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

GREYC ALGORITHMIQUE

Introduction et Motivations

Point de départ : un cryptosystème au déchiffrement efficace

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

$$\begin{array}{rccc} \pi : & (\mathbb{Z}/N\mathbb{Z})^\star & \twoheadrightarrow & (\mathbb{Z}/p\mathbb{Z})^\star \\ & x & \longmapsto & x \pmod p \end{array}$$

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

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

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

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

GREYC ALGORITHMIQUE

Introduction et Motivations

Point de départ : un cryptosystème au déchiffrement efficace

- Consistance :

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

- Sécurité :

GREYC ALGORITHMIQUE

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 :

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

GREYC ALGORITHMIQUE

Introduction et Motivations

Point de départ : un cryptosystème au déchiffrement efficace

- Consistance :

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

- Sécurité :

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

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

GREYC ALGORITHMIQUE

Introduction et Motivations

$$N = pq^2$$

- Cryptosystèmes à la RSA ou à la Paillier
- Cryptosystèmes construits dans des corps quadratiques imaginaires et rééls
- 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 discret
- Many of the exponential algorithms are pure delights

GREYC ALGORITHMIQUE

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

  M. 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)

GREYC ALGORITHMIQUE

Corps quadratiques, formes quadratiques

GREYC ALGORITHMIQUE

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
- $\mathcal{O}_{\Delta_K}$: 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 $\mathcal{O}_{\Delta_f} := \mathcal{O}$

GREYC ALGORITHMIQUE

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 $\mathcal{O}_\Delta$ 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 $\mathcal{O}_\Delta$
- $P(\mathcal{O}_\Delta)$: sous-groupe des idéaux principaux

GREYC ALGORITHMIQUE

Groupe de classes

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

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

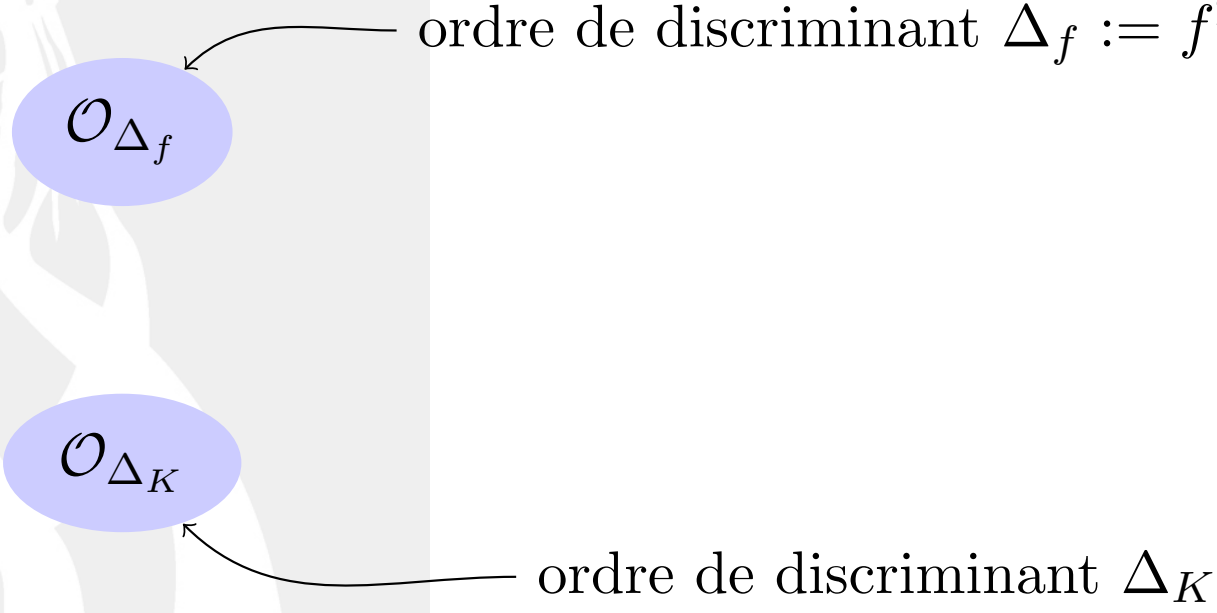
- Relation d'équivalence :

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

- 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, $\Delta_K < 0$

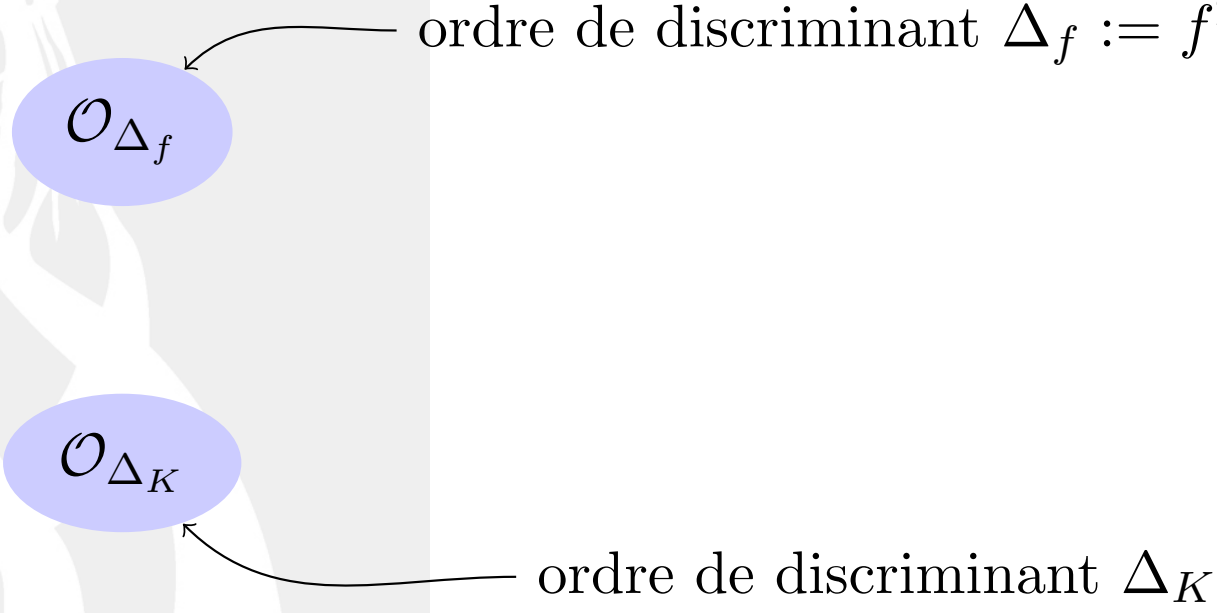
Situation :



