A cryptosystem based on non-maximal imaginary quadratic orders with fast decryption

Detlef Hühnlein[1], Michael J. Jacobson, Jr.[2], Sachar Paulus[2], and Tsuyoshi Takagi[3]

[1] secunet Security Networks GmbH,
Mergenthalerallee 77-81, D-65760 Eschborn, Germany,
E-mail: huehnlein@secunet.de
[2] Technische Universität Darmstadt,
FB Informatik, Institut für theoretische Informatik,
Alexanderstr. 10, 64283 Darmstadt, Germany
E-mail: {jacobs, sachar}@cdc.informatik.tu-darmstadt.de
[3] NTT Software Laboratories
3-9-11, Midori-cho Musashino-shi, Tokyo 180-8585, Japan
E-mail: ttakagi@slab.ntt.co.jp

Abstract. We introduce a new cryptosystem with trapdoor decryption based on the difficulty of computing discrete logarithms in the class group of the *non-maximal* imaginary quadratic order $\mathcal{O}_{\Delta_q}$, where $\Delta_q = \Delta q^2$, Δ square-free and q prime. The trapdoor information is the conductor q. Knowledge of this trapdoor information enables one to switch to and from the class group of the maximal order $\mathcal{O}_\Delta$, where the representatives of the ideal classes have smaller coefficients. Thus, the decryption procedure may be performed in the class group of $\mathcal{O}_\Delta$ rather than in the class group of the public $\mathcal{O}_{\Delta_q}$, which is much more efficient. We show that inverting our proposed cryptosystem is computationally equivalent to factoring the non-fundamental discriminant Δ_q, which is intractable for a suitable choice of Δ and q. We also describe how signature schemes in $\mathcal{O}_{\Delta_q}$ may be set up using this trapdoor information. Furthermore, we illustrate how one may embed key escrow capability into classical imaginary quadratic field cryptosystems.

Keywords: Public key cryptosystem, imaginary quadratic order, trapdoor decryption, factorization, key escrow

1 Introduction

Since Diffie and Hellman's introduction of public key cryptography in [9] a variety of encryption and signature schemes based on the discrete logarithm problem (DLP) have been proposed [11, 23, 22]. Due to the nature of cryptosystems based on the DLP, it is possible to replace the group $\mathbb{Z}/p\mathbb{Z}^*$ in the classical protocols by other finite Abelian groups in which the DLP is more intractable or the implementation yields better performance. Popular examples are the group of points on elliptic curves [20, 15], the divisor class group of hyperelliptic curves

[16], the group $\mathbb{Z}/n\mathbb{Z}^*$, where n is the product of two large primes [19], and the class group of imaginary quadratic fields [5, 18].

In this work we will focus on discrete log cryptosystems based on the class group of *non-maximal* imaginary quadratic orders. This is a slight, but in practice very important generalization of [5, 18], where only the class group of the imaginary quadratic field, i.e., the class group of the *maximal order* was considered. It is known that the computation of discrete logarithms in the class group of an imaginary quadratic order can be used to factor the corresponding discriminant [5, 25]. Thus, the inversion of these cryptosystems is *at least* as difficult as factoring. On the other hand, there is no good algorithm known to compute discrete logs in the class group of the maximal order if only the factorization of the discriminant is known. Therefore, these cryptosystems are very interesting from a *theoretical* point of view. While the best algorithms for computing discrete logarithms in class groups [12, 3] have sub-exponential complexity, they are still too inefficient for large discriminants.

However, the cryptosystems based on discrete logarithms in class groups have not yet gained very much attention in *practice*, because the known implementations are still too inefficient. A step towards *practical* cryptosystems based on imaginary quadratic class groups is presented in this article. We introduce a trapdoor variation of this type of cryptosystem which significantly improves the decryption procedure. The trapdoor information is the factorization of the non-fundamental discriminant $\Delta_q = \Delta q^2$, where Δ is square-free and q is prime. Knowledge of the conductor q enables one to switch to the class group of the maximal order and back. Thus, the key-owner may take advantage of the shortcut via the maximal order when decrypting. This is somewhat similar to the application of the Chinese remainder theorem when generating RSA signatures. However, the relative speedup is much higher in our proposed system.

If an attacker knows the factorization of the discriminant $\Delta_q = \Delta q^2$, our system is no longer secure, since he is able to switch to the class group of the maximal order $\mathcal{O}_\Delta$ where he may easily attack the system using the sub-exponential algorithms from [12, 3]. Hence, breaking our scheme is *"only" equivalent* to factoring the discriminant, unless Δ is chosen sufficiently large.

Using the knowledge of the factorization of Δ_q, one may compute the order of the group of equivalence classes of $\mathcal{O}_{\Delta_q}$ via the maximal order. This enables signature schemes in the class group of $\mathcal{O}_{\Delta_q}$ to be set up. Knowledge of the conductor also enables one to set up a key escrow system by providing a non-maximal order to users of a classical imaginary quadratic field cryptosystem.

