A NICE Cryptanalysis

Éliane Jaulmes[1] and Antoine Joux[2]

[1] SCSSI, 18 rue du Docteur Zamenhof
F-92131 Issy-les-Moulineaux cedex, France
eliane.jaulmes@wanadoo.fr
[2] SCSSI, 18 rue du Docteur Zamenhof
F-92131 Issy-les-Moulineaux cedex, France
Antoine.Joux@ens.fr

Abstract. We present a chosen-ciphertext attack against both NICE cryptosystems. These two cryptosystems are based on computations in the class group of non-maximal imaginary orders. More precisely, the systems make use of the canonical surjection between the class group of the quadratic order of discriminant $\sqrt{-pq^2}$ and the class group of the quadratic order of discriminant $\sqrt{-p}$. In this paper, we examine the properties of this canonical surjection and use them to build a chosen-ciphertext attack that recovers the secret key (p and q) from two ciphertexts/cleartexts pairs.

1 Overview

In [5], Hartmann, Paulus and Takagi have presented a new public-key cryptosystem based on ideal arithmetic in quadratic orders. This system was called NICE, which stands for New Ideal Coset Encryption.

In [7], Hünhlein, Jacobson, Paulus and Takagi have presented a cryptosystem analogous to ElGamal encryption [4] that uses the same properties of arithmetic in imaginary quadratic orders than NICE. They called it HJPT.

The security of the NICE and HJPT cryptosystems is closely related to factoring the discriminant of the quadratic order, which is a composite number of the special form pq^2. While there exists an algorithm that allows the factorization of numbers of the form pq^r, for large r (see [2]), no dedicated algorithm is currently known to factor numbers with a square factor. Furthermore, for appropriate sizes of the parameters, the currently known general factoring algorithms are not applicable to a direct attack. In [8], the authors also give several arguments to prove the security of their cryptosystem. Among these considerations, they argue that the chosen-ciphertext attack is not applicable to their cryptosystem.

Indeed, it seems that from a single chosen ciphertext, one cannot recover the secret key. However, we show that with two well chosen ciphertexts, it is possible to factor pq^2, thus breaking the system.

This paper is organized as follows: we first give a brief reminder of the properties of the class group of a quadratic order and recall the main ideas of the

B. Preneel (Ed.): EUROCRYPT 2000, LNCS 1807, pp. 382–391, 2000.

two cryptosystems. Then we present our chosen-ciphertext attack and finally we give an example of this attack.

2 Theoretical Background

The NICE and HJPT cryptosystems rely on the canonical surjection between the class group of a non-maximal order and the class group of the maximal order in an imaginary quadratic field. We will first recall the properties of the class groups and the surjection before presenting the algorithms.

2.1 Class Group of a Quadratic Order

An introduction to quadratic orders and their class groups can be found in [3]. In this section, we briefly recall the definition and main properties of the class group of a quadratic order.

Definitions and Properties.

Quadratic Field. Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field with $d \neq 1$ squarefree. Let Δ_1 be the discriminant of K. If $d \equiv 1 \bmod 4$, we can take $1, (1+\sqrt{d})/2$ as an integral basis for K and $\Delta_1 = d$, while if $d \equiv 2$ or $3 \bmod 4$, we can take $1, \sqrt{d}$ and we have $\Delta_1 = 4d$.

Fundamental Discriminant. An integer Δ_1 is called a fundamental discriminant if Δ_1 is the discriminant of a quadratic field K. In other words, $\Delta_1 \neq 1$ and either $\Delta_1 \equiv 1 \bmod 4$ and is squarefree, or $\Delta_1 \equiv 0 \bmod 4$, $\Delta_1/4$ is squarefree and $\Delta_1/4 \equiv 2$ or $3 \bmod 4$. In the NICE cryptosystem, we consider only $\Delta_1 < 0$ and such that $\Delta_1 \equiv 1 \bmod 4$.

