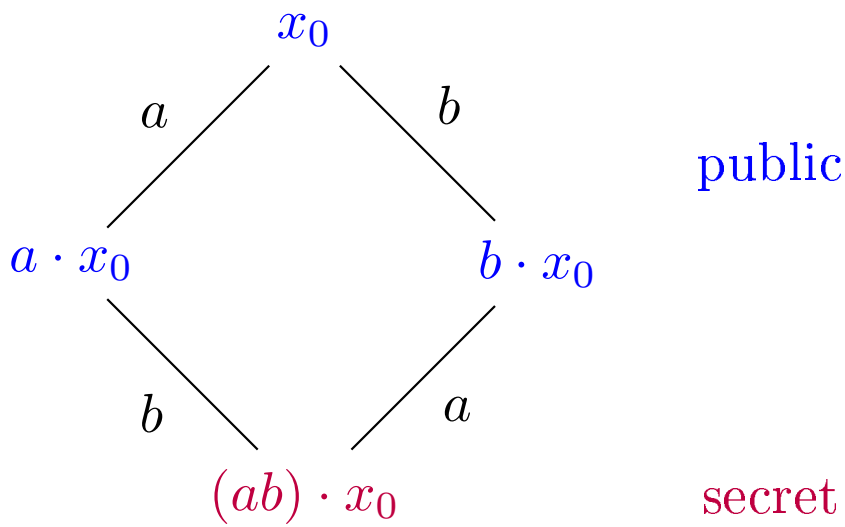
Étude et accélération du protocole d'échange de clés de Couveignes–Rostovtsev–Stolbunov

Exposé au séminaire BAC

Jean Kieffer

28 septembre 2017

Couveignes (1997) : Vision abstraite, généralisable de Diffie–Hellman.



Il faut un « espace homogène difficile » :

- G abélien agit simplement transitivement sur X
- L'action $G \times X \to X$ est facile à calculer
- Inversion difficile : x, y fixés, trouver g tel que $gx = y$.

Ici : X est un ensemble de courbes elliptiques. **Action par isogénies**.

Explicité par Rostovtsev et Stolbunov (2006).

Buts de ce travail :

- Expliquer.
- Calculer l'action : courbes modulaires.
- Attaques, estimer de bons paramètres.
- Accélération du protocole (contribution nouvelle).

Courbes elliptiques

k corps. Une **courbe elliptique** E/k est une courbe algébrique :

- Les points de E définis sur k (ou $\bar{k}$, ou ailleurs) forment un **groupe abélien**.
- Weierstrass :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Le j-invariant donne une courbe à iso près sur $\bar{k}$.

Situation particulière pour $k = \mathbb{C}$: ce sont des tores complexes

$$E = \mathbb{C}/\Lambda, \quad \Lambda \text{ réseau e.g. } \mathbb{Z} + \mathbb{Z}\tau,\ \tau \in \mathbb{H}.$$

Outil très puissant (non algébrique) qui n'existe pas en caractéristique positive.

Isogénies

Isogénie = morphisme non nul entre courbes elliptiques :

- Application rationnelle $\rightarrow$ **degré**
- Morphisme de groupes $\rightarrow$ **noyau**.

Dans le cas séparable : **noyau** = **isogénie** à iso près, représenté par un polynôme.

Les isogénies $E \rightarrow E$ (plus 0) forment l'anneau d'endomorphismes. On regarde le cas d'un **ordre** dans un corps quadratique imaginaire (multiplication complexe ou CM) :

- La plupart des courbes sur un corps fini ($\rightarrow$ crypto),
- Certaines courbes en caractéristique 0.

Théorème principal

On définit la $\mathfrak{a}$-torsion pour $\mathfrak{a}$ idéal de $\mathrm{End}(E)$:

$$E[\mathfrak{a}](\bar{k}) = \{P \in E(\bar{k}) \mid \alpha(P) = 0 \ \forall \alpha \in \mathfrak{a}\}$$

Sous-groupe donc noyau d'une isogénie : $E \to \mathfrak{a} \cdot E$.
Un idéal de norme ℓ donne une isogénie de degré ℓ.

Théorème. Action simplement transitive du **groupe de classes** de $\mathrm{End}(E)$ sur l'ensemble des courbes elliptiques sur k (à iso près) ayant CM par cet anneau.

Preuve.

- Sur $\mathbb{C}$: $\mathfrak{a} \cdot (\mathbb{C}/\Lambda) = \mathbb{C}/(\mathfrak{a}^{-1}\Lambda)$ et calculs directs (Silverman)
- Sur un corps fini : on ne dispose plus de cet outil, il faut regarder les isogénies via les modules de Tate (Waterhouse 1971).

Découpage en petits degrés

On ne calcule pas directement l'action du groupe de classes (isogénies de très grand degré). On découpe en isogénies de petit degré.