The paper is organized as follows: We first briefly discuss the relation between the maximal and non-maximal orders in imaginary quadratic number fields. We give algorithms to switch to and from the class group of the non-maximal order to the class group of the maximal order and explain the parameter setup for the new scheme. The new scheme is discussed in terms of security; this will include a proof that breaking our scheme is computationally equivalent to factoring the non-fundamental discriminant $\Delta_q = \Delta q^2$. We also present run time statistics for various parameter sizes which illustrate the efficiency of our new scheme. Finally,

we discuss how signature schemes and a key escrow system may be set up using class groups of non-maximal imaginary quadratic orders.

2 Orders in imaginary quadratic number fields

Basic notions of imaginary quadratic fields and orders can be found in [2], [13] or [7]. For a more complete treatment of the relationship between maximal and non-maximal orders we refer to [8].

Let Δ be any non-square negative integer congruent to 0 or 1 modulo 4. The quadratic order of discriminant Δ is defined as

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

The maximal order of the quadratic field $\mathbb{Q}(\sqrt{\Delta})$ will be denoted by $\mathcal{O}_{\Delta_1}$, and the non-maximal order with conductor f will be denoted by $\mathcal{O}_{\Delta_f}$, where $\Delta_f = f^2\Delta_1$. If the conductor is prime, we will denote it by q rather than f, and the corresponding non-maximal order will be denoted by $\mathcal{O}_{\Delta_q}$. All primitive ideals of an order $\mathcal{O}_\Delta$ will be presented in *standard representation*:

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

where $a \in \mathbb{Z}_{>0}$, $b^2 \equiv \Delta \pmod{4a}$, and $-a < b \leq a$. Recall that a primitive ideal is reduced if $a \leq c$ and $b \geq 0$, if $a = c$ or $|b| = a$, where $c = (b^2 - \Delta)/4a$. It can be shown that a reduced ideal $\mathfrak{a}$ satisfies $\mathcal{N}(\mathfrak{a}) = a \leq \sqrt{|\Delta|/3}$. On the other hand, if $\mathcal{N}(\mathfrak{a}) =\leq \sqrt{|\Delta|/4}$, then $\mathfrak{a}$ is reduced. The set of all invertible ideals of $\mathcal{O}_\Delta$ will be denoted by $\mathcal{I}_\Delta$, and the set of all invertible, principal ideals by $\mathcal{P}_\Delta$. Ideal equivalence is denoted by $\mathfrak{a} \sim \mathfrak{b}$, and the class group and class number of $\mathcal{O}_\Delta$ are denoted by $Cl(\Delta)$ and $h(\Delta)$, respectively.

Our cryptosystem makes use of the relationship between non-maximal orders $\mathcal{O}_{\Delta_f}$ and the maximal order $\mathcal{O}_{\Delta_1}$ in $\mathbb{Q}(\sqrt{\Delta})$.

Proposition 1. *Let $\mathcal{O}$ be an order in the quadratic field $\mathbb{Q}(\sqrt{\Delta})$. Then $\mathcal{O}$ has finite index in $\mathcal{O}_{\Delta_1}$. If we set $f = [\mathcal{O}_{\Delta_1} : \mathcal{O}]$, then $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_{\Delta_1}$ and the discriminant of $\mathcal{O}$ is equal to $f^2\Delta_1$.*

Proof. See [8, Lemma 7.2, page 133]. □

Note that this proposition also justifies the notation $\mathcal{O}_{\Delta_f}$. A nice property of (nonzero, fractional) ideals in the maximal order $\mathcal{O}_{\Delta_1}$ is that all ideals are invertible. This is *not* true for non-maximal orders $\mathcal{O}_{\Delta_f}$. However, we will see that this holds for a slightly smaller subset, namely the ideals which are prime to the conductor f.

Definition 2. Let $\mathcal{O}_\Delta$ be an order in an imaginary quadratic field and $m \in \mathbb{N}$. We say that a nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_\Delta$ is prime to m if $\mathfrak{a} + m\mathcal{O}_\Delta = \mathcal{O}_\Delta$.

In our case, where we are interested in $\mathcal{O}_{\Delta_f}$-ideals, we have the following:

Proposition 3. *Let $\mathcal{O}_{\Delta_f}$ be an order of conductor f and $\mathfrak{a} \subseteq \mathcal{O}_{\Delta_f}$ be a nonzero $\mathcal{O}_{\Delta_f}$-ideal. Then*

1. *$\mathfrak{a}$ is prime to the conductor if and only if its norm $\mathcal{N}(\mathfrak{a})$ is relatively prime to f, i.e., $\gcd(\mathcal{N}(\mathfrak{a}), f) = 1$.*
2. *If $\mathfrak{a}$ is prime to the conductor f, then $\mathfrak{a}$ is invertible.*

Proof. See [8, Proposition 7.4, page 135 and Lemma 7.18, page 143]. □

Furthermore, we know that the norm of ideals prime to the conductor is multiplicative, as it is for ideals in the maximal order.