Order of a Quadratic Field. An order R in K is a subring of K which as a $\mathbb{Z}$-module is finitely generated and of maximal rank $n = deg(K)$. Every element of an order is an algebraic integer. If K is a quadratic field of discriminant Δ_1, then every order R of K has discriminant $q^2\Delta_1$, where q is a positive integer called the conductor of the order. Conversely, if Δ_q is any non-square integer such that $\Delta_q \equiv 0$ or $1 \bmod 4$, then Δ_q is uniquely of the form $\Delta_q = q^2\Delta_1$ where Δ_1 is a fundamental discriminant, and there exists an unique order R of discriminant Δ_q.

Maximal Order. Let $\mathcal{O}_{\Delta_q}$ be the order of discriminant Δ_q. It can be written as $\mathcal{O}_{\Delta_q} = \mathbb{Z} + w\mathbb{Z}$ where $w = \frac{\Delta_q + i\sqrt{|\Delta_q|}}{2}$. $\mathcal{O}_{\Delta_q}$ is related to $\mathcal{O}_{\Delta_1}$ by the relation $\mathcal{O}_{\Delta_q} = \mathbb{Z} + q\mathcal{O}_{\Delta_1}$ and we have $\mathcal{O}_{\Delta_q} \subset \mathcal{O}_{\Delta_1}$. We call $\mathcal{O}_{\Delta_1}$ the maximal order. It is the ring of integers of the quadratic field $\mathbb{Q}(\sqrt{\Delta_1})$.

Ideals of a Quadratic Order. An ideal $\mathfrak{a}$ of $\mathcal{O}_{\Delta_q}$ can be written as

$$\mathfrak{a} = m\left(a\mathbb{Z} + \frac{b + i\sqrt{|\Delta_q|}}{2}\mathbb{Z}\right)$$

where $m \in \mathbb{Z}$, $m > 0$, $a \in \mathbb{Z}$, $a > 0$, and $b \in \mathbb{Z}$ such that $b^2 \equiv \Delta_q \bmod 4a$. The norm of the ideal is defined as $N(\mathfrak{a}) = ma$. When $m = 1$, we say that $\mathfrak{a}$ is primitive and we represent it by the pair (a, b).

Two ideals $\mathfrak{a}$, $\mathfrak{b} \in \mathcal{O}_{\Delta_q}$ are called equivalent if there exists $\alpha, \beta \in \mathcal{O}^*_{\Delta_q}$ such that $\alpha\mathfrak{a} = \beta\mathfrak{b}$. We denote this relation by $\mathfrak{a} \sim \mathfrak{b}$. For any element $\gamma \in \mathcal{O}_{\Delta_q}$ the ideal $\gamma\mathcal{O}_{\Delta_q}$ is called a principal ideal. If $\mathfrak{a}$ and $\mathfrak{b}$ are two principal ideals, they are equivalent.

For a primitive ideal, we say that $\mathfrak{a} = (a, b)$ is reduced if and if only $|b| \leq a \leq c = (b^2 - \Delta_q)/4a$ and moreover $b \geq 0$ when $a = c$ or $a = |b|$. There exists a unique reduced ideal in the equivalence class of an ideal $\mathfrak{a}$, denoted by $Red_{\Delta_q}(\mathfrak{a})$. An algorithm to compute $Red_{\Delta_q}(\mathfrak{a})$ from $\mathfrak{a}$ is described in [3, p238].

The reduction algorithm works as follows in the quadratic order of discriminant Δ: We start with an ideal (a, b) with $-a < b \leq a$ and proceed by successive steps. In each step, we replace (a, b) by (a', b') where $a' = \frac{b^2 - \Delta}{4a}$ and b' satisfies $-b = b' + 2a'k$ with $-a' < b' \leq a'$. When it reaches a reduced ideal, the algorithm stops.

For any reduced ideal $\mathfrak{a} = (a, b)$, $a < \sqrt{|\Delta_q|/3}$. Conversely, for a primitive ideal, if $a < \sqrt{|\Delta_q|/4}$, then $\mathfrak{a}$ is reduced.

