

Un échange de clés dans le monde des calculateurs quantiques

Annamaria Iezzi

Retraite MANTA

8 janvier, 2019

Échange de clés non interactif



En communiquant à travers un canal publique, **ALICE** and **BOB** veulent se mettre d'accord sur un *secret commun* sans que **EVE** puisse le découvrir.

Échange de clés Diffie-Hellman (1976)

Soit $G = \langle g \rangle$ un **groupe fini cyclique** d'ordre n .



$$0 < a < |G|$$
$$A = g^a$$



$$0 < b < |G|$$
$$B = g^b$$

$$B^a = g^{ab} = A^b$$

Problème (DLP) : Étant donné g^a trouver a .

Exemples de groupe pour Diffie-Hellman

- Protocole original :

$$G = \left(\frac{\mathbb{Z}}{p\mathbb{Z}} \right)^\times.$$

- Elliptic-curve Diffie-Hellman (ECDH) :

$$G = E(\mathbb{F}_q),$$

où E est une courbe elliptique définie sur \mathbb{F}_q .

La sécurité de ces cryptosystèmes est basée sur la difficulté du **problème du logarithme discret**.

L'algorithme de Shor



P. Shor

En 1994, Peter Shor a décrit un algorithme quantique qui factorise en temps polynomial un entier N .

Cet algorithme peut être étendu à la résolution du problème du logarithme discret dans tous les groupes finis.

Plusieurs cryptosystèmes actuels, tels que RSA et ECDH, deviendraient donc vulnérables dans un monde de calculateurs quantiques.

La menace, est-elle vraiment sérieuse ?

"at present,... I estimate a 1/7 chance of breaking RSA-2048 by 2026 and a 1/2 chance by 2031." (Mosca, 2015)



En août 2015, la NSA a annoncé une mise à jour de sa Suite B de protocoles cryptographiques afin de prendre en compte la menace quantique.

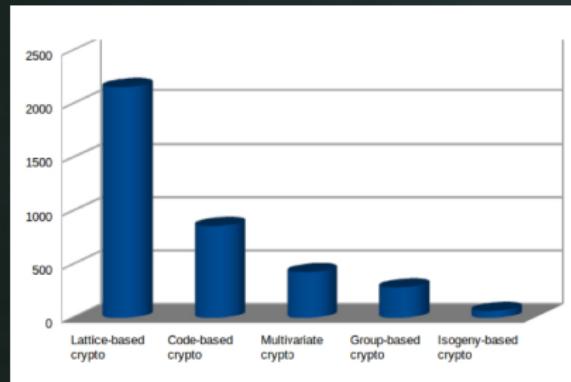
En November 2017, le NIST a commencé un procès de standardisation de primitives post-quantiques (PQ).



Quelles sont les alternatives quantum-safe ?

Post-quantum cryptography :

- Lattice-based crypto
- Code-based crypto
- Multivariate crypto
- Group-based crypto
- **Isogeny-based crypto**



Principal homogeneous space (PHS)

Définition

Un *principal homogeneous space* (PHS) pour un groupe G est un ensemble X avec une action de G sur X :

$$\begin{aligned} G \times X &\rightarrow X \\ (g, x) &\mapsto g * x \end{aligned}$$

telle que

$$\forall x, x' \in X, \exists! g \in G \text{ tel que } g * x = x'.$$

Hard-homogeneous spaces (HHS)

Définition (Couveignes, 97)

Un *hard homogeneous space* (HHS) est un PHS tel que :

- Opération “**facile**” (e.g. temps polynomial) :
donnés $g \in G$ et $x \in X$, calculer $g * x$.
- Opération “**difficile**” (e.g. temps non polynomial) :
donnés $x, x' \in X$, trouver $g \in G$ tel que $g * x = x'$.

Tout HHS X pour un **groupe abélien** G peut être utilisé pour construire un échange de clés.

Échange de clés basé sur HHS

Paramètre public : $x_0 \in X$



$$a \in G$$

$$x_1 = a * x_0$$

$$b \in G$$

$$x_2 = b * x_0$$

$$a * x_2 = a * (b * x_0) = ab * x_0 = ba * x_0 = b * (a * x_0) = b * x_1$$

Problème : Étant donné $a * x_0$ trouver a .

Échange de clés basé sur HHS

Cas particulier

- $X = \langle x \rangle$ un groupe cyclique d'ordre p .
- $G = \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$

$$\begin{array}{ccc} G \times X \setminus \{1\} & \rightarrow & X \setminus \{1\} \\ (g, x) & \mapsto & g * x = x^g \end{array}$$

Trouver g étant donné $g * x = x^g$ est le **DLP**.