GREYC ALGORITHMIQUE

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

Situation :



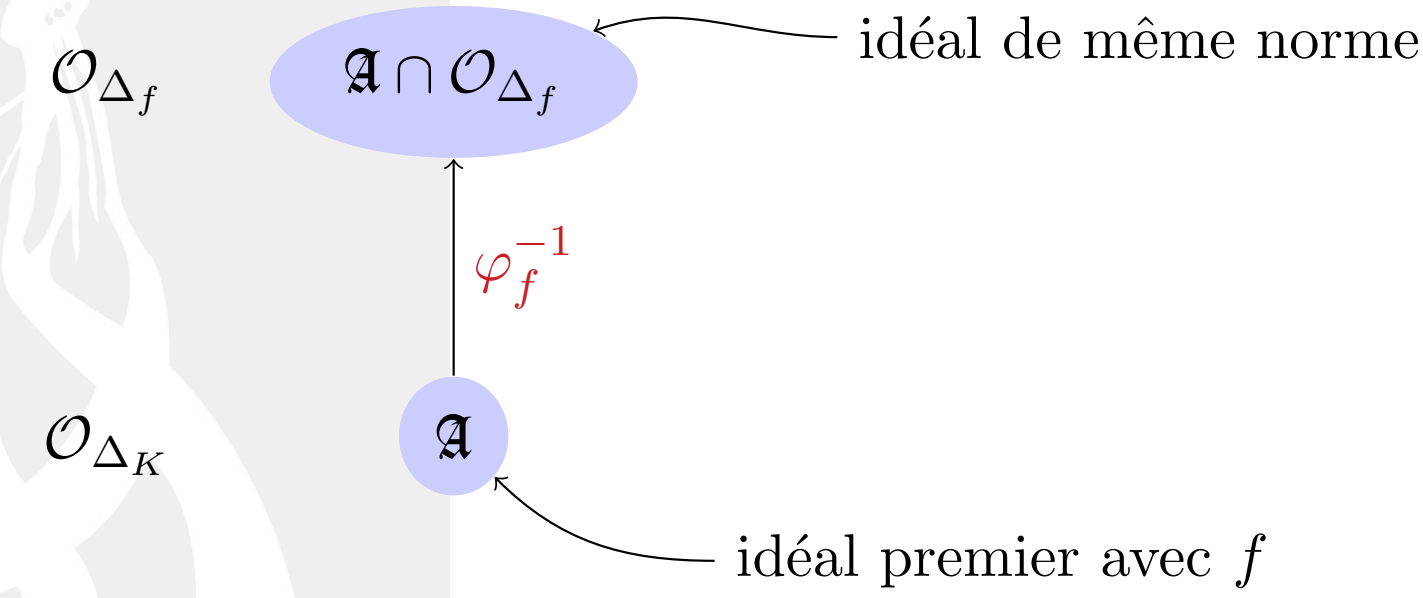
Idéal premier avec le conducteur :

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

GREYC ALGORITHMIQUE

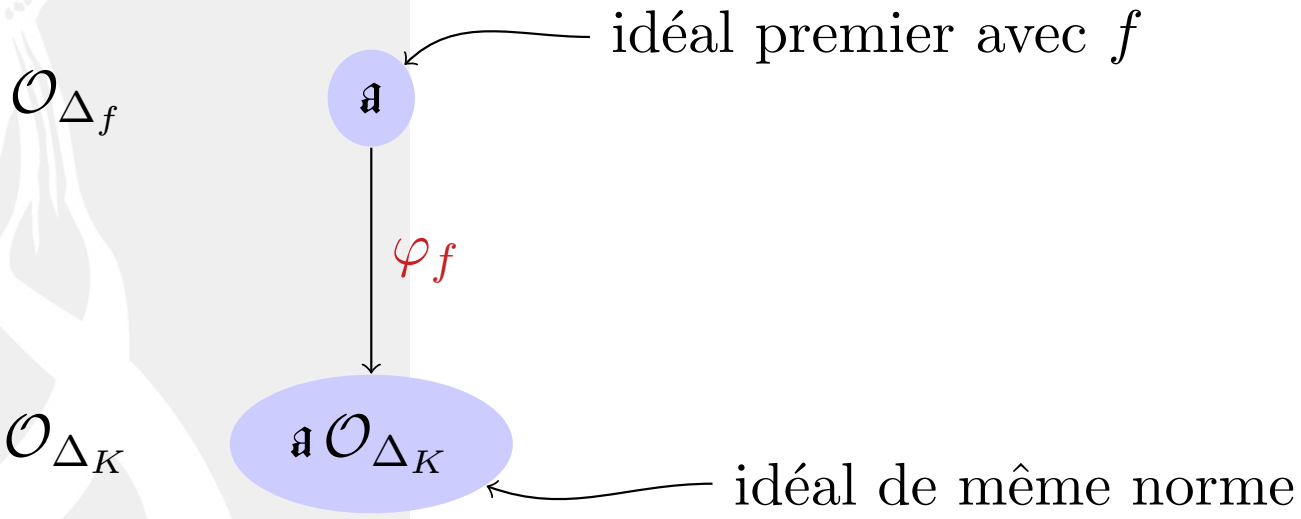
Relations entre deux groupes de classes, $\Delta_K < 0$

Situation :