Class Group. The ideals of $\mathcal{O}_{\Delta_q}$, respectively $\mathcal{O}_{\Delta_1}$, whose norm is prime to f form an Abelian group. They are called ideals prime to f. We denote this group by $I_{\Delta_q}(f)$, respectively $I_{\Delta_1}(f)$. If q is a prime and $\sqrt{|\Delta_1|/3} < q$, then all the reduced ideals in $\mathcal{O}_{\Delta_1}$ have a norm prime to q. From now on, we will suppose that this is the case.

In $\mathcal{O}_{\Delta_q}$, the principal ideals prime to q form a subgroup of $I_{\Delta_q}(q)$. We denote it by $P_{\Delta_q}(q)$. The quotient group $I_{\Delta_q}(q)/P_{\Delta_q}(q)$ is called the class group of $\mathcal{O}_{\Delta_q}$ and denoted by $Cl(\Delta_q)$.

We can consider the following map:

$$\begin{aligned} \varphi_q : Cl(\Delta_q) &\to Cl(\Delta_1) \\ \mathfrak{a} &\mapsto Red_{\Delta_1}(\mathfrak{a}\mathcal{O}_{\Delta_1}) \end{aligned}$$

φ_q is a surjective group morphism.

We can also defined a restricted inverse map, denoted φ_q^{-1}.

$$\varphi_q^{-1}(A, B) = (A, Bq \bmod 2A)$$

We have indeed $\varphi_q(\varphi_q^{-1}(\mathfrak{a})) = Red_{\Delta_1}(\mathfrak{a})$. Conversely, for an ideal $\mathfrak{a} = (a, b) \in \mathcal{O}_{\Delta_q}$ such that $a < \sqrt{|\Delta_1|/4}$, we have $\varphi_q^{-1}(\varphi_q(\mathfrak{a})) = \mathfrak{a}$. However, if $a \geq \sqrt{|\Delta_1|/4}$, we may have $\varphi_q^{-1}(\varphi_q(\mathfrak{a})) \neq \mathfrak{a}$. Our attack relies on this observation.

How to Compute φ_q. Let Φ_q be the map between the primitive ideals of $\mathcal{O}_{\Delta_q}$ and the primitive ideals of $\mathcal{O}_{\Delta_1}$ defined by $\Phi_q(\mathfrak{a}) = \mathfrak{a}\mathcal{O}_{\Delta_1}$. We clearly have $\varphi_q = Red_{\Delta_1}(\Phi_q)$. To compute $\Phi_q(\mathfrak{a})$ from $\mathfrak{a} = (a, b)$, proceed as follows: $\Phi_q(a, b) = (A, B)$ where $A = a$ and $b\mu + ab_{\mathcal{O}}\nu = 2ka + B$ with $-a < B \leq a$, $b_{\mathcal{O}} = \Delta_q \bmod 2$, $1 = \mu q + \nu a$ for $\mu,\nu \in \mathbb{Z}$. To compute $\varphi_q(\mathfrak{a})$, we must then apply to (A, B) the reduction algorithm described in section 2.1.

2.2 Description of the Cryptosystems

Description of NICE.

The Key Generation. The key generation consists in generating two random primes p,$q > 4$ with $p \equiv 3 \bmod 4$ and $\sqrt{p/3} < q$. We then let

$$\Delta_1 = -p$$
$$\Delta_q = -pq^2,$$

and choose an ideal $\mathfrak{p}$ in $Cl(\Delta_q)$, where $\varphi_q(\mathfrak{p}) = 1_{Cl(\Delta_1)}$. To generate such a $\mathfrak{p}$, proceed as follows: choose a number $\alpha \in \mathcal{O}_{\Delta_1}$ with norm less than $\sqrt{|\Delta_q|/4}$, compute the standard representation of the ideal $\alpha\mathcal{O}_{\Delta_1}$ and compute $\varphi_q^{-1}(\alpha\mathcal{O}_{\Delta_1})$.

Let k and l be the bit lengths of $\lfloor\sqrt{|\Delta_1|/4}\rfloor$ and $q - \left(\frac{\Delta_1}{q}\right)$ respectively, where $\left(\frac{\Delta_1}{q}\right)$ is the Kronecker symbol. The public key is $(\mathfrak{p}, \Delta_q, k, l)$ and the secret key is (Δ_1, q). None of the maps Φ_q, φ_q, φ_q^{-1} are public.