Proposition 4. *Let $\mathcal{O}_{\Delta_f}$ be an order of conductor f and $\mathfrak{a}, \mathfrak{b}$ be nonzero $\mathcal{O}_{\Delta_f}$-ideals. Then $\mathcal{N}(\mathfrak{ab}) = \mathcal{N}(\mathfrak{a})\mathcal{N}(\mathfrak{b})$.*

Proof. See [8, Lemma 7.14, page 140]. □

The set of invertible ideals of $\mathcal{O}_{\Delta_f}$, i.e., the ideals which are prime to f, will be denoted by $\mathcal{I}_{\Delta_f}(f)$. Then the above propositions show that they form a subgroup of $\mathcal{I}_{\Delta_f}$. Inside this subgroup we have a smaller subgroup, the principal ideals of $\mathcal{O}_{\Delta_f}$ which are prime to f. This subgroup is denoted by $\mathcal{P}_{\Delta_f}(f)$.

Proposition 5. *There is an isomorphism*

$$\mathcal{I}_{\Delta_f}(f) \Big/ \mathcal{P}_{\Delta_f}(f) \simeq \mathcal{I}_{\Delta_f} \Big/ \mathcal{P}_{\Delta_f} = Cl(\Delta_f) \ .$$

Proof. See [8, Proposition 7.19, page 143]. □

This shows that we may "neglect" the $\mathcal{O}_{\Delta_f}$-ideals which are not prime to the conductor if we are only interested in the class group $Cl(\Delta_f)$. To express how this isomorphism can be used for our purposes, we have the following:

Proposition 6. *Let $\mathcal{O}_{\Delta_f}$ be an order of conductor f in an imaginary quadratic field $\mathbb{Q}(\sqrt{\Delta})$ with maximal order $\mathcal{O}_{\Delta_1}$.*

1. *If $\mathfrak{A}$ is an $\mathcal{O}_{\Delta_1}$-ideal prime to f, then $\mathfrak{a} = \mathfrak{A} \cap \mathcal{O}_{\Delta_f}$ is an $\mathcal{O}_{\Delta_f}$-ideal prime to f and $\mathcal{N}(\mathfrak{A}) = \mathcal{N}(\mathfrak{a})$.*
2. *If $\mathfrak{a}$ is an $\mathcal{O}_{\Delta_f}$-ideal prime to f, then $\mathfrak{A} = \mathfrak{a}\mathcal{O}_{\Delta_1}$ is an $\mathcal{O}_{\Delta_1}$-ideal prime to f and $\mathcal{N}(\mathfrak{a}) = \mathcal{N}(\mathfrak{A})$.*
3. *The map $\varphi : \mathfrak{A} \mapsto \mathfrak{A} \cap \mathcal{O}_{\Delta_f}$ induces an isomorphism $\mathcal{I}_{\Delta_1}(f) \tilde{\to} \mathcal{I}_{\Delta_f}(f)$. The inverse of this map is $\varphi^{-1} : \mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_{\Delta_1}$.*

Proof. See [8, Proposition 7.20, page 144]. □

The next proposition shows that if we are only concerned with *equivalence classes of ideals*, then the primality condition in Proposition 6 does not impose an insurmountable obstacle.

Proposition 7. *Let $\mathcal{O}_\Delta$ be an order in an imaginary quadratic field. Given a nonzero integer f, then every ideal class in $Cl(\Delta)$ contains an $\mathcal{O}_\Delta$-ideal prime to f.*

Proof. See [8, Corollary 7.17, page 142]. □

We will restrict ourselves to the case where the conductor is prime in our cryptosystem. To implement our scheme, we will need constructive versions of Proposition 6 and 7. Therefore, we will give simple algorithms for computing an $\mathcal{O}_\Delta$-ideal prime to the conductor q and for switching from $\mathcal{I}_{\Delta_1}$ to $\mathcal{I}_{\Delta_q}$ and back.

