Échange de clés à base d'isogénies CM sur un corps fini

JNCF, CIRM 2019

Jean Kieffer

INRIA & Université de Bordeaux

7 février 2019

Motivation

Couveignes, Rostovtsev–Stolbunov : échange de clé à base de graphes d'isogénies entre courbes elliptiques ordinaires sur $\mathbb{F}_p$.

Très coûteux mais possibilités intéressantes (échange non-interactif, post-quantique...)

Question

Peut-on rendre ce protocole moins coûteux ?

[De Feo, K., Smith, Asiacrypt 2018]

Une analogie : Diffie–Hellman

G groupe fini d'ordre n (par exemple $\mathbb{F}_p^\times$), $g \in G$ fixé.

Alice | Bob

Une analogie : Diffie–Hellman

G groupe fini d'ordre n (par exemple $\mathbb{F}_p^\times$), $g \in G$ fixé.

Alice	Bob
$a \leftarrow \mathbb{Z}/n\mathbb{Z}$	$b \leftarrow \mathbb{Z}/n\mathbb{Z}$

Une analogie : Diffie–Hellman

G groupe fini d'ordre n (par exemple $\mathbb{F}_p^\times$), $g \in G$ fixé.

Alice		Bob
$a \leftarrow \mathbb{Z}/n\mathbb{Z}$	$\xrightarrow{g^a}$ $\xleftarrow{g^b}$	$b \leftarrow \mathbb{Z}/n\mathbb{Z}$

Une analogie : Diffie–Hellman

G groupe fini d'ordre n (par exemple $\mathbb{F}_p^\times$), $g \in G$ fixé.

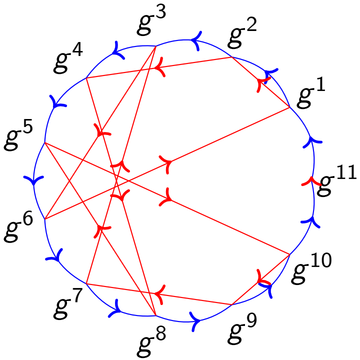
Alice		Bob
$a \leftarrow \mathbb{Z}/n\mathbb{Z}$	$\xrightarrow{g^a}$	$b \leftarrow \mathbb{Z}/n\mathbb{Z}$
$g^{ab} = (g^b)^a$	$\xleftarrow{g^b}$	$g^{ab} = (g^a)^b$

Une analogie : Diffie–Hellman

G groupe fini d'ordre n (par exemple $\mathbb{F}_p^\times$), $g \in G$ fixé.

Alice		Bob
$a \leftarrow \mathbb{Z}/n\mathbb{Z}$	$\xrightarrow{g^a}$	$b \leftarrow \mathbb{Z}/n\mathbb{Z}$
$g^{ab} = (g^b)^a$	$\xleftarrow{g^b}$	$g^{ab} = (g^a)^b$

Calcul de g^a : square-and-multiply

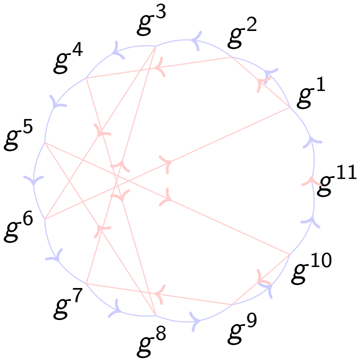


Une analogie : Diffie–Hellman

G groupe fini d'ordre n (par exemple $\mathbb{F}_p^\times$), $g \in G$ fixé.

