

Factorisation des entiers $N = \pm pq^2$

Fabien LAGUILLAUMIE

`fabien.laguillaumie@info.unicaen.fr`

`http://users.info.unicaen.fr/~flaguill/`

avec G. CASTAGNOS (Bordeaux), A. JOUX (Versailles),
P. Q. NGUYEN (Paris)

Séminaire Caramel - Nancy



Plan

- ▶ Introduction et Motivations
- ▶ Corps quadratiques, formes quadratiques
- ▶ Factorisation des entiers $N = \pm pq^2$ avec des indices
 - ▶ Indice n° 1 : $[\mathfrak{h}] \in \ker \bar{\varphi}_q$
 - ▶ Méthode n° 1 : le lift
 - ▶ Méthode n° 2 : Coppersmith
 - ▶ Indice n° 2 : un petit régulateur
- ▶ Conclusion



Introduction et Motivations

Point de départ : un cryptosystème au déchiffrement efficace

- ▶ Soit $N = pq$, un entier RSA et $\mathcal{M} = (\mathbb{Z}/p\mathbb{Z})^*$

$$\begin{array}{ccc} \pi : (\mathbb{Z}/N\mathbb{Z})^* & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^* \\ x & \longmapsto & x \pmod{p} \end{array}$$

- ▶ $\ker(\pi) \simeq (\mathbb{Z}/q\mathbb{Z})^*$

Génération des clés : $\text{KeyGen}(\lambda) = \{(N, h), p\}$ $h \in \ker(\pi)$

Chiffrement : $\text{Encrypt}((N, h), m, r) = mh^r \pmod{N}$

Déchiffrement : $\text{Decrypt}(p, c) = \pi(c) = m \pmod{p}$



Introduction et Motivations

Point de départ : un cryptosystème au déchiffrement efficace

- ▶ Consistance :

$$\pi(c) = \pi(m)\pi(h^r) = \pi(m) = m$$

- ▶ Sécurité :



Introduction et Motivations

Point de départ : un cryptosystème au déchiffrement efficace

- ▶ Consistance :

$$\pi(c) = \pi(m)\pi(h^r) = \pi(m) = m$$

- ▶ Sécurité :

h générateur de $\ker \pi$?



Introduction et Motivations

Point de départ : un cryptosystème au déchiffrement efficace

- ▶ Consistance :

$$\pi(c) = \pi(m)\pi(h^r) = \pi(m) = m$$

- ▶ Sécurité :

$$h \text{ générateur de } \ker \pi \implies \begin{cases} h \equiv 1 \pmod{p} \\ h \not\equiv 1 \pmod{q} \end{cases}$$



Introduction et Motivations

Point de départ : un cryptosystème au déchiffrement efficace

- ▶ Consistance :

$$\pi(c) = \pi(m)\pi(h^r) = \pi(m) = m$$

- ▶ Sécurité :

$$h \text{ générateur de } \ker \pi \implies \begin{cases} h \equiv 1 \pmod{p} \\ h \not\equiv 1 \pmod{q} \end{cases}$$

Cryptanalyse : $\text{pgcd}(h - 1, N) = p$



Introduction et Motivations

$$N = pq^2$$

- ▶ Cryptosystèmes à la RSA ou à la Paillier
- ▶ Cryptosystèmes construits dans des corps quadratiques
imaginaires et réels
- ▶ Problème de la “squarefree part” (calcul de l’anneau des entiers d’un corps quadratique)
- ▶ Factorisation - complexité exponentielle

Crandall-Pomerance

- An exponential algorithm is often the algorithm of choice for small inputs
- In some cases, an exponential algorithm is a direct ancestor of a subexponential algorithm
- the fastest, rigorously analyzed *deterministic* factoring algorithm is exponential
- factoring algorithms, [...] exponential [...], are the basis for analogous algorithms for discrete
- Many of the exponential algorithms are pure delights



Introduction et Motivations

$$N = pq^2$$

- ▶ Cryptosystèmes à la RSA ou à la Paillier
 - ▶ Takagi $N = p^r q$
(déchiffrement rapide)
 - ▶ signature Esign
(complexité quadratique de la signature et de la vérification)
 - ▶ Okamoto and Uchiyama
(homomorphe)



Introduction et Motivations

Cryptographie et corps quadratiques

$$N = pq^2$$

- ▶ Échange de clé (Diffie-Hellman) dans le groupe de classes d'un corps quadratique imaginaire

J. Buchmann and H. C. Williams. *A Key-Exchange System based on Imaginary Quadratic Fields*. J. Cryptology, 1, 107–118 (1988)

- ▶ Elgamal, RSA, Rabin,...

