Corps de nombres et cryptologie

Jean-François Biasse
(A. Sylvester, M. Jacobson, D. Sutherland)

University of Calgary

20 mars 2012

Le problème du logarithme discret

Problème du logarithme discret (DLP)

Étant donné un groupe $(G, .)$ et deux éléments $x, y \in G$, on cherche $a \in \mathbb{Z}$ tel que

$$y = x^a.$$

Intérêt cryptographique

La difficulté du DLP dans G permet de définir

- Protocole d'échange de clef
- Protocole d'encryption
- Signature
- Fonction de hachage

Protocole d'échange de clef Diffie-Helman

Une illustration classique de protocole basé sur le DLP. Alice et Bob veulent échanger un secret sur un canal écouté par Eve.

Protocole DH

Soit $g \in G$ connu de tous.

1. Alice choisit $a \in \mathbb{Z}$ au hasard
2. Bob choisit $b \in \mathbb{Z}$ au hasard
3. Alice transmet g^a. Bob transmet g^b
4. Alice calcul $(g^b)^a$. Bob calcul $(g^a)^b$

Alice et bob disposent de g^{ab}.

Résoudre le DLP permet de résoudre le problème DH.

Classes de complexité

Aucune instance du DLP n'est insolvable. On recherche des instances « difficiles »du DLP. Soit $\log(N)$ la taille de l'entrée N.

Complexités classique

- Si le problème est en $O(N^b)$, il est « dûr ».
- Si le problème est en $O(\log(N)^b)$, il est « facile ».

On utilise

$$L_N(a, b) := e^{b((\log(N))^a(\log\log(N))^{1-a}}.$$

Propriétés

1. $L_N(0, b) = \log(N)^b$.
2. $L_N(1, b) = N^b$.
3. $\forall 0 < a < 1,\ L_N(0, b) < L_N(a, b) < L_N(1, b)$.

Instances particulières du DLP

Suivant la nature du groupe G, la difficulté du DLP n'est pas la même.

Instances classiques

1. Courbes elliptiques sur $\mathbb{F}_q$: $O\left(\sqrt{q}\right)$.
2. Courbes hyperelliptiques de genre g fixé sur $\mathbb{F}_q$: $\tilde{O}\left(q^2\right)$.
3. Corps de nombres quadratique de discriminant Δ : $L_\Delta(1/2, O(1))$.
4. Corps finis F_q : $L_q(1/3, O(1))$.

En comparaison, factoriser N se fait en temps

1. $L_N(1/2, O(1))$ (complexité prouvée).
2. $L_N(1/3, O(1))$ (complexité heuristique).

Cas des corps de nombres

Un corps de nombres K et une extension finie de $\mathbb{Q}$.

Propriété

À un corps de nombre K de discriminant Δ, on peut associer

$$K \longleftrightarrow \mathrm{Cl}(K)$$

- $\mathrm{Cl}(K)$ est un groupe fini.
- Le calcul de $\mathrm{Cl}(K)$ est en $L_{\Delta}(1/2, O(1))$
- Le calcul du DLP dans $\mathrm{Cl}(K)$ est en $L_{\Delta}(1/2, O(1))$

Intérêt du DLP dans $\mathrm{Cl}(K)$ car

1. Pas de réduction connue entre DLP pour courbes et dans $\mathrm{Cl}(K)$.
2. Réduction de la factorization d'entier au DLP dans $\mathrm{Cl}(K)$.

Isogénies

L'utilisation d'isogénies a des connexions avec les algorithmes de résolution du DLP dans $\mathrm{Cl}(K)$.

Définitions

Soient deux croubes algébriques $\mathcal{C}_1$ et $\mathcal{C}_2$ sur un corps fini $\mathbb{F}_q$.

- Les cryptosystèmes sont basé dans le groupe fini $\mathcal{J}(\mathcal{C})$ associé à $\mathcal{C}$.
- Une isogénie entre $\mathcal{C}_1$ et $\mathcal{C}_2$ est un morphisme

$$\phi : \mathcal{J}(\mathcal{C}_1) \longrightarrow \mathcal{J}(\mathcal{C}_2).$$

Les isogénies ont un intérêt cryptographique, en particulier car :

- Elles permettent d'attaquer le DLP dans $\mathcal{J}(\mathcal{C}_1)$ à partir du DLP dans $\mathcal{J}(\mathcal{C}_2)$.
- Elles permettent de contruire des cryptosystèmes où la clef secrète est une isogénie entre une courbe « facile »et une courbe « dûre ».

Plan de l'exposé

Objectifs

Dans cet exposé, nous voulons faire le lien entre

- Algorithmes pour le DLP dans $\mathrm{Cl}(K)$
- Algorithmes pour le DLP dans $\mathcal{J}(\mathcal{C})$
- Calcul d'isogénies entre courbes.

DLP dans $\mathrm{Cl}(K)$

- Utilisation du crible quadratique
- Estimations de sécurité

Plan de l'exposé (2)

DLP dans $\mathcal{J}(\mathcal{C})$

- Utilisation du crible quadratique (analogue aux méthodes pour $\mathrm{Cl}(K)$)
- Intérêt des isogénies (construction $\ll$ à la Teske $\gg$)

Isogénies entre courbes

Utilisation de la théorie de la multiplication complexe.

- Lien entre calcul d'isogénies et relations dans $\mathrm{Cl}(K)$
- Lien entre calcul de l'anneau d'endomorphisme et relations dans $\mathrm{Cl}(K)$.

Corps de nombres

Un **corps de nombre** $\mathbb{K}$ est une extension finie $\mathbb{Q} \subset \mathbb{K}$ de dimension n.

$$\begin{array}{c} \mathbb{K} \\ | \\ \mathbb{Q} \end{array}$$

Dans notre étude, on se restreint aux extensions **quadratiques** (ie $n = 2$).

Anneau des entiers

Les entiers de K sont les éléments

$$\mathcal{O}_{\mathbb{K}} := \{x \in K \mid \exists P \in \mathbb{Z}[X] \text{ unitaire tel que } P(x) = 0\}.$$

1. $\mathcal{O}_{\mathbb{K}}$ est un anneau.
2. On résout le DLP entre idéaux de $\mathcal{O}_{\mathbb{K}}$.

Modules

Il est souvent pratique de représenter un ensemble M sous forme de $\mathbb{Z}$-module

$$M = \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_n := \{z_1a_1 + \cdots + z_na_n \mid (z_1, \cdots, z_n) \in \mathbb{Z}^n\}.$$

Anneau des entiers

L'anneau des entiers d'un corps de nombres est un $\mathbb{Z}$-module. En particulier, dans le cas $n = 2$,

$$\mathcal{O}_{\mathbb{K}} = \mathbb{Z} + \frac{\Delta + \sqrt{\Delta}}{2}\mathbb{Z},$$

où Δ est le discriminant de K ($K = \mathbb{Q}(\sqrt{\Delta})$, Δ sans facteurs carrés).