Alice		Bob
$a \leftarrow \mathbb{Z}/n\mathbb{Z}$	$\xrightarrow{g^a}$	$b \leftarrow \mathbb{Z}/n\mathbb{Z}$
$g^{ab} = (g^b)^a$	$\xleftarrow{g^b}$	$g^{ab} = (g^a)^b$

Calcul de g^a : square-and-multiply

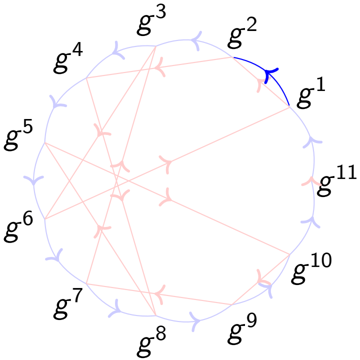


Une analogie : Diffie–Hellman

G groupe fini d'ordre n (par exemple $\mathbb{F}_p^\times$), $g \in G$ fixé.

$$\begin{array}{ccc} \text{Alice} & & \text{Bob} \\ a \leftarrow \mathbb{Z}/n\mathbb{Z} & \xrightarrow{g^a} & b \leftarrow \mathbb{Z}/n\mathbb{Z} \\ g^{ab} = (g^b)^a & \xleftarrow{g^b} & g^{ab} = (g^a)^b \end{array}$$

Calcul de g^a : square-and-multiply

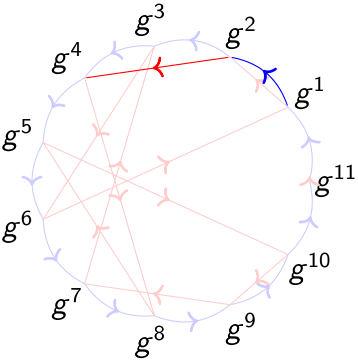


Une analogie : Diffie–Hellman

G groupe fini d'ordre n (par exemple $\mathbb{F}_p^\times$), $g \in G$ fixé.

Alice		Bob
$a \leftarrow \mathbb{Z}/n\mathbb{Z}$	$\xrightarrow{g^a}$	$b \leftarrow \mathbb{Z}/n\mathbb{Z}$
$g^{ab} = (g^b)^a$	$\xleftarrow{g^b}$	$g^{ab} = (g^a)^b$

Calcul de g^a : square-and-multiply

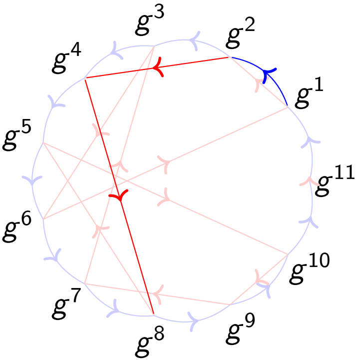


Une analogie : Diffie–Hellman

G groupe fini d'ordre n (par exemple $\mathbb{F}_p^\times$), $g \in G$ fixé.

Alice		Bob
$a \leftarrow \mathbb{Z}/n\mathbb{Z}$	$\xrightarrow{g^a}$	$b \leftarrow \mathbb{Z}/n\mathbb{Z}$
$g^{ab} = (g^b)^a$	$\xleftarrow{g^b}$	$g^{ab} = (g^a)^b$

Calcul de g^a : square-and-multiply



Structure des graphes d'isogénies

Calcul d'un pas

Sélection du graphe

Multiplication complexe

$E/\mathbb{F}_q$ courbe elliptique ordinaire. Anneau $\mathrm{End}(E)$.

- Commutatif
- Plus précisément : $\exists K$ corps quadratique imaginaire dont $\mathrm{End}(E)$ est un ordre (sous-anneau d'indice fini de $\mathcal{O}_K$).

$\mathcal{O}$ ordre de K. On note $\mathrm{Ell}(\mathcal{O}) = \{E/\mathbb{F}_q \text{ t.q. } \mathrm{End}(E) \simeq \mathcal{O}\}$, à iso et twist près.

Théorème (multiplication complexe) :

Action simplement transitive de $\mathcal{C}(\mathcal{O})$ sur $\mathrm{Ell}(\mathcal{O})$.

Correspondance isogénie/idéaux/sous-groupes

$\mathfrak{a} \subset \mathcal{O}$ idéal. Sous-groupe $E[\mathfrak{a}] = \{P \in E(\bar{\mathbb{F}}_q)$ tués par $\mathfrak{a}\}$.

