# On the Security of Cryptosystems with Quadratic Decryption: The Nicest Cryptanalysis

Guilhem Castagnos*[1] and Fabien Laguillaumie[2]

[1] PRISM - Université de Versailles St-Quentin-en-Yvelines
45, avenue des États-Unis, 78035 Versailles Cedex, France
guilhem.castagnos@prism.uvsq.fr
[2] GREYC - Université de Caen-Basse Normandie
Boulevard du Maréchal Juin, BP 5186, 14032 Caen Cedex, France
fabien.laguillaumie@info.unicaen.fr

**Abstract.** We describe the first *polynomial time chosen-plaintext total break* of the NICE family of cryptosystems based on ideal arithmetic in imaginary quadratic orders, introduced in the late 90's by Hartmann, Paulus and Takagi [HPT99]. The singular interest of these encryption schemes is their natural quadratic decryption time procedure that consists essentially in applying Euclid's algorithm. The only current specific cryptanalysis of these schemes is Jaulmes and Joux's chosen-ciphertext attack to recover the secret key [JJ00]. Originally, Hartmann *et al.* claimed that the security against a total break attack relies *only* on the difficulty of factoring the public discriminant $\Delta_q = -pq^2$, although the public key was also composed of a specific element of the class group of the order of discriminant $\Delta_q$, which is crucial to reach the quadratic decryption complexity. In this article, we propose a drastic cryptanalysis which factors $\Delta_q$ (and hence recovers the secret key), only given this element, in cubic time in the security parameter. As a result, performing our cryptanalysis on a cryptographic example takes less than a second on a standard PC.

**Keywords:** Polynomial time total break, quadratic decryption, NICE cryptosystems, imaginary quadratic field-based cryptography

## 1 Introduction

We propose an original and radical cryptanalysis of a large class of schemes designed within imaginary quadratic fields, based on the NICE cryptosystem (cf. [HPT99,PT99,PT00]) which recovers the secret key from the sole public key. These systems have been intensively developed and studied in the late 90's, since they offer a very efficient secret operation (decryption or signature), compared to cryptosystems based on traditional number theory. The one-wayness of these

* This work was done while this author was with the GREYC - ENSICAEN.

schemes rely on the difficulty of the *Smallest Kernel-Equivalent Problem* (SKEP) and their security against a total break was believed to rely on the difficulty of the factorisation of numbers of the form $pq^r$. The first and only cryptanalysis of the NICE encryption scheme, proposed by Jaulmes and Joux's at Eurocrypt'00 [JJ00], recovers the secret key with an access to a decryption oracle[3]. In the setting of the NICE cryptosystems, the public key contains a discriminant $\Delta_q = -pq^2$ *and* the representation of a reduced ideal $\mathfrak{h}$ whose class belongs to the kernel of the surjection from the class group of the quadratic order of (public) discriminant $\Delta_q = -pq^2$ to the class group of the maximal order of (secret) discriminant $\Delta_K = -p$. We will show that with this knowledge of $\mathfrak{h}$ we can actually factor the public discriminant in cubic time in the security parameter.

### 1.1 Imaginary Quadratic Field-based Cryptography

The first use of class groups of imaginary quadratic fields allowed to achieve a Diffie-Hellman key exchange. This paper by Buchmann and Williams [BW88] was the first of several attempts to design imaginary quadratic field-based cryptosystems. Key exchange was also discussed by McCurley in [McC89]. Ten years after, a new encryption scheme appeared in the literature, in the work of Hühnlein, Jacobson, Paulus and Takagi [HJPT98]. The goal of this paper was also to improve the efficiency of the seminal cryptosystems. In fact, the key point of these Elgamal-like encryption schemes is the switching between the class group of the maximal order and the class group of a non-maximal order, which can be done with quadratic complexity (as already mentioned). Unfortunately, Hühnlein *et al.*'s scheme, although using this efficient switching, did not benefit from a quadratic time decryption since the decryption of this scheme really needed a final exponentiation (like in Elgamal).

Soon after, quadratic decryption time was eventually reached with a new encryption scheme, called *NICE*, for *New Ideal Coset Encryption*, described in [HPT99, PT99, PT00]. In [HPT99], it is shown that the decryption time of NICE is comparably as fast as the encryption time of RSA with public exponent $e = 2^{16} + 1$ and an even better implementation is described by Hühnlein in [Huh00]. The key idea of NICE is not to mask the message by a power of the public key (which leads to a cubic decryption like in Elgamal), but by an element which belongs to the kernel of the map which switches between the class group of a non-maximal order to the maximal order. This hiding element is added to the public key and naturally disappears from the ciphertext when applying the map.

As the semantic security of NICE holds only under a chosen-plaintext attack, Buchmann, Sakurai and Takagi patched the scheme by adapting classical techniques to obtain a chosen-ciphertext security in the random oracle model [BST02]. This enhanced scheme, based on REACT [OP01] is called NICE-X, and of course resists Jaulmes and Joux's attack [JJ00]. Hühnlein, Meyer and Takagi also built in [HMT99] Rabin and RSA analogues based on non-maximal imaginary quadratic orders, but the only advantages over the original systems

[3] This attack can actually be deflected by adding a suitable padding.

is their seemingly natural immunity against low exponent attacks and some chosen-ciphertext attacks.

The design of signature schemes has also been addressed in [HM00, Huh01] with an adaptation of Schnorr signatures (cf. [Sch00]). Again an element of the kernel of the switching between two class groups is published: this element is crucial for the efficiency of the signature generation. An undeniable signature scheme has been designed in [BPT04], and again, the public element of the kernel is needed for the design of an efficient scheme.

### 1.2 Related Work on Security Issues of Quadratic Field-based Cryptography

All the NICE schemes share the same public information: a discriminant of the form $\Delta_q = -pq^2$ and the representation of a reduced ideal $\mathfrak{h}$ whose class belongs to the kernel of the surjection from the class group of the quadratic order of (public) discriminant $\Delta_q = -pq^2$ to the class group of the maximal order of (secret) discriminant $\Delta_K = -p$. Of course, a factorisation of the discriminant obviously totally breaks the scheme. Therefore, the security parameters are set such that the factorisation of numbers of the form $pq^r$ is difficult. This particular factorisation has been addressed by Boneh, Durfee and Howgrave-Graham in [BDH99], but for small $r$ (such as 2), their method is not better than Lenstra's ECM method [Len87] or the Number Field Sieve [LL93]. In [BST02], the authors also mention the *Quadratic Order Discrete Logarithm Problem* (QODLP). The fastest algorithm to solve the QODLP is the Hafner-McCurley algorithm [HM89], but its running time has a worse subexponential complexity than the fastest factoring algorithm. In [PT00], Paulus and Takagi argue that "the knowledge of $\mathfrak{h}$ does not substantially help to factor $\Delta_q$ using currently known fast algorithms". They also mention the possibility to find a power of the class $[\mathfrak{h}]$ of order 2, but computing the order of the class $[\mathfrak{h}]$ in the class group of the order of discriminant $\Delta_q$ is essentially equivalent to factor this discriminant. The problem of factoring the discriminant $\Delta_q$ given $[\mathfrak{h}]$ is called the Kernel Problem in [BPT04] and again is assumed to be "intractable".

Up to now, the sole specific cryptanalysis of this family of encryption schemes is the *chosen-ciphertext* nice cryptanalysis from [JJ00]. This attack uses the fact that the decryption fails (*i.e.*, does not recover the plain message) if the norm of the ideal representing the message is greater than $\sqrt{|\Delta_K|/3}$, so that the decoded message will expectedly be one step from being reduced. The relation between two pairs original message/decoded message leads to a Diophantine equation of the form $k = XY$ for a known "random" integer $k$ of the size of the secret primes. The authors suggest to factor this integer to find out $X$ and $Y$ and then factor $\Delta_q$. This attack is feasible for the parameters proposed in [HPT99], but can be defeated by enlarging the key size by a factor of 3. No complexity analysis is given for this attack, and the scheme can also be repaired by adding redundancy to the message as suggested in [JJ00] and [BST02]. Note that, contrary to ours, Jaulmes and Joux's attack also applies to [HJPT98].