Remarque : dans le cas trivial $K = \mathbb{Q}$, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}$.

Idéaux de $\mathcal{O}_{\mathbb{K}}$

Les éléments impliqués dans le DLP sont des idéaux de $\mathcal{O}_{\mathbb{K}}$. Étant donnés I et J idéaux de $\mathcal{O}_{\mathbb{K}}$ on peut définir

$$I + J = \{i + j \mid i \in I, j \in J\}$$
$$IJ = \{i_1 j_1 + \cdots, i_k j_k \mid k \in \mathbb{Z}_{\geq 0}, (i_l)_{l \leq k} \in I, (j_l)_{l \leq k} \in J\}$$

Idéaux fractionnaires

La notion d'idéal de $\mathcal{O}_{\mathbb{K}}$ est généralisée par les idéaux fractionnaires de K. Ce sont les modules de la forme

$$\mathfrak{a} := q\left(a\mathbb{Z} + \frac{b + \sqrt{\Delta}}{2}\mathbb{Z}\right),$$

où $a, b \in \mathbb{Z}, q \in \mathbb{Q}$.

Propriété des idéaux fractionnaires

soit

$$\mathfrak{a} := q\left(a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z}\right),$$

Propriétés

1. Si $q \in \mathbb{Z}$, $\mathfrak{a}$ est un idéal de $\mathcal{O}_{\mathbb{K}}$
2. Si $q = 1$, $a = p$ premier, $\mathfrak{a}$ est un idéal premier.

Remarques

1. Les idéaux fractionnaires de K sont inversibles.
2. Les idéaux fractionnaires ont une unique factorisation en idéaux premiers.

Groupe de classes d'idéaux

Problématique

On étudie le problème du logarithme discret dans $\mathrm{Cl}(\mathcal{O}_{\mathbb{K}})$ pour $K = \mathbb{Q}(\sqrt{\Delta})$ et $\Delta < 0$ (cas quadratique imaginaire).

Soit K un corps de nombre, on note

1. $\mathcal{I}$ les idéaux fractionnaires de K.
2. $\mathcal{P} \subseteq \mathcal{I}$ les idéaux principaux fractionnaires.

Définition

Le groupe de classes d'idéaux est donné par

$$\mathrm{Cl}(\mathcal{O}_{\mathbb{K}}) := \mathcal{I}/\mathcal{P}.$$

C'est à dire : on identifie $\mathfrak{a}$ et $\mathfrak{b}$ si $\exists \alpha \in K$, $\mathfrak{a} = (\alpha)\mathfrak{b}$.

Logarithme discret d'infrastructure

Le test de principalité de l'idéal $\mathfrak{a}$ consiste à trouver, s'il existe $\alpha \in \mathcal{O}_{\mathbb{K}}$ tel que

$$\mathfrak{a} = (\alpha).$$

DLP d'infrastructure

Étant donné $d > 0$, le DLP d'infrastructure consiste à trouver $\mathfrak{a}$ principal tel que

$$\log |\alpha| \text{ est le plus proche de } d,$$

où $\mathfrak{a} = (\alpha)$.

- Il existe des équivalents des principaux protocoles basés sur le DLP pour le DLP d'infrastructure.
- Ce DLP ne repose pas sur une structure de groupe.

Résolution du DLP dans $\mathrm{Cl}(\mathcal{O}_{\mathbb{K}})$

Problématique

Soient $\mathfrak{a}, \mathfrak{b} \in \mathrm{Cl}(\mathcal{O}_{\mathbb{K}})$, on cherche $a \in \mathbb{Z}$ tel que

$$\mathfrak{b} = \mathfrak{a}^a.$$

- On suppose que l'on dispose de $\mathcal{B} := \{\mathfrak{p}_1, \cdots, \mathfrak{p}_n\}$ engendrant $\mathrm{Cl}(\mathcal{O}_{\mathbb{K}})$.
- On calcule une base de l'ensemble $\mathcal{L}$ des vecteurs $(d_1, \cdots, d_n)$ tels que
$$\mathfrak{p}_1^{d_1} \cdots \mathfrak{p}_n^{d_n} = 1.$$
- On décompose $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$
- On décompose $\mathfrak{b} = \mathfrak{p}_1^{f_1} \cdots \mathfrak{p}_n^{f_n}$

Résolution du DLP dans $\mathrm{Cl}(\mathcal{O}_{\mathbb{K}})$

Observation

Si les lignes de M engendrent $\mathcal{L}$, alors les lignes de

$$M' := \begin{pmatrix} M & 0 & 0 \\ (f_i) & 0 & -1 \\ (e_i) & -1 & 0 \end{pmatrix}$$

engendrent les relations entre $\{\mathfrak{p}_1, \cdots, \mathfrak{p}_n, \mathfrak{a}, \mathfrak{b}\}$

Une solution a du DLP engenre la relation $\mathfrak{a}\mathfrak{b}^{-1} = 1$. Cette relation est engendrée par les lignes de M'. On peut trouver a en résolvant

$$(0, \cdots, 0, 1) = \vec{X} \begin{pmatrix} M & (0) \\ (f_i) & 0 \\ (e_i) & -1 \end{pmatrix}.$$

$a \leftarrow -\vec{X}^{(N+1)}$

Décomposer un idéal

Dans $\mathrm{Cl}(\mathcal{O}_{\mathbb{K}})$, chaque classe contient un idéal de la forme

$$\mathfrak{a} = \left(a\mathbb{Z} + \frac{b + \sqrt{\Delta}}{2}\mathbb{Z} \right)$$

où $\mathcal{N}(\mathfrak{a}) := a \leq \sqrt{|\Delta|}$.

On se donne un ensemble générateur de $\mathrm{Cl}(\mathcal{O}_{\mathbb{K}})$

$$\mathcal{B} = \{\mathfrak{p} \text{ premier } \mid \mathcal{N}(\mathfrak{p}) \leq B\} = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_n\}.$$

Décomposition de l'idéal $\mathfrak{a}$ suivant les éléements de $\mathcal{B}$

- Tant que la décomposition n'est pas trouvée
  1. Tire $(e_1, \cdots, e_n)$ au hasard.
  2. Teste si $\mathfrak{a}\mathfrak{p}^{e_1} \cdots \mathfrak{p}^{e_n}$ se décompose suivant $\mathcal{B}$.