Algorithm 1 (FindIdealPrimeTo).
Input: A primitive $\mathcal{O}_\Delta$-ideal $\mathfrak{a} = (a, b)$ and a prime q
Output: A primitive $\mathcal{O}_\Delta$-ideal $\mathfrak{A} \sim \mathfrak{a} = (A, B)$, such that $\gcd(\mathcal{N}(\mathfrak{A}), q) = \gcd(A, q) = 1$

1. IF $\gcd(a, q) > 1$ THEN
   (a) $c \leftarrow (b^2 - \Delta)/4a$
   (b) IF $\gcd(c, q) > 1$ THEN /* *Compute* $\mathfrak{A}_2$ */
      i. $A \leftarrow a + b + c$
      ii. $B \leftarrow -b - 2a$
   (c) ELSE /* *Compute* $\mathfrak{A}_1$ */
      i. $A \leftarrow c$
      ii. $B \leftarrow -b$
   (d) RETURN(A, B)
2. ELSE RETURN (a, b)

Proof (Correctness). Let $c = (b^2 - \Delta)/4a$. Then for any ideal $\mathfrak{a} = (a, b)$ we have $\gcd(a, b, c) = 1$ by definition.

First we will show that at least one of the numbers $a, c, a + b + c$ is relatively prime to q. Suppose that $\gcd(a, q) > 1$, and $\gcd(c, q) > 1$, i.e., $q \mid a$ and $q \mid c$, Further, suppose that $\gcd(a + b + c, q) > 1$, i.e., $q \mid (a + b + c)$. This implies that $q \mid b$, which is a contradiction to $\gcd(a, b, c) = 1$.

Now we will show that the new coefficients $A, B, C = (B^2 - \Delta)/4A$ satisfy $\gcd(A, B, C) = 1$, and therefore (A, B) is the standard representation of a primitive ideal. $\mathfrak{A}_1 = (c, -b)$ is obviously an ideal in standard representation, because $\gcd(c, -b, a) = 1$. Next we consider $\mathfrak{A}_2$. Note that $C = ((-b - 2a)^2 - \Delta)/(4(a + b + c)) = a$. A similar argument as above shows that $\gcd(a+b+c, -b-2a, a) = 1$.

It remains to show that the ideals $\mathfrak{A}_1$ or $\mathfrak{A}_2$ are indeed equivalent to $\mathfrak{a}$. Let $\theta = \frac{b+\sqrt{\Delta}}{2a}$, $\theta_1 = -\frac{1}{\theta} = \frac{-b+\sqrt{\Delta}}{2c}$, $\theta_2 = -\frac{1}{\theta+1} = \frac{-b-2a+\sqrt{\Delta}}{2(a+b+c)}$ and $\mathfrak{A}_i = (\mathbb{Z} + \theta_i\mathbb{Z})$, $i \in \{1, 2\}$. Then easy calculation shows that

$$\mathfrak{a} = a(\mathbb{Z} + \theta\mathbb{Z}) = a\theta(\frac{1}{\theta}\mathbb{Z} + \mathbb{Z}) = a\theta(\mathbb{Z} - \frac{1}{\theta}\mathbb{Z}) = \frac{a\theta}{c}(c\mathbb{Z} + c\theta_1\mathbb{Z}) = \frac{a\theta}{c}\mathfrak{A}_1$$

and

$$\mathfrak{a} = a(\mathbb{Z} + (\theta + 1)\mathbb{Z}) = a(\theta + 1)(\mathbb{Z} - \frac{1}{\theta + 1}\mathbb{Z}) = \frac{a(\theta + 1)}{a + b + c}\mathfrak{A}_2 \ .$$

□

We now give algorithms for switching from the set of invertible ideals of the maximal order $\mathcal{I}_{\Delta_1}$ to the set of invertible ideals of the non-maximal order $\mathcal{I}_{\Delta_q}$ and back. These algorithms will be the key ingredients of our proposed scheme, which is discussed in more detail in Section 3.

Algorithm 2 (GoToNonMaxOrder).
Input: A primitive $\mathcal{O}_{\Delta_1}$-ideal $\mathfrak{A} = (A, B)$, the conductor q
Output: A primitive $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{a} = \varphi(\mathfrak{B}) = (\mathfrak{B}) \cap \mathcal{O}_{\Delta_q} = (a, b)$, where $\mathfrak{B} \sim \mathfrak{A}$ and $\gcd(\mathcal{N}(\mathfrak{B}), q) = 1$

1. $(a, b_q) \leftarrow$FindIdealPrimeTo$(\mathfrak{A}, q)$
2. $b \leftarrow b_q q \bmod 2a$
3. RETURN (a, b)

Proof (Correctness). After Step 1 we have $\gcd(a, q) = 1$ and may apply φ from Proposition 6. Now $\mathcal{N}(\mathfrak{B}) = \mathcal{N}(\mathfrak{a}) = a$ by Proposition 6(1). The assertion about b is immediate by Proposition 1 and the uniqueness of $b \bmod 2a$. □

The step from $\mathcal{I}_{\Delta_q}$ back to the maximal order is almost as simple. This algorithm allows anybody who knows the fundamental discriminant Δ_1 and/or the conductor q to switch to the maximal order $\mathcal{O}_{\Delta_1}$.