- $E[\mathfrak{a}]$ est défini sur $\mathbb{F}_q$, de taille $N(\mathfrak{a})$.

Correspondance isogénie/idéaux/sous-groupes

$\mathfrak{a} \subset \mathcal{O}$ idéal. Sous-groupe $E[\mathfrak{a}] = \{P \in E(\bar{\mathbb{F}}_q)$ tués par $\mathfrak{a}\}$.

- $E[\mathfrak{a}]$ est défini sur $\mathbb{F}_q$, de taille $N(\mathfrak{a})$.

$G \subset E(\bar{\mathbb{F}}_q)$ sous-groupe. Isogénie $E \to E/G$, de degré $\#G$.

- Si $G = E[\mathfrak{a}]$, alors $\mathrm{End}(E/G) = \mathcal{O}$.
- $\mathfrak{a} \cdot E = E/E[\mathfrak{a}]$.

Correspondance isogénie/idéaux/sous-groupes

$\mathfrak{a} \subset \mathcal{O}$ idéal. Sous-groupe $E[\mathfrak{a}] = \{P \in E(\bar{\mathbb{F}}_q)$ tués par $\mathfrak{a}\}$.

- $E[\mathfrak{a}]$ est défini sur $\mathbb{F}_q$, de taille $N(\mathfrak{a})$.

$G \subset E(\bar{\mathbb{F}}_q)$ sous-groupe. Isogénie $E \to E/G$, de degré $\#G$.

- Si $G = E[\mathfrak{a}]$, alors $\mathrm{End}(E/G) = \mathcal{O}$.
- $\mathfrak{a} \cdot E = E/E[\mathfrak{a}]$.

Réciproquement, supposons ℓ scindé dans $\mathcal{O}$.
Si $E \in \mathrm{Ell}(\mathcal{O})$ et $\phi : E \to E'$ de degré ℓ définie sur $\mathbb{F}_q$, alors

- $E' \in \mathrm{Ell}(\mathcal{O})$
- ϕ provient d'un idéal de $\mathcal{O}$ de norme ℓ.

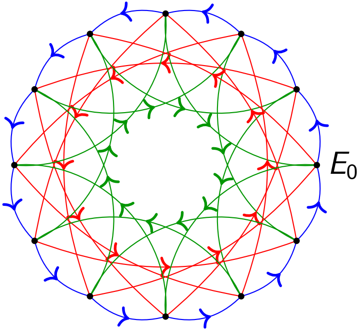
Les isogénies dans $\mathrm{Ell}(\mathcal{O})$ sont entièrement décrites par l'action de $\mathcal{C}(\mathcal{O})$.

Graphe d'isogénies

Bloc de base : calcul d'isogénie de degré ℓ, petit premier scindé dans $\mathcal{O}$.

Graphe d'isogénies

Bloc de base : calcul d'isogénie de degré ℓ, petit premier scindé dans $\mathcal{O}$.



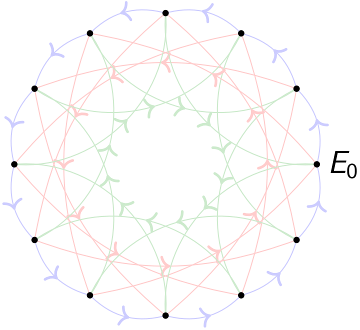
Pourquoi des cycles orientés ? Deux idéaux de norme ℓ.

Graphe d'isogénies

Bloc de base : calcul d'isogénie de degré ℓ, petit premier scindé dans $\mathcal{O}$.