Nous recherchons un HHS qui n'est pas basé sur aucun problème du logarithme discret.

Isogénies entre courbes elliptiques

Soient E_1 et E_2 deux courbes elliptiques définies sur \mathbb{F}_q et soit

$$\phi : E_1 \rightarrow E_2$$

une application entre elles.

Les affirmations suivantes sont équivalentes :

- ϕ est une application rationnelle non constante de variétés projectives telle que $\phi(O_{E_1}) = O_{E_2}$.
- ϕ est un homomorphisme de groupes surjectif.
- ϕ est un homomorphisme de groupes avec noyau fini.

Dans ces cas ϕ est appelée une *isogénie* entre E_1 et E_2 .

Isogénies entre courbes elliptiques

- Une isogénie est *définie sur* \mathbb{F}_q si elle est définie sur \mathbb{F}_q comme application rationnelle.
- Le *degré* d'une isogénie est son degré comme application rationnelle.
Une isogénie de degré ℓ est appelée ℓ -isogénie.
- Pour toute ℓ -isogénie $\phi : E \rightarrow E'$ il existe une unique ℓ -isogénie $\hat{\phi} : E' \rightarrow E$ telle que $\hat{\phi} \circ \phi = [\ell]$, où

$$\begin{aligned} [\ell] : \quad &E \quad \rightarrow \quad E \\ &P \quad \mapsto \quad [\ell]P \end{aligned}$$

Une relation d'équivalence

- Deux courbes elliptiques sont dites *isogènes* s'il existe une isogénie entre elles.
- Être isogène est une relation d'équivalence.
- E_1 et E_2 sont isogènes sur \mathbb{F}_q si et seulement si $|E_1(\mathbb{F}_q)| = |E_2(\mathbb{F}_q)|$ (Tate).

Isomorphismes

- Deux courbes elliptiques E_1 et E_2 sont dites *isomorphes* sur \mathbb{F}_q (resp. $\overline{\mathbb{F}}_q$) s'il existe deux isogénies

$$\phi : E_1 \rightarrow E_2 \quad \psi : E_2 \rightarrow E_1$$

définie sur \mathbb{F}_q (resp. $\overline{\mathbb{F}}_q$) dont la composition est l'idéntité.

- En d'autres termes, un isomorphisme est une isogénie de degré 1.

Classes d'isomorphisme

- Si $\text{char}(\mathbb{F}_q) \neq 2, 3$, alors toute courbe elliptique définie sur \mathbb{F}_q est isomorphe à une *équation de Weierstrass* :

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_q, \quad 4a^3 + 27b^2 \neq 0.$$

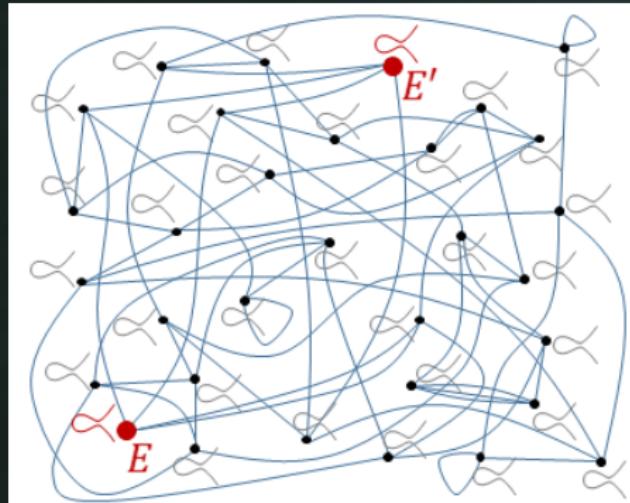
- On appelle *j*-invariant de E le nombre :

$$j(E) = 1728 \cdot \frac{4a^3}{4a^3 + 27b^2} \in \mathbb{F}_q$$

- E_1 et E_2 sont isomorphes sur $\overline{\mathbb{F}}_q$ si et seulement si $j(E_1) = j(E_2)$.
- Toute classe d'isomorphisme peut être représentée à travers son invariant.

Graphe d'isogénies

- **Sommets** : Courbes elliptiques à isomorphismes près.
- **Arêtes** : Isogénies à isomorphismes près.



