

NICE Cryptanalyses

Guilhem CASTAGNOS

PRISM,
Université de Versailles Saint-Quentin-en-Yvelines

Institut de Mathématiques de Bordeaux,
Université Bordeaux I

ECC 2009

Outline

- 1 Introduction
- 2 Class Groups of Imaginary Quadratic Fields
- 3 NICE Cryptanalysis in Imaginary Quadratic Fields
Joint Work with F. Laguillaumie
- 4 NICE Cryptanalysis in Real Quadratic Fields
Joint Work with A. Joux, F. Laguillaumie and P. Q. Nguyen
- 5 Conclusion

Outline

- 1 Introduction
- 2 Class Groups of Imaginary Quadratic Fields
- 3 NICE Cryptanalysis in Imaginary Quadratic Fields
Joint Work with F. Laguillaumie
- 4 NICE Cryptanalysis in Real Quadratic Fields
Joint Work with A. Joux, F. Laguillaumie and P. Q. Nguyen
- 5 Conclusion

Introduction

- Cryptography in Class Groups of Quadratic Fields:
 - Key exchange in Imaginary Quadratic Fields (Diffie-Hellman), Buchmann and Williams, JoC 88
 - Adaptations of Elgamal, RSA, Rabin...
 - *New Ideal Coset Encryption* (NICE): **Quadratic Decryption**
 - Imaginary Quadratic Fields, Paulus and Takagi, JoC 00
 - Real Quadratic Fields, Jacobson, Scheidler, Weimer, Africacrypt'08

NICE in $\mathbf{Z}/n\mathbf{Z}$

- Let $n = pq$ be an RSA integer, product of two λ bits primes

Morphism π

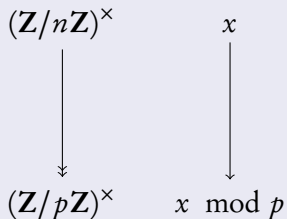
$$\begin{array}{ccc} (\mathbf{Z}/n\mathbf{Z})^\times & & x \\ \downarrow & & \downarrow \\ (\mathbf{Z}/p\mathbf{Z})^\times & & x \bmod p \end{array}$$

- Encryption of m :
 $mh \in (\mathbf{Z}/n\mathbf{Z})^\times$ where h is a random element of $\ker \pi$
- Fast decryption with π

NICE in $\mathbf{Z}/n\mathbf{Z}$

- Let $n = pq$ be an RSA integer, product of two λ bits primes

Morphism π



- Encryption of m :
 $mh \in (\mathbf{Z}/n\mathbf{Z})^\times$ where h is a random element of $\ker \pi$
- Fast decryption with π

Public Key: n and h a generator of $\ker \pi$

Algorithm Description

- **Public Key:** $n = pq, h \in \ker \pi$
- **Private Key:** p of λ bits
- **Encryption:** Let m of $\lambda - 1$ bits,

$$\text{Encrypt}(m, r) = mh^r \pmod{n}$$

- **Decryption:**

$$\text{Decrypt}(c) = \pi(c) = c \pmod{p}$$

Algorithm Description

- Public Key: $n = pq, h \in \ker \pi$
- Private Key: p of λ bits
- Encryption: Let m of $\lambda - 1$ bits,

$$\text{Encrypt}(m, r) = mh^r \pmod{n}$$

- Decryption:

$$\text{Decrypt}(c) = \pi(c) = c \pmod{p}$$

Correct

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

Cryptanalysis

Morphism π

 $(\mathbf{Z}/n\mathbf{Z})^\times$  $(\mathbf{Z}/p\mathbf{Z})^\times$ x  $x \bmod p$

b generator of $\ker \pi$



$$\begin{cases} b \equiv 1 \pmod{p} \\ b \not\equiv 1 \pmod{q} \end{cases}$$

Cryptanalysis

Morphism π

$$\begin{array}{ccc}
 (\mathbf{Z}/n\mathbf{Z})^\times & & x \\
 \downarrow & & \downarrow \\
 (\mathbf{Z}/p\mathbf{Z})^\times & & x \bmod p
 \end{array}$$

h generator of $\ker \pi$

\Downarrow

$$\begin{cases} h \equiv 1 \pmod{p} \\ h \not\equiv 1 \pmod{q} \end{cases}$$

Cryptanalysis

$$\gcd(h - 1, n) = p$$

Outline

- 1 Introduction
- 2 Class Groups of Imaginary Quadratic Fields
- 3 NICE Cryptanalysis in Imaginary Quadratic Fields
Joint Work with F. Laguillaumie
- 4 NICE Cryptanalysis in Real Quadratic Fields
Joint Work with A. Joux, F. Laguillaumie and P. Q. Nguyen
- 5 Conclusion