Recherche de relation via trial division

Notre algorithme de décomposition teste successivement si

$$\mathfrak{a} = \left(a\mathbb{Z} + \frac{b + \sqrt{\Delta}}{2}\mathbb{Z} \right)$$

se décompose suivant $\mathcal{B}$, où

$$\mathcal{B} = \{\mathfrak{p} \text{ premier } \mid \mathcal{N}(\mathfrak{p}) \leq B\} = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_n\}.$$

Propriété

Si $a = \mathcal{N}(\mathfrak{a})$ se décompose en produit de nombres premiers bornés par B, alors $\mathfrak{a}$ se décompose suivant $\mathcal{B}$.

- Test successifs de a par « trial division »
- Test simultané de plusieurs a par « batch smoothness test »

Crible quadratique

Flassenberg et Paulus ont proposé un algorithme s'appliquant aux corps quadratiques.

Soit $\mathfrak{a} = a\mathbb{Z} + (b + \sqrt{\Delta})/2\mathbb{Z}$, $\gamma \in \mathfrak{a}$ et $x, y \in \mathbb{Z}$ tels que

$$\gamma = ax + \left(\frac{b + \sqrt{\Delta}}{2}\right) y.$$

Soit c tel que $b^2 - 4ac = \Delta$ discriminant de $\mathbb{K}$, on a

$$\mathcal{N}(\gamma) = \gamma\overline{\gamma} = a\left(ax^2 + 2bxy + cy^2\right) =: \psi(x, y).$$

Stratégie

Soit $\mathcal{B} = \{\mathfrak{p} \text{ premier } \mid \mathcal{N}(\mathfrak{p}) \leq B\}$. Chaque valeur B-friable de de $\psi(X, Y)$ engendre une relation dela forme

$$(\gamma) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_N^{e_N} = 1 \in \mathrm{Cl}(K).$$

Idée principale

On souhaite décomposer $\mathfrak{a}$ suivant $\mathcal{B} = \{\mathfrak{p} \mid \mathcal{N}(\mathfrak{p}) \leq B\}$.

Approche traditionnelle

L'approche traditionnelle repose sur

- Calcul successif d'idéaux de la forme $\mathfrak{a}\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$.
- Pour chaque idéal, on teste si un entier se décompose en facteurs bornés par B.

Approche par méthode de crible

- Calcul d'une forme $\psi(X, Y) = aX^2 + bX + c$ associée à $\mathfrak{a}$.
- Recherche de couples $(x, y) \in \mathbb{Z}^2$ tels que $\psi(x, y)$ se décompose en facteurs bornés par B.

Line sieving

Problématique

- Objectif : trouver les $u \in [-M, M]$ tels que $\psi(u, 1)$ est B-friable.
- Idée : rapidement présélectionner certains u que l'on teste par $\ll$ trial division $\gg$.

Observation principale :

$$\psi(r_p, 1) \equiv 0 \mod p \iff \forall i,\ \psi(r_p + ip, 1) \equiv 0 \mod p.$$

Avantage

Une fois qu'on a x tel que $p \mid \psi(x, 1)$, on a tous les $x \in [-M, M]$ vérifiant cette propriété.

Line sieving

On initialise à 0 un tableau représenant $[-M, M]$

$$\forall u \in [-M, M]\ S[u] \leftarrow 0.$$

Algorithme pour le calcul de valeurs friables $u \in [-M, M]$ de $\psi(X, 1)$

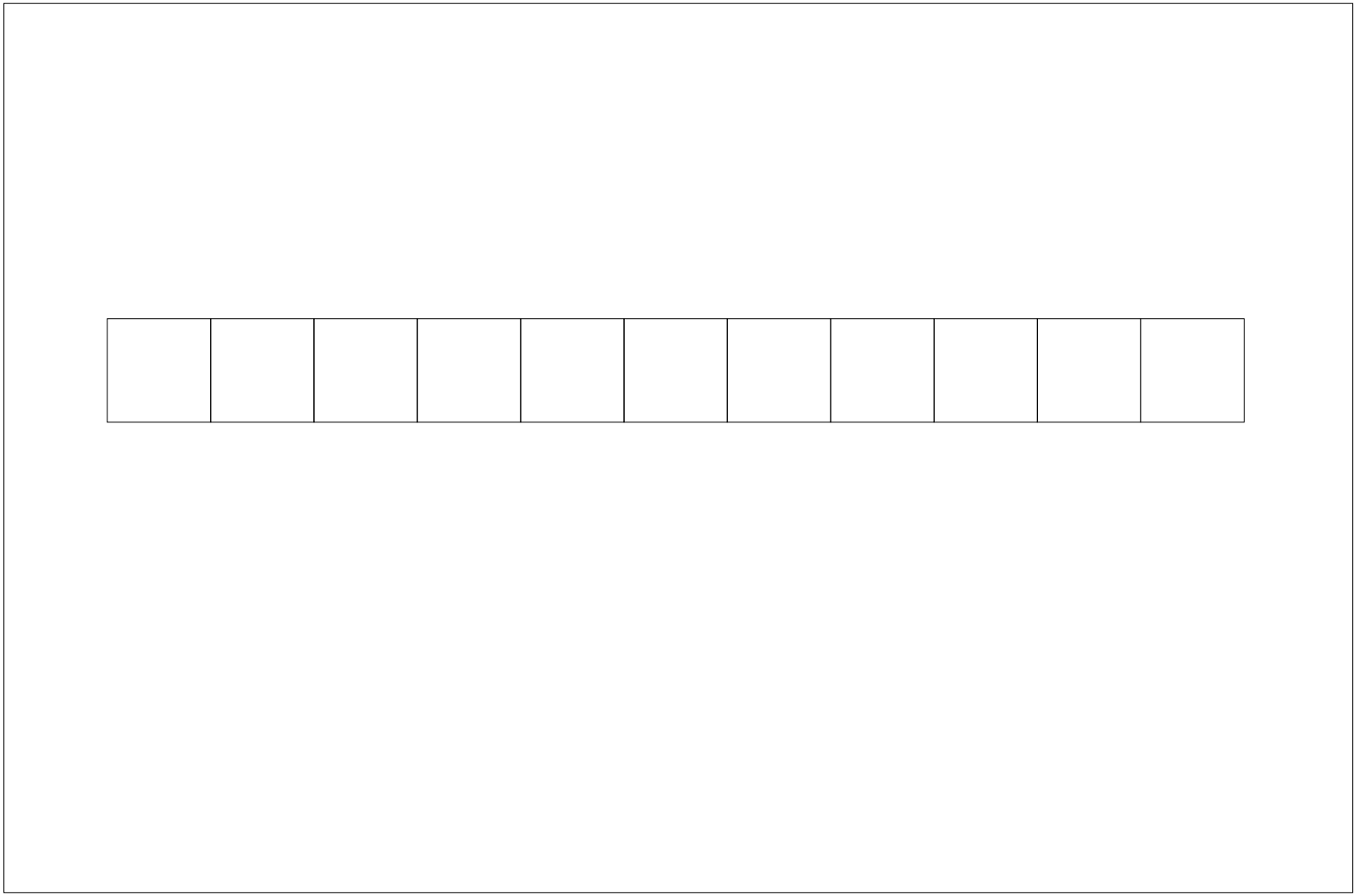
Entrée : ψ, M , B.
Sortie : Valeurs B-friables de $\psi(X, 1)$ dans $[-M, M]$.

