Algorithmes arithmétiques pour la cryptologie — 6 Février 2016, Paris

Crible algébrique (NFS)

Razvan Barbulescu
CNRS et IMJ-PRG

L'intérêt des diagrammes commutatifs

Exemple pour log discret (avec les entiers de Gauss)

- But: Logs discrets dans $\mathbb{F}_p$ pour $p \equiv 1 \mod 4$.
- Calculer une racine de $r^2 + 1 = 0$ dans $\mathbb{F}_p$ et mettre $f = x - r$ et $g = x^2 + 1$.
- Calculer les paires d'entiers (a, b) telles que $F(a, b) = a - rb$ et $G(a, b) = a^2 + b^2$ sont friables.
- Factoriser $a - br = \prod q_i^{e_i}$ et $(a - \sqrt{-1}b) = \prod(\pi_j + \sigma_j\sqrt{-1})^{\epsilon_j}$
  ($\mathbb{Z}[\sqrt{-1}]$ est factoriel).
  Puisque $G(a, b) = a^2 + b^2 = \prod_j(\pi_j^2 + \sigma_j^2)$, tous q_i, π_j et σ_j sont petits.
- On obtient, dans $\mathbb{F}_p^*$:

$$\prod q_i^{e_i} \equiv a - br \equiv \prod(\pi_j + \sigma_j r)^{\epsilon_j} \mod p.$$

- Prendre le logarithme discret des deux côtés de l'équation.
- Continuer comme dans Index Calculus.

Que change?

Si f et g ont des petits coefficients, on remplace la probabilité de friabilité d'un grand entier par celle que deux entiers très petits soient friables au même temps.

Sélection polynomiale

But

Trouver deux polynômes f et $g \in \mathbb{Z}[x]$ ayant une racine commune modulo un entier donné (N composé pour la factorisation et p premier pour le log discret) qui n'est pas commune dans $\mathbb{Z}$ et qui ont des petits degrés et coefficients.

Entiers de Gauss

Dans l'exemple précédent on utilise la reconstruction rationnelle(EEA) pour écrire $r \equiv u/v \mod p$ avec $u, v \approx \sqrt{p}$. Remplacer f par $u - xv$, donc $\|f\|_\infty \approx \sqrt{p}$. Alors

1. $F(a, b) \approx \sqrt{p}$,
2. $G(a, b)$ très petit.

C'est comme si on testait la friabilité de nombres de taille $\sqrt{p}$ au lieu de p.

Base-m

On pose $m = \lfloor N^{1/d} \rfloor$ et on écrit $N = m^d + N_{d-1}m^{d-1} + \cdots N_1 m + N_0$ en base M et pose

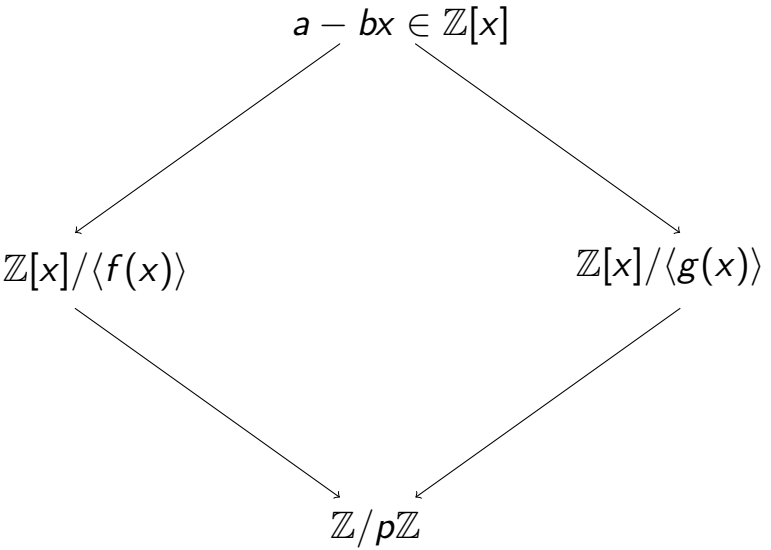
- $f = x^d + \cdots + N_1 x + N_0$;
- $g = x - m$.