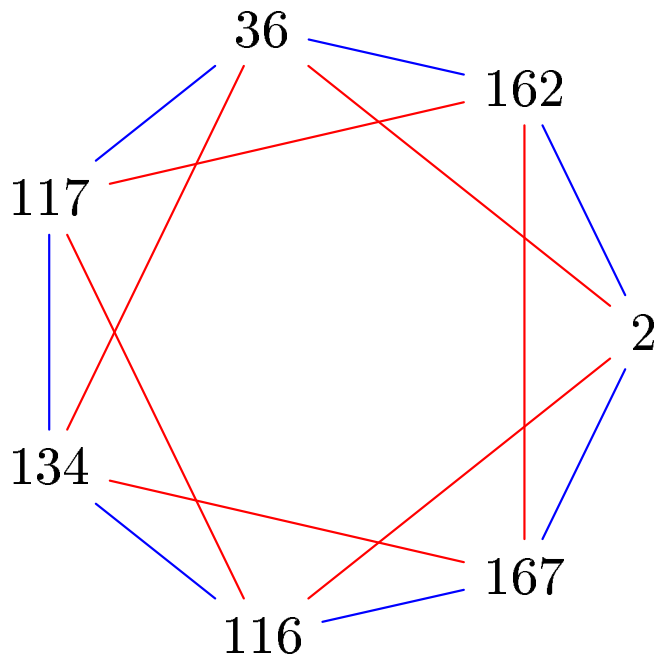
On utilise donc **quelques « générateurs »** de G : pour un $g \in G$ général, on marche comme dans un graphe de Cayley.

Si k est un corps fini, *graphe d'isogénies* :

- Sommets = courbes elliptiques (à iso près) ayant CM par un même anneau
- Arêtes = isogénies de différents degrés.

Graphe d'isogénies

Graphe sur $\mathbb{F}_{173}$ avec isogénies de degré 3 (bleu) et 7 (rouge) :



Action d'un groupe $\rightarrow$ régularité et forme. On regardera des graphes de taille cryptographique, e.g. 2^{256} sommets.

Instanciation de l'échange de clés

Paramètres publics : L (petits premiers), M_ℓ pour $\ell \in L$, E_0

Génération de clés : $|k_\ell| \leq M_\ell$ aléatoires (2 directions possibles)

Algorithme ACTION :

Input: E courbe, $|k_\ell| \leq M_\ell$ pour $\ell \in L$

Output: E' tq $E \to E'$ est une isogénie correspondant à $\prod_{\ell \in L} (\mathfrak{a}_\ell)^{k_\ell}$

for $\ell \in L$ **do**

  for $0 \leq i < |k_\ell|$ **do**

    $E \leftarrow$ *voisine* liée par une ℓ-isogénie, dans la *bonne direction*

  end

end

return E

Questions :

- Soit ℓ un nombre premier et E/k une courbe elliptique CM, quelles sont les courbes liées à E par une isogénie de degré ℓ ?
- Laquelle correspond à quel idéal de $\mathrm{End}(E)$?

On utilise les courbes modulaires :

Courbes qui paramétrisent les courbes elliptiques munies d'une certaine structure.

Courbes modulaires

Ici : structure $E \xrightarrow{\phi} E'$ où ϕ est une ℓ-isogénie.

Théorème. La courbe modulaire $Y_0(\ell)$ paramétrise ces structures à $\bar{k}$-iso près sur tout corps où $\ell \neq 0$.
Mieux : équations **universellement valides**.

Preuve.

- Sur $\mathbb{C}$: description de E sous la forme $\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$, $\tau \in \mathbb{H}$.
  $Y_0(\ell)$ est un quotient de $\mathbb{H}$, surface de Riemann compacte (...)
  donc algébrique.
- Sur les corps finis/en général : c'est un théorème difficile (Katz et Mazur).

Polynômes modulaires

Concrètement :

- On calcule une équation sur $\mathbb{C}$. Les fonctions sur cette courbe sont des *fonctions modulaires* de poids 0 au sens « usuel ».
- Coefficients entiers $\rightarrow$ on la réduit modulo p (on peut montrer qu'elle reste valide dans $\mathbb{F}_p$).

Dans le cas de la ℓ-isogénie, on utilise $j(\tau)$ et $j(\ell\tau)$:

$$\Phi_\ell(j(\tau), j(\ell\tau)) = 0$$

C'est le ℓ-ième *polynôme modulaire*.

Les solutions de l'équation $\Phi_\ell(j(E), Y) = 0$ sont les j-invariants des courbes liées à E par une isogénie de degré ℓ.

Quelle direction ?

Problème : On trouve deux voisins ! (un idéal et son inverse)

Pour les distinguer :

- *Calculer le noyau* de l'isogénie.
- Regarder l'action du Frobenius

$$(x, y) \mapsto (x^p, y^p)$$

sur le noyau.

$E[\ell](\bar{k})$ est un $(\mathbb{Z}/\ell\mathbb{Z})$-e.v. de dimension 2, le Frobenius est un endomorphisme et le noyau une droite stable (défini sur k).
Une valeur propre pour chacune des 2 directions.