Imaginary Quadratic Orders (1)

Imaginary Quadratic Fields

- $K = \mathbf{Q}(\sqrt{\Delta_K}), \Delta_K < 0$
- Fundamental Discriminant:
 - $\Delta_K \equiv 1 \pmod{4}$ square-free
 - $\Delta_K \equiv 0 \pmod{4}$ and $\Delta_K/4 \equiv 2, 3 \pmod{4}$ square-free

Imaginary Quadratic Orders

- \mathcal{O} is a subring of K containing 1 and \mathcal{O} is a free \mathbf{Z} -module of rank 2

Imaginary Quadratic Orders

Characterisation of Orders

- \mathcal{O}_{Δ_K} : ring of integers of K is the maximal order,

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

- $\mathcal{O} \subset \mathcal{O}_{\Delta_K}$, $\ell := [\mathcal{O}_{\Delta_K} : \mathcal{O}]$ is the **conductor**,

$$\mathcal{O} = \mathbf{Z} + \frac{\Delta_\ell + \sqrt{\Delta_\ell}}{2} \mathbf{Z}$$

$\Delta_\ell = \ell^2 \Delta_K$ is the **non fundamental discriminant** of $\mathcal{O}_{\Delta_\ell} := \mathcal{O}$

Ideals of Quadratic Orders

Ideals of \mathcal{O}_Δ

- Fractional Ideals: $\mathfrak{a} \subset \mathbb{K}$ such that $\exists d \in \mathbb{N}$, $d\mathfrak{a}$ is an ideal of \mathcal{O}_Δ
- Invertible Fractional Ideals: \mathfrak{a} such that there exists \mathfrak{b} such that $\mathfrak{a}\mathfrak{b} = \mathcal{O}_\Delta$
- Principal Fractional Ideals: $\alpha \mathcal{O}_\Delta$ where $\alpha \in \mathbb{K}^\times$
- Norm of \mathfrak{a} is $N(\mathfrak{a}) = [\mathcal{O}_\Delta : \mathfrak{a}]$

Notation

- $I(\mathcal{O}_\Delta)$: **group** of Invertible Fractional Ideals of \mathcal{O}_Δ
- $P(\mathcal{O}_\Delta)$: sub-group of Principal Ideals

Class Group

Class Group of discriminant Δ

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

its (**finite**) cardinal is the **class number** denoted $h(\mathcal{O}_\Delta)$

- Equivalence relation:

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

- Class Number: On average $h(\mathcal{O}_\Delta) \approx 0.461559\sqrt{|\Delta|}$

Map between two Class Groups

Theorem

- Let Δ_K be a fundamental negative discriminant, ℓ a conductor, and $\Delta_\ell = \ell^2 \Delta_K$
- There exists a surjective morphism, denoted $\bar{\varphi}_\ell$, between $C(\Delta_\ell)$ and $C(\Delta_K)$

In Practice

- $\bar{\varphi}_\ell$ is effective, can be computed with quadratic complexity if ℓ is known

Class Groups and Binary Quadratic Forms

Definite Positive Binary Quadratic Forms of Discriminant Δ

- $f(x, y) = ax^2 + bxy + cy^2$ with $b^2 - 4ac = \Delta < 0$ and $a > 0$
- We denote $f = (a, b, c)$
- Norm of f : $N(f) = a$

Equivalence relation

- $f \sim g$ if and only if there exists $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ with
 $A, B, C, D \in \mathbf{Z}$ and $\det(M) = 1$ and

$$g(Ax + By, Cx + Dy) = f(x, y)$$

Class Groups and Binary Quadratic Forms

Definite Positive Binary Quadratic Forms of Discriminant Δ

- $f(x, y) = ax^2 + bxy + cy^2$ with $b^2 - 4ac = \Delta < 0$ and $a > 0$
- We denote $f = (a, b, c)$
- Norm of f : $N(f) = a$