On a $|F(a, b)| \approx E^d m$ et $|G(a, b)| \approx Em$ où E est le majorant de $|a|$ et $|b|$.

Le crible algébrique (NFS): diagramme

NFS for DLP in $\mathbb{F}_p$

Soient $f, g \in \mathbb{Z}[x]$ deux polynômes irréductibles, qui ont une racine commune m modulo p.



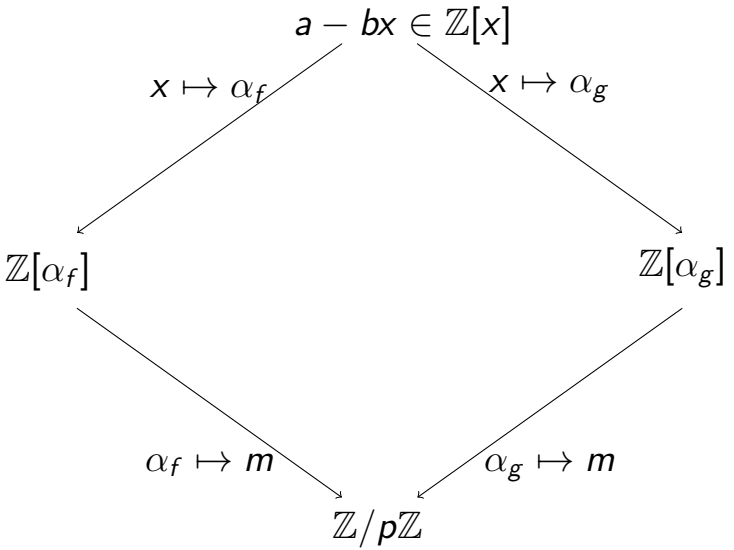
Calculs dans $\mathbb{Z}[\alpha_f]$?

- Les parties mathématiques sont négligeables en temps, mais cause de bugs.
- Implantations disponibles: PARI/GP, Magma, CADO.

Le crible algébrique (NFS): diagramme

NFS for DLP in $\mathbb{F}_p$

Soient $f, g \in \mathbb{Z}[x]$ deux polynômes irréductibles, qui ont une racine commune m modulo p.



Calculs dans $\mathbb{Z}[\alpha_f]$?

- Les parties mathématiques sont négligeables en temps, mais cause de bugs.
- Implantations disponibles: PARI/GP, Magma, CADO.

NFS: algorithme pour logs discrets

Input a finite field $\mathbb{F}_{p^n}$, two elements t (generator) and s
Output $\log_t s$

1: (Polynomial selection) Choose two polynomials f and g in $\mathbb{Z}[x]$ such that one has the diagram presented before;

2: (Sieve) Collect coprime pairs (a, b) such that $F(a, b)$ and $G(a, b)$ are B-smooth (for a parameter B);

3: Write a linear equation for each pair (a, b) found in the Sieve stage.

4: (Linear algebra) Solve the linear system to find (virtual) logarithms of the prime ideals of norm less than B;

5: (Individual logarithm) Write $\log_t s$ in terms of the previously computed logs.

Base de facteurs

Attention: on factorise en idéaux et non pas en éléments. On a $F(a, b)G(a, b)$ friable si et seulement si $(a - \alpha_f b)$ et $(a - b\alpha_g)$ se factorise en idéaux de la base de facteurs.

NFS: algorithme pour factorisation

Input an integer N
Output with probability 50% a non-trivial factor of N

1: (Polynomial selection) Choose two polynomials f and g in $\mathbb{Z}[x]$ such that one has the diagram presented before;

2: (Sieve) Collect coprime pairs (a, b) such that $F(a, b)$ and $G(a, b)$ are B-smooth (for a parameter B);

3: Write an exponent vector for each pair (a, b) found in the Sieve stage, modulo 2.

4: (Linear algebra) Find a linear combination of the rows of M which sum to zero;

5: (Square root) Compute a product in the number fields to obtain $X^2 \equiv Y^2 \mod N$.