- ▶ *New Ideal Coset Encryption (NICE)* :

S. Paulus and T. Takagi. *A New Public-Key Cryptosystem over a Quadratic Order with Quadratic Decryption Time*. J. Cryptology, 13(2), 263–272 (2000)

- ▶ NICE réel

J. Jacobson, Jr, R. Scheidler, D. Weimer. *An Adaptation of the NICE Cryptosystem to Real Quadratic Orders*. Proc. of Africacrypt'08, Springer LNCS Vol. 5023, 191-208 (2008)



Corps quadratiques, formes quadratiques



Corps quadratiques

- ▶ $K = \mathbb{Q}(\sqrt{\Delta_K})$
- ▶ **Discriminant fondamental** :
 - ▶ $\Delta_K \equiv 1 \pmod{4}$ sans facteur carré
 - ▶ $\Delta_K \equiv 0 \pmod{4}$ et $\Delta_K/4 \equiv 2, 3 \pmod{4}$ sans facteur carré
- ▶ **Ordre quadratique** : $\mathcal{O} \subset K$, \mathcal{O} est un sous-anneau de K contenant 1, et tel que \mathcal{O} soit un \mathbb{Z} -module libre de rang 2
- ▶ \mathcal{O}_{Δ_K} : **anneau des entiers** de K est l'ordre maximal,

$$\mathcal{O}_{\Delta_K} = \mathbb{Z} + \frac{\Delta_K + \sqrt{\Delta_K}}{2} \mathbb{Z}$$

- ▶ $\mathcal{O} \subset \mathcal{O}_{\Delta_K}$, $f := [\mathcal{O}_{\Delta_K} : \mathcal{O}]$ est le **conducteur**,

$$\mathcal{O} = \mathbb{Z} + \frac{\Delta_f + \sqrt{\Delta_f}}{2} \mathbb{Z}$$

et $\Delta_f = f^2 \Delta_K$ est le discriminant de $\mathcal{O}_{\Delta_f} := \mathcal{O}$



Corps quadratiques

- ▶ **Idéaux principaux** : $\alpha \mathcal{O}_\Delta$ où $\alpha \in \mathcal{O}_\Delta$
- ▶ **Idéaux fractionnaires** : $\mathfrak{a} \subset K$ tel que $d\mathfrak{a}$ est un idéal de \mathcal{O}_Δ pour un entier d non nul
- ▶ Idéal fractionnaire \mathfrak{a} est **propre** si

$$\left\{ \beta \in K, \beta\mathfrak{a} \subset \mathfrak{a} \right\} = \mathcal{O}_\Delta$$

- ▶ Les idéaux fractionnaires inversibles sont les idéaux fractionnaires propres
- ▶ $I(\mathcal{O}_\Delta)$: groupe des idéaux fractionnaires propres de \mathcal{O}_Δ
- ▶ $P(\mathcal{O}_\Delta)$: sous-groupe des idéaux principaux



Groupe de classes

$$C(\mathcal{O}_\Delta) := I(\mathcal{O}_\Delta)/P(\mathcal{O}_\Delta)$$

son cardinal (**fini**) est le nombre de classes noté $h(\mathcal{O}_\Delta)$

- ▶ Relation d'équivalence :

$$\mathbf{a} \sim \mathbf{b} \iff \exists \alpha \in K^\times, \mathbf{b} = \alpha \mathbf{a}$$

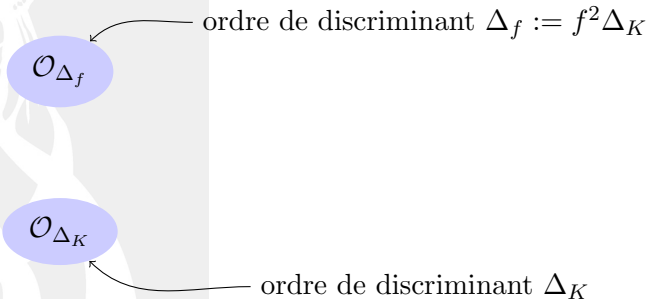
- ▶ Nombre de classes si $\Delta < 0$:

- ▶ En moyenne $h(\Delta) \approx 0.461559\sqrt{|\Delta|}$
- ▶ Calculable en temps $L_{1/2,3/\sqrt{8}+o(1)}(|\Delta|)$



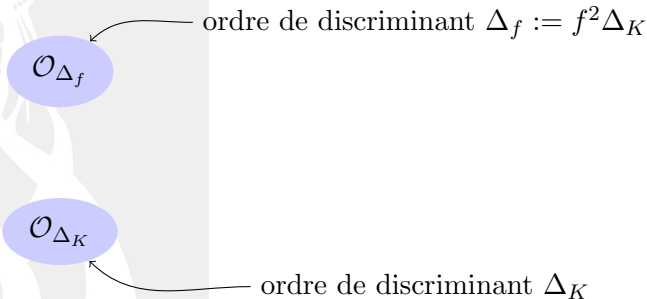
Relations entre deux groupes de classes, $\Delta_K < 0$

Situation :



Relations entre deux groupes de classes, $\Delta_K < 0$

Situation :



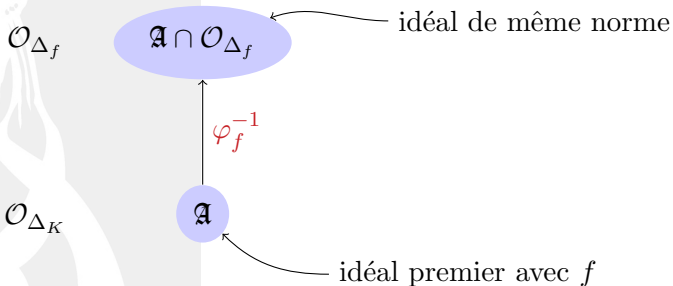
Idéal premier avec le conducteur :

- ▶ un idéal \mathfrak{a} est **premier avec** f si $N(\mathfrak{a})$ est première avec f