Algorithm 3 (GoToMaxOrder).
Input: A primitive $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{a} = (a, b)$, the fundamental discriminant Δ_1 and the conductor q
Output: A primitive $\mathcal{O}_{\Delta_1}$-ideal $\mathfrak{A} = \varphi^{-1}(\mathfrak{b}) = (\mathfrak{b})\mathcal{O}_{\Delta_1} = (A, B)$, where $\mathfrak{b} \sim \mathfrak{a}$ and $\gcd(\mathcal{N}(\mathfrak{b}), q) = 1$

1. $(A, B) \leftarrow$FindIdealPrimeTo$(\mathfrak{a}, q)$
2. $b_{\mathcal{O}} \leftarrow \Delta \bmod 2$
3. Solve $1 = \mu q + \lambda A$ for $\mu, \lambda \in \mathbb{Z}$
4. $B \leftarrow B\mu + A b_{\mathcal{O}} \lambda \bmod 2A$
5. RETURN (A, B)

Proof (Correctness). After Step 1 we have $\gcd(A, q) = 1$ and may apply φ^{-1} from Proposition 6. Again, $\mathcal{N}(\mathfrak{b}) = \mathcal{N}(\mathfrak{A}) = A$ by Proposition 6(2). Note that we constructed μ in Step 3 such that $\mu \equiv f^{-1} \pmod{A}$. This inversion is always possible, because $\gcd(A, q) = 1$. Furthermore, the assertion about B follows from the standard algorithm for ideal multiplication. □

Our proposed cryptosystem in Section 3 is constructed over $\Delta_q = \Delta_1 q^2$, where q is a prime integer. In this case, the condition for a reduced ideal to be prime to the conductor q is given by the following Lemma.

Lemma 8. *Let $\Delta_q = \Delta_1 q^2$. If q is a prime such that $\sqrt{|\Delta_1|} < q$, then every reduced ideal in $Cl(\Delta_q)$ is prime to q.*

Proof. Let $\mathfrak{a} = (a, b)$ be a reduced ideal in $Cl(\Delta_q)$, and $c = (b^2 - \Delta_q)/4a$. Assume contrary to our assertion that $\gcd(a, q) > 1$, which implies $q \mid a$ because q is prime. We know that $b^2 - 4ac = \Delta_1 q^2$. Since $q \mid a$, this implies that $q \mid b^2$, $q \mid b$ and $q^2 \mid b^2$. Because $\mathfrak{a}$ is reduced it holds that $a < \sqrt{|\Delta_1|q^2/3} = q\sqrt{|\Delta_1|/3}$. Thus, since $q \mid a$, we must have $q^2 \not| a$, because $\sqrt{|\Delta_1|/3} < \sqrt{|\Delta_1|} < q$. Since $q^2 \mid b^2$ it follows that $q \mid c$, because $4ac = b^2 - \Delta_1 q^2$, $b^2 \mid q^2$ and $q^2 \not| a$. However, this is a contradiction to the requirement $\gcd(a, b, c) = 1$ for a reduced ideal. □

Thus, if we chose the conductor q such that $\sqrt{|\Delta_1|} < q$, then all reduced ideals in the non-maximal order are prime to q.

It is important to note that the isomorphism φ is between the ideal groups $\mathcal{I}_{\Delta_1}(q)$ and $\mathcal{I}_{\Delta_q}(q)$, and unfortunately not the class groups. If, for $\mathfrak{A}, \mathfrak{B} \in \mathcal{I}_{\Delta_1}(q)$ we have $\mathfrak{A} \sim \mathfrak{B}$, it is not necessarily true that $\varphi(\mathfrak{A}) \sim \varphi(\mathfrak{B})$. On the other hand, equivalence *does* hold under φ^{-1} :

Theorem 9. *For $\mathfrak{a}, \mathfrak{b} \in \mathcal{I}_{\Delta_q}(q)$ such that $\mathfrak{a} \sim \mathfrak{b}$, $\varphi^{-1}(\mathfrak{a}) \sim \varphi^{-1}(\mathfrak{b})$.*

Proof. This follows from the exact sequence:

$$Cl(\Delta_q) \longrightarrow Cl(\Delta) \longrightarrow 1$$

(see [21, Theorem 12.9, p. 82]). □

We will make use of the following lemma in our proposed cryptosystem:

Lemma 10. *For $\mathfrak{a} \in \mathcal{I}_{\Delta_q}(q)$,*

$$\varphi^{-1}(\mathfrak{a})^x \sim \varphi^{-1}(\mathfrak{a}^x) \ .$$

Proof. Use the fact that φ is an isomorphism between ideal groups and combine this with Theorem 9. □

Furthermore, we can show that the isomorphism φ induces a correspondence between reduced ideals in $Cl(\Delta)$ and $Cl(\Delta_q)$ if we restrict ourselves to reduced ideals with small norm.