Probabilité de Succés

Quand on utilise Block Wiedemann on calcule au moins 32 solutions à la fois. On répète uniquement le calcule de racine carré (x et y à partir de $x^2 \equiv y^2 \pmod N$). On réussit avec probabilité $1 - 2^{-32}$.

Sélection polynomiale

Exemple facile $p = 65537$

$f = x^2 + 1$ et $g = x - 256$ ont une racine commune modulo p car $p = 256^2 + 1$.

Cas général (méthode de la base m): ex $p = 314159$

- on choisit d en fonction des autres étapes de l'algorithme, en pratique $d \leq 6$, par exemple $d = 2$;
- on choisit un entier m proche de $p^{\frac{1}{d+1}}$, par exemple $m = 100 \approx 314159^{\frac{1}{3}}$;
- on écrit p en base m, par exemple $p = 31 \cdot 100^2 + 41 \cdot 100 + 59$, et on pose $f = 31x^2 + 41x + 59$ et $g = x - m = x - 100$.

En effet, f et g ont m comme racine commune modulo p.

Collecte de relations

Crible (identique dans le cas facile et le cas général)

Fixer deux paramètrs E et B. Énumérer toutes les paires (a, b) d'entiers de valeur absolue $\leq E$ pour un paramètre E, avec $a > 0$, et trouver celles où

- $\sum_{i=0}^{d} f_i a^i b^{d-i}$ est B-friable;
- $a - bm$ est B-friable;
- $\mathrm{pgcd}(a, b) = 1$.

Exemple $p = 314159$

- $E = B = 50$;
- conditions: $\mathrm{pgcd}(a, b) = 1$ et $31a^2 + 41ab + 59b^2$ et $a - 100b$ sont 50-friables;
- relations=$\{$(1, 0), (2, -9), (3, -4), (4, -11), (4, -1), (4, 3), (4, 31), (5, -4), (5, -1), (5, 2), (5, 16), (5, 27), (6, 1), (7, -38), (8, -25), (8, -1), (9, -2), (10, -3), (11, -32), (11, 3), (11, 10), (13, 1), (16, 5), (18, -11), (19, -14), (25, -19), (25, 24), (25, 49), (26, 17), (28, -41), (29, -43), (31, 4), (34, 3), (35, -26), (41, -8), (44, -29), (45, -31)$\}$.

Exemple $p = 65537$

- $E = 50$ et $B = 20$;
- conditions: $\mathrm{pgcd}(a, b) = 1$ et $a^2 + b^2$ et $a - 256b$ sont 20-friables;
- relations=$\{$ (0, -1), (0, 1), (1, -2), (1, 0), (1, 1), (2, -3), (4, -1), (4, 1), (7, 24), (8, -1), (12, -5), (13, 1), (16, -13), (18, 1), (23, -7), (23, 11), (24, 7), (32, 43), (38, -1), (41, -23), (46, 3), (47, 1)$\}$.

Intermezzo mathématique

Factorisation dans un corps de nombres

Si $f \in \mathbb{Q}[x]$ on note α une racine complexe de f. Alors tout entier de de $\mathbb{Q}(\alpha)$ se factorise de manière unique en idéaux premiers (théorie algébrique des nombres).

exemple facile $f = x^2 + 1$: L'anneau des entiers est

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

Theorème: Les éléments premiers de $\mathbb{Z}[i]$ sont $1 + i$, les premiers de $\mathbb{Z}$ congriuents à 3 modulo 4 et les nombres $a \pm ib$ où $a, b \in \mathbb{Z}$ sont tels que $a^2 + b^2 = p$ premier congruent à 1 modulo 4.