### 1.3 Our contributions

We propose the first definitive cryptanalysis of cryptosystems based on NICE, which have been resisting for almost 10 years. All these schemes contain in the public key the representation of the reduced ideal $\mathfrak{h}$ whose class belongs to the kernel of the surjection from the class group of the quadratic order of discriminant $\Delta_q = -pq^2$ to the class group of the maximal order of discriminant $\Delta_K = -p$. The key point of our attack is the fact that this ideal $\mathfrak{h}$ is indeed always equivalent to a non-reduced ideal of norm $q^2$, as we will show in Theorem 2. The core of our attack then consists of lifting the class of $\mathfrak{h}$ in the class group of the order of discriminant $\Delta_q r^2$, where $r$ is chosen to make the ideals of norm $q^2$ reduced. This operation will reveal an ideal of norm $q^2$ and thus the factorisation of $\Delta_q$, leading to a total break of the scheme.

Note that the public ideal $\mathfrak{h}$ is crucial in the design of NICE: Random powers of this element are used to hide the message. As it is in the kernel of a surjective map, this randomness can be removed from the ciphertext and the message recovered by applying this map which leads to a decryption algorithm with quadratic complexity (the computation is done with Euclid's algorithm).

The attack described in this paper thus uses this extra piece of information given in the public key to factor the public discriminant. Therefore, this setting is insecure in order to build a cryptosystem with quadratic decryption time. Note that such a scheme with quadratic decryption is a very rare object in group theory based cryptography. Although some schemes built from lattices or coding theory problems have this property, to our knowledge, very few schemes built from the integer factorisation or the discrete logarithm problems have it (*e. g.*, variants of Okamoto-Uchiyama and Paillier's cryptosystems, cf. [CNP99,Pai99]).

As a matter of fact, the encryption schemes built on NICE from [HPT99, PT99, PT00, BST02, Huh00], the signature schemes [Huh01, HM00] and the undeniable signature scheme [BPT04] totally succumb to our attack.

The rest of the paper is organised as follows: The next section gives a background on orders of imaginary quadratic fields to understand the NICE cryptosystem, and then Section 3 is the core of the paper. We describe the cryptanalysis by first discussing the (im-)possibility of reversing the reduction process applied on the reduced ideal $\mathfrak{h}$ in Subsection 3.1. Then, in Subsection 3.2, we describe our attack (Algorithm 3) whose correctness is then proved with Theorem 3 and Corollary 1. Finally, we illustrate the attack with an example.

## 2 Background

The next subsection widely follows the description from [Cox99].

### 2.1 Computations in Quadratic Orders.

A *quadratic field* $K$ is a subfield of the field of complex numbers $\mathbb{C}$ which has degree 2 over $\mathbb{Q}$. Such a field can be uniquely written as $\mathbb{Q}(\sqrt{n})$ where $n$ is a

square-free integer, different from 1 and 0. Its (fundamental) *discriminant* $\Delta_K$ is defined as $n$ if $n \equiv 1 \pmod 4$ and $4n$ otherwise. We will then consider $K$ in terms of its discriminant : $K = \mathbb{Q}(\sqrt{\Delta_K})$ with $\Delta_K \equiv 0, 1 \pmod 4$. An *order* $\mathcal{O}$ in $K$ is a subset of $K$ such that $\mathcal{O}$ is a subring of $K$ containing 1 and $\mathcal{O}$ is a free $\mathbb{Z}$-module of rank 2. The ring $\mathcal{O}_{\Delta_K}$ of integers[4] in $K$ is the *maximal* order of $K$ in the sense that it contains all the other orders of $K$. It can be written as $\mathbb{Z} + \frac{1}{2}(\Delta_K + \sqrt{\Delta_K})\mathbb{Z}$. If we set $f = [\mathcal{O}_{\Delta_K} : \mathcal{O}]$ the *finite* index of any order $\mathcal{O}$ in $\mathcal{O}_{\Delta_K}$, then $\mathcal{O} = \mathbb{Z} + f\frac{1}{2}(\Delta_K + \sqrt{\Delta_K})\mathbb{Z} = \mathbb{Z} + f\mathcal{O}_{\Delta_K}$. The integer $f$ is called the *conductor* of $\mathcal{O}$. The discriminant of $\mathcal{O}$ is then $\Delta_f = f^2\Delta_K$. We will then use the notation $\mathcal{O}_{\Delta_f}$ for such an order.

Now we discuss the ideals of an order $\mathcal{O}_\Delta$ of discriminant $\Delta$. If $\mathfrak{a}$ is a nonzero ideal of $\mathcal{O}_\Delta$, its norm is defined as $\mathrm{N}(\mathfrak{a}) = |\mathcal{O}_\Delta/\mathfrak{a}|$. An ideal $\mathfrak{a}$ is said to be *proper* if $\{\beta \in K : \beta\mathfrak{a} \subset \mathfrak{a}\} = \mathcal{O}_\Delta$. This definition can be extended to *fractional* ideals, which are of the form $\alpha\mathfrak{a}$ where $\alpha \in K^\times$ and $\mathfrak{a}$ is an ideal of $\mathcal{O}_\Delta$. If we denote by $I(\mathcal{O}_\Delta)$ the set of proper fractional ideals of $\mathcal{O}_\Delta$ and its subgroup $P(\mathcal{O}_\Delta)$ consisting of principal ideals, the *ideal class group* of $\mathcal{O}_\Delta$ is defined as $C(\mathcal{O}_\Delta) = I(\mathcal{O}_\Delta)/P(\mathcal{O}_\Delta)$. Its cardinality is the *class number* of $\mathcal{O}_\Delta$ denoted as $h(\mathcal{O}_\Delta)$.

Every ideal $\mathfrak{a}$ of $\mathcal{O}_\Delta$ can be written as

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

with $m \in \mathbb{Z}$, $a \in \mathbb{N}$ and $b \in \mathbb{Z}$ such that $b^2 \equiv \Delta \pmod{4a}$. In the sequel, we will only consider *primitive* ideals, which are those with $m = 1$. This expression is unique if $-a < b \leq a$ and we will now denote a primitive ideal by $(a, b)$. The norm of such an ideal is then $a$.

This notation represents also the positive definite binary quadratic form $ax^2 + bxy + cy^2$ with $b^2 - 4ac = \Delta$. Theorem 7.7 from [Cox99] shows that, up to equivalence relations, it is essentially equivalent to work with ideals and positive definite quadratic forms. An ideal $(a, b)$ of $\mathcal{O}_\Delta$ is said to be *reduced* if the corresponding quadratic form is reduced, which means that $|b| \leq a \leq c$ and $b \geq 0$ if one of the inequalities is not strict. Note that in every class of $\mathcal{O}_\Delta$-ideals there exists exactly one reduced ideal. From the theory of quadratic forms, we can efficiently compute a reduced equivalent ideal. The algorithm, which is due to Gauss, is described in [Coh00, Algorithm 5.4.2 p. 243] and is called Red in the rest of the paper. In general, instead of working with classes, we will work with reduced ideals. The product of ideals is also efficiently computable with the composition of quadratic forms algorithm, see [Coh00, Algorithm 5.4.7 p. 243]. These two algorithms have *quadratic* complexity. A crucial fact for our purpose is described in Lemma 5.3.4 from [Coh00]: If an ideal $\mathfrak{a} = (a, b)$ is reduced, then $a \leq \sqrt{\Delta/3}$ and conversely, if $a < \sqrt{\Delta/4}$ and $-a < b \leq a$, then $\mathfrak{a}$ is reduced.

Let $\left(\frac{a}{b}\right)$ be the Kronecker symbol of $a$ and $b$. The formula for the class number is given by the following theorem.