Graphe d'isogénies (source : W. Castryck)

L'anneau des endomorphismes

Un *endomorphisme* défini sur \mathbb{F}_q (resp. $\overline{\mathbb{F}}_q$) d'une courbe elliptique E est :

- soit une isogénie ϕ définie sur \mathbb{F}_q (resp. $\overline{\mathbb{F}}_q$) entre E et elle même :

$$\phi : E \rightarrow E.$$

- soit le morphisme nul.

Nous dénotons :

- $\text{End}(E)$: ensemble des endomorphismes définis sur $\overline{\mathbb{F}}_q$
- $\text{End}_{\mathbb{F}_q}(E)$: ensemble des endomorphismes définis sur \mathbb{F}_q

L'anneau des endomorphismes

Un *endomorphisme* défini sur \mathbb{F}_q (resp. $\overline{\mathbb{F}}_q$) d'une courbe elliptique E est :

- soit une isogénie ϕ définie sur \mathbb{F}_q (resp. $\overline{\mathbb{F}}_q$) entre E et elle même :

$$\phi : E \rightarrow E.$$

- soit le morphisme nul.

Nous dénotons :

- $\text{End}(E)$: anneau des endomorphismes définis sur $\overline{\mathbb{F}}_q$
- $\text{End}_{\mathbb{F}_q}(E)$: anneau des endomorphismes définis sur \mathbb{F}_q

Exemples d'endomorphismes

Pour toute courbes elliptique E définie sur \mathbb{F}_q nous avons les endomorphismes suivants :



$$\begin{aligned}[m] : \quad E &\rightarrow \quad E \\ P &\mapsto [m]P\end{aligned}$$

- L'endomorphisme de Frobenius :

$$\begin{aligned}\pi : \quad E &\rightarrow \quad E \\ (x, y) &\mapsto (x^q, y^q)\end{aligned}$$

On obtient $\mathbb{Z}[\pi] \subseteq \text{End}(E)$.

Théorème (Deuring)

Théorème (Deuring)

Soit E une courbe elliptique définie sur \mathbb{F}_q . L'anneau $\text{End}(E)$ est isomorphe à l'un des suivants :

- **Cas ordinaire**

Un ordre dans un corps quadratique imaginaire K (i.e. $K = \mathbb{Q}(\sqrt{-D})$, $D > 0$).

- **Cas supersingulier**

Un ordre maximal dans l'algèbre des quaternion.

Situation dans le cas ordinaire :

$$\mathbb{Z}[\pi] \subseteq \text{End}(E) \subseteq \mathcal{O}_K \subseteq K = \mathbb{Q}(\sqrt{-D})$$

Le groupe des classes d'idéaux

Soit $\text{End}(E) = \mathcal{O} \subseteq \mathbb{Q}(\sqrt{-D})$. On définit :

- $\mathcal{I}(\mathcal{O})$: groupe des idéaux fractionnaires invertibles.
- $\mathcal{P}(\mathcal{O})$: groupe des idéaux principaux.

Le groupe des classes d'idéaux de \mathcal{O} est le groupe quotient :

$$\text{Cl}(\mathcal{O}) = \frac{\mathcal{I}(\mathcal{O})}{\mathcal{P}(\mathcal{O})}.$$

- $\text{Cl}(\mathcal{O})$ est un groupe abélien fini.
- $h(\mathcal{O}) := |\text{Cl}(\mathcal{O})|$ est appelé le *nombre de classes* de \mathcal{O} .

Une action de groupe abélien

Soit $\mathcal{O} \subseteq \mathbb{Q}(\sqrt{-D})$, $D > 0$, un ordre.

- **Ensemble** : $\mathcal{E}\mathcal{H}_q(\mathcal{O}) \neq \emptyset$

Ensemble des courbes elliptiques E définies sur \mathbb{F}_q à \mathbb{F}_q -isomorphismes près telles que $\text{End}(E) \cong \mathcal{O}$.

- **Groupe** : $\text{Cl}(\mathcal{O})$

- **Action libre et transitive** :

$$\begin{array}{ccc} \text{Cl}(\mathcal{O}) \times \mathcal{E}\mathcal{H}_q(\mathcal{O}) & \rightarrow & \mathcal{E}\mathcal{H}_q(\mathcal{O}) \\ ([\mathfrak{a}], \overline{E}) & \mapsto & [\mathfrak{a}] * \overline{E} \end{array}$$

c'est-à-dire pour tout $\overline{E}_1, \overline{E}_2 \in \mathcal{E}\mathcal{H}_q(\mathcal{O})$, $\exists! [\mathfrak{a}] \in \text{Cl}(\mathcal{O})$ tel que