Alice

$a = (2, 1, -1)$



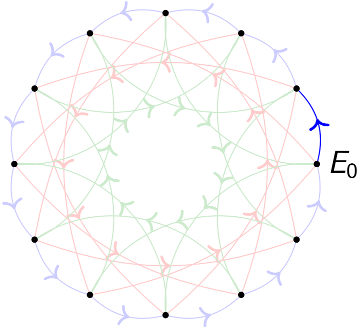
Pourquoi des cycles orientés ? Deux idéaux de norme ℓ.

Graphe d'isogénies

Bloc de base : calcul d'isogénie de degré ℓ, petit premier scindé dans $\mathcal{O}$.

Alice

$a = (2, 1, -1)$



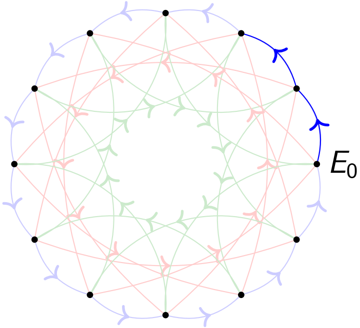
Pourquoi des cycles orientés ? Deux idéaux de norme ℓ.

Graphe d'isogénies

Bloc de base : calcul d'isogénie de degré ℓ, petit premier scindé dans $\mathcal{O}$.

Alice

$a = (2, 1, -1)$



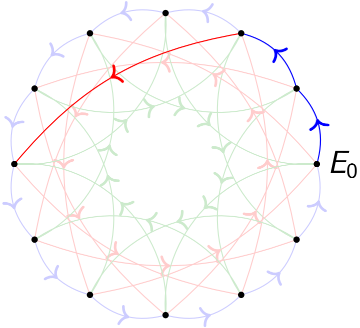
Pourquoi des cycles orientés ? Deux idéaux de norme ℓ.

Graphe d'isogénies

Bloc de base : calcul d'isogénie de degré ℓ, petit premier scindé dans $\mathcal{O}$.

Alice

$a = (2, 1, -1)$



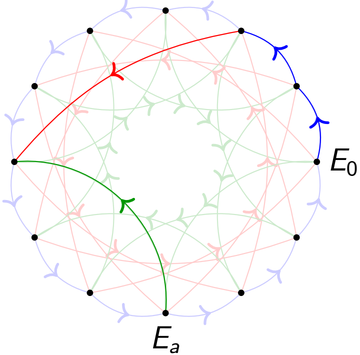
Pourquoi des cycles orientés ? Deux idéaux de norme ℓ.

Graphe d'isogénies

Bloc de base : calcul d'isogénie de degré ℓ, petit premier scindé dans $\mathcal{O}$.

Alice

$a = (2, 1, -1)$



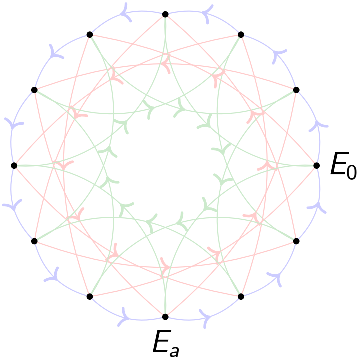
Pourquoi des cycles orientés ? Deux idéaux de norme ℓ.

Graphe d'isogénies

Bloc de base : calcul d'isogénie de degré ℓ, petit premier scindé dans $\mathcal{O}$.

Alice

$a = (2, 1, -1)$



Bob

$b = (-2, 0, 1)$

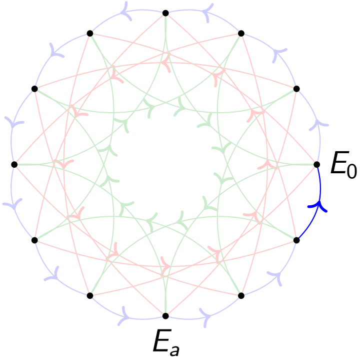
Pourquoi des cycles orientés ? Deux idéaux de norme ℓ.

Graphe d'isogénies

Bloc de base : calcul d'isogénie de degré ℓ, petit premier scindé dans $\mathcal{O}$.