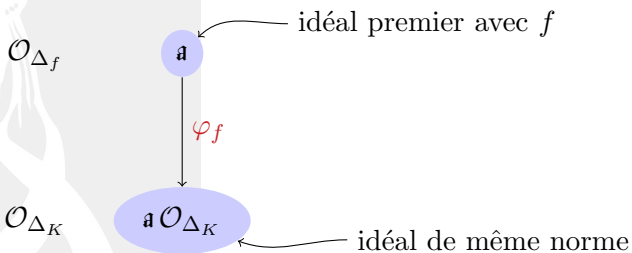
Relations entre deux groupes de classes, $\Delta_K < 0$

Situation :



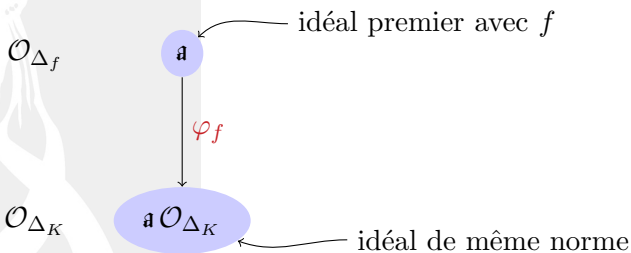
Relations entre deux groupes de classes, $\Delta_K < 0$

Situation :



Relations entre deux groupes de classes, $\Delta_K < 0$

Situation :



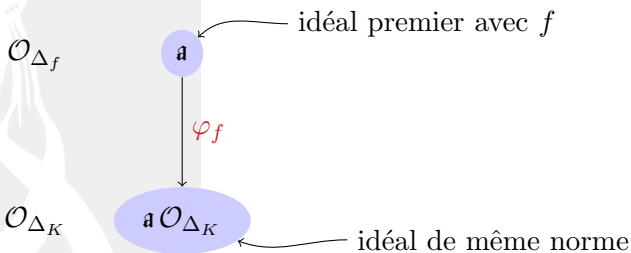
φ_f et φ_f^{-1} :

- ▶ φ_f et φ_f^{-1} sont des isomorphismes calculables avec complexité quadratique **si on connaît le conducteur f**



Relations entre deux groupes de classes, $\Delta_K < 0$

Situation :



Passage au quotient :

- ▶ φ_f induit une surjection :

$$\bar{\varphi}_f : C(\mathcal{O}_{\Delta_f}) \longrightarrow C(\mathcal{O}_{\Delta_K})$$



Corps quadratiques

- ▶ \mathcal{O}_Δ^* est le groupe des unités dans \mathcal{O}_Δ

$$\mathcal{O}_\Delta^* = \begin{cases} \{\pm 1\} & \text{si } \Delta < -4 \\ \mu_6 & \text{si } \Delta = -3 \\ \mu_4 & \text{si } \Delta = -4 \\ \langle -1, \varepsilon_\Delta \rangle & \text{si } \Delta > 0 \end{cases}$$

ε_Δ est l'unité fondamentale.

- ▶ $R_\Delta = \log(\varepsilon_\Delta)$ est le **régulateur** of \mathcal{O}_Δ

$$\log \left(\frac{1}{2}(\sqrt{\Delta - 4} + \sqrt{\Delta}) \right) \leq R_\Delta < \sqrt{\frac{1}{2}\Delta} \left(\frac{1}{2} \log \Delta + 1 \right)$$

$$\frac{h(\mathcal{O}_{\Delta_q})}{h(\mathcal{O}_{\Delta_K})} = \begin{cases} q - (\Delta_K/q) & \text{if } \Delta_K < -4, \\ (q - (\Delta_K/q)) \frac{R_{\Delta_K}}{R_{\Delta_q}} & \text{si } \Delta_K > 0. \end{cases}$$



Formes quadratiques

► \mathfrak{a} idéal de \mathcal{O}_Δ :

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

avec $m \in \mathbb{Z}$, $a \in \mathbb{N}$ et $b \in \mathbb{Z}$ tel que $b^2 \equiv \Delta \pmod{4a}$.

Dans la suite : idéaux *primitifs* ($m = 1$)



Formes quadratiques

- ▶ \mathfrak{a} idéal de \mathcal{O}_Δ :

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

avec $m \in \mathbb{Z}$, $a \in \mathbb{N}$ et $b \in \mathbb{Z}$ tel que $b^2 \equiv \Delta \pmod{4a}$.

Dans la suite : idéaux *primitifs* ($m = 1$)

- ▶ f **forme quadratique** : $f(x, y) = ax^2 + bxy + cy^2$ avec $a, b, c \in \mathbb{Z}$, notée $[a, b, c]$, de **discriminant** $\Delta = b^2 - 4ac$.
- ▶ Si $\Delta < 0$ et $a > 0$, f est dite **définie positive**
- ▶ Si $\Delta > 0$, f est dite **indéfinie**
- ▶ Soit $M \in \text{GL}_2(\mathbb{Z})$ avec $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, $f.M$ est la forme

$$f(\alpha x + \beta y, \gamma x + \delta y).$$



Formes quadratiques

Formes définies positives primitives ($\text{pgcd}(a, b, c) = 1$)

- ▶ $f \sim g \iff \exists M \in \text{SL}_2(\mathbb{Z})$ telle que $g = f.M$.
- ▶ $f = [a, b, c]$ est **normale** si $-a < b \leq a$.
Elle est **réduite** si
 - ▶ $-a < b \leq a \leq c$
 - ▶ et si $b \geq 0$ pour $a = c$.
- ▶ unicité de la forme réduite dans une classe modulo $\text{SL}_2(\mathbb{Z})$
- ▶ Si f est normale et $a < \sqrt{|\Delta|/4}$, f est réduite



