1,0)$ à (x,y) :

$$\mathbb{P}^1_{\mathbb{F}_q} \ni t \mapsto \left(\frac{t^2+D}{t^2-D}, \frac{2t}{t^2-D}\right) \in \mathbb{T}_{2,\mathbb{F}_q}$$

(défini pour $t^2 \neq D$).

Remarque : pour $t \in \mathbb{F}_q$ l'élément $\frac{t+\sqrt{D}}{t-\sqrt{D}}$ de norme 1 est $z/\operatorname{Frob}(z)$ où $z = t + \sqrt{D}$. Cf. Hilbert 90.

Le cas de $\mathbb{T}_2$ (suite)

On peut utiliser l'application $t \mapsto (\frac{t^2+D}{t^2-D}, \frac{2t}{t^2-D})$ de réciproque $(x,y) \mapsto \frac{x+1}{y}$ pour transporter directement la multiplication de $\mathbb{T}_2$ à $\mathbb{P}^1 \setminus \{\pm\sqrt{D}\}$:

$$u * v = \frac{uv + D}{u + v}$$

(élément neutre ∞).

Ceci permet de travailler directement dans $T_{2,q} = \mathbb{T}_2(\mathbb{F}_q)$ (groupe d'ordre $q+1$ des éléments de norme 1 de $\mathbb{F}_{q^2}$).

Édouard Lucas (1842–1891) *in memoriam*

Certaines opérations sur $\mathbb{T}_{2,\mathbb{F}_q} = \{(x,y) : x^2 - Dy^2 = 1\}$ peuvent se faire en utilisant uniquement la coordonnée x (on a alors affaire à $\mathbb{T}_2/\mathfrak{S}_2 \cong \mathbb{A}^1$) :
on peut calculer la coordonnée x_s de la puissance s-ième de (x,y) en utilisant seulement la coordonnée x de (x,y) :
$x_2 = 2x^2 - 1$, $x_3 = 4x^3 - 3x$, $x_4 = 8x^4 - 8x^2 + 1$,
$x_5 = 16x^5 - 20x^3 + 5x$... (polynômes de Čebyšëv) :
récurrence : $x_{2s} = 2x_s^2 - 1$ et $x_{s+1} = 2xx_s - x_{s-1}$.

Ceci permet de pratiquer Diffie-Hellman (« LUC »).

Une autre formulation : $x = \frac{1}{2}\operatorname{tr} \colon \mathfrak{R}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\mathbb{G}_{\mathrm{a},\mathbb{F}_{q^2}}) \to \mathbb{G}_{\mathrm{a},\mathbb{F}_q}$, or $\operatorname{tr}(z)$ détermine $\operatorname{tr}(z^s)$.

Suites utilisées par Lucas pour prouver *à la main* (en 19 ans de calcul) la primalité de $2^{127} - 1$.

Rationalité de $\mathbb{T}_6$

Soit $\mathbb{F}_{q^2} = \mathbb{F}_q(\alpha)$, et soit $\{1, \beta, \beta^2\}$ une base de $\mathbb{F}_{q^3}$ sur $\mathbb{F}_q$.
Alors $\{1, \beta, \beta^2, \alpha, \alpha\beta, \alpha\beta^2\}$ est une base de $\mathbb{F}_{q^6} \cong \mathbb{F}_{q^2} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^3}$.
Si $z = u_0 + u_1\beta + u_2\beta^2$, on peut définir $j(u_0, u_1, u_2) = \frac{z+\alpha}{z+\alpha^q}$.
Par construction, $\mathrm{N}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^3}}(j(u_0, u_1, u_2)) = 1$.
On vérifie par le calcul que

$$Q = \{(u_0, u_1, u_2) : \mathrm{N}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(j(u_0, u_1, u_2)) = 1\}$$

est une *quadrique* en u_0, u_1, u_2, dont on connaît le point $(1, 0, 0)$. On peut paramétrer rationnellement Q par la direction de la droite passant par $(1, 0, 0)$ et (u_0, u_1, u_2).

$\Longrightarrow$ « CEILIDH » sur $\mathbb{T}_6$ (Rubin & Silverberg, 2003) et, via des traces à $\mathbb{T}_6/\mathfrak{S}_3$, « XTR » (Lenstra & Verheul, 2000) et d'autres systèmes.