Alice

$a = (2, 1, -1)$



Bob

$b = (-2, 0, 1)$

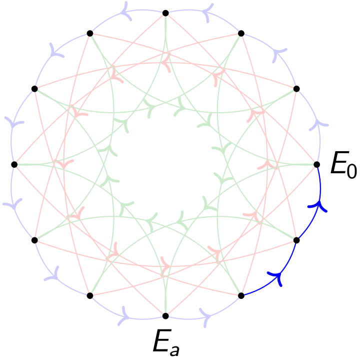
Pourquoi des cycles orientés ? Deux idéaux de norme ℓ.

Graphe d'isogénies

Bloc de base : calcul d'isogénie de degré ℓ, petit premier scindé dans $\mathcal{O}$.

Alice

$a = (2, 1, -1)$



Bob

$b = (-2, 0, 1)$

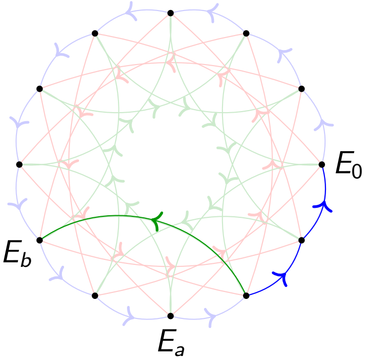
Pourquoi des cycles orientés ? Deux idéaux de norme ℓ.

Graphe d'isogénies

Bloc de base : calcul d'isogénie de degré ℓ, petit premier scindé dans $\mathcal{O}$.

Alice

$a = (2, 1, -1)$



Bob

$b = (-2, 0, 1)$

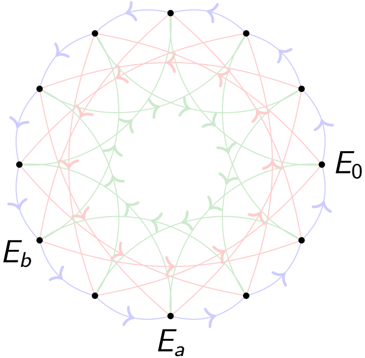
Pourquoi des cycles orientés ? Deux idéaux de norme ℓ.

Graphe d'isogénies

Bloc de base : calcul d'isogénie de degré ℓ, petit premier scindé dans $\mathcal{O}$.

Alice

$a = (2, 1, -1)$



Bob

$b = (-2, 0, 1)$

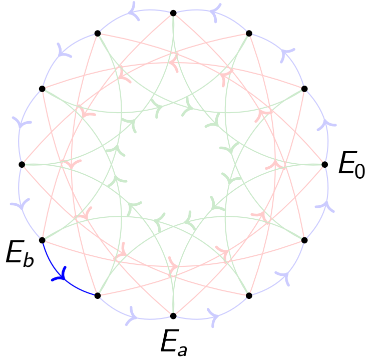
Pourquoi des cycles orientés ? Deux idéaux de norme ℓ.

Graphe d'isogénies

Bloc de base : calcul d'isogénie de degré ℓ, petit premier scindé dans $\mathcal{O}$.

Alice

$a = (2, 1, -1)$



Bob

$b = (-2, 0, 1)$

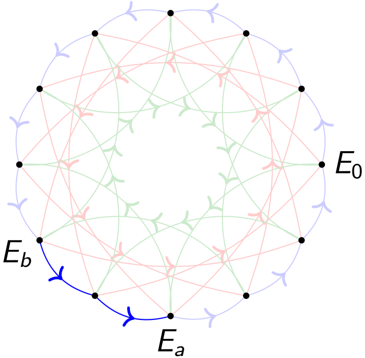
Pourquoi des cycles orientés ? Deux idéaux de norme ℓ.

Graphe d'isogénies

Bloc de base : calcul d'isogénie de degré ℓ, petit premier scindé dans $\mathcal{O}$.