$$\overline{E}_2 = [\mathfrak{a}] * \overline{E}_1.$$

Échange de clés

Paramètre public : $\overline{E} \in \mathcal{E}ll_q(\mathcal{O})$



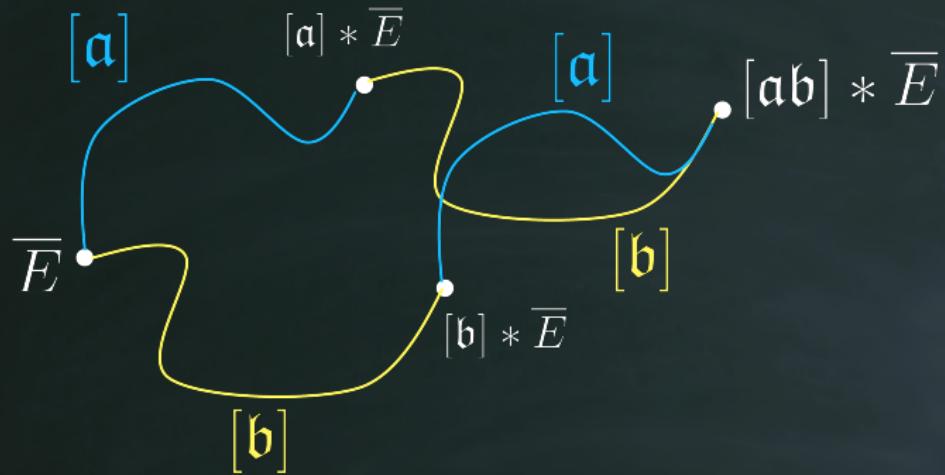
$$\begin{aligned} [\mathfrak{a}] &\in \text{Cl}(\mathcal{O}) \\ \overline{E}_1 &= [\mathfrak{a}] * \overline{E} \end{aligned}$$

$$\begin{aligned} [\mathfrak{b}] &\in \text{Cl}(\mathcal{O}) \\ \overline{E}_2 &= [\mathfrak{b}] * \overline{E} \end{aligned}$$

$$[\mathfrak{a}] * \overline{E}_2 = [\mathfrak{a}] * ([\mathfrak{b}] * \overline{E}) = [\mathfrak{ab}] * \overline{E} = [\mathfrak{b}] * ([\mathfrak{a}] * \overline{E}) = [\mathfrak{b}] * \overline{E}_1$$

Problème : Étant donné $\overline{E}_1 = [\mathfrak{a}] * \overline{E}$ trouver $[\mathfrak{a}]$.

Marches aléatoires sur le graphe d'isogénies



Exemples

- Couveignes - 1997
- Rostovtsev and Stolbounov - 2006 and 2010
- De Feo, Kieffer, Smith - 2018
- CSIDH - 2018
 - *Courbes elliptiques supersingulières définies sur \mathbb{F}_p et l'anneau d'endomorphismes définis sur \mathbb{F}_p .*

Problème

La sécurité des systèmes précédents repose sur le problème mathématique suivant :

Soient E_1 et E_2 deux courbes elliptiques isogènes définies sur un corps fini telles qu'il existe un ordre quadratique imaginaire \mathcal{O} qui satisfait :

$$\mathcal{O} \cong \text{End}(E_i), i = 1, 2.$$

Problème : Trouver une isogénie

$$\phi : E_1 \rightarrow E_2 .$$

Problème

La sécurité des systèmes précédents repose sur le problème mathématique suivant :

Soient E_1 et E_2 deux courbes elliptiques isogènes définies sur un corps fini telles qu'il existe un ordre quadratique imaginaire \mathcal{O} qui satisfait :

$$\mathcal{O} \cong \text{End}(E_i), i = 1, 2.$$

Problème : Trouver une isogénie $[\alpha] \in \text{Cl}(\mathcal{O})$ tel que

$$\phi : E_1 \rightarrow E_2, \quad \bar{E}_2 = [\alpha] * \bar{E}_1.$$

Comment attaquer le problème ?