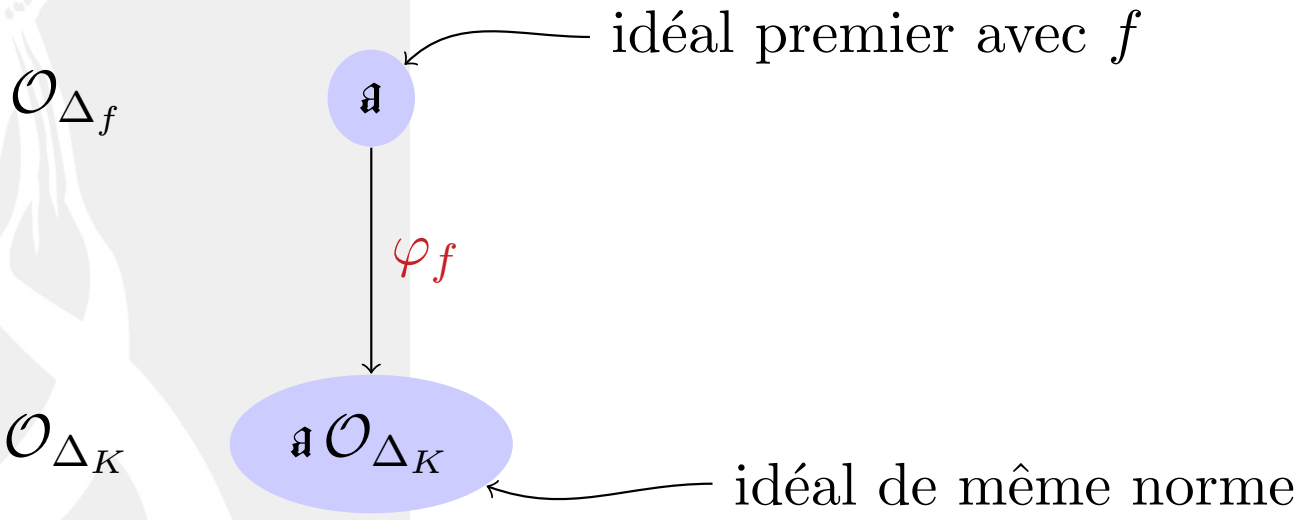
Relations entre deux groupes de classes, $\Delta_K < 0$

Situation :



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

Situation :



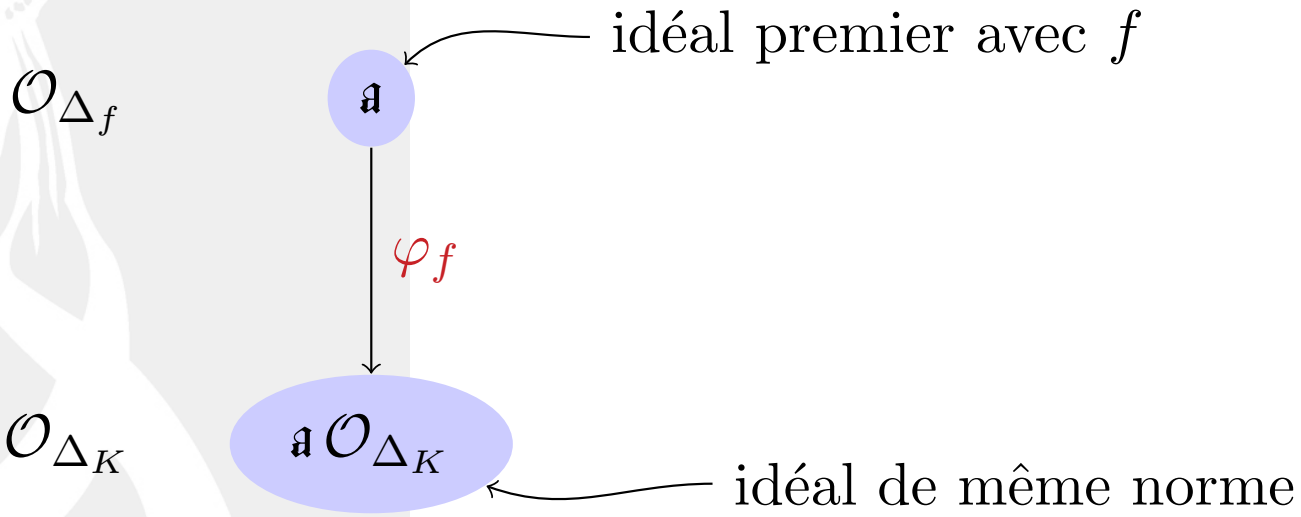
φ_f et φ_f^{-1} :

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

GREYC ALGORITHMIQUE

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

Situation :



Passage au quotient :

- φ_f induit une surjection :

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

GREYC ALGORITHMIQUE

Corps quadratiques

- $\mathcal{O}_\Delta^\star$ est le groupe des unités dans $\mathcal{O}_\Delta$

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

ε_Δ est l'*unité fondamentale.*

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

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

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

GREYC ALGORITHMIQUE

Formes quadratiques

- $\mathfrak{a}$ idéal de $\mathcal{O}_\Delta$:

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

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 $\mathcal{O}_\Delta$:

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

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 $M \in \mathsf{GL}_2(\mathbb{Z})$ avec $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, $f.M$ est la forme

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

GREYC ALGORITHMIQUE

Formes quadratiques

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

- $f \sim g \iff \exists M \in \mathsf{SL}_2(\mathbb{Z})$ 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 $\mathsf{SL}_2(\mathbb{Z})$

- Si f est normale et $a < \sqrt{|\Delta|/4}$, f est réduite

GREYC ALGORITHMIQUE

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 : $[a, b, c] \rightsquigarrow [a, b + 2sa, as^2 + bs + c]$