Lemma 11. *Let $\mathfrak{A}$ be a reduced ideal in $\mathcal{O}_{\Delta_1}$ prime to q where q is a prime. Then $\mathfrak{a} = \varphi(\mathfrak{A})$ is also reduced in $\mathcal{O}_{\Delta_1}$.*

Proof. Let $\mathfrak{A}$ be a reduced ideal in $\mathcal{O}_{\Delta_1}$, which is prime to q. Then $\mathcal{N}(\mathfrak{A}) \leq \sqrt{|\Delta_1|/3}$ holds. By Proposition 6 we know that $\mathcal{N}(\mathfrak{a}) = \mathcal{N}(\mathfrak{A}) = A \leq \sqrt{|\Delta_1|/3} < \sqrt{|\Delta_q|/4} = \sqrt{|\Delta_1|q^2/4}$, for $q > 1$. This implies that $\mathfrak{a}$ is also reduced in $\mathcal{O}_{\Delta_1}$. □

Lemma 12. *Let $\mathfrak{a} = (a, b)$ be a reduced ideal in $\mathcal{O}_{\Delta_q}$ prime to q, where q is a prime. If $a \leq \sqrt{|\Delta_1|/4}$, then $\mathfrak{A} = \varphi^{-1}(\mathfrak{a})$ is a reduced ideal in $\mathcal{O}_{\Delta_1}$.*

Proof. By Proposition 6, we know that $\mathcal{N}(\mathfrak{A}) = \mathcal{N}(\mathfrak{a}) \leq \sqrt{|\Delta_1|/4}$. This implies that $\mathfrak{A}$ is reduced in $\mathcal{O}_{\Delta_1}$. □

By these two Lemmas and Proposition 6 there is a one-to-one correspondence between reduced ideals in $Cl(\Delta_q)$ and $Cl(\Delta_1)$ whose norms are smaller than $\sqrt{|\Delta_1|/4}$.

Finally, we give the relationship between the class numbers $h(\Delta_1)$ and $h(\Delta_f)$.

Theorem 13. *Let $\mathcal{O}_{\Delta_f}$ be the order of conductor f in an imaginary quadratic field $\mathbb{Q}(\sqrt{\Delta})$ with maximal order $\mathcal{O}_{\Delta_1}$. Then*

$$h(\Delta_f) = \frac{h(\Delta_1) f}{[\mathcal{O}^*_{\Delta_1} : \mathcal{O}^*_{\Delta_f}]} \prod_{p \mid f} \left(1 - \frac{(\Delta_1/p)}{p}\right) = n h(\Delta_1),$$

where $n \in \mathbb{N}$ and (Δ_1/p) is the Kronecker-symbol.

Proof. See [8, Theorem 7.24, page 146]. □

3 The new cryptosystem

3.1 System setup

The setup of the proposed cryptosystem is very simple. Alice chooses a large prime p. If $p \equiv 3 \pmod 4$ then $\Delta = -p$, else $\Delta = -4p$. Obviously Δ is a fundamental discriminant. Next she chooses another large prime q and computes the non-fundamental discriminant $\Delta_q = \Delta q^2$, i.e., q will be the conductor of the publicly available non-maximal order $\mathcal{O}_{\Delta_q}$.

Alice now chooses any prime $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{g} = (g, b_g)$. This may be done by selecting a prime g where $(\Delta_q/g) = 1$ and computing b_g, i.e., a square-root of $\Delta_q \bmod 4g$ using Shanks' probabilistic algorithm RESSOL. A version of RESSOL with expected run time $O((\log g)^3 + \log \Delta_q \cdot \log g)$, and a deterministic algorithm for computing the Kronecker-symbol (Δ_q/g) in $O((\log g)^2 + \log g \cdot \log \Delta_q)$ may be found in, for example, [10, page 43 ff]. Alice must then compute her individual keys. She chooses a random integer $a \in [2, \lfloor\sqrt{|\Delta_q|}\rfloor]$ and computes the reduced ideal $\mathfrak{a}$ equivalent to $\mathfrak{g}^a$. The exponentiation is done via some Square & Multiply variant and the algorithms Multiply, Square and Reduce from [4] or NUCOMP and NUDUPL from [26]. We summarize the public and private system parameters:

Public	Private
non-fundamental discriminant Δ_q	secret key a
$\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{g}$ (base ideal)	conductor q
$\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{a}$ (public key)	

3.2 Encryption

Encryption is done completely analogous to ElGamal encryption [11] in the non-maximal order $\mathcal{O}_{\Delta_q}$. We embed the plaintext in an $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{m}$, select an integer k, and compute:

$$e_k(\mathfrak{m}, k) = (\mathfrak{y}_1, \mathfrak{y}_2),$$

where $\mathfrak{y}_1$ and $\mathfrak{y}_2$ are reduced ideals in $\mathcal{I}_{\Delta_q}$ and

$$\mathfrak{y}_1 = \mathfrak{g}^k, \quad \mathfrak{y}_2 = \mathfrak{m}\mathfrak{a}^k \ .$$

Note that the encryption is carried out entirely in the class group of the non-maximal order, and that all ideal arithmetic is performed with reduced ideals. Furthermore, we require $\mathcal{N}(\mathfrak{m}) < \sqrt{|\Delta|/4}$ in order to uniquely decrypt the message $\mathfrak{m}$ (see Lemma 12).