Encryption and Decryption Proceedings. A message is represented by an ideal $\mathfrak{m}$, where $\mathfrak{m}$ is reduced in $Cl(\Delta_q)$ and $\log_2 N(\mathfrak{m}) < k$, which means that $\Phi_q(\mathfrak{m})$ is also reduced in $Cl(\Delta_1)$. The embedding of a message into an ideal that represents it may be done as follows: let x be the message and t a random number of length $k - 2 - \lfloor\log_2 x\rfloor + 1$. We determine the smallest prime a larger than the concatenation of x and t as bit strings with $\left(\frac{\Delta_q}{a}\right) = 1$. Then we need to compute b such that $\Delta_q \equiv b^2 \bmod 4a$, $-a < b \leq a$. Our message is finally encoded as $\mathfrak{m} = (a, b)$.

We encrypt the message by computing $\mathfrak{c} = Red_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$, where r is a random $l - 1$ bit integer.

To decrypt, we compute $\mathfrak{k} = \varphi_q(\mathfrak{c})$.
Since

$$\varphi_q(\mathfrak{m}\mathfrak{p}^r) = \varphi_q(\mathfrak{m})\varphi_q(\mathfrak{p}^r) = \varphi_q(\mathfrak{m}),$$

the plaintext is then $\mathfrak{m} = \varphi_q^{-1}(\mathfrak{k})$.

Note that this is a probabilistic encryption and the multiplication by $\mathfrak{p}^r$ allows to choose a random pre-image of $\varphi_q(\mathfrak{m})$ by φ_q.

Description of HJPT. In this cryptosystem, the encryption is done completely analogous to ElGamal encryption [4] in the non-maximal order $\mathcal{O}_{\Delta_q}$. All ideals are chosen prime to q. The public parameters are the discriminant Δ_q, an ideal $\mathfrak{g} \in \mathcal{O}_{\Delta_q}$, called the base ideal, and an ideal $\mathfrak{a} \in \mathcal{O}_{\Delta_q}$ such that $\mathfrak{a} = Red_{\Delta_q}(\mathfrak{g}^a)$, where a is a random integer $a \in [2, \lfloor\sqrt{\Delta_1}\rfloor]$. The secret key is a and q.

We embed the message in an ideal $\mathfrak{m} \in \mathcal{O}_{\Delta_q}$ as in NICE, select an integer k and compute $(\mathfrak{n}_1, \mathfrak{n}_2)$ where $\mathfrak{n}_1, \mathfrak{n}_2$ are reduced ideals in $\mathcal{O}_{\Delta_q}$ and

$$\mathfrak{n}_1 = Red_{\Delta_q}(\mathfrak{g}^k)$$

$$\mathfrak{n}_2 = Red_{\Delta_q}(\mathfrak{m}\mathfrak{a}^k)$$

We require $N(\mathfrak{m}) < \sqrt{|\Delta_1|/4}$ in order to uniquely decrypt the message $\mathfrak{m}$.

The decryption works in the maximal order $\mathcal{O}_{\Delta_1}$. We compute:

$$\mathfrak{N}_1 = \varphi_q(\mathfrak{n}_1)$$

$$\mathfrak{N}_2 = \varphi_q(\mathfrak{n}_2)$$

$$\mathfrak{M} = \mathfrak{N}_2(\mathfrak{N}_1^a)^{-1}$$

$$\mathfrak{m} = \varphi_q^{-1}(\mathfrak{M})$$

$\mathfrak{m}$ is the decoded message.

Security Considerations. The security of the cryptosystems depends on the difficulty of factoring the discriminant Δ_q. If it can be factored, the cryptosystems are clearly broken.

To prevent a direct factorization of Δ_q using general methods such as the number field sieve or the elliptic curve method, the authors suggest that we choose p and q larger than 256 bits. Although Δ_q is of the special form pq^2, there exists no dedicated algorithm better than the general ones. They conclude that their system is secure against attacks by factorization.