Reduced Form

- Class Representative: **unique reduced** (a, b, c) such that
 - $-a < b \leq a \leq c$
 - and $b \geq 0$ if $a = c$
- If $a < \sqrt{|\Delta|/4}$ and $-a < b \leq a$, (a, b, c) is reduced

Computation in the Class Group

Class Representative

- Reduction Algorithm of Lagrange–Gauss, quadratic complexity

Product of Classes

- Composition of BQF of Gauss, corresponds to a product of two ideals, quadratic complexity
- Neutral: $[(1, \Delta, \Delta(\Delta - 1)/2)]$, principal class
- Opposite: $[(a, b, c)]^{-1} = [(a, -b, c)]$

Outline

- 1 Introduction
- 2 Class Groups of Imaginary Quadratic Fields
- 3 NICE Cryptanalysis in Imaginary Quadratic Fields**
Joint Work with F. Laguillaumie
- 4 NICE Cryptanalysis in Real Quadratic Fields
Joint Work with A. Joux, F. Laguillaumie and P. Q. Nguyen
- 5 Conclusion

Description of NICE

- Let p and q be two λ bits primes with $p \equiv 3 \pmod{4}$,
 $\Delta_K = -p$, $\Delta_q = -pq^2$

Morphism $\bar{\varphi}_q$

 $C(\Delta_q)$
 $[f]$

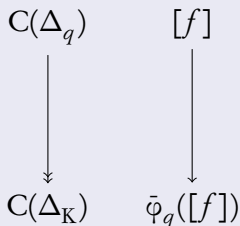
 $C(\Delta_K)$
 $\bar{\varphi}_q([f])$

- Encryption of $[m]$:
 $[m][h] \in C(\Delta_q)$ where $[h]$ is a
 random element of $\ker \bar{\varphi}_q$
- Fast decryption with $\bar{\varphi}_q$

Description of NICE

- Let p and q be two λ bits primes with $p \equiv 3 \pmod{4}$,
 $\Delta_K = -p$, $\Delta_q = -pq^2$

Morphism $\bar{\varphi}_q$



- Encryption of $[m]$:
 $[m][h] \in C(\Delta_q)$ where $[h]$ is a random element of $\ker \bar{\varphi}_q$
- Fast decryption with $\bar{\varphi}_q$

The Public Key contains $[h]$ an element of $\ker \bar{\varphi}_q$

Algorithm Description

- Hartmann, Hühnlein, Paulus and Takagi (ICISC'98, CHESS'99, SAC'99, JoC 00)
- Public Key: $\Delta_q = -pq^2$, $[h] \in \ker \bar{\varphi}_q$
- Private Key: q
- Encryption: Let m be a reduced form of small norm,

$$\text{Encrypt}(m, r) = [m][h]^r$$

- Decryption:

$$\text{Decrypt}(c) = \bar{\varphi}_q([m][h]^r) = \bar{\varphi}_q([m]) \rightsquigarrow m$$

NICE Features (1)

Advantage of NICE:

- Quadratic Decryption thanks to $[b]$

Security:

- TB-CPA: *believed to rely* on the hardness of factorisation of $\Delta_q = -pq^2$
- Rely precisely on the hardness of the *Kernel Problem*:

Given Δ_q and $[b] \in \ker \bar{\varphi}_q$, Factor Δ_q

- TB-CCA : attack of Jaulmes and Joux (Eurocrypt'00), can be deflected by adding a suitable padding

NICE Features (2)

Security (cont.):

- OW-CPA and IND-CPA under *ad hoc* hypothesis
- IND-CCA version based on REACT proposed by Buchmann, Sakurai and Takagi (ICISC'01)

Signature schemes based on the *Kernel Problem*:

- Hühnlein and Merkle (PKC'00, RSA-CT'01)
- Undeniable Signatures by Biehl, Paulus and Takagi (DCC 04)

Cryptanalysis Intuition (1)

Kernel Problem

Given Δ_q and $[b] \in \ker \bar{\varphi}_q$, Factor Δ_q

Well known Lemma

There exists an effective isomorphism

$$G_q := \left(\mathcal{O}_{\Delta_K} / q \mathcal{O}_{\Delta_K} \right)^\times / (\mathbf{Z} / q \mathbf{Z})^\times \xrightarrow{\sim} \ker \bar{\varphi}_q$$

Cryptanalysis Intuition (2)

Theorem

In each non trivial class of $\ker \bar{\varphi}_q$, there exists a form of norm q^2

Cryptanalysis Intuition (2)

Theorem

In each non trivial class of $\ker \bar{\varphi}_q$, there exists a form of norm q^2

Proof (sketch).