Formes quadratiques

Formes indéfinies primitives

- ▶ $f = [a, b, c]$ est **réduite** si

$$\left| \sqrt{\Delta} - 2|a| \right| < b < \sqrt{\Delta}$$

et **normale** si

- ▶ $-|a| < b \leq |a|$ pour $|a| \geq \sqrt{\Delta}$
 - ▶ et $\sqrt{\Delta} - 2|a| < b < \sqrt{\Delta}$ pour $|a| < \sqrt{\Delta}$.
-
- ▶ **Normalise** : $[a, b, c] \rightsquigarrow [a, b + 2sa, as^2 + bs + c]$
 - ▶ **Rho** : $[a, b, c] \rightsquigarrow \text{Normalise}([c, -b, a])$

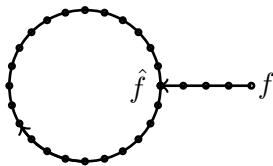
Reduction step



Formes quadratiques

Formes indéfinies

- ▶ le **cycle** de f est la suite $(\rho^i(g))_{i \in \mathbb{Z}}$ où g une forme réduite équivalente à f



- ▶ ℓ la **période** :

$$\frac{R_{\Delta}}{\log \Delta} \leq \ell \leq \frac{2R_{\Delta}}{\log 2} + 1.$$



Factorisation des entiers $N = \pm pq^2$ avec des indices.



Factorisation de $N = pq^2$

Les méthodes de factorisation existantes (spécifiques) :

$$N = pq^2$$

► Résultats connus :

- amélioration d'ECM d'un facteur $\log(p)$ (Peralta 2001)
- factorisation des entiers $p^r q$ (Boneh, Durfee 1999)
 - Coppersmith - $\tilde{O}(p^{1/3}) \rightsquigarrow \tilde{O}(N^{1/9})$
- Pollard-Strassen version Bostan-Gaudry-Schost
 - $\tilde{O}(N^{1/6}) + \tilde{O}(N^{1/6})$ en espace

► Nos résultats

- Connaissance d'un élément particulier
- Condition arithmétique sur p
 - $\tilde{O}(p^{1/2}) \rightsquigarrow \tilde{O}(N^{1/6})$
 - $\tilde{O}(\text{Poly}(\log(p)))$ dans les cas favorables



Factorisation de $N = pq^2$

Indice n° 1 : $[\mathfrak{h}] \in \ker \bar{\varphi}_q$



Indice n° 1 : $[\mathfrak{h}] \in \ker \bar{\varphi}_q$

Morphisme $\bar{\varphi}_q$:

$$\begin{array}{ccc} C(\mathcal{O}_{\Delta_q}) & & [\mathfrak{a}] \\ \downarrow & & \downarrow \\ C(\mathcal{O}_{\Delta_K}) & & [\mathfrak{a} \mathcal{O}_{\Delta_K}] \end{array}$$

Lemme (Cox)

Il existe un isomorphisme effectif

$$\psi_q : (\mathcal{O}_{\Delta_K}/q\mathcal{O}_{\Delta_K})^\times / (\mathbb{Z}/q\mathbb{Z})^\times \xrightarrow{\sim} \ker \bar{\varphi}_q$$



Indice n° 1 : $[\mathfrak{h}] \in \ker \bar{\varphi}_q$



- ▶ $\alpha = x + y \frac{\Delta_K + \sqrt{\Delta_K}}{2}$ avec $\text{pgcd}(N(\alpha), q) = 1$
- ▶ $\psi_q(\alpha) = [\varphi_q^{-1}(\alpha \mathcal{O}_K)]$

[BTW95]



- ▶ $\mathfrak{h} \in I(\mathcal{O}_{\Delta_q}, q)$
- ▶ calcul de $\alpha \in \mathcal{O}_K$ tel que $\alpha \mathcal{O}_K = \varphi_q(\mathfrak{h})$
- ▶ $\psi_q^{-1}([\mathfrak{h}]) = [\alpha]$

[HJPT98]

[HJW03]

- ▶ $\# \ker \bar{\varphi}_q = q - \left(\frac{\Delta_K}{q}\right).$

[BTW95] : J. Buchmann, C. Thiel and H. C. Williams. *Short Representation of Quadratic Integers*. Proc. of CANT'92, Math. Appl. 325, Kluwer Academic Press, 159–185 (1995)

[HJPT98] D. Hühnlein, M. Jacobson, Jr., S. Paulus and T. Takagi. *A Cryptosystem Based on Non-Maximal Imaginary Quadratic Orders with Fast Decryption*. Proc. of Eurocrypt'98, Springer LNCS Vol. 1403, 294–307 (1998)

[HJW03] D. Hühnlein, M. Jacobson, Jr. and D. Weber. *Towards Practical Non Interactive Public-Key Cryptosystems Using Non-Maximal Imaginary Quadratic Orders*. Des. Codes Cryptography 30(3) 281–299 (2003)



Indice n° 1 : $[\mathfrak{h}] \in \ker \bar{\varphi}_q$

Théorème

Dans chaque classe non triviale de $\ker \bar{\varphi}_q$, il existe un idéal de norme q^2 .