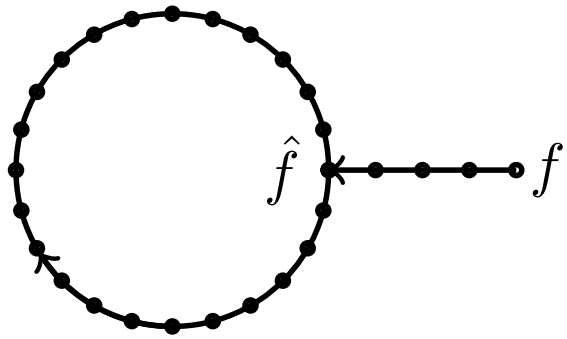
- Rho : $[a, b, c] \rightsquigarrow$ Normalise$([c, -b, a])$ Reduction step

GREYC ALGORITHMIQUE

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
    - $\tilde{O}(p^{1/2}) \rightsquigarrow \tilde{O}(N^{1/6})$
    - $\tilde{O}(\mathsf{Poly}(\log(p))$ dans les cas favorables

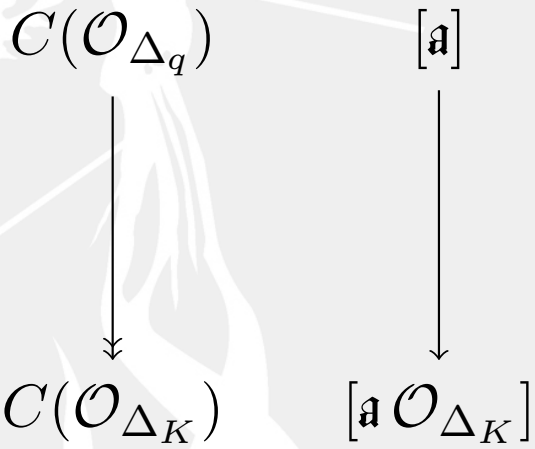
GREYC ALGORITHMIQUE

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 $\bar{\varphi}_q$:



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

- $\longrightarrow$
  - $\alpha = x + y\frac{\Delta_K + \sqrt{\Delta_K}}{2}$ avec $\mathrm{pgcd}(N(\alpha), q) = 1$
  - $\psi_q(\alpha) = [\varphi_q^{-1}(\alpha \mathcal{O}_K)]$ [BTW95]
- $\longleftarrow$
  - $\mathfrak{h} \in I(\mathcal{O}_{\Delta_q}, q)$ [HJPT98]
  - calcul de $\alpha \in \mathcal{O}_K$ tel que $\alpha \mathcal{O}_K = \varphi_q(\mathfrak{h})$ [HJW03]
  - $\psi_q^{-1}([\mathfrak{h}]) = [\alpha]$
- $\# \ker \bar{\varphi}_q = q - \left(\frac{\Delta_K}{q}\right)$.

[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*.*

GREYC ALGORITHMIQUE

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).

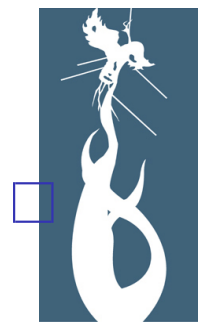
- Système de représentants de $(\mathcal{O}_{\Delta_K}/q\mathcal{O}_{\Delta_K})^\times / (\mathbb{Z}/q\mathbb{Z})^\times$:

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

  avec $\mathrm{N}(\alpha_x)$ 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

GREYC ALGORITHMIQUE

Indice n^o 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)

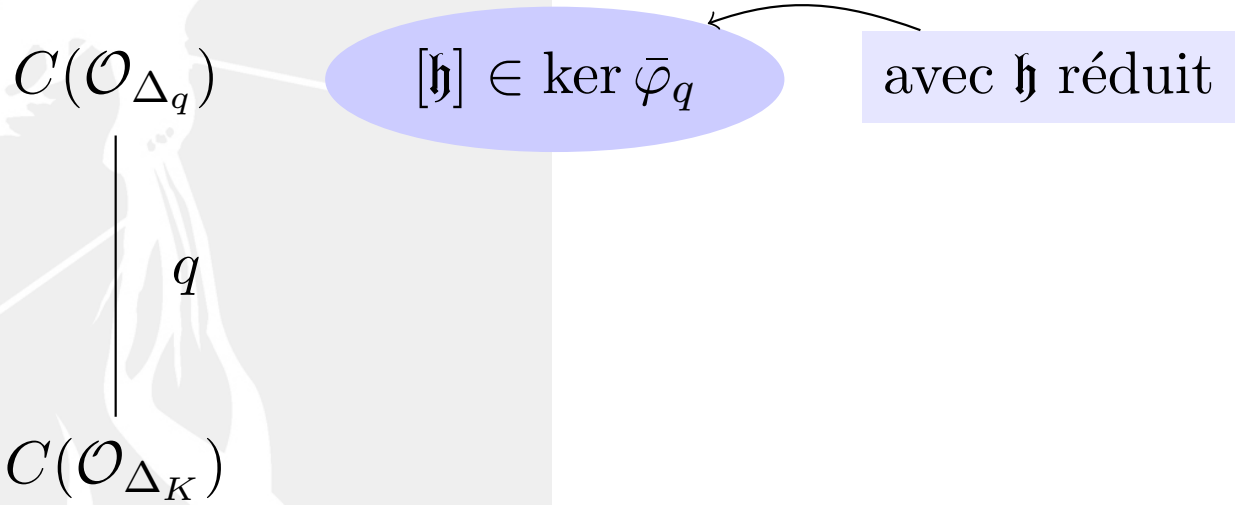
GREYC ALGORITHMIQUE

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

Méthode n° 1 : le lift

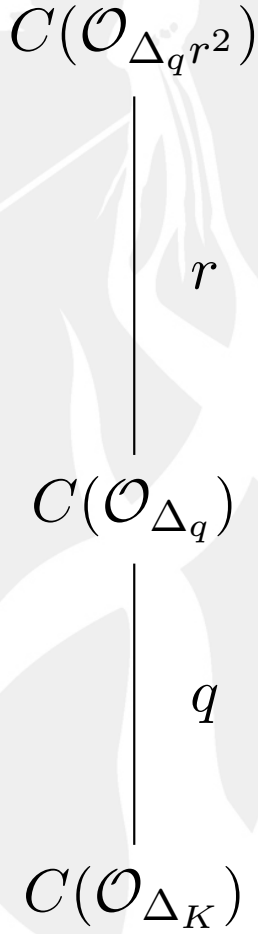
Indice n° 1 : $[\mathfrak{h}] \in \ker \bar{\varphi}_q$