- Set of representatives of $(\mathcal{O}_{\Delta_K}/q\mathcal{O}_{\Delta_K})^\times / (\mathbf{Z}/q\mathbf{Z})^\times$:

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

with $N(\alpha_x)$ prime to q

- Computation of

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



Cryptanalysis Intuition (2)

Theorem

In each non trivial class of $\ker \bar{\varphi}_q$, there exists a form of norm q^2

Consequence

- In the NICE public key, the reduced form h is equivalent to a non reduced form of norm q^2 : $(q^2, -, -)$
- First idea: Inverting the reduction process

Cryptanalysis Intuition (2)

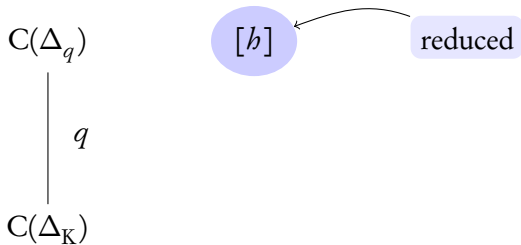
Theorem

In each non trivial class of $\ker \bar{\varphi}_q$, there exists a form of norm q^2

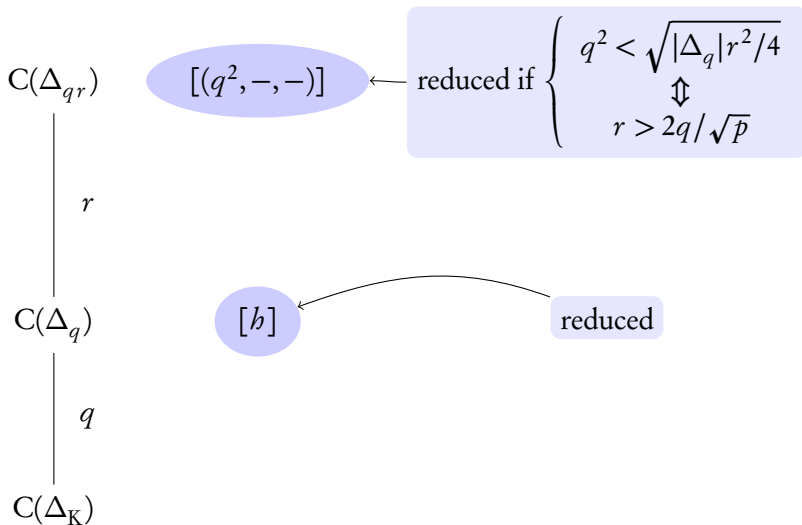
Consequence

- In the NICE public key, the reduced form h is equivalent to a non reduced form of norm q^2 : $(q^2, -, -)$
- First idea: Inverting the reduction process **Inefficient!**

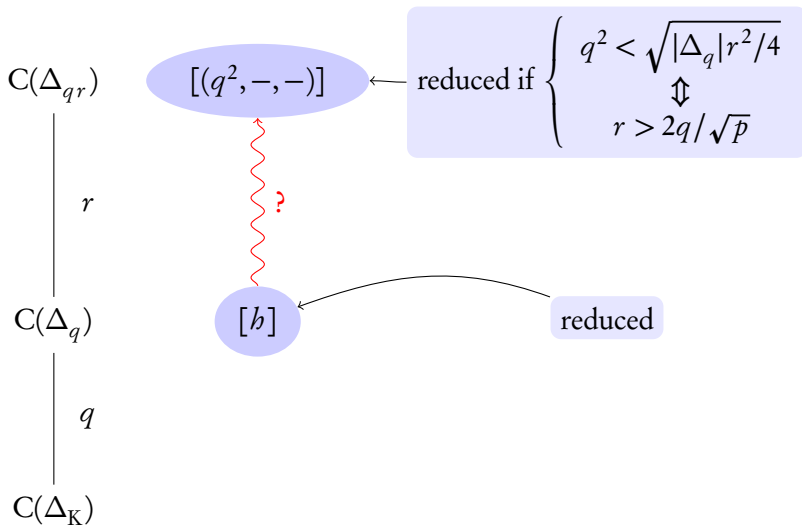
Second idea: lift $[b]$



Second idea: lift $[h]$



Second idea: lift $[b]$



How to lift $[h]$?