Problème : Trouver $[\alpha] \in \text{Cl}(\mathcal{O})$ tel que

$$\overline{E}_2 = [\alpha] * \overline{E}_1.$$

- Limiter le nombre d'essais dans $\text{Cl}(\mathcal{O})$:
→ **Hidden Shift Problem**
- Calculer $[\alpha] * \overline{E}_1$ de manière efficiente :
→ **Décomposer $[\alpha]$ en un produit “court”**

Hidden Shift Problem

Problème : Trouver $[\mathfrak{s}] \in \text{Cl}(\mathcal{O})$ tel que

$$\overline{E}_2 = [\mathfrak{s}] * \overline{E}_1.$$

Pour $i = 1, 2$, soient $f_i : \text{Cl}(\mathcal{O}) \rightarrow \mathcal{E}\mathbb{H}_q(\mathcal{O})$, définies par :

$$\left[\begin{array}{l} f_1 : [\mathfrak{a}] \mapsto [\mathfrak{a}] * \overline{E}_1 \\ f_2 : [\mathfrak{a}] \mapsto [\mathfrak{a}] * \overline{E}_2. \end{array} \right.$$

Pour tout $[\mathfrak{a}] \in \text{Cl}(\mathcal{O})$ f_1 et f_2 satisfont :

$$f_2([\mathfrak{a}]) = f_1([\mathfrak{a}\mathfrak{s}]),$$

et nous voulons trouver $[\mathfrak{s}]$ (**shift**).

L'algorithme de Kuperberg

Trouver $[\mathfrak{s}]$ revient à trouver les périodes H d'un oracle f :

$$f : \frac{\mathbb{Z}}{2\mathbb{Z}} \times \text{Cl}(\mathcal{O}) \rightarrow \{\text{Etats quantiques}\}$$

$$f(x, [\mathfrak{a}]) := \begin{cases} |[\mathfrak{a}] * \overline{E}_1\rangle = |f_1([\mathfrak{a}])\rangle, & x = 0 \\ |[\mathfrak{a}]^{-1} * \overline{E}_2\rangle = |f_2([\mathfrak{a}]^{-1})\rangle, & x = 1 \end{cases}$$

Si $N = |\text{Cl}(\mathcal{O})|$ l'algorithme de Kuperberg trouve H en utilisant :

- $2^{O(\sqrt{\log(N)})}$ appels à f et $2^{O(\sqrt{\log(N)})}$ mémoire quantique.
- $2^{O(\sqrt{\log(N)} \log \log(N))}$ appels à f et mémoire quantique polynomiale.

Décomposer $[\mathfrak{a}]$ en un produit “court”

Soit $S = \{[\mathfrak{p}_i]\}_{i=1,\dots,k}$ un ensemble de générateurs de $\text{Cl}(\mathcal{O})$. Alors pour tout $[\mathfrak{a}] \in \text{Cl}(\mathcal{O})$ il existe $(y_1, \dots, y_k) \in \mathbb{Z}^k$ tel que

$$[\mathfrak{a}] = [\mathfrak{p}_1]^{y_1} \cdots [\mathfrak{p}_k]^{y_k}.$$

L'action $[\mathfrak{a}] * \overline{E}_1$ peut être alors calculée de manière itérative à travers :

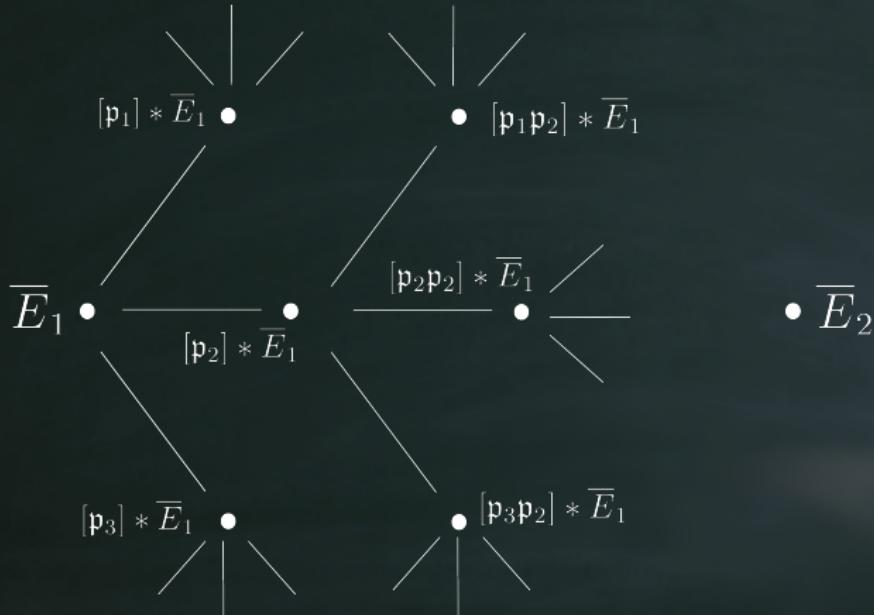
$$([\mathfrak{p}_1]^{y_1} \cdots [\mathfrak{p}_k]^{y_k}) * \overline{E}_1$$

Pour un calcul efficace, nous voulons :

- k “pas trop grand” ;
- \mathfrak{p}_i de norme “pas trop grande” ;
- vecteur (y_1, \dots, y_k) de norme “petite”.