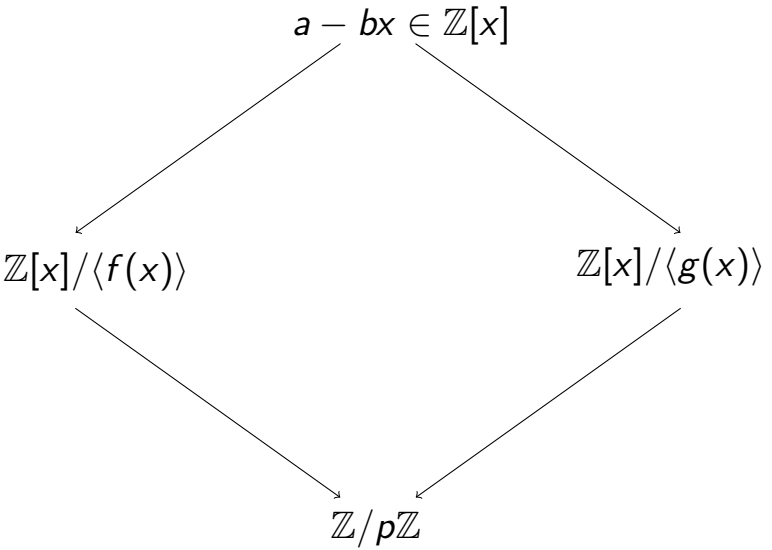
Norme d'un élément d'un corps de nombres

- cas général: on appelle norme de $a \in \mathbb{Q}(\alpha)$ le déterminant de l'application $x \mapsto ax$. Théorème: la norme de a est le produit des normes des iéaux premiers de sa factorisation (norm d'un idéal=indice dans l'anneau des entiers).
- cas de $f = x^2 + 1$: $N(a + ib) = a^2 + b^2 = |a + ib|^2$. Par exemple $8 + i = (-i)(2 + 3i)(2 + i)$ et alors $N(8 + i) = 8^2 + 1 = N(i)N(2 + 3i)N(2 + i) = 1 \cdot (2^2 + 3^2) \cdot (2^2 + 1^2)$.

Construction des équations (1/2)

NFS for DLP in $\mathbb{F}_p$

Soient $f, g \in \mathbb{Z}[x]$ deux polynômes irréductibles, qui ont une racine commune m modulo p.



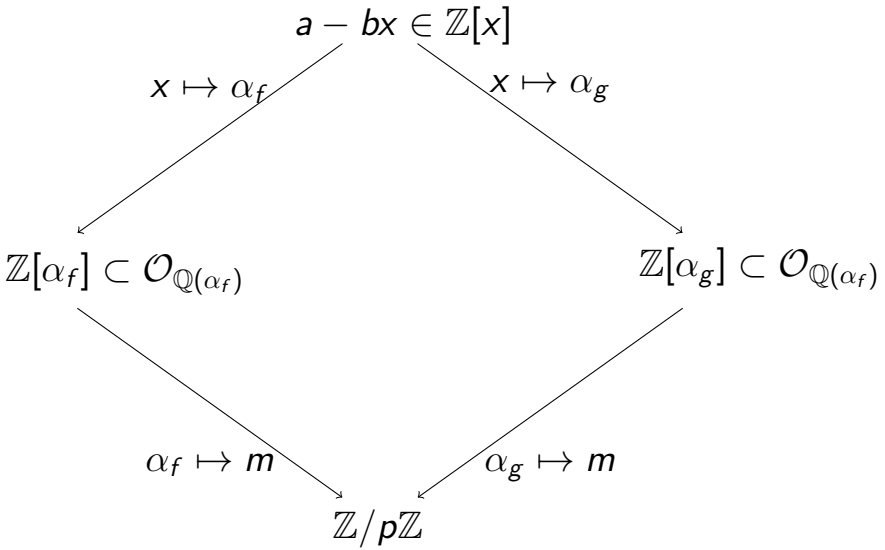
Calculs dans $\mathbb{Z}[\alpha_f]$?

- Les parties mathématiques sont négligeables en temps, mais causent de bugs.
- Implantations disponibles: PARI/GP, Magma, CADO.

Construction des équations (1/2)

NFS for DLP in $\mathbb{F}_p$

Soient $f, g \in \mathbb{Z}[x]$ deux polynômes irréducibles, qui ont une racine commune m modulo p.



Calculs dans $\mathbb{Z}[\alpha_f]$?