Indice n° 1 : $[\mathfrak{h}] \in \ker \bar{\varphi}_q$

Théorème

Dans chaque classe non triviale de $\ker \bar{\varphi}_q$, il existe un idéal de norme q^2 .

Démonstration (sketch).

- ▶ Système de représentants de $(\mathcal{O}_{\Delta_K}/q\mathcal{O}_{\Delta_K})^\times / (\mathbb{Z}/q\mathbb{Z})^\times$:

$$1 \text{ et } \alpha_x = x + \frac{\Delta_K + \sqrt{\Delta_K}}{2} \text{ avec } x \in \{0, \dots, q-1\},$$

avec $N(\alpha_x)$ première avec q .

- ▶ Calcul de

$$(\mathcal{O}_{\Delta_K}/q\mathcal{O}_{\Delta_K})^\times / (\mathbb{Z}/q\mathbb{Z})^\times \longrightarrow \ker \bar{\varphi}_q$$



Indice n° 1 : $[\mathfrak{h}] \in \ker \bar{\varphi}_q$

Théorème

Dans chaque classe non triviale de $\ker \bar{\varphi}_q$, il existe un idéal de norme q^2 .

Conséquence :

L'idéal réduit \mathfrak{h} est équivalent à un idéal non réduit de norme q^2



Indice n° 1 : $[\mathfrak{h}] \in \ker \bar{\varphi}_q$

► Première idée : remonter la réduction (mauvaise)

► Deuxième idée : *lifter* \mathfrak{h} (bonne)

On the Security of Cryptosystems with Quadratic Decryption : The Nicest Cryptanalysis.
G. Castagnos, F. Laguillaumie. Proc. of Eurocrypt'09. Springer LNCS Vol. 5479, 260-277
(2009)

► Troisième idée : trouver les petites racines de la forme quadratique associée (bonne)

Factoring pq^2 with Quadratic Forms : Nice Cryptanalyses.
G. Castagnos, A. Joux, F. Laguillaumie, P. Q. Nguyen. Proc. of Asiacrypt'09, Springer
LNCS Vol. 5912, 469-486 (2009)



Indice n° 1 : $[\mathfrak{h}] \in \ker \bar{\varphi}_q$

Méthode n° 1 : le lift



Indice n° 1 : $[\mathfrak{h}] \in \ker \bar{\varphi}_q$

Méthode n° 1 : le lift

$C(\mathcal{O}_{\Delta_q})$

$[\mathfrak{h}] \in \ker \bar{\varphi}_q$

avec \mathfrak{h} réduit

q

$C(\mathcal{O}_{\Delta_K})$



Indice n° 1 : $[\mathfrak{h}] \in \ker \bar{\varphi}_q$

Méthode n° 1 : le lift

$C(\mathcal{O}_{\Delta_q r^2})$

r

$C(\mathcal{O}_{\Delta_q})$

q

$C(\mathcal{O}_{\Delta_K})$

$[(q^2, -)]$

réduit si $\begin{cases} q^2 < \sqrt{|\Delta_q|} r^2 / 4 \\ \updownarrow \\ r > 2q / \sqrt{p} \end{cases}$

$[\mathfrak{h}] \in \ker \bar{\varphi}_q$

avec \mathfrak{h} réduit



Indice n° 1 : $[\mathfrak{h}] \in \ker \bar{\varphi}_q$

Méthode n° 1 : le lift

$C(\mathcal{O}_{\Delta_q r^2})$

r

$C(\mathcal{O}_{\Delta_q})$

q

$C(\mathcal{O}_{\Delta_K})$

$[(q^2, -)]$

réduit si $\begin{cases} q^2 < \sqrt{|\Delta_q|} r^2 / 4 \\ \updownarrow \\ r > 2q / \sqrt{p} \end{cases}$

$[\mathfrak{h}] \in \ker \bar{\varphi}_q$

avec \mathfrak{h} réduit



Indice n° 1 : $[\mathfrak{h}] \in \ker \bar{\varphi}_q$

Méthode n° 1 : le lift

$C(\mathcal{O}_{\Delta_{qr^2}})$

$[(q^2, -)] \in \ker \bar{\varphi}_{qr}$

r

$C(\mathcal{O}_{\Delta_q})$

$[\mathfrak{h}] \in \ker \bar{\varphi}_q$

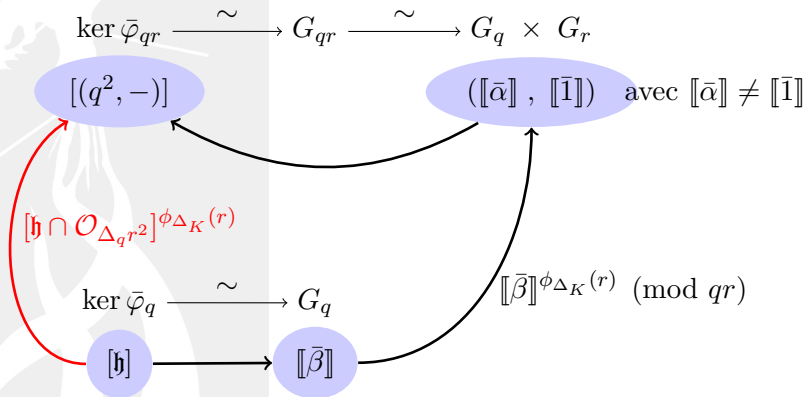
q

$C(\mathcal{O}_{\Delta_K})$



Indice n° 1 : $[\mathfrak{h}] \in \ker \bar{\varphi}_q$

Méthode n° 1 : le lift



Notation :

$$G_f := (\mathcal{O}_{\Delta_K} / f\mathcal{O}_{\Delta_K})^\times / (\mathbb{Z}/f\mathbb{Z})^\times \text{ et } \phi_{\Delta_K}(f) := \#G_f$$