Pour tout $p \leq B$.

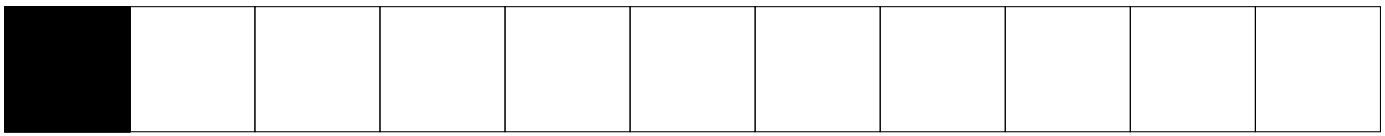
- Calcul des racines r_p de $\psi \mod p$.
- $\forall p \leq p$, $\forall i$ tel que $r_p + ip \in [-M, M]$, $S[r_p + ip] \leftarrow S[r_p + ip] + \log(p)$

Pour chaque u tel que $S[u]$ est « grand », tester $\psi(u, 1)$.

Exemple

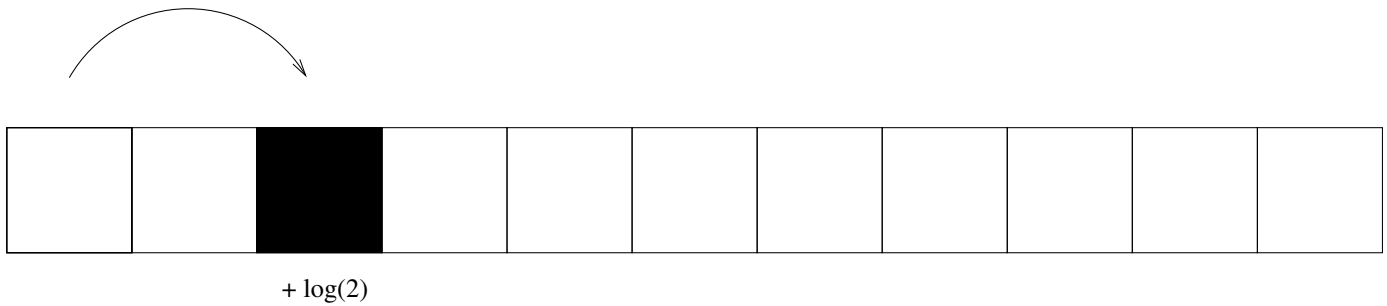


Exemple

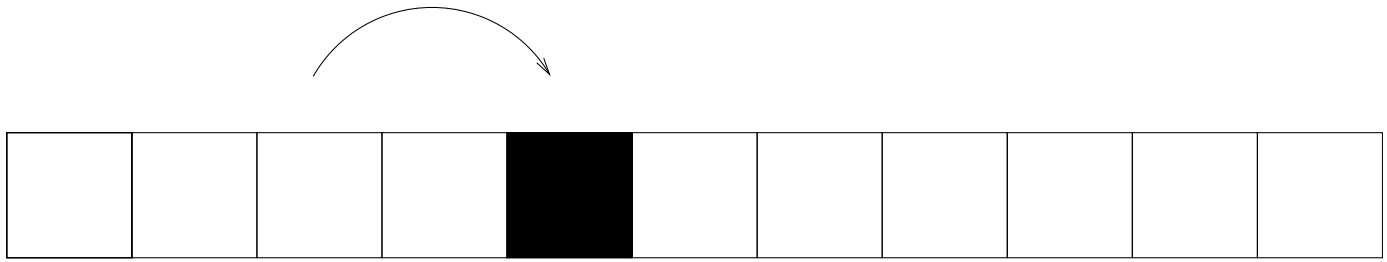


+ log(2)