$$\ker \bar{\phi}_{qr} \xrightarrow{\sim} G_{qr} \xrightarrow{\sim} G_q \times G_r$$

$[(q^2, -, -)]$

$([\bar{\alpha}], [\bar{1}])$

with $[\bar{\alpha}] \neq [\bar{1}]$

Notation:

$$\mathbf{G}_\ell := (\mathcal{O}_{\Delta_K} / \ell \mathcal{O}_{\Delta_K})^\times / (\mathbf{Z} / \ell \mathbf{Z})^\times \text{ and } \phi_{\Delta_K}(\ell) := \#\mathbf{G}_\ell$$

How to lift $[b]$?

$$\ker \bar{\varphi}_{qr} \xrightarrow{\sim} G_{qr} \xrightarrow{\sim} G_q \times G_r$$

 $[(q^2, -, -)]$
 $([\bar{\alpha}], [\bar{1}])$

 with $[\bar{\alpha}] \neq [\bar{1}]$

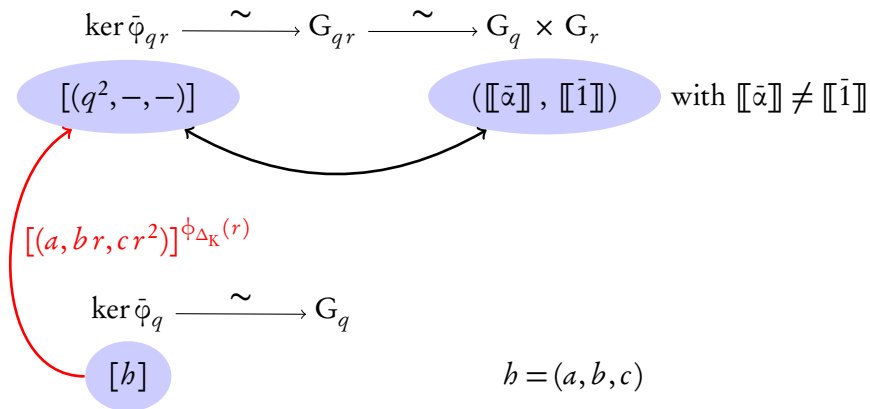
$$\ker \bar{\varphi}_q \xrightarrow{\sim} G_q$$

 $[b]$

Notation:

$$\mathbf{G}_\ell := (\mathcal{O}_{\Delta_K} / \ell \mathcal{O}_{\Delta_K})^\times / (\mathbf{Z} / \ell \mathbf{Z})^\times \text{ and } \phi_{\Delta_K}(\ell) := \#\mathbf{G}_\ell$$

How to lift $[h]$?



Notation:

$$\mathbf{G}_\ell := (\mathcal{O}_{\Delta_K} / \ell \mathcal{O}_{\Delta_K})^\times / (\mathbf{Z} / \ell \mathbf{Z})^\times \text{ and } \phi_{\Delta_K}(\ell) := \#\mathbf{G}_\ell$$

Summary of the Cryptanalysis

Sketch of the Algorithm

- Select $r \in \mathbf{N}$ such that the forms of norm q^2 are reduced in $\mathcal{O}_{\Delta_{qr}}$
- Compute $\phi_{\Delta_K}(r) = r \prod_{\ell|r} \left(1 - \left(\frac{\Delta_K}{\ell}\right) \frac{1}{\ell}\right)$
- Given $h = (a, b, c)$ of discriminant $\Delta_q = -pq^2$, such that $[h] \in \ker \bar{\varphi}_q$, compute $[(a, br, cr^2)]^{\phi_{\Delta_K}(r)}$
- Retrieve q^2

Complexity

- Cubic complexity in the security parameter
- A couple of milliseconds on a standard PC on a cryptographic example

Second Approach (1)

Joint work with A. Joux, F. Laguillaumie and P. Q. Nguyen

How to find q^2 from $h = (a, b, c)$?