Méthode n° 1 : le lift



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

Méthode n° 1 : le lift

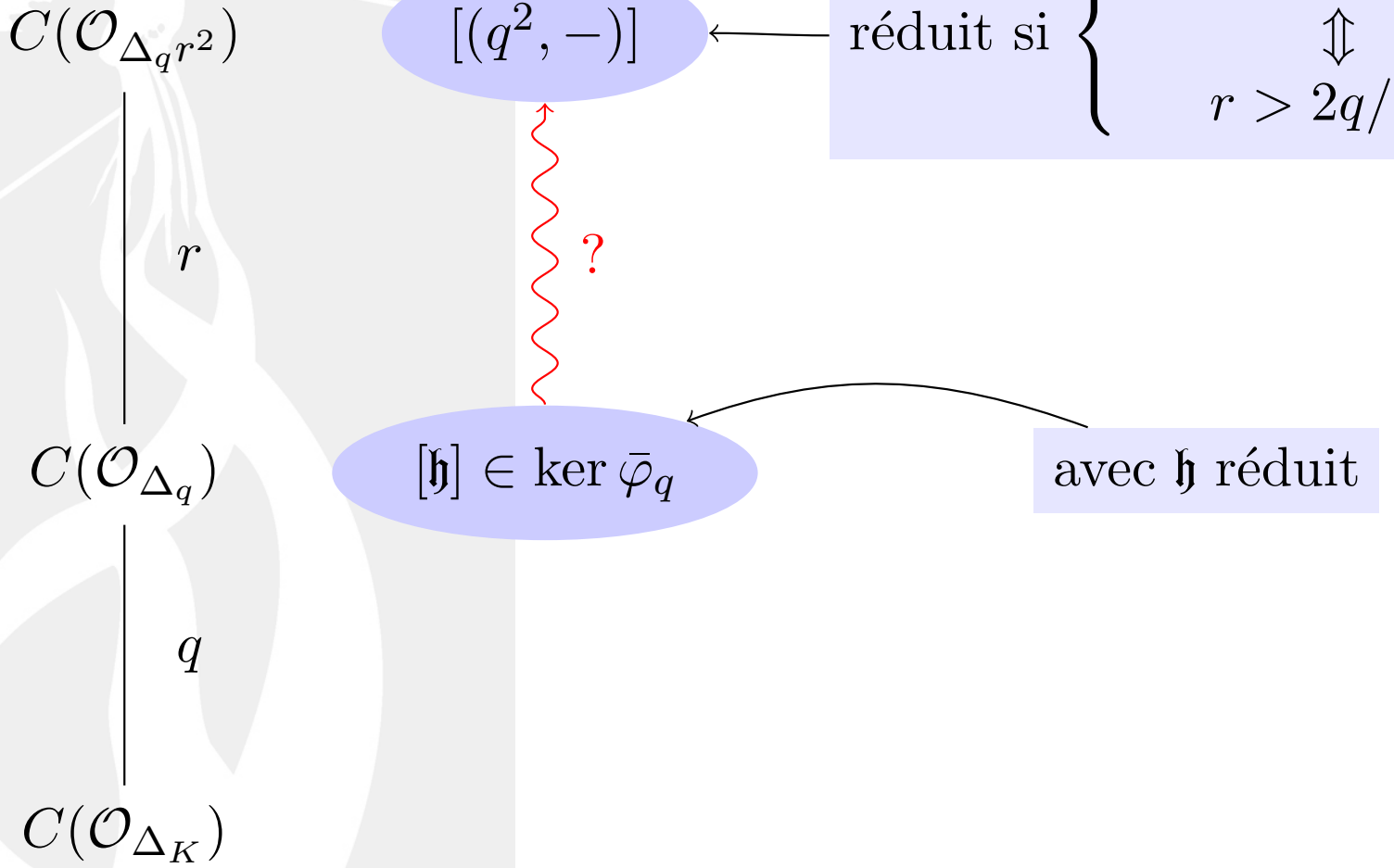


$[(q^2, -)]$ ⟵ réduit si $\begin{cases} q^2 < \sqrt{|\Delta_q| r^2/4} \\ \Updownarrow \\ r > 2q/\sqrt{p} \end{cases}$