[4] *i.e.*, the set of all $\alpha \in K$ which are roots of a monic polynomial in $\mathbb{Z}[X]$

**Theorem 1 ([Cox99, Theorem 7.24]).** *Let $\mathcal{O}_{\Delta_f}$ be the order of conductor $f$ in an imaginary quadratic field $K$ (i. e., $\Delta_f = f^2\Delta_K$). Then*

$$h(\mathcal{O}_{\Delta_f}) = \frac{h(\mathcal{O}_{\Delta_K})f}{[\mathcal{O}_{\Delta_K}^\times : \mathcal{O}_{\Delta_f}^\times]} \prod_{p|f} \left(1 - \left(\frac{\Delta_K}{p}\right)\frac{1}{p}\right).$$

Given an order $\mathcal{O}_{\Delta_f}$ of conductor $f$, a nonzero $\mathcal{O}_{\Delta_f}$-ideal $\mathfrak{a}$ is said to be *prime to* $f$ if $\mathfrak{a} + f\mathcal{O}_{\Delta_f} = \mathcal{O}_{\Delta_f}$ (it is equivalent to say that its norm $\mathrm{N}(\mathfrak{a})$ is prime to $f$ – see Lemma 7.18 from [Cox99]). We denote by $I(\mathcal{O}_{\Delta_f}, f)$ the subgroup of $I(\mathcal{O}_{\Delta_f})$ generated by ideals prime to $f$. $P(\mathcal{O}_{\Delta_f}, f)$ is the subgroup generated by the principal ideals $\alpha\mathcal{O}_{\Delta_f}$ where $\alpha \in \mathcal{O}_{\Delta_f}$ has a norm prime to $f$. Note that in every ideal class, there exists an ideal prime to $f$ (cf. [Cox99, Corollary 7.17]). To establish Theorem 1, Cox has studied the links between the class group of the maximal order of an imaginary quadratic field and the class groups of any of its orders. The following propositions throw a light on such fundamental links.

**Proposition 1 ([Cox99, Proposition 7.19]).** *The inclusion $I(\mathcal{O}_{\Delta_f}, f) \subset I(\mathcal{O}_{\Delta_f})$ induces an isomorphism*

$$I(\mathcal{O}_{\Delta_f}, f)/P(\mathcal{O}_{\Delta_f}, f) \simeq I(\mathcal{O}_{\Delta_f})/P(\mathcal{O}_{\Delta_f}) = C(\mathcal{O}_{\Delta_f}).$$

**Proposition 2 ([Cox99, Proposition 7.20]).** *Let $\mathcal{O}_{\Delta_f}$ be an order of conductor $f$ in an imaginary quadratic field $K$.*

*i. If $\mathfrak{A}$ is an $\mathcal{O}_{\Delta_K}$-ideal prime to $f$, then $\mathfrak{A} \cap \mathcal{O}_{\Delta_f}$ is an $\mathcal{O}_{\Delta_f}$-ideal prime to $f$ of the same norm.*
*ii. If $\mathfrak{a}$ is an $\mathcal{O}_{\Delta_f}$-ideal prime to $f$, then $\mathfrak{a}\mathcal{O}_{\Delta_K}$ is an $\mathcal{O}_{\Delta_K}$-ideal prime to $f$ of the same norm.*
*iii. The map $\varphi_f : I(\mathcal{O}_{\Delta_f}, f) \longrightarrow I(\mathcal{O}_{\Delta_K}, f)$ such that $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_{\Delta_K}$ is an isomorphism.*

Consequently, the map $\varphi_f$ from Proposition 2 induces a surjection

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

that can be computed as follows: given a class $[\mathfrak{a}] \in C(\mathcal{O}_{\Delta_f})$, one finds $\mathfrak{b} \in [\mathfrak{a}]$ such that $\mathfrak{b} \in I(\mathcal{O}_{\Delta_f}, f)$ (see standard techniques [HJPT98, Algorithm 1]) and $\bar{\varphi}_f([\mathfrak{a}]) = [\varphi_f(\mathfrak{b})] = [\mathfrak{b}\mathcal{O}_{\Delta_K}]$. The next two algorithms compute $\varphi_f$ and its inverse (cf. [PT00]).

**Input**: $\mathfrak{A} = (A, B) \in I(\mathcal{O}_{\Delta_K}, f)$
**Output**: $\mathfrak{A} \cap \mathcal{O}_{\Delta_f} = (a, b) \in I(\mathcal{O}_{\Delta_f}, f)$
1. $a \leftarrow A$
2. $b \leftarrow Bf \mod_c 2a$ $(|b| < a)$ [centered euclidean division]
3. **Return** $(a, b)$

**Algorithm 1**: Algorithm to compute $\varphi_f^{-1}$

**Input**: $\mathfrak{a} = (a, b) \in I(\mathcal{O}_{\Delta_f}, f), \Delta_f$
**Output**: $\mathfrak{a}\mathcal{O}_{\Delta_K} = (A, B) \in I(\mathcal{O}_{\Delta_K}, f)$
1. $A \leftarrow a$
2. $\delta \leftarrow \Delta_f \mod 2$
3. Compute $u$ and $v \in \mathbb{Z}$ such that $1 = uf + a\delta v$ [extended Euclidean algorithm]
4. $B \leftarrow bu + a\delta v \mod_c 2a$ $(|B| < a)$ [centered euclidean division]
5. **Return** $(A, B)$

**Algorithm 2**: Algorithm to compute $\varphi_f$

Takagi and Paulus showed, in Section 4.2 from [PT00], that in the NICE setting the computation of this homomorphism $\varphi_f$ cannot be done without the knowledge of the prime secret conductor.

The following effective lemma was used in [Cox99] to prove the formula of Theorem 1 by computing the order of $\ker \bar{\varphi}_f$ and by Hühnlein, for example in [Huh00, Huh01] to efficiently compute in $\ker \bar{\varphi}_f$. It also proves the correctness of our attack. Indeed with a well-known system of representatives of $(\mathcal{O}_{\Delta_K}/f\mathcal{O}_{\Delta_K})^\times / (\mathbb{Z}/f\mathbb{Z})^\times$, we will derive a suitable system of representatives for $\ker \bar{\varphi}_f$, which is essential for the proofs of Theorem 2 and Lemma 2.

**Lemma 1.** *Let $\Delta_K$ be a fundamental negative discriminant, different from $-3$ and $-4$, and $f$ a conductor. Then there exists an effective isomorphism*

$$\psi_f \colon (\mathcal{O}_{\Delta_K}/f\mathcal{O}_{\Delta_K})^\times / (\mathbb{Z}/f\mathbb{Z})^\times \xrightarrow{\sim} \ker \bar{\varphi}_f.$$

*We will denote by $\phi_{\Delta_K}(f) := f \prod_{p|f} \left(1 - \left(\frac{\Delta_K}{p}\right) \frac{1}{p}\right)$ the order of $\ker \bar{\varphi}_f$.*

*Proof.* The proof follows the line of the proof of [Cox99, Proposition 7.22 and Theorem 7.24]. □

*Remark 1.* To effectively map a class from $(\mathcal{O}_{\Delta_K}/f\mathcal{O}_{\Delta_K})^\times / (\mathbb{Z}/f\mathbb{Z})^\times$ to $\ker \bar{\varphi}_f$, one takes a representative $\alpha \in \mathcal{O}_{\Delta_K}$, $\alpha := x + y \frac{\Delta_K + \sqrt{\Delta_K}}{2}$ where $x, y \in \mathbb{Z}$ and $\gcd(\mathrm{N}(\alpha), f) = 1$ (to ensure that $\alpha$ is invertible modulo $f\mathcal{O}_{\Delta_K}$), and computes

$$\psi_f\big([\alpha]\big) = \big[\varphi_f^{-1}(\alpha\mathcal{O}_{\Delta_K})\big],$$

which is in $\ker \bar{\varphi}_f$. In this computation, the representation of $\alpha\mathcal{O}_{\Delta_K}$ can be obtained with [BTW95, Proposition 2.9] and the evaluation of $\varphi_f^{-1}$ with Algorithm 1.

Conversely, given a class of $\ker \bar{\varphi}_f$ usually represented by its reduced ideal, one finds a representative ideal $\mathfrak{h} \in I(\mathcal{O}_{\Delta_f}, f)$ (with [HJPT98, Algorithm 1]) and computes $\alpha \in \mathcal{O}_{\Delta_K}$ such that $\alpha\mathcal{O}_{\Delta_K} = \varphi_f(\mathfrak{h})$ ($\varphi_f$ is evaluated with Algorithm 2 and $\alpha$ can be found with [HJW03, Algorithm 1]). Eventually, $\psi_f^{-1}([\mathfrak{h}]) = [\alpha] \in (\mathcal{O}_{\Delta_K}/f\mathcal{O}_{\Delta_K})^\times / (\mathbb{Z}/f\mathbb{Z})^\times$.