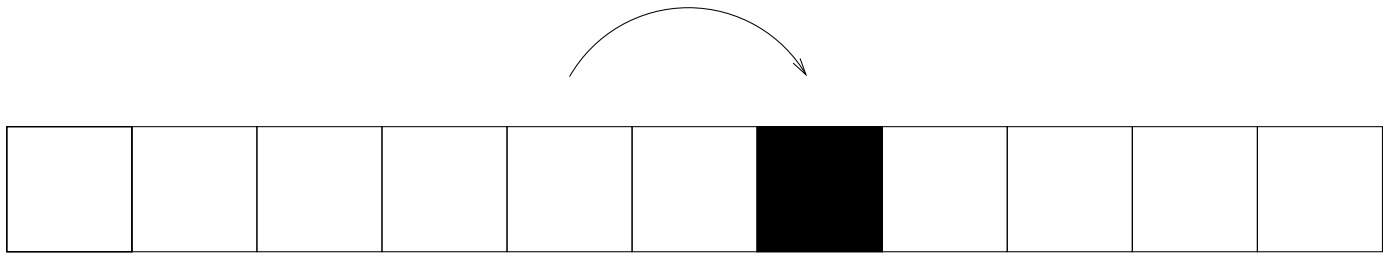
Exemple



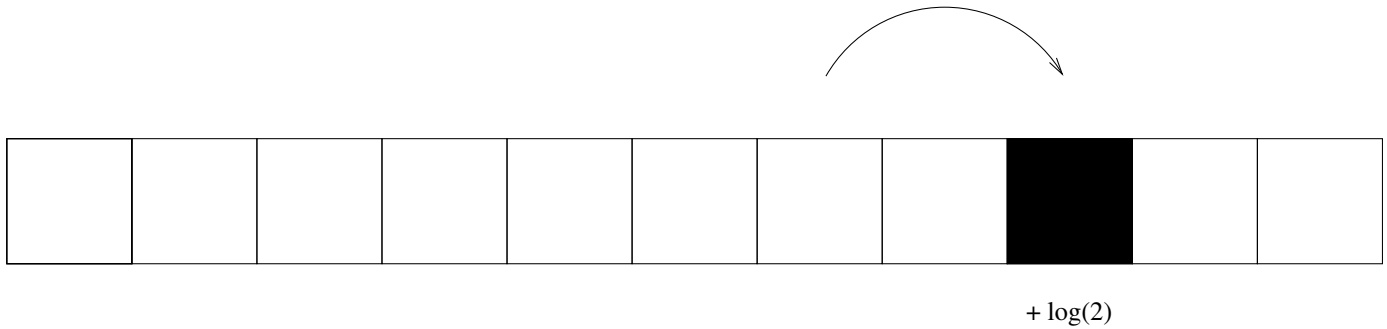
Exemple



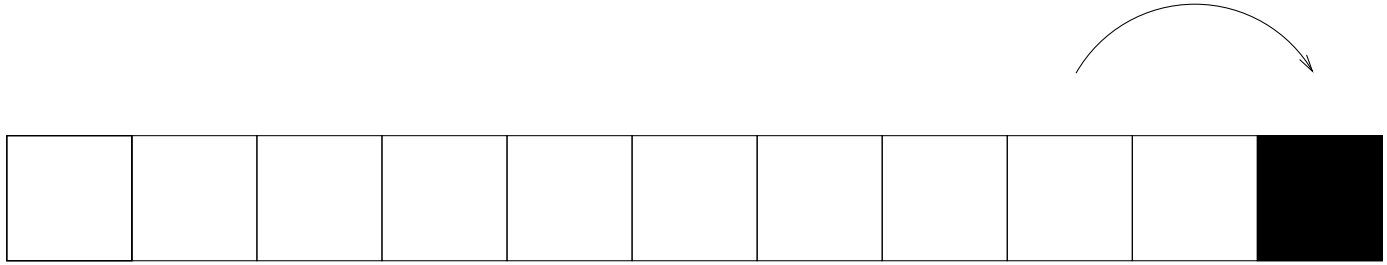
Exemple



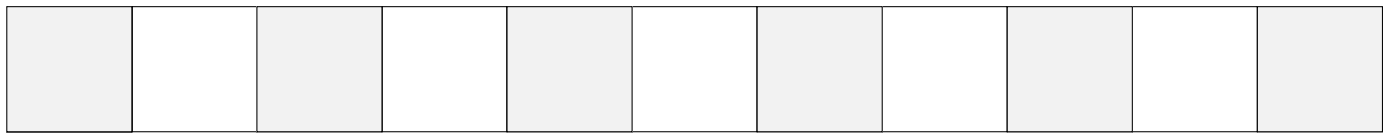
Exemple



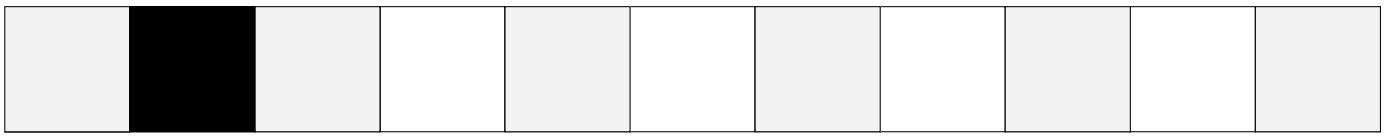
Exemple



Exemple



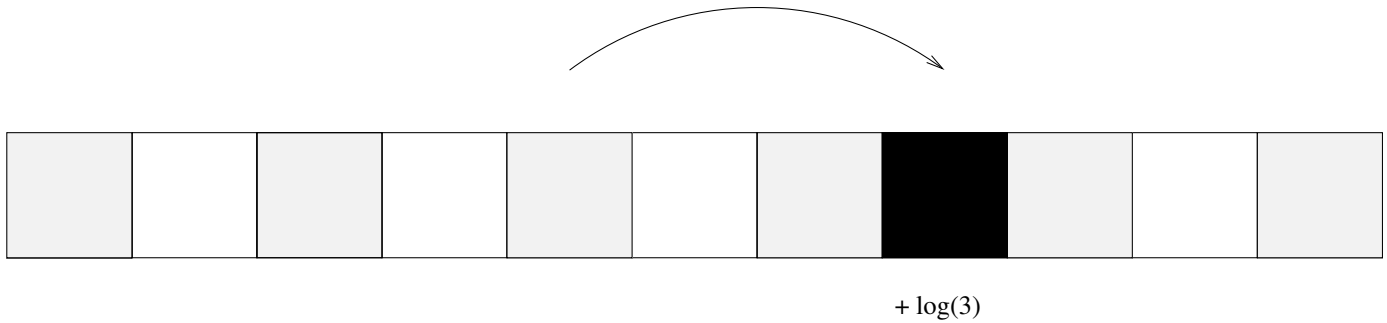
Exemple



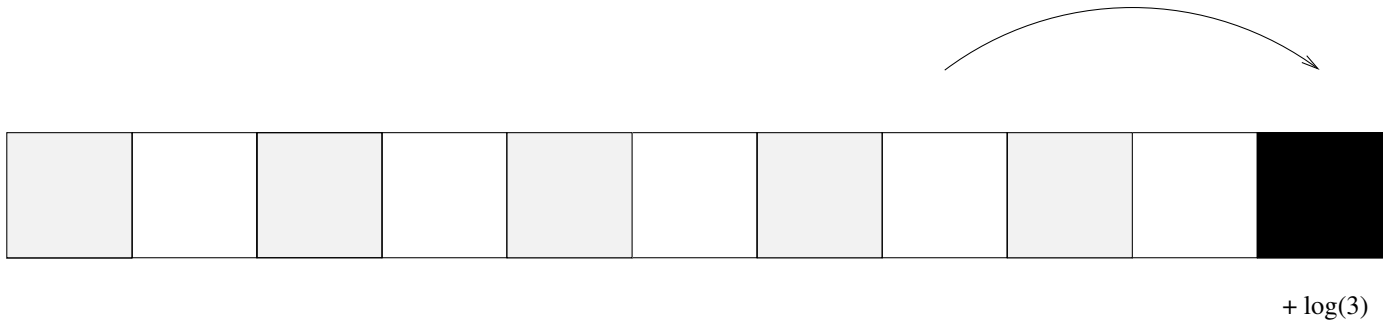
+ log(3)