Au même temps dans le graphe d'isogénies..

Supposons que $G = \langle [\mathfrak{p}_1], [\mathfrak{p}_2], [\mathfrak{p}_3] \rangle$ et qu'on veuille trouver un vecteur court (y_1, y_2, y_3) tel que $[\mathfrak{p}_1^{y_1} \mathfrak{p}_2^{y_2} \mathfrak{p}_3^{y_3}] * \overline{E}_1 = \overline{E}_2$.



Réseaux pour trouver un produit court

Problème : étant donné un ensemble de générateurs $\{[\mathfrak{p}_i]\}_{i=1,\dots,k}$ de $\text{Cl}(\mathcal{O})$ et $[\mathfrak{a}] \in \text{Cl}(\mathcal{O})$, trouver une décomposition courte pour $[\mathfrak{a}]$.

- Soit

$$\mathcal{L} \subseteq \mathbb{Z}^k = \left\{ \vec{e} = (e_1, \dots, e_k) : [\mathfrak{p}_1]^{e_1} [\mathfrak{p}_2]^{e_2} \cdots [\mathfrak{p}_k]^{e_k} = 1_{\text{Cl}(\mathcal{O})} \right\}.$$

- Soit $\vec{x} = (x_1, \dots, x_k) \in \mathbb{Z}^k$ tel que

$$[\mathfrak{a}] = [\mathfrak{p}_1]^{x_1} [\mathfrak{p}_2]^{x_2} \cdots [\mathfrak{p}_k]^{x_k}.$$

- Pour $\vec{e} \in \mathcal{L}$, soit $\vec{y} = \vec{x} - \vec{e}$. Alors

$$[\mathfrak{a}] = [\mathfrak{p}_1]^{y_1} [\mathfrak{p}_2]^{y_2} \cdots [\mathfrak{p}_k]^{y_k}.$$

BDD : Trouver $\vec{e} \in \mathcal{L}$ tel que $\|\vec{y}\| = \|\vec{x} - \vec{e}\|$ est petit.

Coûts

Décomposition de $[\mathfrak{a}]$ en un produit “court” :

$$[\mathfrak{a}] = [\mathfrak{p}_1]^{y_1} [\mathfrak{p}_2]^{y_2} \cdots [\mathfrak{p}_k]^{y_k}.$$

- Coût du calcul du réseaux \mathcal{L} : Polynomial [BS16]
- Coût de décomposition de $[\mathfrak{a}]$: Polynomial [BS16]
- Coût de BDD : Polynomial [Ba86]

Évaluation de l'action $[\mathfrak{p}_1]^{y_1} [\mathfrak{p}_2]^{y_2} \cdots [\mathfrak{p}_k]^{y_k} * \overline{E} : 2^{\tilde{O}\left(\sqrt[3]{\log(N)}\right)}$

Heuristiques

Heuristique

Soit $c > 1$ et \mathcal{O} un ordre quadratique imaginaire de discriminant Δ .

Alors il y a $\{\mathfrak{p}_i\}_{i=1,\dots,k}$ pour $k = \log^{2/3}(|\Delta|)$ idéaux premiers de norme inférieure à $\log^c(|\Delta|)$ dont les classes engendrent $\text{Cl}(\mathcal{O})$. De plus, toute classe de $\text{Cl}(\mathcal{O})$ a un représentant de la forme $\prod_i \mathfrak{p}_i^{y_i}$ avec $|y_i| \leq e^{\log^{1/3} |\Delta|}$.

→ Étude de la connectivité et du diamètre du *graphe de Cayley* de $\text{Cl}(\mathcal{O})$.

Conclusions

Nous avons des algorithmes quantiques pour calculer \mathfrak{s} tel que

$$\overline{E}_2 = [\mathfrak{s}] * \overline{E}_1.$$

Temps : $2^{O(\sqrt{\log(N)})}$

Mémoire quantique :
 $2^{O(\sqrt{\log(N)})}$

Temps : $2^{O(\sqrt{\log(N)} \log \log(N))}$

Mémoire quantique : Polynomiale

Merci pour l'attention !