- Les parties mathématiques sont négligeables en temps, mais causent de bugs.
- Implantations disponibles: PARI/GP, Magma, CADO.

Construction des équations (2/2)

Exemple cas facile $p = 65537$ et $(a, b) = (8, -1)$

- 1ère demi-équation: $a - ib = 8 + i = (-i)(2 + 3i)(2 + i)$ d'où $8 + 256 \equiv (-256)(2 + 3 \cdot 256)(2 + 256) \pmod{65537}$.
- 2ème demi-équation: $a - mb = 8 - 256 \cdot (-1) = 264 = 2^3 \cdot 3 \cdot 11$ d'où $8 + 256 \equiv 2^3 \cdot 3 \cdot 11 \pmod{65537}$.
- équation: $(-256)(2 + 3 \cdot 256)(2 + 256) \equiv 2^3 \cdot 3 \cdot 11 \pmod{65537}$ d'où $\log(-256) + \log(2 + 3 \cdot 256) + \log(2 + 3 \cdot 256) \equiv 3 \log 2 + \log 3 + \log 11 \pmod{65537 - 1}$

Inconnues

- base de facteurs = les éléments premiers de $\mathbb{Z}[\alpha_f]$ de norme $\leq B$(ou des idéaux premiers de $\mathcal{O}_{\mathbb{Q}(\alpha)}$ dont la norme est puissance d'un premier $\leq B$) pour le côté de f et les nombres premiers rationnels de norme $\leq B$ pour le côté de g.
- inconnues: logarithmes discrets des images dans $\mathbb{Z}/p\mathbb{Z}$ des éléments de la base de facteurs.

Lemme

La norme de $a - b\alpha_f$, $\sum_{i=0}^{\deg f} f_i a^i b^{\deg f - i}$, est B-friable si et seulement si tous les facteurs de $a - b\alpha_f$ sont dans la base de facteurs.

Algèbre linéaire

Matrice M

- lignes = relations (a, b)
- colonnes = base de facteurs
- M(relation,premier π de $\mathcal{O}_{\mathbb{Q}(\alpha)}$)$=\pm \mathrm{val}_\pi(a - b\alpha)$ avec signe $+$ pour f et $-$ pour g.

Example $f = x^2 + 1$**,** $(a, b) = (8, -1)$**:** $M\left((a, b), (2 + i)\right) = 1$.

Wiedemann

- l'algèbre linéaire consiste à résoudre l'équation $Mx = 0$;
- coût: $B^{2+o(1)}$ car la base de facteurs a $(2 + o(1))B/\log B$ éléments;
- résultat: logarithmes discrets des éléments de la base de facteurs.

Changement de complexité

Idée

Au lieu de demander la friabilité d'un nombre grand on demande la friabilité de 2 nombres très petits: les normes $\sum_{i=0}^{d} f_i a^i b^{d-i}$ et $a - bm$.

Pourquoi $L_p(1/3)$?

- Les normes ont taille $\sum_{i=0}^{d} f_i a^i b^{d-i} \approx E^d p^{\frac{1}{d}}$ et $g \approx E p^{\frac{1}{d}}$.
- En prenant $E \approx 2^{\sqrt[3]{\log p}}$ et $d = \sqrt[3]{\log p}$ les deux normes ont taille $2^{(\sqrt[3]{\log p})^2}$.
- Le théorème de Canfield-Erdös-Pomerance dit que pour $B \approx 2^{\sqrt[3]{\log p}}$ la probabilité qu'une des deux normes soit B-friable est $1/2^{\sqrt[3]{\log p}}$.
- Le coût du crible est $E^{2+o(1)} = L(1/3)$, ça donne autant d'équation que d'inconnues. Le coût de l'algèbre linéaire est $B^{2+o(1)}$

Niveau de sécurité

Definition

On dit qu'un cryptosystème offre la sécurité s si la meilleure attaque connue requière 2^s opérations élémentaires.

Utilisation

1. On peut comparer la vitesse des différents cryptosystèmes en les réglant à la même sécurité.
2. Si on utilise ensemble de la cryptographie symétrique et asymétrique on peut les régler au même niveau de sécurité.