- In the NICE public key, the reduced form $h = (a, b, c)$ of discriminant Δ_q is equivalent to a non reduced form of norm q^2 : $(q^2, -, -)$
- $\exists(x_0, y_0) \in \mathbf{Z}, ax_0^2 + bx_0y_0 + cy_0^2 = q^2$
- Experimentally, x_0 and y_0 are relatively **small** compared to Δ_q
- **Second Approach**: Find the small roots (x_0, y_0) with a variant of Coppersmith Algorithm

Second Approach (2)

Problem

- Given $h(x, y) = ax^2 + bxy + cy^2$ and $|\Delta_q| = pq^2$ an integer of unknown factorisation
- Find $(x_0, y_0) \in \mathbf{Z}^2$ such that

$$h(x_0, y_0) \equiv 0 \pmod{q^2}$$

while $|x_0| \leq X$ and $|y_0| \leq Y$, where $X, Y \in \mathbf{N}$.

Known Solutions

- Find small modular roots of a bivariate polynomial
- Usual technique for this kind of problems: **heuristic**
- Here h is **homogeneous**

Second Approach (3)

Same technique already used by Bernstein for Goppa codes decoding in 08!

Lemma (Variant of Howgrave-Graham in the homogeneous case)

- Let $B \in \mathbf{N}$ and $f(x, y) \in \mathbf{Z}[x, y]$ be homogeneous of degree d with at most $\omega (\leq d + 1)$ monomials
- Suppose that $f(x_0, y_0) \equiv 0 \pmod{B}$ where $|x_0| \leq X$ and $0 < |y_0| \leq Y$ and $\|f(xX, yY)\| < B/\sqrt{\omega}$
- Then the univariate polynomial $\tilde{f}(r) = (1/y^d)f(x, y)$ (with $r = x/y$) is such that

$$\tilde{f}(x_0/y_0) = 0 \text{ holds over } \mathbf{Q}$$

Second Approach (4)

Construction of the small polynomial

- Construction of a lattice spanned by a family of homogeneous polynomials with the same roots (x_0, y_0) modulo q^2 than $b(x, y) = ax^2 + bxy + cy^2$
- Reduction of the lattice with the LLL Algorithm
- Result: If $|x_0|, |y_0| < |\Delta_q|^{1/9}$ then the first vector of the reduced basis gives a polynomial with the root x_0/y_0 over \mathbb{Q}

Experimental results

- For cryptographic examples, the roots x_0 and y_0 of b are smaller than $|\Delta_q|^{1/9}$
- With a 13-dimensional lattice, we can get x_0 and y_0 and then q^2 in half a second on a standard PC

Outline

- 1 Introduction
- 2 Class Groups of Imaginary Quadratic Fields
- 3 NICE Cryptanalysis in Imaginary Quadratic Fields
Joint Work with F. Laguillaumie
- 4 NICE Cryptanalysis in Real Quadratic Fields
Joint Work with A. Joux, F. Laguillaumie and P. Q. Nguyen
- 5 Conclusion

What is different in the Real Case? (1)

Real Quadratic Fields

- $K = \mathbb{Q}(\sqrt{\Delta_K}), \Delta_K > 0$

Units

- \mathcal{O}_Δ^* is the group of units in \mathcal{O}_Δ

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

ε_Δ is the **fundamental unit**

- $R_\Delta = \log(\varepsilon_\Delta)$ is the **regulator** of \mathcal{O}_Δ

What is different in the Real Case? (2)

Indefinite Binary Quadratic Forms of Discriminant Δ

- $f(x, y) = ax^2 + bxy + cy^2$ with $b^2 - 4ac = \Delta > 0$

Reduced Form

- $f = (a, b, c)$ is reduced if

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

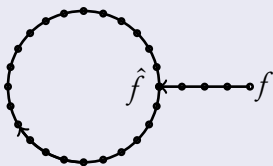
- Class representatives: **more than one reduced form by class!**

What is different in the Real Case? (2)

Indefinite Binary Quadratic Forms of Discriminant Δ

- $f(x, y) = ax^2 + bxy + cy^2$ with $b^2 - 4ac = \Delta > 0$

Cycle of Reduced Forms



- Reduction process is periodic, giving all the reduced forms of a class
- Period length of the cycle of reduced forms $\approx R_\Delta$