Exemple

Exemple

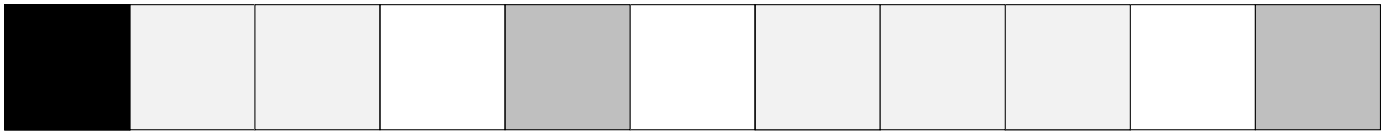


Exemple



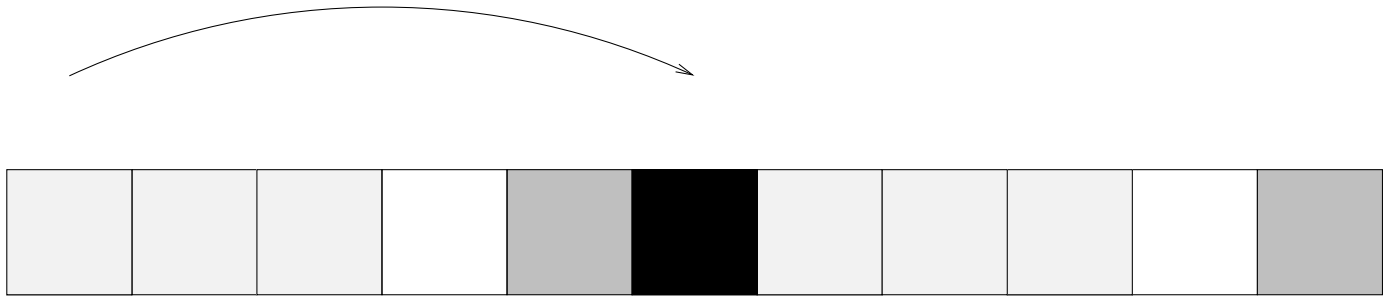
Exemple

Exemple

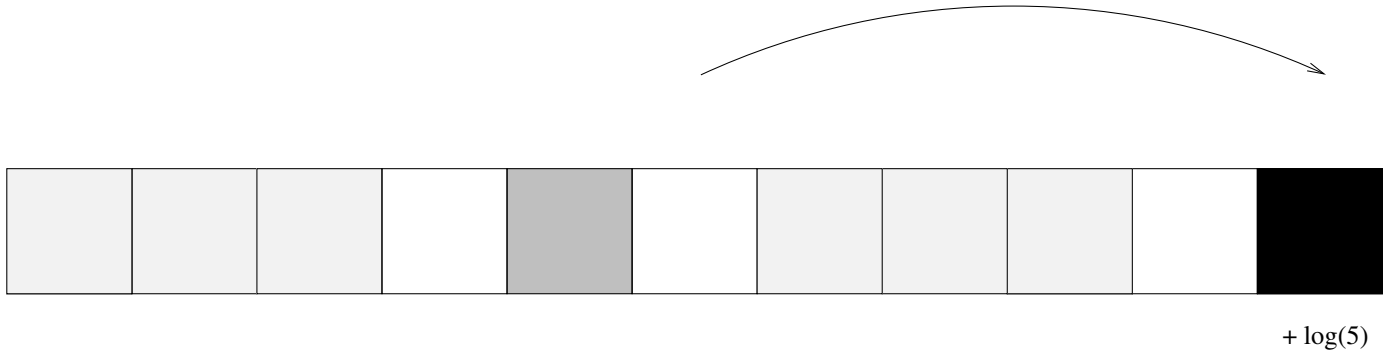


+ log(5)