### 2.2 The NICE family

We will now describe in Fig. 1 the original NICE cryptosystem as it is presented in [PT00]. For our purpose, it is only important to concentrate on the key generation which outputs an element $[\mathfrak{h}]$ of $\ker \bar{\varphi}_q$ as a part of the public key. Other encryption schemes which share this key generation can be found in [HPT99, PT00, BST02, Huh00, PT99], and signature schemes in [Huh01, HM00, BPT04]. As already mentioned, all these cryptosystems succumb to our attack.

**KeyGen**$(1^\lambda)$**:**

- Let $p$ be a $\lambda$-bit prime such that $p \equiv 3 \pmod 4$ and let $q$ be a prime such that $q > \sqrt{p/3}$.
- Set
$$\begin{cases} \Delta_K = -p \\ \Delta_q = \Delta_K q^2 = -pq^2 \end{cases}$$
- Let $k$ and $l$ be the bit lengths of $\lfloor \sqrt{|\Delta_K|/4} \rfloor$ and $q - \left(\frac{\Delta_K}{q}\right)$ respectively.
- Let $[\mathfrak{h}]$ be an element of $\ker \bar{\varphi}_q$, where $\mathfrak{h}$ is a reduced $\mathcal{O}_{\Delta_q}$- ideal.

The public key $pk$ consists of the quadruple $(\Delta_q, \mathfrak{h}, k, l)$, and the secret key $sk$ consists of the pair $(p, q)$.

**Encrypt**$(1^\lambda, pk, m)$**:**

- A message $m$ is embedded into a reduced $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{m}$ with $\log_2(N(\mathfrak{m})) < k$.
- Pick randomly $r \in [\![1, 2^{l-1}]\!]$ and compute $\mathfrak{c} = \mathsf{Red}(\mathfrak{m} \times \mathfrak{h}^r)$.

**Decrypt**$(1^\lambda, sk, \mathfrak{c})$**:** Compute $\varphi_q^{-1}(\mathsf{Red}(\varphi_q(\mathfrak{c}))) = \mathfrak{m}$.

**Fig. 1.** Description of NICE

**Underlying Algorithmic Assumptions** The security against a total break (resp. of the one-wayness) of the NICE cryptosystem is proved to rely on the hardness of the following problems:

**Definition 1 (Kernel Problem [BPT04]).** *Let $\lambda$ be an integer, $p$ and $q$ be two $\lambda$-bit primes with $p \equiv 3 \pmod 4$. Fix a non-fundamental discriminant $\Delta_q = -pq^2$. Given an element $[\mathfrak{h}]$ of $\ker \bar{\varphi}_q$, factor the discriminant $\Delta_q$.*

**Definition 2 (Smallest Kernel-Equivalent Problem [BST02, BPT04] (SKEP)).** *Let $\lambda$ be an integer, $p$ and $q$ be two $\lambda$-bit primes with $p \equiv 3 \pmod 4$. Fix a non-fundamental discriminant $\Delta_q = -pq^2$. Given an element $[\mathfrak{h}]$ of $\ker \bar{\varphi}_q$ and an element $[\mathfrak{m}] \in C(\mathcal{O}_{\Delta_q})$, compute the ideal with the smallest norm in the equivalence class, modulo the subgroup generated by $[\mathfrak{h}]$, of $[\mathfrak{m}]$.*

It is clear that an algorithm which solves the Kernel Problem also solves the Smallest Kernel-Equivalent Problem. The insecurity of the Kernel Problem will be discussed in the next section.

## 3 The Cryptanalysis

### 3.1 Intuition

In the NICE setting, $\Delta_K = -p$, $\Delta_q = \Delta_K q^2$ where $p$ and $q$ are two large primes, and the schemes are totally broken if one can recover $p$ and $q$ from $\Delta_q$. (Un-)fortunately, another piece of information is given in the public key: an ideal $\mathfrak{h}$ whose class belongs to the kernel of $\bar{\varphi}_q$, the surjection from $C(\mathcal{O}_{\Delta_q})$ to $C(\mathcal{O}_{\Delta_K})$. In [PT00] (for example), the authors suppose that no ideal whose class is in $\ker \bar{\varphi}_q$ leaks a factor of the public discriminant $\Delta_q$, except if this element has order 2, but then a subexponential computation is required to find it.

While investigating this assumption, we experimentally found non-reduced ideals of the form $(q^2, kq)$, with $k$ odd and $|k| < q$ whose classes belong to the kernel of $\bar{\varphi}_q$, and which obviously give the factorisation of $\Delta_q$. By using the effective isomorphism of Lemma 1, we actually prove in the next theorem that one can build a representative set of this kernel with ideals of norm $q^2$.

**Theorem 2.** *Let $\Delta_K$ be a fundamental negative discriminant, different from $-3$ and $-4$ and $q$ an odd prime conductor. There exists an ideal of norm $q^2$ in each nontrivial class of* $\ker \bar{\varphi}_q$.

*Proof.* Let us recall the effective isomorphism from Lemma 1:

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

We are going to build a set of representatives of $\left(\mathcal{O}_{\Delta_K}/q\mathcal{O}_{\Delta_K}\right)^\times / \left(\mathbb{Z}/q\mathbb{Z}\right)^\times$ and apply $\psi_q$ (which can be computed according to Remark 1) to obtain ideals of norm $q^2$ which are a set of representatives of $\ker \bar{\varphi}_q$.

Let us set $\alpha_k = k + \frac{\Delta_K + \sqrt{\Delta_K}}{2}$ with $k \in \{0, \ldots, q-1\}$. Clearly $\mathrm{N}(\alpha_k) = \left(k + \frac{\Delta_K}{2}\right)^2 - \frac{\Delta_K}{4} = k^2 + \Delta_K k + \frac{\Delta_K(\Delta_K - 1)}{4}$. Consider the following set of representatives of $\left(\mathcal{O}_{\Delta_K}/q\mathcal{O}_{\Delta_K}\right)^\times / \left(\mathbb{Z}/q\mathbb{Z}\right)^\times$:

$$\left\{1\right\} \cup \left\{\alpha_k \text{ with } k \in \{0, \ldots, q-1\},\ \mathrm{N}(\alpha_k) \not\equiv 0 \pmod{q}\right\},$$

indeed, it is easy to check that all the $\alpha_k$ belong to different classes and that they are in sufficient number: If $\left(\frac{\Delta_K}{q}\right)$ equals 1 (resp. equals 0, resp. equals $-1$) then the order of the quotient $\left(\mathcal{O}_{\Delta_K}/q\mathcal{O}_{\Delta_K}\right)^\times / \left(\mathbb{Z}/q\mathbb{Z}\right)^\times$ is $1 + (q-2)$ (resp. $1 + (q-1)$, resp. $1 + (q+1)$). We are now going to compute the image of this set by $\psi_q$ in $\ker \bar{\varphi}_q$.

Following the proof of [BTW95, Proposition 2.9], we detail here the computation of $\mathfrak{A}_k = \alpha_k \mathcal{O}_{\Delta_K}$. The representation of $\mathfrak{A}_k$ is $(a_k, b_k)$, with $a_k = \mathrm{N}(\alpha_k)$. Let us now find $b_k$. The representation of $\mathcal{O}_{\Delta_K}$ is $\left(1, \frac{\Delta_K + \sqrt{\Delta_K}}{2}\right)$. A simple calculation gives

$$\alpha_k \mathcal{O}_{\Delta_K} = \alpha_k \mathbb{Z} + \left(\frac{k\Delta_K}{2} + \frac{\Delta_K(\Delta_K + 1)}{4} + (k + \Delta_K)\frac{\sqrt{\Delta_K}}{2}\right)\mathbb{Z}$$

which must be equal to $m_k\left(a_k\mathbb{Z}+\frac{-b_k+\sqrt{\Delta_K}}{2}\mathbb{Z}\right)$. As mentioned in the proof of [BTW95, Proposition 2.9], $m_k$ is the smallest positive coefficient of $\sqrt{\Delta_K}/2$ in $\mathfrak{A}_k$: in our case $m_k=\gcd(1,k+\Delta_K)$ and therefore $m_k=1$.