Indice n° 1 : \mathfrak{h}

Méthode n° 1 : le lift

Input: $\lambda \in \mathbb{Z}, \Delta_q = -pq^2 \in \mathbb{Z}, \mathfrak{h} = (a, b) \in I(\mathcal{O}_{\Delta_q}, q)$ with $[\mathfrak{h}] \in \ker \bar{\varphi}_q$ of order > 6

Output: p, q

Initialisation :

1. Set $r' = 3$
2. Set $\delta_{r'} = \lceil \frac{\lambda+3}{2} \frac{\log 2}{\log r'} \rceil$ and $r = r'^{\delta_{r'}}$
3. **If** the order of $[\mathfrak{h}]$ divides $\phi_{\Delta_K}(r)$ **then** set r' to the next prime and **goto** 2.
4. Find $\mathfrak{h}' \in [\mathfrak{h}]$ such that $\mathfrak{h}' \in I(\mathcal{O}_{\Delta_q}, r')$

Core Algorithm :

5. Compute $\mathfrak{g} = \mathfrak{h}' \cap \mathcal{O}_{\Delta_q r^2}$
6. Compute $\mathfrak{f} = \text{Red}(\mathfrak{g}^{\phi_{\Delta_K}(r)})$
7. **Return** $p = \Delta_q / N(\mathfrak{f}), q = \sqrt{N(\mathfrak{f})}$



Indice n° 1 : $[\mathfrak{h}] \in \ker \bar{\varphi}_q$

Méthode n° 2 : Coppersmith



Indice n° 1 : $[\mathfrak{h}] \in \ker \bar{\varphi}_q$

Méthode n° 2 : Coppersmith

$$\Delta = -pq^2$$

▶ $f_k := [q^2, kq, (k^2 + p)/4]$ $f_k(x, y) = q^2 + kqxy + (k^2 + p)/4y^2$

▶ $M_k = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ la matrice telle que $\hat{f}_k = f_k \cdot M_k$:

$$\hat{f}_k \leftrightarrow \mathfrak{h}$$

▶ $q^2 = f_k(1, 0) = \hat{f}_k(\delta, -\gamma)$



Indice n° 1 : $[\mathfrak{h}] \in \ker \bar{\varphi}_q$

Méthode n° 2 : Coppersmith

Factorisation de $\Delta_q = -pq^2$ si on trouve (x_0, y_0) tel que

$$\text{pgcd}(\hat{f}_k(x_0, y_0), \Delta_q) = q^2$$

\rightsquigarrow Coppersmith bivarié

▶ $\tilde{f}_k(x, y) = x^2 + b'xy + c'y^2$ avec

$$\tilde{f}_k(x_0, y_0) \equiv 0 \pmod{q^2} \text{ et } |x_0|, |y_0| < X$$

▶ \tilde{f}_k est homogène de degré 2



Indice n° 1 : $[\mathfrak{h}] \in \ker \bar{\varphi}_q$

Méthode n° 2 : Coppersmith

Lemme (à la Howgrave-Graham)

Soit $B \in \mathbb{N}$ et $h(x, y) \in \mathbb{Z}[x, y]$ *homogène de degré d* avec au plus ω monômes.

Supposons que $h(x_0, y_0) = 0 \pmod{B}$ et

$$\begin{cases} |x_0|, |y_0| \leq X \\ \|h(xX, yX)\| < B/\sqrt{\omega} \end{cases}$$

Alors le polynôme univarié $\tilde{h}(r) = (1/y^d)h(x, y)$ (avec $r = x/y$) est tel que

$$\tilde{h}(x_0/y_0) = 0$$

dans \mathbb{Q} .



Indice n° 1 : $[\mathfrak{h}] \in \ker \bar{\varphi}_q$

Méthode n° 2 : Coppersmith

$$\begin{cases} g_{i,j}(x,y) &= x^j y^{2(t-i)-j} \tilde{f}_k^i \Delta_q^{m-i} & \text{pour } i = 0, 1, \dots, m-1, j = 0, 1 \\ h_i(x,y) &= x^i y^{2t'-i} \tilde{f}_k^m & \text{pour } i = 0, 1, \dots, 2t'. \end{cases}$$

Soit $r = x/y$ et $\tilde{f}(r) = \tilde{f}_k(x,y)/y^2 = r^2 + b'r + c'$. Alors,

$$\begin{cases} g_{i,j}(x,y)/y^{2t} &= x^j y^{-2i-j} f^i(x,y) \Delta_q^{m-i} &= r^j \tilde{f}^i(r) \Delta_q^{m-i} &=: \tilde{g}_{i,j}(r) \\ h_i(x,y)/y^{2t} &= x^i y^{-i-2m} f^m(x,y) &= r^i \tilde{f}^m(r) &=: \tilde{h}_i(r) \end{cases}$$