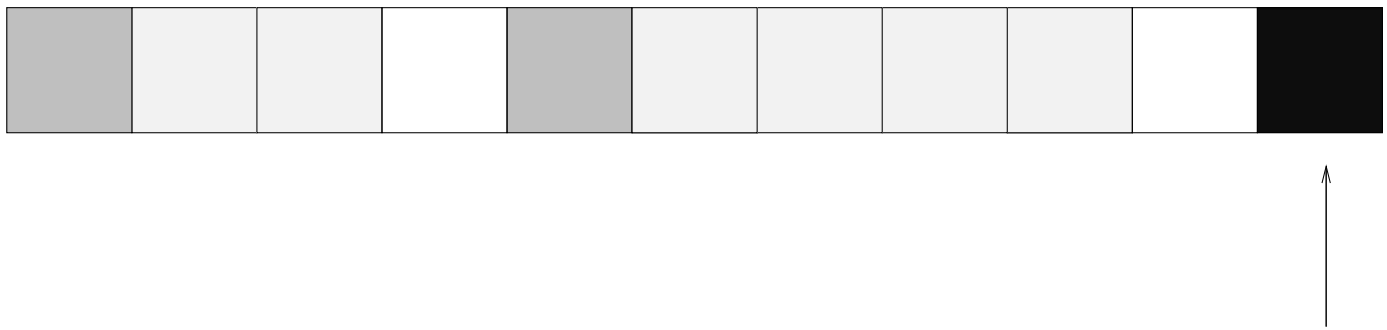
Exemple



Exemple



Exemple



Temps d'exécution de l'algorithme de DLP

Complexité

La complexité prouvée (sous ERH) est

$$L_\Delta(1/2, \sqrt{2}).$$

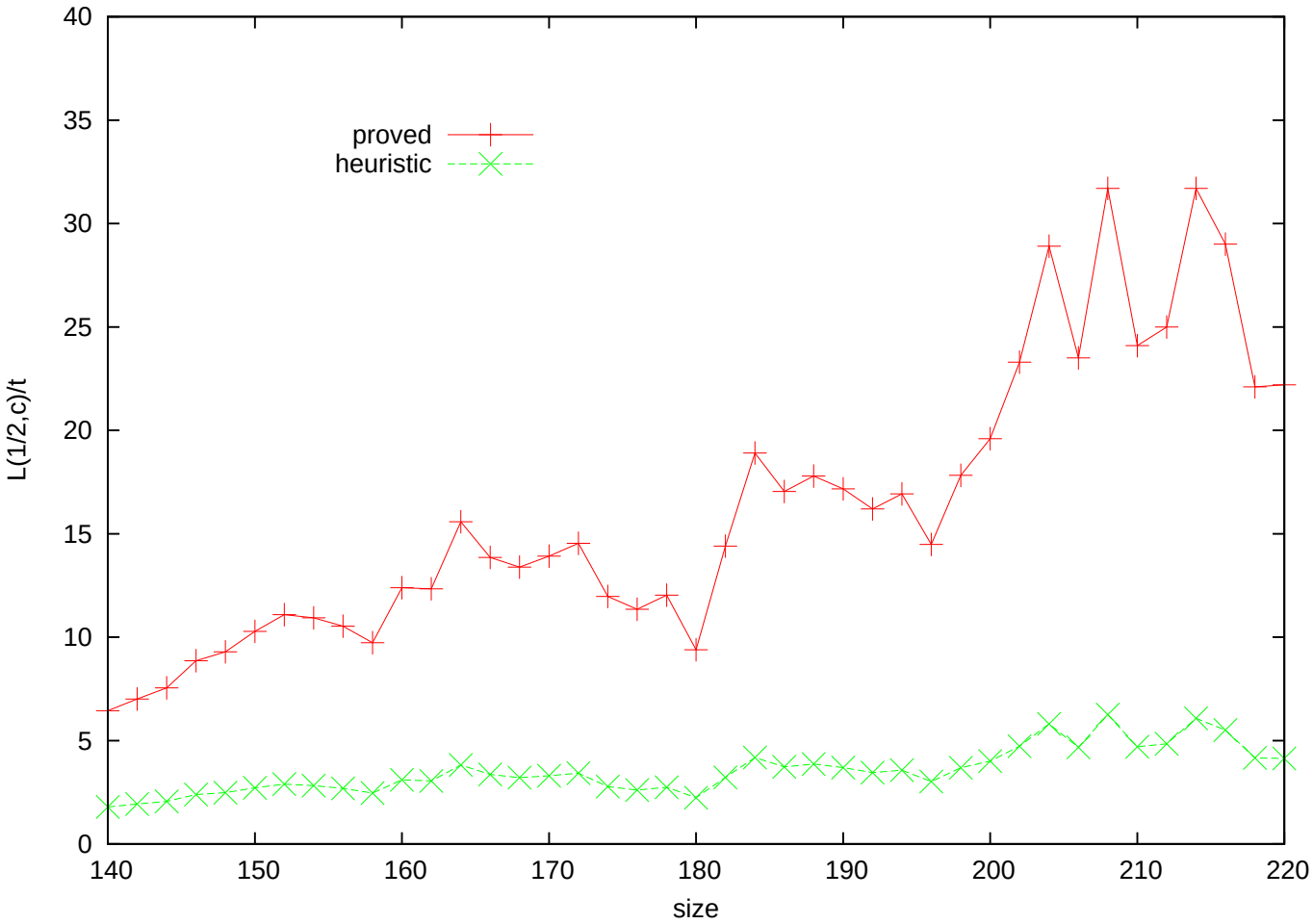
(HamMöl00') : La complexité heuristique

$$L_\Delta(1/2, 1)$$

Pour choisir, on considère $L_\Delta(1/2, c)/t_\Delta$ (qui devrait être une constante), où

- $c \in \{1, \sqrt{2}\}$.
- $\Delta = 140, 142, \ldots, 220$
- t_Δ est le temps moyen de résolution du DLP sur 10 discriminants premiers tirés au hasard

Comparison de $L_\Delta(1/2, c)/t_\Delta$



Estimations de sécurité pour le cas imaginaire

Incorporation d'amélioration pratiques

- Grands premiers
- Test de friabilité en lot
- Élimination structurée

RSA	Δ (imaginary, old)	Δ (imaginary)	Est. run time
768	540	640	8.80×10^6
1024	687	798	1.07×10^{10}
2048	1208	1348	1.25×10^{19}
3072	1665	1827	4.74×10^{25}
7680	n.a	3598	1.06×10^{45}
15360	n.a	5971	1.01×10^{65}

Effort de calcul en MIPS-year.

Estimations de sécurité pour le cas réel

Rappel

Dans le **cas réel** ($\Delta > 0$), les cryptosystèmes reposent sur la difficulté du DLP d'infrastructure.

Aucune estimation pour le cas réel n'était disponible.

RSA	Δ (imaginary)	Δ (real)	Est. run time
768	640	634	8.80×10^{6}
1024	798	792	1.07×10^{10}
2048	1348	1341	1.25×10^{19}
3072	1827	1818	4.74×10^{25}
7680	3598	3586	1.06×10^{45}
15360	5971	5957	1.01×10^{65}

Courbe hyperelliptiques imaginaire

Définition

Une courbe hyperelliptique imaginaire $\mathcal{C}$ de genre g sur un corps fini $\mathbb{F}_q$ est l'ensemble des solutions de

$$Y^2 + h(X)Y = f(X)$$

où $\deg(h) \leq g$ et $\deg(f) = 2g + 1$.

- En général, les points de $\mathcal{C}$ ne forment pas un groupe.
- On associe à $\mathcal{C}$ le groupe fini $\mathcal{J}(\mathcal{C})$ qui satisfait

$$\#\mathcal{J}(\mathcal{C}) \approx q^g.$$

Stratégie

On souhaite traiter $\mathcal{J}(\mathcal{C})$ comme $\mathrm{Cl}(\mathcal{O}_{\mathbb{K}})$ pour y étudier le DLP.

Utilisation des corps de fonctions

Soit $\mathcal{C}$ sur $k = \mathbb{F}_q$ donnée par $Y^2 + h(X)Y = f(X)$.

Définition

On définit

- $k[\mathcal{C}] := k[X, Y]/(Y^2 + h(X)Y = f(X))$
- $k(\mathcal{C}) := \{f/g \mid f, g \in k[\mathcal{C}], g \neq 0\}$

On définit $\mathrm{Cl}(k[\mathcal{C}])$ avec l'analogie

- $\mathbb{Z} \leftrightarrow \mathbb{F}_q[X]$
- $\mathcal{O}_{\mathbb{K}} \leftrightarrow k[\mathcal{C}]$
- $K \leftrightarrow k(\mathcal{C})$

Propriété

Le groupe de classes d'idéaux vérifie

$$\mathrm{Cl}(k[\mathcal{C}]) \simeq \mathcal{J}(\mathcal{C})$$

Recherche de relations dans $\mathcal{J}(\mathcal{C})$

Pour résoudre le problème du logarithme discret dans $\mathcal{J}(\mathcal{C})$, il faut trouver des relations entre éléments de

$$\mathcal{B} = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_n\},$$

où $\mathcal{B}$ engendre $\mathcal{J}(\mathcal{C})$.

Stratégies

- Marche aléatoire (test de produits aléatoires d'éléments dans $\mathcal{B}$).
- Crible quadratique ([Flassenberg-Paulus]). Par analogie au cas $\mathrm{Cl}(\mathcal{O}_{\mathbb{K}})$, on peut réduire la recherche de relations à la recherche de polynômes S, T tels que

$$\psi(S, T) := aS^2 + bST + cT^2$$

soit de degré borné, où $a, b \in \mathbb{F}_q[X]$.

Les techniques de crible se révèlent efficaces pour les genres élevés.

Courbes de genre élevé en cryptologie

Les cryptosystèmes ne reposent pas sur la difficulté du DLP dans la jacobienne d'une courbe de genre élevé.

Descente de Weil ([Hess])

Étant donnée une courbe elliptique E $(g = 1)$ sur $F_{2^{pq}}$, il est possible de plonger

$$\mathcal{J}(E) \longrightarrow \mathcal{J}(\mathcal{C})$$

où $\mathcal{C}$ est une courbe hyperelliptique sur $\mathbb{F}_{2^q}$ de genre $g > 1$.

Les cryptosystèmes ne reposent pas sur la difficulté du DLP dans une courbe elliptique sujette à la descente de Weil.

Cryptosystème à la Teske ([Teske])

On peut utiliser la descente de Weil à des fins constructive.