Alice

$a = (2, 1, -1)$



Bob

$b = (-2, 0, 1)$

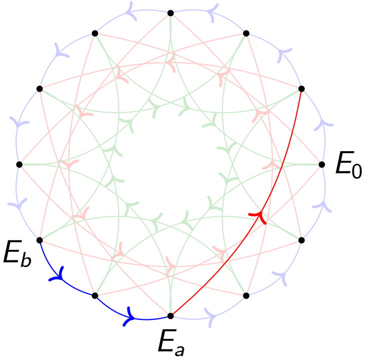
Pourquoi des cycles orientés ? Deux idéaux de norme ℓ.

Graphe d'isogénies

Bloc de base : calcul d'isogénie de degré ℓ, petit premier scindé dans $\mathcal{O}$.

Alice

$a = (2, 1, -1)$



Bob

$b = (-2, 0, 1)$

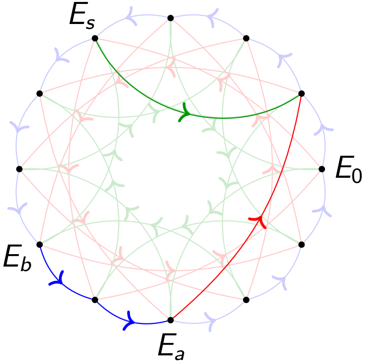
Pourquoi des cycles orientés ? Deux idéaux de norme ℓ.

Graphe d'isogénies

Bloc de base : calcul d'isogénie de degré ℓ, petit premier scindé dans $\mathcal{O}$.

Alice

$a = (2, 1, -1)$



Bob

$b = (-2, 0, 1)$

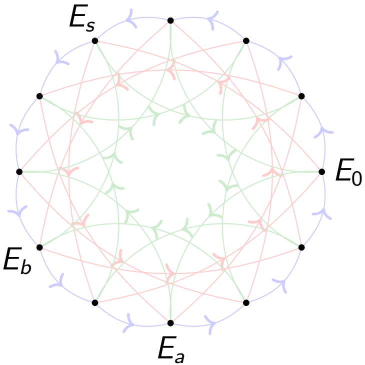
Pourquoi des cycles orientés ? Deux idéaux de norme ℓ.

Graphe d'isogénies

Bloc de base : calcul d'isogénie de degré ℓ, petit premier scindé dans $\mathcal{O}$.

Alice

$a = (2, 1, -1)$



Bob

$b = (-2, 0, 1)$

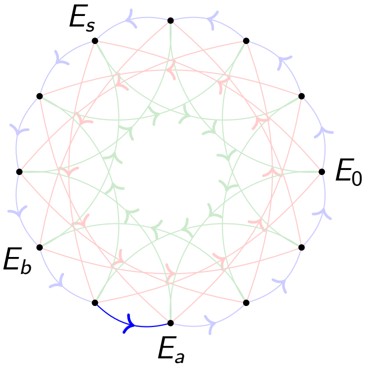
Pourquoi des cycles orientés ? Deux idéaux de norme ℓ.

Graphe d'isogénies

Bloc de base : calcul d'isogénie de degré ℓ, petit premier scindé dans $\mathcal{O}$.

Alice

$a = (2, 1, -1)$



Bob

$b = (-2, 0, 1)$

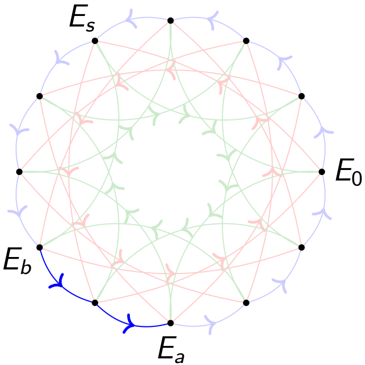
Pourquoi des cycles orientés ? Deux idéaux de norme ℓ.

Graphe d'isogénies

Bloc de base : calcul d'isogénie de degré ℓ, petit premier scindé dans $\mathcal{O}$.