The authors also prove that nobody can compute $\Phi_q(a, b)$ without the knowledge of the conductor q. That means that it is not possible to recover the message from the coded ideal without the knowledge of the factors of Δ_q.

Concerning NICE, Paulus and Takagi then argue that the knowledge of $\mathfrak{p}$ does not substantially help to factor Δ_q. A possible attack would be to find an ideal $\mathfrak{f}$ power of $\mathfrak{p}$ in $\mathcal{O}_{\Delta_q}$ such that $\mathfrak{f}^2 \sim 1$ and $\mathfrak{f} \nsim 1$, however the only apparent way to do that is to compute the order of $\mathfrak{p}$ in the group $Cl(\Delta_q)$ which is much slower to do than factoring Δ_q with the available algorithms.

In [8], Paulus and Takagi also claim that the chosen-ciphertext attack is not applicable to their cryptosystem and give a few observations .

3 The Chosen-Ciphertext Attack

In this section, we study more precisely the question of the chosen-ciphertext attack. As claimed in section 2.2, the knowledge of one coded message and the corresponding decrypted message is indeed not sufficient for factoring Δ_q. However, we show that with two chosen ciphertexts, factoring Δ_q becomes easy.

Both cryptosystems use the following property of the canonical surjection to recover the message after encryption:

$$\varphi^{-1}(\varphi(\mathfrak{m})) = \mathfrak{m} \text{ if } N(\mathfrak{m}) < \sqrt{|\Delta_1|/4}.$$

Conversely, the attack uses the fact that

$$\varphi^{-1}(\varphi(\mathfrak{m})) \neq \mathfrak{m} \text{ if } N(\mathfrak{m}) > \sqrt{|\Delta_1|/3}.$$

3.1 Relation Involving a Single Chosen Ciphertext

The main idea behind our attack is to use a message $\mathfrak{m}$ slightly longer than proper messages and hope that in $\mathcal{O}_{\Delta_1}$ the corresponding ideal will be a single reduction step away from a reduced ideal. Note that after multiplication by a power of $\mathfrak{p}$ (in NICE) or $\mathfrak{a}$ (in HJPT), there is no way for the deciphering process to distinguish a correct ciphertext from an incorrect one, and thus to detect this attack. Of course, if one add some verification bits to the message, then it becomes feasible to make this distinction. This will be further discussed in section 3.3. In order to attack the system we need to make explicit the relation between the original message and the decoded message.

Let $\mathfrak{m} = (m, n) \in Cl(\Delta_q)$ be a message such that

$$\varphi_q^{-1}(\varphi_q(\mathfrak{m})) \neq \mathfrak{m}.$$

It means that $\Phi_q(\mathfrak{m})$ is not reduced in $\mathcal{O}_{\Delta_1}$. If we further suppose that a single reduction step is needed to reduce $\Phi_q(\mathfrak{m})$, we can make precise the relation between $\mathfrak{m}$ and $\varphi^{-1}(\varphi(\mathfrak{m}))$.

We apply the decryption algorithm and one reduction step as described in section 2.1 to $\mathfrak{m}$ and instead of finding $\mathfrak{m}$, we obtain $\mathfrak{m}' = (m', n')$ where (m', n') satisfies:

$$\begin{cases} m' = \frac{N^2 - \Delta_1}{4m} \\ n' \equiv -Nq \pmod{2m'} \end{cases}$$

and N is an integer that satisfies $-m < N < m$.

3.2 How to Find a Suitable Ciphertext

In order to be sure that a given message (m, n) will not be reduced in $Cl(\Delta_1)$ we need to take $m > \sqrt{|\Delta_1|/3}$. Moreover, from [3, p239], we know that if (m, n) is an ideal of $\mathcal{O}_{\Delta_1}$ such that $-m < n \leq m$ and $m < \sqrt{|\Delta_1|}$. Then either (m, n)

is already reduced, or the ideal (o, r) where $o = \frac{n^2-\Delta_1}{2m}$ and $-n = 2ko + r$ with $-o < r \leq o$, obtained by one reduction step, will be reduced.