Since $\alpha_k\in\alpha_k\mathcal{O}_{\Delta_K}$, there exists $\mu_k$ and $\nu_k$ such that $\alpha_k=a_k\mu_k+\frac{-b_k+\sqrt{\Delta_K}}{2}\nu_k$. By identification in the basis $(1,\sqrt{\Delta_K})$, $\nu_k=1$ and by a multiplication by 2, we obtain $2k+\Delta_K=2a_k\mu_k-b_k$. As the value of $b_k$ is defined modulo $2a_k$, we can take

$$b_k=-2k-\Delta_K.$$

We now need to compute $\varphi_q^{-1}(\mathfrak{A}_k)$. From Algorithm 1, it is equal to $(a_k, b_kq \bmod 2a_k)$. Eventually, in every nontrivial class of $\ker\bar{\varphi}_q$, there exists an ideal $(a_k,b_kq)$. This ideal corresponds to the quadratic form $a_kx^2+b_kqxy+c_ky^2$ with

$$c_k=\frac{q^2\left((2k+\Delta_K)^2-\Delta_K\right)}{4(k^2+\Delta_Kk)+\Delta_K(\Delta_K-1)}=q^2,$$

which is then equivalent to the form $q^2x^2-b_kqxy+a_ky^2$ corresponding to the ideal $(q^2,-b_kq)$ whose norm is $q^2$. □

**A first attempt: inverting the reduction process.** From this theorem, the reduced ideal $\mathfrak{h}$ published in the NICE cryptosystems is equivalent to an ideal of norm $q^2$. A first attack is thus to try to do a brute force ascent of the reduction algorithm, *i. e.*, the Gauss algorithm, from $\mathfrak{h}$. To "invert" a step of this algorithm (see Algorithms 1.3.14 and 5.4.2 of [Coh00]), one has to consider all the possible quotients of the Euclidean division. The number of possible quotients is heuristically low (say ten), and the complexity of the attack grows exponentially with the number of reduction steps. If this number is very low, the attack will be feasible. In particular, if $q<\sqrt{p/4}$, all ideals of the form $(q^2,kq)$ are already reduced, so the norm of $\mathfrak{h}$ is $q^2$ and the schemes are insecure. If the parameters for NICE are chosen as proposed in [PT00] (*i. e.*, $\sqrt{p/3}<q$) the number of reduction steps can still be too low. In the given implementation and later papers (*e. g.*, [BST02]), $p$ and $q$ are actually chosen of same size $\lambda$, the security parameter. Let us analyse more generally the numbers of reduction steps needed to reduce ideals of the form $(q^2,kq)$ in $C(\mathcal{O}_{\Delta_q})$.

If we translate the problem in terms of quadratic forms, the quadratic form $q^2x^2+kqxy+c(k)^2y^2$, with $c(k):=\frac{1}{4}(k^2+p)$, can be represented by the matrix

$$\begin{pmatrix} q^2 & kq/2 \\ kq/2 & c(k)\end{pmatrix},$$

which defines (up to an isometry) two vectors $u$ and $v$ of $\mathbb{C}$ such that $|u|^2=q^2$, $|v|^2=c(k)$ and $\langle u,v\rangle=kq/2$, where $\langle\cdot,\cdot\rangle$ denotes the usual scalar product in $\mathbb{C}$. If we consider the complex number $z=\frac{v}{u}$ (we suppose here that $u$ is larger than $v$, *i. e.*, $q^2>\frac{1}{4}(k^2+p)$), then

$$z=\frac{\langle u,v\rangle}{|u|^2}+i\frac{\det(u,v)}{|u|^2}=\frac{kq}{2q^2}+i\frac{\sqrt{|\Delta_q|}}{q^2}=\frac{k}{2q}+i\frac{\sqrt{p}}{q}\,.$$

The mean number of iteration $A_h$ of the Gauss algorithm when the complex number $z$ belongs to the strip $\{|\Im(z)| \leq 1/h\}$ is heuristically

$$A_h \sim \frac{1}{2}\log h \left[\frac{1}{\log(1+\sqrt{2})} - \frac{1}{\log\left(\frac{\pi^2}{6\log\phi}\right)}\right],$$

where $\phi$ is the golden ratio.

Inside this horizontal strip, the complex numbers $z$ for which the number of iterations is of order $\Omega(\log L)$ are those for which their real part $\Re(z)$ is close to a rational number whose continued fraction expansion is of order $\Omega(\log L)$.

Then, since our complex number $z$ is of the form $z = \frac{k}{2q} + i\frac{\sqrt{p}}{q}$, the number of iterations of the Gauss Algorithm on the input $z$ will be (with a high probability) of order $\Omega(\log qp^{-\frac{1}{2}})$ provided that the height of the continued fraction expansion of the rational number $k/q$ is of order $\Omega(\log q)$ (which is always the case, with a high probability). See [VV07] for a precise analysis of Gauss algorithm. If we set $q = p^\alpha$ these theoretical results give a behaviour in $\Omega\big(\big(\alpha - \frac{1}{2}\big)\log p\big)$, and therefore if we set $\alpha = 1$ as suggested in [BST02], we have a number of steps proportional to $\log p/2 = \lambda/2$ so the going up is infeasible. Note that our experiments confirm this complexity. Therefore we have to establish another strategy to recover these non-reduced ideal of norm $q^2$.

### 3.2 An Algorithm to Solve the Kernel Problem

**Description.** In this subsection, we describe an algorithm which totally breaks the NICE family of cryptosystems by solving the Kernel Problem in polynomial time in the security parameter. More precisely, given $\Delta_q = -pq^2$ where $p$ and $q$ are two $\lambda$-bit primes and $\mathfrak{h}$ a reduced ideal whose class is in the kernel of the surjection from $C(\mathcal{O}_{\Delta_q})$ to $C(\mathcal{O}_{\Delta_K})$, this algorithm outputs $p$ and $q$ in cubic time. The next subsection is dedicated to the analysis of the correctness and the complexity of this algorithm. The main result is given in Corollary 1.

The strategy of the attack, detailed in the next algorithm, is as follows. First, in an initialisation phase (steps 1–3), we generate a power $r$ of a small odd prime. This integer $r$ is chosen large enough to make the ideals of norm $q^2$ reduced in $C(\mathcal{O}_{\Delta_q r^2})$. Then, the core of the algorithm consists in lifting $[\mathfrak{h}']$ (where $\mathfrak{h}'$ is equivalent to $\mathfrak{h}$ and prime to $r$) in this class group. In step 5, we compute $\mathfrak{g} = \mathfrak{h}' \cap \mathcal{O}_{\Delta_q r^2}$, which is an $\mathcal{O}_{\Delta_q r^2}$-ideal, with Algorithm 1 (this algorithm still works between two non-maximal orders).

Then, in step 6, we compute the reduced element $\mathfrak{k}$ of the class of $\mathfrak{g}$ raised to the power $\phi_{\Delta_K}(r)$. In the next subsection, we will prove that this lift (steps 5 and 6) maps almost all the elements of $\ker\bar{\varphi}_q$, including $[\mathfrak{h}]$, to elements of $\ker\bar{\varphi}_{qr}$ whose reduced ideal has norm $q^2$. As a consequence, the ideal $\mathfrak{k}$ computed in step 6 has norm $q^2$ and eventually step 7 extracts $p$ and $q$.

**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 $\mathfrak{h}' \in I(\mathcal{O}_{\Delta_q}, r')$ [HJPT98, Algorithm 1]

**Core Algorithm:**

5. Compute $\mathfrak{g} = \mathfrak{h}' \cap \mathcal{O}_{\Delta_q r^2}$ [Algorithm 1]
6. Compute $\mathfrak{f} = \mathsf{Red}(\mathfrak{g}^{\phi_{\Delta_K}(r)})$
7. **Return** $p = \Delta_q / \mathrm{N}(\mathfrak{f})$, $q = \sqrt{\mathrm{N}(\mathfrak{f})}$

**Algorithm 3**: Solving the Kernel Problem

*Remark 2.* We omit elements of small order in the input of our algorithm, because they are useless for the NICE cryptosystems. As we will see in the proof of Corollary 1, this restriction ensures that the incrementation of step 3 will be done at most once. For completeness, if the order of $[\mathfrak{h}]$ is 3, only few iterations will be done to obtain a suitable $r$ such that the order of $[\mathfrak{h}]$ does not divide $\phi_{\Delta_K}(r) = r'^{\delta_{r'}-1}\left(r' - \left(\frac{\Delta_K}{r'}\right)\right)$, and for an order of 5, $r' = 3$ suits. Note also that elements of order 2 (4 and 6) leads to ambiguous ideals which give the factorisation of the discriminant (see [Sch82]).