Alice

$a = (2, 1, -1)$



Bob

$b = (-2, 0, 1)$

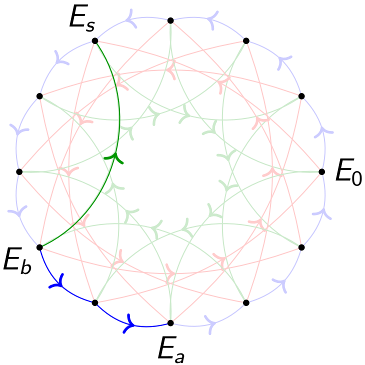
Pourquoi des cycles orientés ? Deux idéaux de norme ℓ.

Graphe d'isogénies

Bloc de base : calcul d'isogénie de degré ℓ, petit premier scindé dans $\mathcal{O}$.

Alice

$a = (2, 1, -1)$



Bob

$b = (-2, 0, 1)$

Pourquoi des cycles orientés ? Deux idéaux de norme ℓ.

Question

Comment calculer efficacement ces marches ?

Structure des graphes d'isogénies

Calcul d'un pas

Sélection du graphe

Équations modulaires

Le polynôme modulaire $\Phi_\ell(X, Y)$ encode la présence d'une ℓ-isogénie :

$$\Phi_\ell(j(E), j(E')) = 0 \iff \exists \phi : E \to E' \text{ de degré } \ell.$$

Degré $\ell + 1$ en chaque variable.

Équations modulaires

Le polynôme modulaire $\Phi_\ell(X, Y)$ encode la présence d'une ℓ-isogénie :

$$\Phi_\ell(j(E), j(E')) = 0 \iff \exists \phi : E \to E' \text{ de degré } \ell.$$

Degré $\ell + 1$ en chaque variable.

Algorithme :

- $\Phi_\ell(j(E), Y)$ (avec Φ_ℓ stocké)
- Racines (Cantor–Zassenhaus). Il y en a deux.
- Orientation ?

Orientation

On connaît E, E' ℓ-isogènes. Savoir si $\mathfrak{l}$ agit et non $\mathfrak{l}^{-1}$?

- Regarder l'action du Frobenius sur le noyau :

$$\pi \ : \ (x, y) \mapsto (x^q, y^q)$$

Si $\pi = \lambda \mod \mathfrak{l}$ ($\lambda \in \mathbb{Z}/\ell\mathbb{Z}$), on doit avoir $\pi(P) = \lambda P$ pour $P \in \operatorname{Ker} \phi$.

Orientation

On connaît E, E' ℓ-isogènes. Savoir si $\mathfrak{l}$ agit et non $\mathfrak{l}^{-1}$?

- Regarder l'action du Frobenius sur le noyau :

$$\pi \ : \ (x, y) \mapsto (x^q, y^q)$$

Si $\pi = \lambda \mod \mathfrak{l}$ ($\lambda \in \mathbb{Z}/\ell\mathbb{Z}$), on doit avoir $\pi(P) = \lambda P$ pour $P \in \operatorname{Ker} \phi$.

- $\operatorname{Ker} \phi$ décrit par $K(X)$ de degré $\frac{\ell-1}{2}$ (Elkies, Bostan et al.)
- Calcul de X^p, Y^p modulo $K(X)$ et l'équation de E.

Coût total

$O(\ell^2 \log q)$ (arithmétique naïve) pour trouver les voisins et déterminer l'orientation.

Points de torsion

Par exemple : $\pi^r = 1 \mod \mathfrak{l}$ et $\pi^r \neq 1 \mod \mathfrak{l}^{-1}$.

- Le sous-groupe $E[\mathfrak{l}]$ est défini sur $\mathbb{F}_{q^r}$, et le reste de $E[\ell]$ ne l'est pas.

Points de torsion

Par exemple : $\pi^r = 1 \mod \mathfrak{l}$ et $\pi^r \neq 1 \mod \mathfrak{l}^{-1}$.