In order to be sure that our ciphertext will have the described properties, we need to choose m as follows:

$$\sqrt{|\Delta_1|/3} < m < \sqrt{|\Delta_1|}.$$

Since we can estimate Δ_1 to be approximately $\sqrt[3]{|\Delta_q|}$, m should be of the size of $\sqrt[6]{|\Delta_q|}$. Moreover, the maximum size of possible messages, that is the bit length of $\lfloor\sqrt{|\Delta_1|/4}\rfloor$, is public, thus giving us the bit length of $\sqrt{|\Delta_1|/3}$. With this information, we need only two ciphertexts in the correct range to break the system. However, if the given maximum size has been underestimated, it may be that our first try for m we will still be in the allowed range of correct decryption. We may thus have to decrypt a few more messages, multiplying steps of $\sqrt{3}$ before finding a suitable m.

3.3 Using Two Chosen Ciphertexts

With only one pair $(\mathfrak{m}, \mathfrak{m}')$ we cannot find Δ_1, but with two such pairs $(\mathfrak{m}_1, \mathfrak{m}'_1)$, $(\mathfrak{m}_2, \mathfrak{m}'_2)$, we have:

$$\begin{cases} m'_1 = \frac{N_1^2-\Delta_1}{4m_1} \\ m'_2 = \frac{N_2^2-\Delta_1}{4m_2} \end{cases}$$

and then:

$$p = -\Delta_1 = 4m_1m'_1 - N_1^2 = 4m_2m'_2 - N_2^2.$$

We need to find N_1,N_2. That means we have to find an integer solution of the equation:

$$4m_1m'_1 - 4m_2m'_2 = N_1^2 - N_2^2.$$

Let $X = N_1 + N_2$, $Y = N_1 - N_2$ and $k = 4m_1m'_1 - 4m_2m'_2$, the equation now is:

$$k = XY,$$

where k is known and X, Y unknown. Once X is found, we can easily compute N_1, N_2 and p. Since X is a factor of k, it suffices to factor k and try every divisor as a possible value for X. Since the number of factors of k is quite small, the possible X can be tested in a reasonable amount of time. When $4m_1m'_1 - N_1^2 = 4m_2m'_2 - N_2^2$, there is a high probability that we have found the correct X. We just need to check that this value of Δ_1 divides Δ_q.

The size of k is approximately the size of m^2. As we choose m approximately of size $\sqrt[6]{|\Delta_q|}$, the size of k is $\sqrt[3]{|\Delta_q|}$. With the parameters given in [8], p, q and k all have 256 bits, thus k is easy to factor and the attack succeeds.

If we want to prevent the attack from succeeding, we need a size for k that prevent its factorization. Since k is an ordinary number, it may well have many small factors. Moreover, using more ciphertexts, we may choose between many values of k one that factors easily. This means that, for the algorithms to be

secure, k should have at the very least 768 bits. We would then have keys of 2304 bits.

To repair the cryptosystem, one could add redundancy to the plaintext, before encryption. If after decryption, the obtained message does not have this redundancy, the output is discarded, thus preventing someone from feeding wrong messages to the decryption algorithm. However, this should preferably be done in a provably secure way. Ideas from the OAEP work of Bellare and Rogaway [1] may be of use. However, as usual with this approach, it will decrease the number of information bits in the message.

4 Example

The example described in this section is based on the NICE cryptosystem. In [8], it is suggested that security should be assured for the factorization attack if p and q are larger than 256 bits and if Δ_q is larger than 768 bits. In our example, we took Δ_q of 770 bits, a p of 256 bits and a q of 257 bits.

Public key:

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

$$\begin{aligned}\mathfrak{p} &= (a, b)\\ a &= 57022687708942583181685884381175588713007831807699951950927158957551737003991414868957313847478\\ b &= -33612360405827547849585862980179491106487317456059301646668195696067550297730744158230398470078\end{aligned}$$