**Correctness.** Again, the proof of correctness of Algorithm 3 will be done by using the effective isomorphisms between $\ker \bar{\varphi}_q$ and $\left(\mathcal{O}_{\Delta_K}/q\mathcal{O}_{\Delta_K}\right)^\times / \left(\mathbb{Z}/q\mathbb{Z}\right)^\times$ and between $\ker \bar{\varphi}_{qr}$ and $\left(\mathcal{O}_{\Delta_K}/qr\mathcal{O}_{\Delta_K}\right)^\times / \left(\mathbb{Z}/qr\mathbb{Z}\right)^\times$. The integer $r$ is an odd integer prime to $q$ and $\Delta_K$ such that $r > 2q/\sqrt{|\Delta_K|}$, *i. e.*, such that ideals of norm $q^2$ are reduced in $C(\mathcal{O}_{\Delta_q r^2})$.

First in Lemma 2, we prove that nontrivial elements of a certain subgroup of the quotient $\left(\mathcal{O}_{\Delta_K}/qr\mathcal{O}_{\Delta_K}\right)^\times / \left(\mathbb{Z}/qr\mathbb{Z}\right)^\times$ map to classes of $\ker \bar{\varphi}_{qr}$ whose reduced element has norm $q^2$. Actually, this subgroup contains the image of a particular lift of $\left(\mathcal{O}_{\Delta_K}/q\mathcal{O}_{\Delta_K}\right)^\times / \left(\mathbb{Z}/q\mathbb{Z}\right)^\times$ following the Chinese remainder theorem: A class $[\alpha]$ modulo $q$ is lifted to a class $[\beta]$ modulo $qr$ such that $[\beta] \equiv 1 \pmod{r}$ and $[\beta] \equiv [\alpha]^{\phi_{\Delta_K}(r)} \pmod{q}$.

Then, in Theorem 3, we prove that the lift computed in steps 4 and 6 of Algorithm 3 corresponds to the lift previously mentioned on the quotients of $\mathcal{O}_{\Delta_K}$. As a result, this lift evaluated on an element of $\ker \bar{\varphi}_q$ either gives the trivial class or a class corresponding to the nontrivial elements of the subgroup of Lemma 2, *i. e.*, a class whose reduced element has norm $q^2$.

Finally, in Corollary 1, we prove that Algorithm 3 is polynomial and correct, *i. e.*, that the choice of $r$ done in the initialisation of the algorithm ensures that the lift will produce a nontrivial class and hence an ideal of norm $q^2$.

**Lemma 2.** *Let $\Delta_K$ be a fundamental negative discriminant, different from $-3$ and $-4$ and $q$ an odd prime conductor and $r$ be an odd integer prime to $q$ and $\Delta_K$ such that $r > 2q/\sqrt{|\Delta_K|}$. The isomorphism $\psi_{qr}$ of Lemma 1 maps the nontrivial elements of the kernel of this natural surjection*

$$\pi : \left(\mathcal{O}_{\Delta_K}/qr\mathcal{O}_{\Delta_K}\right)^\times / \left(\mathbb{Z}/qr\mathbb{Z}\right)^\times \twoheadrightarrow \left(\mathcal{O}_{\Delta_K}/r\mathcal{O}_{\Delta_K}\right)^\times / \left(\mathbb{Z}/r\mathbb{Z}\right)^\times$$

*to classes of $\ker \bar{\varphi}_{qr} \subset C(\mathcal{O}_{\Delta_K q^2 r^2})$, whose reduced element has norm $q^2$.*

*Proof.* This proof is similar to the proof of Theorem 2, but relative to $r$ (more precisely, specialising $r = 1$ in this lemma yields Theorem 2). Let us set $\alpha_k = k + r\frac{\Delta_K + \sqrt{\Delta_K}}{2}$ where $k \in \mathbb{Z}$ takes $\phi_{\Delta_K}(q)$ values s.t. $\begin{cases} k \not\equiv 0 \pmod r, \\ k \equiv 0, \ldots, q-1 \pmod q, \\ k^2 \not\equiv r^2\Delta_K \pmod q. \end{cases}$
and denote $\mathcal{S} = \{1\} \cup \{\alpha_k\}_k$. For each $k$, the norm $\mathrm{N}(\alpha_k)$ is equal to $\left(k + r\frac{\Delta_K}{2}\right)^2 - \Delta_K\frac{r^2}{4}$.

Since $r$ is prime to $q$, the Chinese remainder theorem gives the isomorphism between $\left(\mathcal{O}_{\Delta_K}/qr\mathcal{O}_{\Delta_K}\right)^\times / \left(\mathbb{Z}/qr\mathbb{Z}\right)^\times$ and

$$\left(\left(\mathcal{O}_{\Delta_K}/q\mathcal{O}_{\Delta_K}\right)^\times / \left(\mathbb{Z}/q\mathbb{Z}\right)^\times\right) \times \left(\left(\mathcal{O}_{\Delta_K}/r\mathcal{O}_{\Delta_K}\right)^\times / \left(\mathbb{Z}/r\mathbb{Z}\right)^\times\right).$$

As all the elements of $\mathcal{S}$ map to the neutral element in $\left(\mathcal{O}_{\Delta_K}/r\mathcal{O}_{\Delta_K}\right)^\times / \left(\mathbb{Z}/r\mathbb{Z}\right)^\times$ and gives all the elements of $\left(\mathcal{O}_{\Delta_K}/q\mathcal{O}_{\Delta_K}\right)^\times / \left(\mathbb{Z}/q\mathbb{Z}\right)^\times$, $\mathcal{S}$ is actually a set of representatives of $\ker \pi$.

Let us now compute $\mathfrak{A}_k = \alpha_k\mathcal{O}_{\Delta_K}$. Its representation is $(a_k, b_k)$, with $a_k = \mathrm{N}(\alpha_k)$ and then

$$\alpha_k\mathcal{O}_{\Delta_K} = \alpha_k\mathbb{Z} + \left(k + r\frac{\Delta_K + \sqrt{\Delta_K}}{2}\right)\left(\frac{\Delta_K + \sqrt{\Delta_K}}{2}\right)\mathbb{Z},$$

which must be equal to $m_k\left(a_k\mathbb{Z} + \frac{-b_k + \sqrt{\Delta_K}}{2}\mathbb{Z}\right)$. The integer $m_k$ is then equal to $\gcd(r, r\Delta_K + k)$ which is equal to 1 since $\gcd(k, r) = 1$.

As $\alpha_k \in \alpha_k\mathcal{O}_{\Delta_K}$, there exists $\mu_k$ and $\nu_k$ such that $\alpha_k = a_k\mu_k + \frac{-b_k + \sqrt{\Delta_K}}{2}\nu_k$. By identification in the basis $(1, \sqrt{\Delta_K})$, $\nu_k = r$ and by multiplying by 2, we obtain $2k + r\Delta_K = 2a_k\mu_k - rb_k$ and again we can take

$$b_k = \frac{-2k}{r} - \Delta_K.$$

Then $\varphi_{qr}^{-1}(\mathfrak{A}_k)$ is equal to $(a_k, B_k)$ where $B_k = b_k qr$. This ideal corresponds to the quadratic form $a_k x^2 + B_k xy + c_k y^2$ with

$$c_k = \frac{B_k^2 - q^2r^2\Delta_K}{4a_k} = q^2,$$

which is then equivalent to the form $q^2x^2-B_kxy+a_ky^2$ corresponding to the ideal $(q^2,-B_k)=(q^2,-B_k \mod_c 2q^2)$, where the subscript $c$ designates the centered euclidean division. Finally, this ideal is reduced because $|-B_k \mod_c 2q^2| < q^2 < \sqrt{\Delta_K q^2 r^2/4}$ . □

**Theorem 3.** *Let $\Delta_K$ be a fundamental negative discriminant, different from $-3$ and $-4$ and $q$ be an odd prime conductor. Let $r$ be an odd integer, prime to both $q$ and $\Delta_K$ such that $r > 2q/\sqrt{|\Delta_K|}$. Given a class of* $\ker\bar{\varphi}_q$ *and $\mathfrak{h}$ a representative in $I(\mathcal{O}_{\Delta_q}, qr)$ , then the class*

$$[\mathfrak{h} \cap \mathcal{O}_{\Delta_q r^2}]^{\phi_{\Delta_K}(r)}$$

*is trivial if the order of $[\mathfrak{h}]$ divides $\phi_{\Delta_K}(r)$ and has a reduced element of norm $q^2$ otherwise.*