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

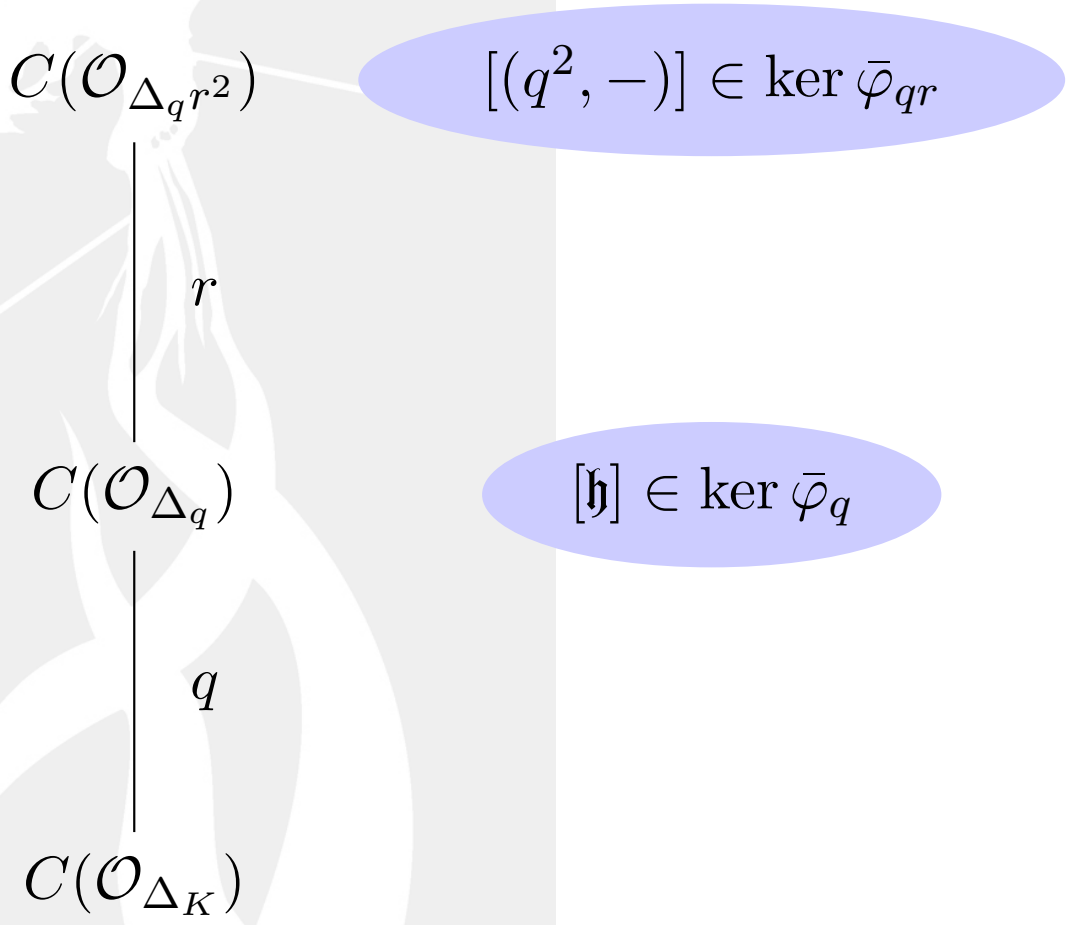
Indice n° 1 : $[\mathfrak{h}] \in \ker \bar{\varphi}_q$

Méthode n° 1 : le lift



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

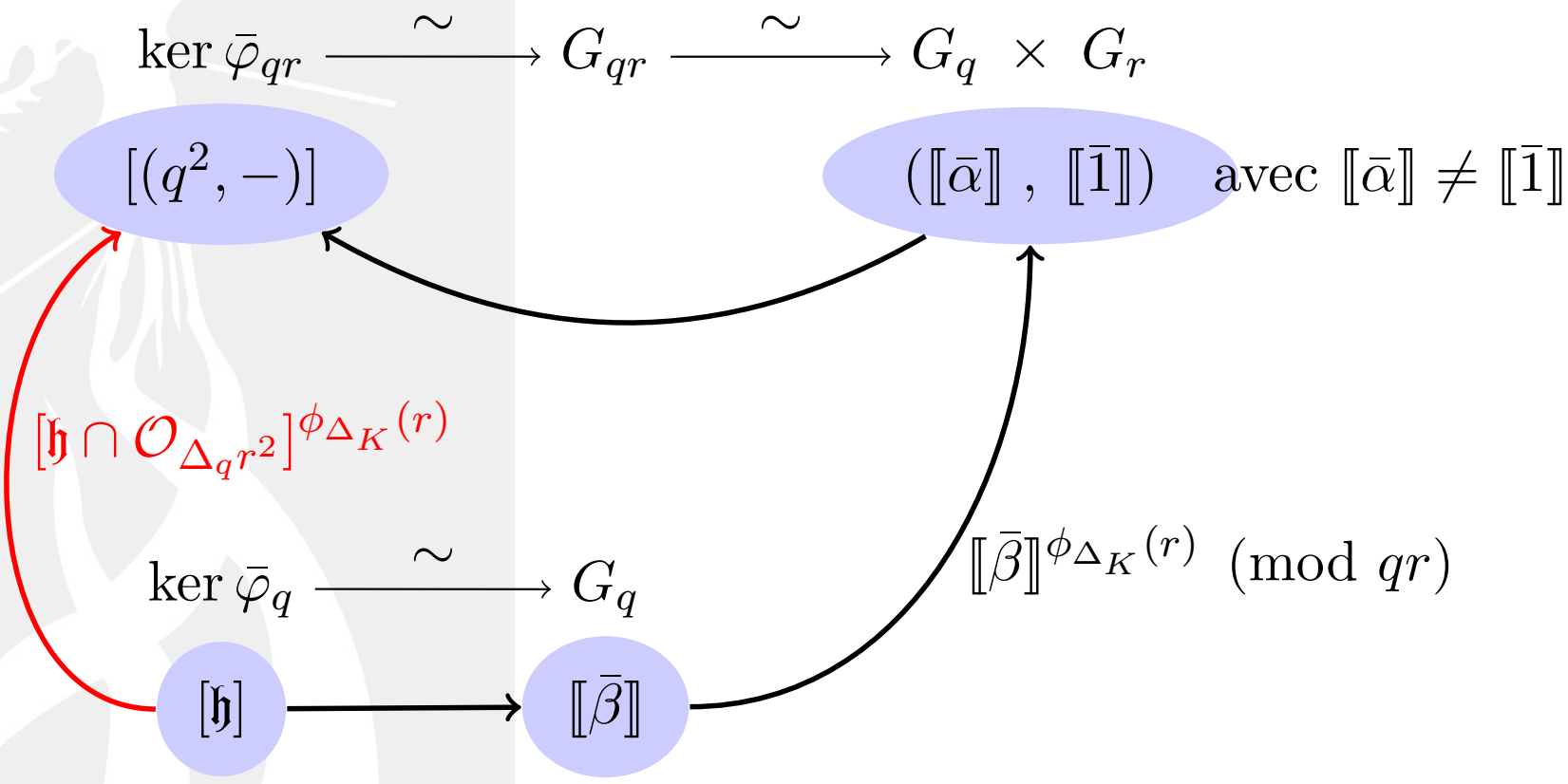
Méthode n° 1 : le lift



GREYC ALGORITHMIQUE

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

Méthode n° 1 : le lift



Notation :