Calcul d'isogénies

Calculer le noyau connaissant E_1, E_2 et le degré :

- Elkies (années 1990)
- Bostan et al. (2008)
- Autres méthodes : interpolation sur des sous-groupes, calcul dans les groupes formels...

On utilise Bostan, Morain, Salvy et Schost (grande caractéristique).
Résolution d'une équa diff : $O(\ell \log(\ell))$ $\mathbb{F}_p$-opérations.
(Manipuler le polynôme modulaire est déjà $\Omega(\ell^2)$).

$\rightarrow$ On sait maintenant instancier l'échange de clés.

L'attaque classique

Meilleure attaque : trouver un chemin entre deux courbes E_1, E_2 dans le graphe d'isogénies (Galbraith 1999).

- Construire des « arbres d'isogénies » enracinés en E_1 et E_2,
- Collision $\rightarrow$ chemin d'isogénies entre E_1 et E_2.

« Paradoxe des anniversaires » : temps et espace $O(\sqrt{N})$, où $N =$ taille du graphe $=$ nombre de classes.

Pour 128 bits de sécurité classique :

- Choisir p et $E_0/\mathbb{F}_p$ tels que $\#\mathcal{C}(\mathrm{End}(E_0)) \sim 2^{256}$
- S'assurer de la *bonne dispersion* des marches dans le graphe.

Réponses heuristiques

Contrôle du nombre de classes : pour un corps quadratique imaginaire K, théorème de Brauer–Siegel :

$$\frac{\ln h_K}{\ln \sqrt{D_K}} \longrightarrow 1$$

Versions effectives.
Ici D_K est la partie sans carré de $t^2 - 4p$, où t est la trace du Frobenius et vérifie $|t| \leq 2\sqrt{p}$.
On supposera que D_K est de l'ordre de p.

Bonne répartition : GRH $\rightarrow$ bonne dispersion à partir du degré $6\ln(|D|)^2$.
Utiliser cette borne n'est pas raisonnable, il faut une hypothèse forte (bonne répartition dès $\ln(|D|)$). On sait qu'il n'y a pas de petits cycles.

En conclusion :

- On choisit un nombre premier p de 512 bits ;
- On supposera que la courbe elliptique $E_0/\mathbb{F}_p$ choisie vérifie une série d'hypothèse fortes (mais plausibles) au sujet de la structure du graphe d'isogénies.

On espère ainsi atteindre 128 bits de sécurité classique.

Une attaque quantique existe contre les espaces homogènes difficiles, non étudiée ici (Childs et al. 2010).

Points de torsion rationnels

Étapes coûteuses du protocole : recherche de racines et calcul du Frobenius.

Idée (SIDH) : si les points du noyau sont k-rationnels (i.e. la valeur propre du Frobenius est $v = 1$),

- Chercher un point de ℓ-torsion rationnel non nul sur la courbe ($\#E(\mathbb{F}_p)/\ell \times$ un point au hasard)
- Calculer ses multiples $\to$ noyau
- Trouver la courbe image par les formules de Vélu.

Autres astuces :

- Si $p = -1 \mod \ell$, utiliser la courbe *tordue* pour l'autre direction : **donne le choix de** p.
- Modèle de Montgomery
- Accepter v de petit ordre multiplicatif.

Recherche de courbes

Il faut trouver des courbes sur $\mathbb{F}_p$ ayant des **propriétés de torsion**.

Recherche naïve : calculer le cardinal de courbes au hasard.

Recherche plus intelligente :

- Générer de bons candidats à l'aide d'une courbe modulaire de petit niveau (15-30), plutôt Y_1
- Pour de petits premiers ℓ, vérifier que l'on a bien 2 voisins et les valeurs propres sont ± 1,
- Calculer le cardinal.

C'est un SEA *early-abort* sur de bons candidats. Utiliser des courbes modulaires de niveau supérieur est trop coûteux. En pratique : $X_1(17)$, $X_0(30)$.

Résultats

Avec les paramètres déterminés précédemment, coût d'une Action (3.20GHz Intel Xeon) :

- 880 secondes sans améliorations,
- 241 secondes avec une bonne courbe.

Sage/PARI pour la recherche de racines, Julia/Nemo pour la multiplication scalaire.

La courbe choisie admet un point de ℓ-torsion rationnel pour

$$\ell \in \{3, 5, 7, 11, 13, 17, 103, 523, 821, 947, 1723\}.$$

De meilleures courbes existent, mais les trouver est difficile. On y a consacré environ 17000 heures CPU (Sage).

Conclusion et questions

Conclusion :

- On a accéléré le protocole d'un facteur ~ 4,
- On pourrait faire un peu mieux sans espoir d'être compétitif.

Questions :

- Vérifier les heuristiques pour E_0 ?
- Le log discret sur E_0 est faible, influence sur la sécurité ?
- Si le groupe de classes a des facteurs, influence sur la sécurité ?
- Influence des propriétés de torsion sur la structure du groupe ?