- ▶ Construction d'un réseau L à partir des $g_{i,j}(r)$ et $h_i(r)$
- ▶ $\det(L) = \Delta_q^{m(m+1)} X^{2t(2t+1)}$
- ▶ Comparaison avec la borne sur la norme du premier vecteur sorti par LLL :

$$X = \Delta_q^{1/9}$$



Indice n° 1 : $[h] \in \ker \bar{\varphi}_q$

Méthode n° 2 : Coppersmith

Exemple avec $m = 2, t = 3$

$$\begin{array}{ccccccc} y^6 & y^5x & y^4x^2 & & y^3x^3 & y^2x^4 & yx^5 & x^6 \\ \left(\begin{array}{ccccccc} N^2 & & & & & & & \\ 0 & N^2 & & & & & & \\ Nc & Nb & N & & & & & \\ 0 & Nc & Nb & N & & & & \\ c^2 & 2bc & 2c + b^2 & 2b & 1 & & & \\ 0 & c^2 & 2bc & 2c + b^2 & 2b & 1 & & \\ 0 & 0 & c^2 & 2bc & 2c + b^2 & 2b & 1 & \end{array} \right) \begin{array}{l} y^6 N^2 \\ xy^5 N^2 \\ y^4 N h \\ xy^3 N h \\ y^2 h^2 \\ xy h^2 \\ x^2 h^2 \end{array} \end{array}$$



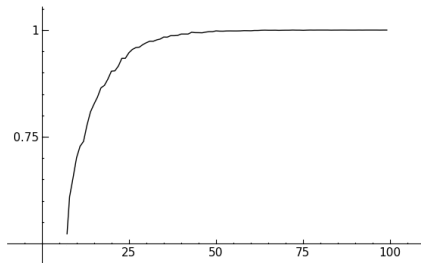
Indice n° 1 : $[\mathfrak{h}] \in \ker \bar{\varphi}_q$

Méthode n° 2 : Coppersmith

On note $|M|$ la norme max de M .

Heuristique

Étant donné un élément réduit \hat{f}_k d'une classe non-triviale de $\ker \bar{\varphi}_q$, la matrice de la réduction M_k est telle que $|M_k| < |\Delta_q|^{1/9}$ avec une probabilité asymptotiquement proche de 1.



Indice n° 1 : $[h] \in \ker \bar{\varphi}_q$

Méthode n° 2 : Coppersmith

$$\begin{aligned} \Delta_q &= -100113361940284675007391903708261917456537242594667 \\ &4915149340539464219927955168182167600836407521987097 \\ &2619973270184386441185324964453536572880202249818566 \\ &5592983708546453282107912775914256762913490132215200 \\ &22224671621236001656120923 \end{aligned}$$

$$\begin{aligned} a &= 57022687708942583181685884381175588713007831807699951 \\ &95092715895755173700399141486895731384747 \end{aligned}$$

$$\begin{aligned} b &= 33612360405827547849585862980179491106487317456059301 \\ &64666819569606755029773074415823039847007 \end{aligned}$$

Notre algorithme trouve en moins d'1/2 seconde $r_0 = \frac{-103023911}{349555951}$
telle que

$$\begin{aligned} h(\text{Num}(r_0), \text{Dénom}(r_0)) &= 5363123171977038839829609999282338450991746328236957351089 \\ &4245774887056120365979002534633233830227721465513935614971 \\ &593907712680952249981870640736401120729 \\ &= q^2 \end{aligned}$$



Factorisation de $N = pq^2$

Indice n° 2 : un petit régulateur



Indice n° 2 : le régulateur de p

Théorème

Soit Δ_K un discriminant fondamental positif, $\Delta_q = \Delta_K q^2$ où q est un conducteur impair. Soit ε_{Δ_K} (resp. ε_{Δ_q}) l'unité fondamentale de \mathcal{O}_{Δ_K} (resp. \mathcal{O}_{Δ_q}) et t tel que $\varepsilon_{\Delta_K}^t = \varepsilon_{\Delta_q}$.

Alors les idéaux principaux de \mathcal{O}_{Δ_q} générés par $q\varepsilon_{\Delta_K}^i$ correspondent aux formes quadratiques

$$f_{k(i)} = [q^2, k(i)q, (k(i)^2 - p)/4]$$

avec $i \in \{1, \dots, t-1\}$ et $k(i)$ un entier défini modulo $2q$ calculable à partir de $\varepsilon_{\Delta_K}^i \pmod{q}$.



Indice n° 2 : le régulateur de p

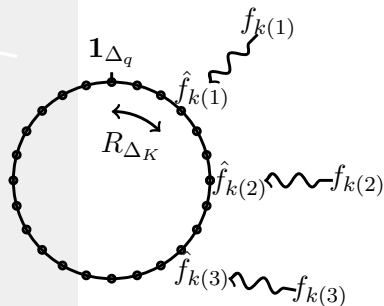


FIG.: Répartition des formes $\hat{f}_k(i)$ le long du cycle principal

Indice n° 2 : le régulateur de p

Heuristique

À partir de la forme principale $\mathbf{1}_{\Delta_q}$, une forme réduite \hat{f}_k telle que la matrice de réduction M_k satisfait $|M_k| < \Delta_q^{1/9}$, peut être trouvée au bout de $\mathcal{O}(R_{\Delta_K})$ applications successives de Rho .