*Proof.* Let $\mathfrak{h} \in I(\mathcal{O}_{\Delta_q}, q)$ be a representative of a class of $\ker\bar{\varphi}_q$. Let $\alpha \in \mathcal{O}_{\Delta_K}$ such that $\mathfrak{h}\mathcal{O}_{\Delta_K} = \alpha\mathcal{O}_{\Delta_K}$. Let us remark first that $\mathfrak{h} \cap \mathcal{O}_{\Delta_q r^2}$, which is an $\mathcal{O}_{\Delta_q r^2}$-ideal, is equal to $\alpha\mathcal{O}_{\Delta_K} \cap \mathcal{O}_{\Delta_q r^2}$. Therefore $[\mathfrak{h} \cap \mathcal{O}_{\Delta_q r^2}]$ is in $\ker\bar{\varphi}_{qr}$. By the isomorphisms of Lemma 1, $[\mathfrak{h}] \in \ker\bar{\varphi}_q$ corresponds to $\big([\alpha] \pmod q\big) \in \left(\mathcal{O}_{\Delta_K}/q\mathcal{O}_{\Delta_K}\right)^\times / \left(\mathbb{Z}/q\mathbb{Z}\right)^\times$ and $[\mathfrak{h} \cap \mathcal{O}_{\Delta_q r^2}]$ corresponds to $\big([\alpha] \pmod{qr}\big)$ in the quotient $\left(\mathcal{O}_{\Delta_K}/qr\mathcal{O}_{\Delta_K}\right)^\times / \left(\mathbb{Z}/qr\mathbb{Z}\right)^\times$.

Once again, we are going to use properties of quotients of $\mathcal{O}_{\Delta_K}$ to obtain some information on the kernel of $\bar{\varphi}_q$ and $\bar{\varphi}_{qr}$. Let

$$\begin{array}{rccc} s : & \left(\mathcal{O}_{\Delta_K}/q\mathcal{O}_{\Delta_K}\right)^\times / \left(\mathbb{Z}/q\mathbb{Z}\right)^\times & \longrightarrow & \left(\mathcal{O}_{\Delta_K}/qr\mathcal{O}_{\Delta_K}\right)^\times / \left(\mathbb{Z}/qr\mathbb{Z}\right)^\times \\ & [\alpha] & \longmapsto & [\alpha]^{\phi_{\Delta_K}(r)} . \end{array}$$

The map $s$ is a well-defined morphism. Indeed, if $\alpha$ and $\beta$ are two elements of $\mathcal{O}_{\Delta_K}$ such that $[\alpha]=[\beta]$ in $\left(\mathcal{O}_{\Delta_K}/q\mathcal{O}_{\Delta_K}\right)^\times / \left(\mathbb{Z}/q\mathbb{Z}\right)^\times$, then, in the Chinese remainder isomorphism (describing the quotient $\left(\mathcal{O}_{\Delta_K}/qr\mathcal{O}_{\Delta_K}\right)^\times / \left(\mathbb{Z}/qr\mathbb{Z}\right)^\times$), $[\alpha]^{\phi_{\Delta_K}(r)}$ maps to $([\alpha]^{\phi_{\Delta_K}(r)} \pmod q, [1] \pmod r)$. On the other hand, the element $[\beta]^{\phi_{\Delta_K}(r)}$ maps to $([\beta]^{\phi_{\Delta_K}(r)} \pmod q, [1] \pmod r)$ and therefore $s([\alpha]) = s([\beta])$. Note that the kernel of $s$ is the subgroup of $\phi_{\Delta_K}(r)$-th roots of unity of $\left(\mathcal{O}_{\Delta_K}/q\mathcal{O}_{\Delta_K}\right)^\times / \left(\mathbb{Z}/q\mathbb{Z}\right)^\times$.

Let us define the morphism $\hat{s}$ between $\ker\bar{\varphi}_q$ and $\ker\bar{\varphi}_{qr}$ such that the following diagram commutes:

$$\begin{array}{ccc} \ker\bar{\varphi}_q & \xrightarrow{\quad\hat{s}\quad} & \ker\bar{\varphi}_{qr} \\ \uparrow{\scriptstyle\psi_q} \wr & \circlearrowleft & \uparrow{\scriptstyle\psi_{qr}} \wr \\ \left(\mathcal{O}_{\Delta_K}/q\mathcal{O}_{\Delta_K}\right)^\times / \left(\mathbb{Z}/q\mathbb{Z}\right)^\times & \xrightarrow{\quad s\quad} & \left(\mathcal{O}_{\Delta_K}/qr\mathcal{O}_{\Delta_K}\right)^\times / \left(\mathbb{Z}/qr\mathbb{Z}\right)^\times \end{array}$$

Now, we prove that $\hat{s}([\mathfrak{h}]) = [\mathfrak{h} \cap \mathcal{O}_{\Delta_q r^2}]^{\phi_{\Delta_K}(r)}$. Indeed, $\hat{s}([\mathfrak{h}]) = \hat{s} \circ \psi_q([\alpha] \pmod q)$ and by commutativity of the diagram

$$\begin{aligned}
\hat{s} \circ \psi_q([\alpha] \pmod q) &= \psi_{qr} \circ s([\alpha] \pmod q) \\
&= \psi_{qr}\Big(([\alpha] \pmod q)^{\phi_{\Delta_K}(r)}\Big) \\
&= \psi_{qr}\Big(([\alpha] \pmod {qr})^{\phi_{\Delta_K}(r)}\Big) \\
&= \psi_{qr}\Big([\alpha] \pmod {qr}\Big)^{\phi_{\Delta_K}(r)} = [\mathfrak{h} \cap \mathcal{O}_{\Delta_q r^2}]^{\phi_{\Delta_K}(r)}.
\end{aligned}$$

By construction, $\ker \hat{s}$ is the subgroup of $\phi_{\Delta_K}(r)$-th roots of unity of $\ker \bar{\varphi}_q$ and therefore, if the order of $[\mathfrak{h}]$ divides $\phi_{\Delta_K}(r)$, then $\hat{s}([\mathfrak{h}]) = [\mathcal{O}_{\Delta_q r^2}]$. Otherwise, as the image of $s$ is a subset of the kernel of the surjection $\pi$ of Lemma 2, the reduced ideal of the class $\hat{s}([\mathfrak{h}])$ has norm $q^2$. □

**Corollary 1.** *Algorithm 3 solves the Kernel Problem and totally breaks the NICE family of cryptosystems in cubic time in the security parameter.*

*Proof.* The correctness of Algorithm 3 follows from the previous theorem: All the assumptions are verified. In particular, $r > 2q/\sqrt{|\Delta_K|}$ and $\mathfrak{h}'$ is a representative of $[\mathfrak{h}]$ in $I(\mathcal{O}_{\Delta_q}, qr)$: The ideal $\mathfrak{h}'$ is chosen prime to $r'$ and will be also prime to $q$, otherwise the factorisation of $\Delta_q$ is already recovered. Now, $[\mathfrak{f}]$ is trivial if the order of $[\mathfrak{h}]$ divides $\phi_{\Delta_K}(r) = r'^{\delta_{r'}-1}\left(r' - \left(\frac{\Delta_K}{r'}\right)\right)$. As we suppose that the order of $[\mathfrak{h}]$ is greater than 6 (see Remark. 2), at most one iteration of step 3 will be done, otherwise the order of $[\mathfrak{h}]$ divides both $\phi_{\Delta_K}(3^{\delta_3})$ and $\phi_{\Delta_K}(5^{\delta_5})$, which is impossible (since their gcd is 2, 4 or 6, according to the value of the Kronecker symbols). Eventually, $\mathfrak{f}$ has norm $q^2$ and therefore Algorithm 3 outputs a nontrivial factorisation of $\Delta_q$.