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

GREYC ALGORITHMIQUE

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 $\mathfrak{k} = \mathsf{Red}(\mathfrak{g}^{\phi_{\Delta_K}(r)})$
7. **Return** $p = \Delta_q / \mathrm{N}(\mathfrak{k})$, $q = \sqrt{\mathrm{N}(\mathfrak{k})}$

GREYC ALGORITHMIQUE

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

$$\Delta = -pq^2$$

- $f_k := [q^2, kq, (k^2+p)/4]$ $\qquad f_k(x,y) = q^2 + kqxy + (k^2+p)/4y^2$
- $M_k = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathsf{SL}_2(\mathbb{Z})$ la matrice telle que $\hat{f}_k = f_k.M_k$:

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

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

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

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

$\rightsquigarrow$ Coppersmith bivarié

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

  $\tilde{f}_k(x_0, y_0) \equiv 0 \pmod{q^2}$ 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

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

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 :

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

GREYC ALGORITHMIQUE

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

Méthode n° 2 : Coppersmith

Exemple avec $m = 2$, $t = 3$

$$
\begin{array}{c}
\begin{array}{cccccccc} y^6 & y^5x & y^4x^2 & y^3x^3 & y^2x^4 & yx^5 & x^6 & \end{array} \\
\begin{pmatrix}
N^2 & & & & & & & \\
0 & N^2 & & & & & & \\
Nc & Nb & N & & & & & \\
0 & Nc & Nb & N & & & & \\
c^2 & 2bc & 2c+b^2 & 2b & 1 & & & \\
0 & c^2 & 2bc & 2c+b^2 & 2b & 1 & & \\
0 & 0 & c^2 & 2bc & 2c+b^2 & 2b & 1
\end{pmatrix}
\begin{array}{c} y^6N^2 \\ xy^5N^2 \\ y^4Nh \\ xy^3Nh \\ y^2h^2 \\ xyh^2 \\ x^2h^2 \end{array}
\end{array}
$$

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.*

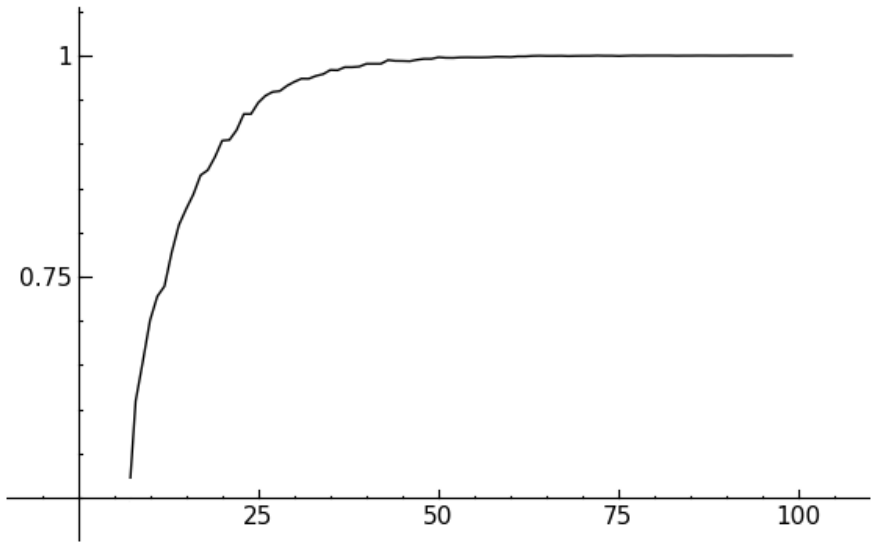


FIG.: Probabilité que $|M_k| < |\Delta_q|^{1/9}$ en fonction de la taille λ de p et q.

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

Méthode n° 2 : Coppersmith

$$\begin{aligned}
\Delta_q &= -100113361940284675007391903708261917456537242594667\\
&\quad 491514934053946421992795516818216760083640752198709726199732701843864411853249644535365728802022498185665592983708546453282107912775914256762913490132215200\\
&\quad 222246716212360016561209 23\\
a &= 570226877089425831816858843811755887130078318076999519509271589575517370039914148689573138474 7\\
b &= 336123604058275478495858629801794911064873174560593016466681956960675502977307441582303984700 7
\end{aligned}$$

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

$$\begin{aligned}
h(\mathsf{Num}(r_0), \mathsf{Dénom}(r_0)) &= 536312317197703883982960999928233845099174632823695735108942457748870561203659790025346332338302277214655139356149715939077126809522499818706407364011207 29\\
&= q^2
\end{aligned}$$

GREYC ALGORITHMIQUE

Factorisation de $N = pq^2$

Indice n$^{\text{o}}$ 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 fondamental de $\mathcal{O}_{\Delta_K}$ (resp. $\mathcal{O}_{\Delta_q}$) et t tel que $\varepsilon_{\Delta_K}^t = \varepsilon_{\Delta_q}$.

Alors les idéaux principaux de $\mathcal{O}_{\Delta_q}$ 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 $i \in \{1, \ldots, t-1\}$ et $k(i)$ un entier défini modulo $2q$ calculable à partir de $\varepsilon_{\Delta_K}^i \mod q$.