Rationalité des tores

On dit qu'un tore S sur k est *(k-)rationnel* lorsqu'il existe $\psi\colon \mathbb{A}^r_k \dashrightarrow S$ (définie sur k) qui est une équivalence birationnelle (=isomorphisme entre un ouvert de la source et un ouvert de la cible). De façon équivalente, $k(S) \cong k(T_1, \ldots, T_r)$.

Klyačko (1988) : Si $\ell \neq \ell'$ sont premiers, alors $\mathbb{T}_{\ell\ell'}$ est rationnel.

Voskresenskiĭ (1999) : Affirme la rationnalité de tout tore déployé par une extension [de groupe de Galois] cyclique (en particulier tous les $\mathbb{T}_n$), mais avec une erreur.
2009 : Résultat plus général (tout tore stablement rationnel est rationnel).

Obtenir un paramétrage rationnel explicite de $\mathbb{T}_{30}$ est encore un problème ouvert.

Rationalité stable

On dit qu'un tore S sur k est *stablement (k-)rationnel* lorsqu'il existe $\psi\colon \mathbb{A}_k^{r+s} \dashrightarrow S \times \mathbb{A}_k^s$ (définie sur k) qui est une équivalence birationnelle. De façon équivalente, $k(S, T_1, \dots, T_s) \cong k(T_1, \dots, T_{r+s})$.

(On connaît des exemples de variétés algébriques stablement rationnelles mais non rationnelles (Beauville, Colliot-Thélène, Sansuc & Swinnerton-Dyer (1984)).)

Voskresenskiĭ (1991) : $\mathbb{T}_n$ est stablement rationnel.

Rationalité stable (suite)

Van Dijk & Woodruff (2004) : utilisent l'égalité

$$\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(n/d)}$$

(où μ est la fonction de Möbius) pour construire une « presque bijection » facilement calculable entre $T_{n,q} \times \mathbb{F}_q^s$ et $\mathbb{F}_q^t$ où $s = \sum_{\mu(n/d)=-1} d$ et $t = \sum_{\mu(n/d)=+1} d = \varphi(n) + s$. En particulier, entre $T_{30,q} \times \mathbb{F}_q^{32}$ et $\mathbb{F}_q^{40}$.

Van Dijk & al (2005) : Améliorent l'excès en une « presque bjection » entre $T_{30,q} \times \mathbb{F}_q^2$ et $\mathbb{F}_q^{10}$.

Jacobiennes généralisées

Kohel (preprint) : On peut représenter des tores algébriques comme jacobiennes généralisées de courbes hyperelliptiques.

Exemple : les points de la courbe elliptique dégénérée $y^2 = x^3 + Dx^2$ sont en bijection avec $\mathbb{F}_q(\sqrt{D})^\times$ par $(x,y) \mapsto \frac{y-\sqrt{D}x}{y+\sqrt{D}x}$, et cette bijection préserve la loi de groupe.

Malheureusement, ceci ne permet de fournir de représentation relativement efficace que pour $\mathbb{T}_\ell$ et $\mathbb{T}_{2\ell}$ avec ℓ premier impair.

Analogue additif

La définition de $\mathbb{T}_n$ comme groupe des éléments de norme 1 (vers toute extension intermédiaire) dans $\mathfrak{R}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\mathbb{G}_{\mathrm{m},\mathbb{F}_{q^n}})$ admet un analogue pour les variétés abéliennes : si A est une variété abélienne de dimension g sur $\mathbb{F}_q$, on peut définir $\mathfrak{R}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(A_{\mathbb{F}_{q^n}})$, variété abélienne de dimension ng, et une sous-variété de dimension $\varphi(n)\,g$ de celle-ci dont les éléments sont ceux dont la trace est nulle vers toute extension $\mathbb{F}_{q^d}$ intermédiaire.

Exemple : Si $E/\mathbb{F}_q$ est une courbe elliptique $y^2 = x^3 + ax + b$ et $n = 2$, on obtient la tordue quadratique $Dy^2 = x^3 + ax + b$ de E.

Construction utilisée par Rubin & Silverberg (2002, 2009) pour améliorer la sécurité MOV des variétés abéliennes supersingulières.