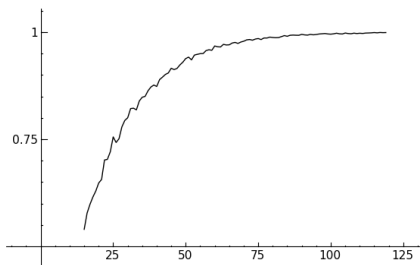


FIG.: Probabilité que $|M_k| < |\Delta_q|^{1/9}$ en fonction de la taille λ de p et q .



Indice n° 2 : le régulateur de p

Algorithme de factorisation des pq^2

Input: $N = pq^2, m, t$

Output: p, q

1. $h \leftarrow [1, \lfloor \sqrt{\Delta_q} \rfloor, (\lfloor \sqrt{\Delta_q} \rfloor^2 - \Delta_q)/4]$
2. $S \leftarrow \emptyset$
3. **while** $S = \emptyset$ **do**
 - 3.1. $h \leftarrow \text{Rho}(h)$
 - 3.2. $S \leftarrow \text{HomogeneousCoppersmith}(h, N, m, t)$
4. $x_0 \leftarrow \text{Numerator}(S), y_0 \leftarrow \text{Denominator}(S)$
5. $q \leftarrow \text{Sqrt}(\text{Gcd}(h(x_0, y_0), N))$
6. **return** $(N/q^2, q)$



Indice n° 2 : le régulateur de p

Complexité :

- ▶ en temps : $O(R_p \text{Poly}(\log N))$
- ▶ en espace : $O(\log N)$

Pire cas : $O(p^{1/2} \log p \text{Poly}(\log N))$

- ▶ Dans NICE réel :

Schinzel sleeper : $p = a^2x^2 + 2bx + c$ avec
 $a, b, c, x \in \mathbb{Z}, a \neq 0$ et $b^2 - 4ac \mid 4\text{pgcd}(a^2, b)^2$

et

$$R_{\Delta_K} < c(\log(a)) \log(\sqrt{\Delta_K})$$

- ▶ D'autres entiers avec petit régulateur : $\begin{cases} p = x^2 + 4 \\ p = x^2 + 1 \end{cases}$



Expérience

- ▶ Le polynôme de Schinzel $S(X) = 154^2 X^2 + 2 \cdot 1848X + 145$ produit un premier fondamental de 1024 bits p pour

$$X_0 = 742580904152459207040996305843978694225348656778318732499703298404473916608514503632356111724888120733946935414993974514560831140974654762720960708608.$$

- ▶ Son régulateur : $R_{\Delta_K} \simeq 350.82$.

$$\Delta_q = 8652847730371352983096555365546286774757127665924565803276204832022803237080423741454699916227786011114500556129463757561738298276973390597175848561496535655648688056781327476022119563059127314330539380497240895130406201250507731150708556480929050152128898114797218723575096087294275095902442453309230711498360948363625638548834916968787118133041710325523135541140228834079648990856373731137530135928339443245508463937482434535141169172566442343227177356582530049603640870247222293894279750265546775352346079134658349631258789015809773848552718311277726174765150408024751980489080021592540083431808559617147769808532171593543541461225474397133863532953635652832410883944107305459341466829533199631980727938016162651991683135904386509828788775800657585341532091993804066166249557043317391403133704097175873766807067074798513170848927018650117899951833745544010204738131060558944255239298998192229174748761931322766954974944297$$



Expérience

- ▶ Notre algorithme retrouve

$q =$ 813420349147370484191937392353743987057216867229000519389617165443345442965791153
590600055431858367339657249724776138214723135174812646684135350615452945702161509
056620645273845046756878630355206667163387506843081902301543694713928158259509441
47273074042188107662930334328568639880205200204373157188449446587141

à partir de Δ_q (3072 bits) après 126 itérations en 657.12 secondes.

- ▶ La racine rationnelle :

2381688390651907786346063545375320574105612285596517115735418576228401466663504525041781
3121736667298312791332305258966423823047969665345852691023433833742187009250650452020082

- ▶ Le numérateur x_0 et le dénominateur y_0 satisfont $\log(\Delta_q)/\log(x_0) \simeq 10.597$ et $\log(\Delta_q)/\log(y_0) \simeq 10.583$.



Améliorations

Aurore Bernard (XLIM) et Nicolas Gama (GREYC) :

- ▶ Nouvel algorithme de réduction des formes indéfinies :

- ▶ nombre d'itérations $\leq \frac{\log(|a|/\sqrt{\Delta})}{2 \log(\omega)} + 4$

- ▶ $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$

$$\sqrt{|\gamma\delta|} \leq \sqrt{21} \sqrt{|a|/\sqrt{\Delta}}$$

(Buchmann : $\sqrt{|\gamma\delta|} \leq (|a|/\sqrt{\Delta})(1 + 1/\sqrt{\Delta})$)

- ▶ $\frac{u}{v} \equiv c \pmod{q}$

- ▶ ils obtiennent les formes déséquilibrées



Conclusion

- ▶ Cryptanalyse totale des schémas basés sur NICE :
 - ▶ h dans la clé publique de NICE imaginaire
 - ▶ p de petit régulateur dans NICE réel
- ▶ Peu d'espoir d'avoir un déchiffrement quadratique dans des corps quadratiques
- ▶ Nouvel algorithme déterministe (heuristique) de factorisation des entiers pq^2 donc la complexité dépend du régulateur de $\mathbb{Q}(\sqrt{p})$ (en général de l'ordre de \sqrt{p}).