La loi de Moore

À cause de l'évolution des ordinateurs (loi de Moore), le même niveau de sécurité est considérer suffisant à un moment donné mais trop faible quelques années plus tard. En 2015, les principaux niveaux de sécurité sont:

- 80 bits
- 128 bits
- 256 bits.

Taille des clés RSA (1/2)

Complexité

Le meilleur algorithme pour factoriser des clés RSA est le crible algébrique (NFS).

- sa complexité est $L_N(1/3, c)^{1+o(1)}$ avec $c = \sqrt[3]{64/9} \approx 1.923$; le terme $o(1)$ est problématique pour extrapoler;
- selon un travail de Lenstra et Verheul (Selecting cryptographic key sizes, 2001), le terme $o(1)$ est petit pour les tailles cryptographique et sa dérivée est négligeable, donc on peut extrapoler sur des petits intervalles.
- il est raisonnable d'utiliser le modèle de complexité $\kappa L_N(1/3, c)$ pour une constante κ à déterminer expérimentalement.

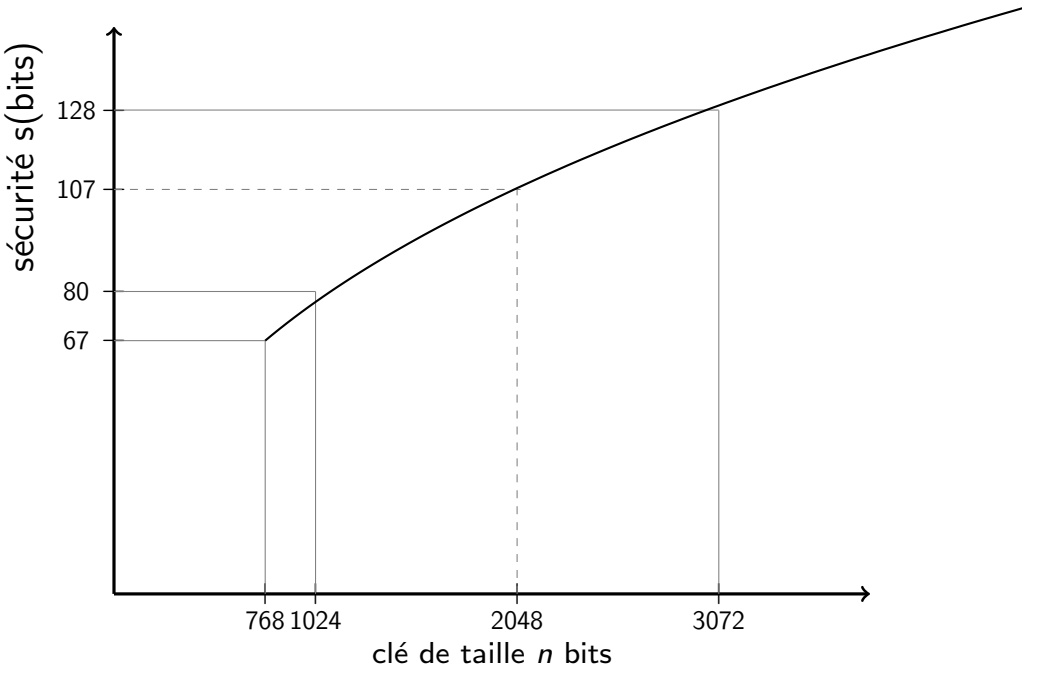
Records de factorisation

- RSA challenge, 768 bits;
- 2009, équipe commune à Nancy, Lausanne, Bonn, Tokyo, Amsterdam et Redmond;
- coût: 2000 années CPU sur des coeurs de 3GHz:

$$\log_2(3G \cdot 2000 \cdot 3.15e7) \approx 66.7.$$

RSA 768 offre une sécurité de 67 bits.

Taille des clés RSA (2/2)



Formule d'extrapolation

$$2^s = 2^{67} \frac{L_{2^n}(1/3, c)}{L_{2^{768}}(1/3, c)}$$