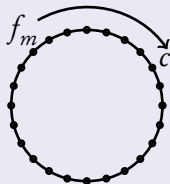
$$\log \left(\frac{1}{2} (\sqrt{\Delta - 4} + \sqrt{\Delta}) \right) \leq R_\Delta < \sqrt{\frac{1}{2} \Delta} \left(\frac{1}{2} \log \Delta + 1 \right)$$

Description of NICE in Real Quadratic Fields

- Weimer (Master's Thesis 04); Jacobson, Scheidler, Weimer (Africacrypt'08)
- Let p and q be two λ bits primes with $p \equiv 1 \pmod{4}$, $\Delta_K = p$, $\Delta_q = pq^2$, such that
 - R_{Δ_K} is **small** ($\approx \log p$)
 - R_{Δ_q} is **large** ($\approx q \log p$)

Encryption

- **Public Key:** Δ_q
- **Encryption of m :** In \mathcal{O}_{Δ_q} , embed m and a bit pattern in a reduced form f_m with small norm, then...

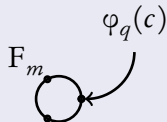


Description of NICE in Real Quadratic Fields

- Weimer (Master's Thesis 04); Jacobson, Scheidler, Weimer (Africacrypt'08)
- Let p and q be two λ bits primes with $p \equiv 1 \pmod{4}$, $\Delta_K = p$, $\Delta_q = pq^2$, such that
 - R_{Δ_K} is **small** ($\approx \log p$)
 - R_{Δ_q} is **large** ($\approx q \log p$)

Decryption

- Private Key: q
- Decryption of c : Apply $\varphi_q(\cdot)$ to c , to go in \mathcal{O}_{Δ_K} , then...



Cryptanalysis

TB-CPA

Given $\Delta_q = pq^2$ where R_p is small ($\approx \log p$), factor Δ_q

Theorem

Let Δ_K be a fundamental positive discriminant, $\Delta_q = \Delta_K q^2$ where q is an odd prime conductor. Let ε_{Δ_K} (resp. ε_{Δ_q}) be the fundamental unit of \mathcal{O}_{Δ_K} (resp. \mathcal{O}_{Δ_q}) and t such that $\varepsilon_{\Delta_K}^t = \varepsilon_{\Delta_q}$. Then the principal ideals of \mathcal{O}_{Δ_q} generated by $q\varepsilon_{\Delta_K}^i$, $i = 1, \dots, t - 1$ correspond to quadratic forms

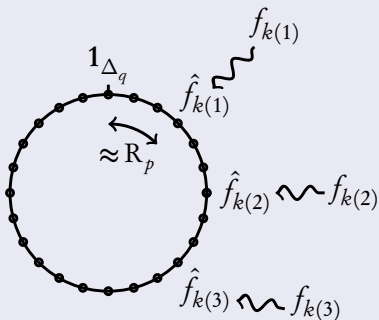
$$f_{k(i)} = (q^2, k(i)q, (k(i)^2 - p)/4)$$

Cryptanalysis

TB-CPA

Given $\Delta_q = pq^2$ where R_p is small ($\approx \log p$), factor Δ_q

Principal Cycle of \mathcal{O}_{Δ_q}



Summary of the Cryptanalysis

Sketch of the Algorithm

- From the principal form $1_{\Delta_q} = [1, \lfloor \sqrt{\Delta_q} \rfloor, (\lfloor \sqrt{\Delta_q} \rfloor^2 - \Delta_q)/4]$ go across the principal cycle
- For each form, try to find small roots with the Homogeneous Coppersmith Algorithm
- Once small roots have been found, retrieve q^2

Complexity

- Experimentally, small roots are found in $\mathcal{O}(R_p)$ iterations
- Couple of minutes on a standard PC on a cryptographic example

Outline

- 1 Introduction
- 2 Class Groups of Imaginary Quadratic Fields
- 3 NICE Cryptanalysis in Imaginary Quadratic Fields
Joint Work with F. Laguillaumie
- 4 NICE Cryptanalysis in Real Quadratic Fields
Joint Work with A. Joux, F. Laguillaumie and P. Q. Nguyen
- 5 Conclusion

Conclusion

- Total break of all the schemes based on NICE
- Few hope to get a quadratic decryption from class groups of quadratic fields
- New deterministic (heuristic) factoring algorithm for $N = pq^2$, complexity given by the regulator of $\mathbf{Q}(\sqrt{p})$ (generally $\approx \sqrt{p}$)