GREYC ALGORITHMIQUE

Indice n^o 2 : le régulateur de p

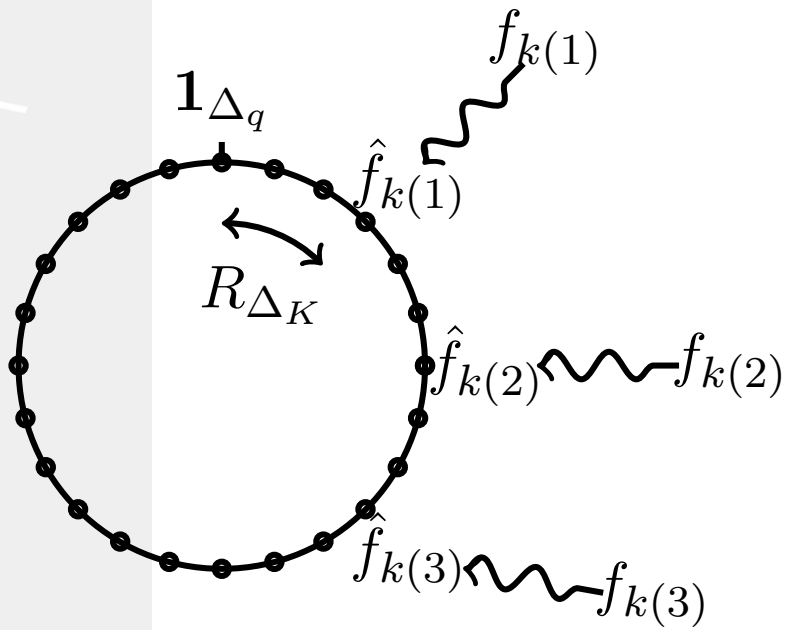


FIG.: Répartition des formes $\hat{f}_{k(i)}$ le long du cycle principal

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 *satifait* $|M_k| < \Delta_q^{1/9}$*, peut être trouvée au bout de* $\mathcal{O}(R_{\Delta_K})$ *applications successives de* Rho.

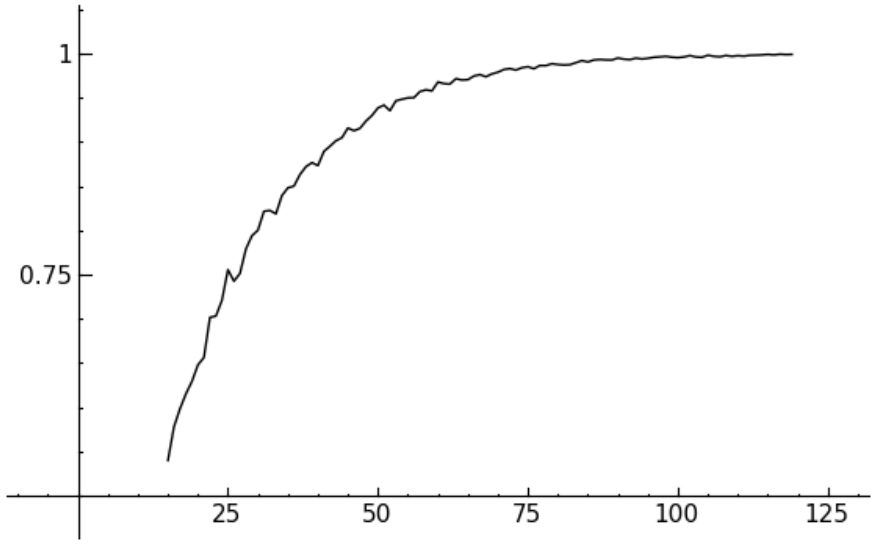


FIG.: Probabilité que $|M_k| < |\Delta_q|^{1/9}$ en fonction de la taille λ de p et q.

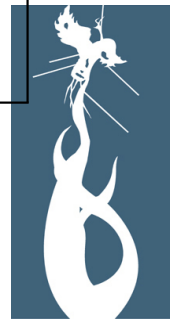
Indice n° 2 : le régulateur de p

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. $h \leftarrow \mathsf{Rho}(h)$
   - 3.2. $S \leftarrow \mathsf{HomogeneousCoppersmith}(h, N, m, t)$
4. $x_0 \leftarrow \mathsf{Numerator}(S)$, $y_0 \leftarrow \mathsf{Denominator}(S)$
5. $q \leftarrow \mathsf{Sqrt}(\mathsf{Gcd}(h(x_0, y_0), N))$
6. **return** $(N/q^2, q)$



GREYC ALGORITHMIQUE

Indice n° 2 : le régulateur de p

Complexité :

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

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

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

  et

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

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

GREYC ALGORITHMIQUE

Expérience

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

$$X_0 = 74258090415245920704099630584397869422534865677831873249970329840447391660851450363235611172488812073394693541499397451456083114097465476272096070860 8.$$

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

$$\Delta_q = 86528477303713529830965553655462867747571276659245658032762048320228032370804237414546999162277860111145005561294637575617382982769733905971758485614965356556486880567813274760221195630591273143305393804972408951304062012505077311507085564809290501521288981147972187235750960872942750959024424533092307114983609483636256385488349169687871181330417103255231355411402288340796489908563737311375301359283394432455084639374824345351411691725664423432271773565825300496036408702472222938942797502655467753523460791346583496312587890158097738485527183112777261747651504080247519804890800215925400834318085596171477698085321715935435414612254743971338635329536356528324108839441073054593414668295331996319807279380161626519916831359043865098287887775800657585341532091993804066166249557043317391403133704097175873766807067074798513170848927018650117899951833745544010204738131060558944255239298998192229174748761931322766954974944297$$

Expérience

- Notre algorithme retrouve

$$q = 8134203491473704841919373923537439870572168672290005193896171654433454429657911535906000554318583673396572497247761382147231351748126466841353506154529457021615090566206452738450467568786303552066671633875068430819023015436947139281582595094414727307404218810766293033432856863988020520020437315718844944658714 1$$

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

- La racine rationnelle :

$$\frac{2381688390651907786346063545375320574105612285596517115735418576228401466663504525041781}{3121736667298312791332305258966423823047969665345852691023433833742187009250650452020082}.$$

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

GREYC ALGORITHMIQUE

Améliorations

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

- Nouvel algorithme de réduction des formes indéfinies :
  - nombre d'itérations $\leq \dfrac{\log(|a|/\sqrt{\Delta})}{2\log(\omega)} + 4$
  - $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$

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

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

- $\frac{u}{v} \equiv c \pmod{q}$

- ils obtiennent les formes déséquilibrées

GREYC ALGORITHMIQUE

Conclusion

- Cryptanalyse totale des schémas basés sur NICE :
  - $\mathfrak{h}$ dans la clé publique de NICE imaginaire
  - p de petit régulateur dans NICE rééel

- 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 $\sqrt{p}$).

GREYC ALGORITHMIQUE