The cost of the initialisation phase is essentially cubic in the security parameter. The core of the algorithm consists in applying Algorithm 1 whose complexity is quadratic in $\lambda$, and an exponentiation whose complexity is cubic. □

Corollary 1 implies that all the schemes for which a public element of the kernel of $\bar{\varphi}_q$ is needed are broken in polynomial time. This includes the NICE encryption scheme and its variants, notably the enhanced IND-CCA2 version (cf. [PT99, HPT99,PT00,Huh00,BST02]), the derived signature scheme (cf. [HM00,Huh01]) and the undeniable signature scheme (cf. [BPT04]). Note that this result does not affect the security of the adaptation of seminal cryptosystems in imaginary quadratic fields, *i. e.*, the Diffie-Hellman key exchange of [BW88,McC89], the Rabin and RSA analogues of [HMT99] and the adaptation of Elgamal of [HJPT98].

**Example.** We apply our cryptanalysis on the example of the NICE encryption scheme mentioned in [JJ00], described as follows:

$$\begin{aligned}\Delta_q = &-100113361940284675007391903708261917456537242594667\\ &491514934053946421992795516818216760083640752198709726199732701843864411853249644535365728802022498185665592983708546453282107912775914256762913490132215200\\ &22224671621236001656120923\end{aligned}$$

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

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

The public key consists in $\Delta_q$ and $\mathfrak{h} = (a, b)$.

The ideal $\mathfrak{h} = (a, b)$ is equivalent to the ideal $\mathfrak{h}' = (a', b')$ with norm prime to 3 with $b' = -b$ and $a' = (b^2 - \Delta_q)/4a$:

$$\begin{aligned}a' = &\ 43891898980317792308326285455049173482378605867\\ &42403785190862097985269408138288879224220052968\\ &10150815323915182343893632698778887397967669\end{aligned}$$

$$\begin{aligned}b' = &-33612360405827547849585862980179491106487317456059301\\ &60593016466681956960675502977307441582303984700 7\end{aligned}$$

We used the following power of 3:

$$r = 3^{83} = 399083839418733992953424667557234903522 7$$

Then, in 20ms, we have computed the lift of $(a', b')$ of norm $q^2$:

$$\begin{aligned}\mathfrak{t} = (&53631231719770388398296099992823384509917463282369573510894245774887056120365979002534633233830227721465513935614971593907712680952249981870640736401120729,\\ &50726115195894796350644539158073328654518399170010324260439808053865626730478159167292645232706489579615441563764090965623987919889655079184915879970067243)\end{aligned}$$

The experiments have been done on a standard laptop running Linux with PARI/GP.

## 4 Conclusion

We totally break a large class of cryptosystems based on imaginary quadratic field arithmetic, whose main interest was the quadratic complexity of the secret operation. This polynomial time attack shows that SKEP and the kernel problem are not suited to build cryptosystems and lessen the number of public-key cryptosystems with quadratic decryption time. The adaptation of NICE recently proposed in [JSW08] in the very different setting of real quadratic fields, seems to resist to our attack.

**Acknowledgement.** We warmly thank Denis Simon with whom we had helpful discussions on quadratic forms, Brigitte Vallée for her huge contribution to the analysis of the complexity of our first attack, and last not but least Andreas Enge for his conscientious reviewing of a preliminary version of our paper and for his precious comments.

## References

[BPT04] I. Biehl, S. Paulus and T. Takagi. *Efficient Undeniable Signature Schemes based on Ideal Arithmetic in Quadratic Orders.* Des. Codes Cryptography 31(2), 99–123 (2004)

[BDH99] D. Boneh, G. Durfee and N. Howgrave-Graham. *Factoring $N = p^r q$ for large $r$.* Proc. of Crypto'99, Springer LNCS Vol. 1666, 326–337 (1999)

[BST02] J. Buchmann, K. Sakurai and T. Takagi. *An IND-CCA2 Public-Key Cryptosystem with Fast Decryption.* Proc. of ICISC'01, Springer LNCS Vol. 2288, 51–71 (2002)

[BW88] J. Buchmann and H. C. Williams. *A Key-Exchange System based on Imaginary Quadratic Fields.* J. Cryptology, 1, 107–118 (1988)

[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)

[CNP99] J.-S. Coron, D. Naccache and P. Paillier. *Accelerating Okamoto-Uchiyama public-key cryptosystem.* Electronics Letters, (4) 35, 291–292 (1999)

[Coh00] H. Cohen. *A Course in Computational Algebraic Number Theory.* Springer (2000).

[Cox99] D. A. Cox. *Primes of the form $x^2 + ny^2$.* John Wiley & Sons (1999)

[HM89] J. L. Hafner and K. S. McCurley. *A Rigorous Subexponential Algorithm for Computation of Class Group.* J. Amer. Math. Soc., Vol. 2(4), 837–850 (1989)

[HPT99] M. Hartmann, S. Paulus and T. Takagi. *NICE - New Ideal Coset Encryption.* Proc. of CHES'99, Springer LNCS Vol. 1717, 328–339 (1999)

[Huh00] D. Hühnlein. *Efficient Implementation of Cryptosystems based on Non-Maximal Imaginary Quadratic Orders.* Proc. of SAC'99, Springer LNCS Vol. 1756, 150–167 (2000)

[Huh01] D. Hühnlein. *Faster Generation of NICE-Schnorr-Type Signatures.* Proc. of RSA-CT'01, Springer LNCS Vol. 2020, 1–12 (2001)

[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)

[HM00] D. Hühnlein and J. Merkle. *An Efficient NICE-Schnorr-Type Signature Scheme.* Proc. of PKC'00, Springer LNCS Vol. 1751, 14–27 (2000)

[HMT99] D. Hühnlein, A. Meyer and T. Takagi. *Rabin and RSA Analogues Based on Non-maximal Imaginary Quadratic Orders.* Proc. of ICISC'98, 221-240 (1999)

[JSW08] Michael J. Jacobson, Jr, Renate Scheidler, Daniel Weimer. *An Adaptation of the NICE Cryptosystem to Real Quadratic Orders.* Proc. of Africacrypt'08, Springer LNCS Vol. 5023, 191-208 (2008)

[JJ00] É. Jaulmes and A. Joux. *A NICE Cryptanalysis.* Proc. of Eurocrypt'00, Springer LNCS Vol. 1807, 382–391 (2000)

[LL93] *The Development of the Number Field Sieve.* Springer LNM Vol. 1554, A. K. Lenstra and H. W. Lenstra, Jr. (Eds), VIII, 131p. (1993)

[Len87] Lenstra Jr., H. W. *Factoring integers with elliptic curves.* Annals of Mathematics (2) 126, 649–673 (1987)

[McC89] K. S. McCurley. *Cryptographic Key Distribution and Computation in Class Groups.* Proc. of NATO ASI on Number Theory and Applications, Kluwer Academic Press, 459–479 (1989)

[OP01] T. Okamoto and D. Pointcheval. *REACT: Rapid Enhanced-security Asymetric Cryptosystem Transform.* Proc. of RSA-CT'01, Springer LNCS Vol. 2020, 159–175 (2001)

[Pai99] P. Paillier. *Public-Key Cryptosystems Based on Composite Degree Residuosity Classes.* Proc. of Eurocrypt'99, Springer LNCS Vol. 1592, 223–238 (1999)

[Poi00] D. Pointcheval. *Chosen-Ciphertext security for Any One-Way Cryptosystem.* Proc. of PKC'00, Springer LNCS Vol. 1751, 129–146 (2000)

[Poi05] D. Pointcheval. *Provable Security for Public Key Schemes.* Advanced Courses CRM Barcelona, Advanced Course on Contemporary Cryptology, Birkhäuser Publishers, 133-189 (2005)

[PT99] S. Paulus and T. Takagi. *A generalization of the Diffie-Hellman problem and related cryptosystems allowing fast decryption.* Proc. of ICISC'98, 211-220 (1999)

[PT00] 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)

[Sch82] R. Schoof. *Quadratic fields and factorization.* Computational Methods in Number Theory, MC-Tracts 154/155, 235–286 (1982)

[Sch00] C.P. Schnorr. *Efficient identification and signatures for smart cards.* Proc.of Crypto'89, Springer LNCS Vol. 435, 239-252 (1990)

[VV07] B. Vallée and A. Vera. *Lattice Reduction in Two Dimensions: Analyses under Realistic Probabilistic Models.* Proc. of AofA'07, DMTCS **AH**, 181–216 (2007)