- Le sous-groupe $E[\mathfrak{l}]$ est défini sur $\mathbb{F}_{q^r}$, et le reste de $E[\ell]$ ne l'est pas.

Algorithme :

- $P \in E(\mathbb{F}_{q^r})$ au hasard
- Calcul de $C \cdot P$, où C cofacteur $\simeq q^r$: on obtient $Q \in E[\ell]$ non nul
- Calcul du quotient $E/\langle Q \rangle$ (Vélu).

Coût total

$O(r^3 \log q)$ (arithmétique naïve) pour la multiplication scalaire.

Points de torsion

Par exemple : $\pi^r = 1 \mod \mathfrak{l}$ et $\pi^r \neq 1 \mod \mathfrak{l}^{-1}$.

- Le sous-groupe $E[\mathfrak{l}]$ est défini sur $\mathbb{F}_{q^r}$, et le reste de $E[\ell]$ ne l'est pas.

Algorithme :

- $P \in E(\mathbb{F}_{q^r})$ au hasard
- Calcul de $C \cdot P$, où C cofacteur $\simeq q^r$: on obtient $Q \in E[\ell]$ non nul
- Calcul du quotient $E/\langle Q \rangle$ (Vélu).

Coût total

$O(r^3 \log q)$ (arithmétique naïve) pour la multiplication scalaire.

Lorsque $E[\mathfrak{l}] \subset E(\mathbb{F}_q)$, on a $r = 1$! Bien choisir le graphe...

Structure des graphes d'isogénies

Calcul d'un pas

Sélection du graphe

Recherche d'une bonne courbe ordinaire

WANTED

Une courbe elliptique ordinaire $E/\mathbb{F}_q$ qui admet un point de ℓ-torsion défini sur $\mathbb{F}_q$, pour tout $3 \leq \ell \leq 400$ (environ).

La méthode CM est exclue ($\mathcal{C}(\mathcal{O})$ trop petit).

Recherche d'une bonne courbe ordinaire

WANTED

Une courbe elliptique ordinaire $E/\mathbb{F}_q$ qui admet un point de ℓ-torsion défini sur $\mathbb{F}_q$, pour tout $3 \leq \ell \leq 400$ (environ).

La méthode CM est exclue ($\mathcal{C}(\mathcal{O})$ trop petit).

Algorithme (exponentiel)

SEA : calcule $\#E(\mathbb{F}_q)$ via les restes chinois.

- Tirer E au hasard,
- SEA(E) en s'arrêtant lorsque $\#E(\mathbb{F}_q) \neq 0 \mod \ell$, pour $\ell \leq$ un certain B.

Recherche d'une bonne courbe ordinaire

WANTED

Une courbe elliptique ordinaire $E/\mathbb{F}_q$ qui admet un point de ℓ-torsion défini sur $\mathbb{F}_q$, pour tout $3 \leq \ell \leq 400$ (environ).

La méthode CM est exclue ($\mathcal{C}(\mathcal{O})$ trop petit).

Algorithme (exponentiel)

SEA : calcule $\#E(\mathbb{F}_q)$ via les restes chinois.

- Tirer E au hasard,
- SEA(E) en s'arrêtant lorsque $\#E(\mathbb{F}_q) \neq 0 \mod \ell$, pour $\ell \leq$ un certain B.

Mieux : tirer E à l'aide d'une courbe modulaire (par exemple garantir un point de 17-torsion).

- On atteint péniblement $B = 17$.

Courbes supersingulières

Castryck et al. (Asiacrypt 2018) : choisir $E/\mathbb{F}_p$ avec p premier, supersingulière et non ordinaire.

Dans ce cas $\#E(\mathbb{F}_p) = p + 1$.

- Choisir p pour avoir toute la torsion voulue !
- Tout le reste fonctionne de la même façon.

On obtient un cryptosystème crédible en pratique.

Questions