- Publique : courbe elliptique E_1 non sujette à la descente de Weil.
- Privé : Isogénie $\varphi E_1 \to E_2$ où E_2 est sujette à la descente de Weil.

Efficacité du crible dans les courbes de genre élevé

4 courbes hyperelliptiques de genre $g = 31$ issues d'une descente de Weil (C_q provient d'une courbe elliptique sur $\mathbb{F}_q$).

- C_{62} définie sur $\mathbb{F}_4$,
- C_{93} définie sur $\mathbb{F}_8$,
- C_{124} définie sur $\mathbb{F}_{16}$,
- C_{155} définie sur $\mathbb{F}_{32}$,

Timings sur 1 coeur ([Thèse de Velishka]).

courbe	Marche aléatoire	Crible
C_{62}	27 min 57 sec	21 min 56 sec
C_{93}	2j 5h 46 min	11h 58 min
C_{124}	244j 21 min	81j 8h 3min
C_{155}	6340j (est.)	21j 7h 39min

Isogénies et anneau d'endomorphismes

Isogénies

Soient $\mathcal{C}_1$ et $\mathcal{C}_2$ deux courbes hyperelliptiques de genre g, une isogénie est une application rationnelle $\mathcal{C}_1 \to \mathcal{C}_2$ induisant un morphisme

$$\varphi : \mathcal{J}(\mathcal{C}_1) \to \mathcal{J}(\mathcal{C}_2).$$

$\mathcal{C}_1$ et $\mathcal{C}_2$ sont l-isogènes si $\deg(\varphi) = l$.

Anneau d'endomorphisme

On note $\mathrm{End}(\mathcal{C})$ l'ensemble des morphismes

$$\varphi : \mathcal{J}(\mathcal{C}) \to \mathcal{J}(\mathcal{C}).$$

$\mathrm{End}(\mathcal{C})$ a une structure d'anneau pour l'addition et la composition.

Multiplication complexe

Soit $\mathcal{C}$ une courbe hyperelliptique de genre g. On a dans tous les cas

$$\mathbb{Z} \subseteq \mathrm{End}(\mathcal{C}).$$

Courbe CM

Si on a

$$K \subseteq \mathbb{Q} \otimes \mathrm{End}(\mathcal{C})$$

pour un certain corps de nombres K de degré $2g$, on dit que $\mathcal{C}$ a multiplication complexe par K.

Dans le cas où $\mathcal{C}$ est une courbe elliptique ($g = 1$), on a

$$\mathrm{End}(\mathcal{C}) \simeq \mathcal{O},$$

où $\mathcal{O}$ est un sous-anneau d'un corps quadratique imaginaire K.

Calcul d'isogénies

Chaque classe d'isomorphismes de courbes est identifiable par son j-invariant.

Polynômes modulaires

$\mathcal{C}_1$ et $\mathcal{C}_2$ sont l-isogènes (avec $\gcd(\mathrm{char}(K), l) = 1$) si

$$\Phi_l(j(\mathcal{C}_1), j(\mathcal{C}_2)) = 0,$$

où Φ_l est le l-ième polynôme modulaire.

Calcul d'isogénie

- Calcul de Φ_l [Bröker-Lauter-Sutherland].
- Elkies' algorithm : soit $\mathcal{C}_1$ et Φ_l, calcul de $\mathcal{C}_2$ et $\ker(\varphi)$.
- Formules de Vélu : soit $\ker(\varphi)$, calcul de φ.

Efficace pour les petits degrés

Calcul d'isogénies de large degré ([Bröker-Charles-Lauter])

Soit E une courbe elliptique CM sur $\mathbb{F}_q$ et

$$\mathcal{O} \simeq \mathrm{End}(E).$$

On utilise la correspondance

$$\text{isogénie de degré d} \longleftrightarrow \text{idéal de norme d de } \mathcal{O}$$

Stratégie

On souhaite évaluer une isogénie φ de degré n (large). Soit $B > 0$

- On trouve $\mathfrak{a} \leftrightarrow \varphi$.
- On décompose $[\mathfrak{a}]$ en classes d'idéaux premiers $\mathfrak{p}$ avec $\mathcal{N}(\mathfrak{p}) < B$.
- On calcule φ comme composée des $\varphi_{\mathfrak{p}} \leftrightarrow \mathfrak{p}$

Calcul de End(E) ([Bisson-Sutherland])

End(E) est un anneau satisfaisant

$$\mathbb{Z}[\pi] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_{\mathbb{K}}$$

où π est le Frobenieus.

Observation

Soient $\mathbb{Z}[\pi] \subseteq \mathcal{O}, \mathcal{O}' \subseteq \mathcal{O}_{\mathbb{K}}$ et $\mathfrak{p}_1, \cdots, \mathfrak{p}_n, (e_1, \cdots, e_n)$. Si

$$\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n} = 1 \in \mathrm{Cl}(\mathcal{O})$$
$$\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n} \neq 1 \in \mathrm{Cl}(\mathcal{O})$$

Alors $\mathcal{O} \subsetneq \mathcal{O}'$.

- On dispose d'un critère pour vérifier si $\prod_i \mathfrak{p}_1^{e_i} = 1 \in \mathrm{Cl}(\mathrm{End}(E))$ sans connaître End(E).
- On parcours les anneaux entre $\mathbb{Z}[\pi]$ et $\mathcal{O}_{\mathbb{K}}$ en testant l'inclusion à chaque étape.

Timings

Méthodologie

Moyenne pour le calcul d'une relation dans $\mathrm{Cl}(\mathcal{O})$ pour 10 $\mathcal{O}$ différents où

$$\log_2(\mathrm{disc}(\mathcal{O})) = 200.$$

La relation cherchée implique les éléments de
$\mathcal{B} = \{\mathfrak{p} \text{ idéal premier de } \mathcal{O}_{\mathbb{K}} \mid \mathcal{N}(\mathfrak{p}) \leq B\}$

timings en CPU sec

$\max \mathcal{N}(\mathfrak{p})$	10000	9000	8000	7000	6000	5000	4000	3000
Approche trad.	72	48	72	163	268	421	553	2642
Crible	10	10	13	22	29	39	162	627
Calcul Φ_l	3600	1630	1100	621	395	219	101	47

Conclusion

On a vu le lien entre

- DLP dans $\mathrm{Cl}(K)$.
- DLP dans $\mathcal{J}(\mathcal{C})$
- calcul d'isogénies

Développements futurs

Les techniques de crible existent pour $\dim(K) > 2$ [B. Fieker 2012]. Par analogie, elles permettent d'étudier

- DLP dans la jacobienne d'une courbe non hyperelliptique.
- Isogénies entre courbes de genre $g > 1$.