Messages used for the attack:

$$\begin{aligned}\mathfrak{m}_1 &= (m_1, n_1)\\ m_1 &= 58095147841742924317477872776302056865321326372746508083726049677108164065143558095147841742924317477872776302056898155106350558864599529939169018498480211978671653231911323093405599718880172057\end{aligned}$$

$$\begin{aligned}\mathfrak{m}_2 &= (m_2, n_2)\\ m_2 &= 58095147841742924317477872776302056898155106350558864599529939169018498480211978671653231911323093405599718880172057\\ n_2 &= 55106350558864599529939169018498480211978671653231911323093405599718880172057\end{aligned}$$

Decoded messages:

$$\begin{aligned}\mathfrak{m}'_1 &= (m'_1, n'_1)\\ m'_1 &= 83456697103393374949726594537861474869\\ n'_1 &= 78671653231911323093405599718880172057\end{aligned}$$

$$\begin{aligned}\mathfrak{m}'_2 &= (m'_2, n'_2)\\ m'_2 &= 831363826969102043969673088753836977 67\\ n'_2 &= -799132302773000590439366599288209128 89\end{aligned}$$

That gives us a value for k:

$$\begin{aligned}k = {} & 744348512019197260111329217472677897277 06\\ & 600792815510352758060887027806412 0\end{aligned}$$

k is factored into:

$$\begin{aligned}k = {} & 2^3 * 3 * 5 * 11 * 211 * 557 * 4111 * 155153 * 24329881\\ & *28114214269943 * 413746179653057\\ & *26580133430529627286021\end{aligned}$$

For the following values of X and Y:

$$\begin{aligned}X &= 2^2 * 5 * 11 * 211 * 557 * 4111 * 155153 * 24329881\\ &\quad *413746179653057\\ &= 16601295001642548056622403660641267734 0\\ Y &= 2 * 3 * 28114214269943 * 26580133430529627286021\\ &= 44836773995375102009813566857862008 18\end{aligned}$$

We found:

$$\begin{aligned}p = {} & 18666989127415343787417570818050325965428159 31\\ & 03800953935381353078144162357587\end{aligned}$$

5 Conclusion

Since the discrete logarithm problem in the class group of imaginary quadratic order is a difficult problem (see [6]), it was tempting to build public key cryptosystems on it. However, for performance sake, it was necessary to add more structure, and make use of the canonical surjection from $\mathcal{O}_{\Delta_q}$ to $\mathcal{O}_{\Delta_1}$. Unfortunately, this additional structure opens a way to the chosen-ciphertext attack that was described here.

Nonetheless, the discrete logarithm in class groups is an interesting problem that might yet find other applications to public key cryptography.

References

1. Mihir Bellare and Phillip Rogaway. Optimal asymmetric encryption – how to encrypt with RSA. In A. De Santis, editor, *Advances in Cryptology — EUROCRYPT'94*, volume 950 of *Lecture Notes in Computer Science*. Springer-Verlag, 1994.
2. Dan Boneh, Glenn Durfee, and Nick Howgrave-Graham. Factoring $n = pq^r$ for large r. In M. Wiener, editor, *Advances in Cryptology — CRYPTO'99*, volume 1666 of *Lecture Notes in Computer Science*, pages 326–337. Springer, 1999.
3. Henri Cohen. *A Course in Computational Algebraic Number Theory*. Graduate Texts in Mathematics. Springer, 1995.
4. T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31:469–472, 1985.
5. M. Hartmann, S. Paulus, and T. Takagi. Nice - new ideal coset encryption. In Çetin K. Koç and Christof Paar, editors, *Cryptographic Hardware and Embedded Systems — CHES'99*, pages 341–352. Springer Verlag, 1999. Pre-proceedings, final proceedings to appear in LNCS.
6. Hühnlein and Takagi. Reducing logarithms in totally non-maximal orders to logarithms in finite fields. In *ASIACRYPT'99*, 1999.
7. D. Hühnlein, M. J. Jacobson, S. Paulus Jr., and T. Takagi. A cryptosystem based on non-maximal imaginary quadratic orders with fast decryption. In *Avances in Cryptology — EUROCRYPT'98*, volume 1403 of *Lecture Notes in Computer Science*, pages 294–307, 1998.
8. Sachar Paulus and Tsuyoshi Takagi. A new public-key cryptosystem over quadratic orders with quadratic decryption time. to appear in Journal of Cryptology.