3.3 Decryption

The decryption algorithm is similar to ElGamal decryption, but here we make use of our trapdoor information, namely the factorization of Δ_q. All ideal arithmetic is done with reduced ideals in the maximal order as opposed to the non-maximal order.

Algorithm 4 (Decrypt).
Input: The ciphertext $e_k(\mathfrak{m}, k) = (\mathfrak{y}_1, \mathfrak{y}_2), \mathfrak{y}_1, \mathfrak{y}_2 \in \mathcal{I}_{\Delta_q}$, the conductor q
Output: $\mathfrak{m}$, the $\mathcal{O}_{\Delta_q}$-ideal containing the embedded plaintext.

1. $\mathfrak{Y}_1 =$GoToMaxOrder$(\mathfrak{y}_1, q)$.
2. $\mathfrak{Y}_2 =$GoToMaxOrder$(\mathfrak{y}_2, q)$.
3. $\mathfrak{M} = \mathfrak{Y}_2(\mathfrak{Y}_1^a)^{-1}$.
4. $\mathfrak{m} =$GoToNonMaxOrder$(\mathfrak{M}, q)$.
5. RETURN$(\mathfrak{m})$

Proof (Correctness). By definition, we have $\mathfrak{Y}_1 = \varphi^{-1}(\mathfrak{y}_1)$ and $\mathfrak{Y}_2 = \varphi^{-1}(\mathfrak{y}_2)$. From Lemma 10 it follows that

$$\begin{aligned}\mathfrak{Y}_2 &= \varphi^{-1}(\mathfrak{m}\mathfrak{a}^k) \\ &= \varphi^{-1}(\mathfrak{m})\varphi^{-1}(\mathfrak{a}^k) \\ &\sim \varphi^{-1}(\mathfrak{m})\varphi^{-1}(\mathfrak{a})^k \\ &= \varphi^{-1}(\mathfrak{m})\mathfrak{A}^k\end{aligned}$$

and

$$\begin{aligned}\mathfrak{Y}_1^a &= \varphi^{-1}(\mathfrak{g}^k)^a \\ &\sim \varphi^{-1}(\mathfrak{g})^{ak} \\ &= \mathfrak{G}^{ak} \\ &\sim \mathfrak{A}^k \ .\end{aligned}$$

Thus, we have

$$\begin{aligned}\mathfrak{M} &\sim \varphi^{-1}(\mathfrak{m})\mathfrak{A}^k\mathfrak{A}^{-k} \\ &\sim \varphi^{-1}(\mathfrak{m}) \ .\end{aligned}$$

Since $\mathfrak{m}$ was selected such that $\mathcal{N}(\mathfrak{m}) < \sqrt{|\Delta|/4}$, we can uniquely decrypt $\varphi(\mathfrak{M}) = \mathfrak{m}$, from Lemma 12. □

3.4 Security of the proposed cryptosystem

The main advantage of this protocol over an ElGamal protocol using only arithmetic in the non-maximal order is that decryption is performed in the maximal order, where the coefficients in the ideal representations are significantly smaller than those of the non-maximal order. We will now show that this computational advantage does not incur any loss in security.

Theorem 14. *Assume that we can solve the discrete logarithm problem in $Cl(\Delta)$. Then breaking the proposed cryptosystem is computationally equivalent to factoring the discriminant $\Delta_q = \Delta q^2$.*

Proof. (Sketch) Assume, that there is an algorithm for breaking the proposed cryptosystem which computes the message ideal $\mathfrak{m}$. Then we know the ideals $\mathfrak{g}, \mathfrak{a}, \mathfrak{g}^k$ and $\mathfrak{a}^k$. This means that the Diffie-Hellman problem in $Cl(\Delta_q)$ can be solved using this algorithm. It is proved that (see [5]), an algorithm for solving the Diffie-Hellman problem in the imaginary quadratic class group of $\mathcal{O}_{\Delta_q}$ can be used to find the ambiguous ideals carrying factorizations of $\Delta_q = \Delta q^2$. Hence we can reduce factoring the discriminant to breaking the proposed cryptosystem.

On the other hand, if one is able to factor the non-fundamental discriminant $\Delta_q = \Delta q^2$ he may switch to the maximal order $\mathcal{O}_\Delta$ and solve the discrete logarithm problem in $Cl(\Delta)$ which is assumed to be possible. Thus, the computation of discrete logs in $Cl(\Delta_q)$ can be reduced to factoring $\Delta_q = \Delta q^2$. □

Remark that the assumption of being able to solve the discrete logarithm problem in $Cl(\Delta)$ is not unrealistic, since we choose Δ small to speed up the computations. Note furthermore that unlike the case of factoring of polynomials over finite fields (see, for example, [7, Section 3.4]), no algorithm is known which computes the "square-free factorization" of an integer substantially easier than the complete factorization.

3.5 Parameter Sizes

Since breaking our proposed scheme is equivalent to factoring the public non-fundamental discriminant Δ_q, we have to choose the parameters Δ, q such that factoring $\Delta_q = \Delta q^2$ is infeasible. Considering this situation yields the following requirements:

- Δ_q has to be large enough that it can't be factored with $O(\Delta^{1/6+o(1)})$-methods, see e.g. [24]
- Δ and q have to be large enough that they can't be found with the elliptic curve method [17]
- Δ_q has to be large enough that it can't be factored with the number field sieve [6]
- (signature setup only) Δ has to be small enough that the computation of $h(\Delta)$ is possible.

bit length			ave. time (sec)			
Δ_q	Δ	q	Enc	Dec	Dec_q	Dec_R
768	192	288	4.45	2.23	0.34	0.10
832	192	320	5.55	2.77	0.40	0.13
896	192	352	6.69	3.39	0.53	0.16
960	192	384	7.90	3.98	0.43	0.19
1024	192	416	9.41	4.72	0.46	0.23

Table 1. Runtime Statistics

First, note that usual square root methods reduce to *cube* root methods, because $\Delta_q = \Delta q^2$ and it is sufficient to know all prime factors up to the *cube* root. For example, the deterministic algorithm of Pollard and Strassen (see [24, Section 4]) has running time $O(\Delta_q^{1/6+o(1)})$. If $\Delta_q > 2^{420}$, these methods are certainly infeasible.

The general number field sieve has a conjectured running time $L_{\Delta_q}[1/3, (64/9)^{1/3}]$, where $L_x[a,b] = \exp(b(\log x)^a (\log\log x)^{1-a})$. Hence, selecting $\Delta_q > 2^{512}$ will ensure that attempting to factor it with the number field sieve is infeasible today.

The elliptic curve method has been used to find factors of up to 156 bits length. Hence, we must select $\Delta, q > 2^{170}$ to ensure that an adversary cannot factor Δ_q. If $\Delta < 2^{216}$, the DL problem in $Cl(\Delta)$ can be solved in reasonable time by anyone who knows the factorization of Δ_q [14], so selecting $\Delta > 2^{216}$ may add an even greater level of security to our scheme.

3.6 Run-time Statistics

In order to demonstrate the improved efficiency of our trapdoor decryption, we implemented our scheme using the LiDIA library [1]. It should be emphasized here that our implementation was not optimized for cryptographic purposes — it is only intended to provide a comparison between decrypting in the non-maximal order and using our trapdoor decryption. For five different non-maximal orders of various sizes, we have computed the average run time for encryption, classical decryption, and our trapdoor decryption of fifty randomly selected messages using randomly selected exponents. The results of these computations can be found in Table 1. Dec denotes the average time for classical decryption and Dec_q denotes the average time for the trapdoor decryption. The encryption is identical in both schemes, and the average time is denoted by Enc. We also give the run time for RSA decryption (Dec_R) using a modulus of the same size as Δ_q. All run times are given in CPU seconds on a 160 Mz SPARC-ultra machine.

As expected, our results clearly demonstrate an improvement in the decryption time. This is due to the fact that almost all of the arithmetic is carried out with reduced ideals in the maximal order. Hence, the operands are of size approximately $\sqrt{|\Delta|}$, rather than $\sqrt{|\Delta|q^2}$ as in the case where the trapdoor in-

formation is not used. Our decryption method is still not as fast as that of RSA, but it is at least comparable.

4 Further applications

It is in principal possible to use knowledge of the factorization of Δ_q to set up ElGamal-style and RSA-style signature schemes. If we select the fundamental discriminant Δ such that computing $h(\Delta)$ is feasible, then we can use the following corollary of Theorem 13 to compute $h(\Delta_q)$ at very little extra cost.

Corollary 15. *Let $p, q > 4$ be primes and $\Delta = -p$, if $p \equiv 3 \pmod 4$, or $\Delta = -4p$, otherwise and (Δ/q) be the Kronecker-symbol. Then*

$$h(\Delta_q) = h(\Delta q^2) = h(\Delta)\,(q - (\Delta/q)) \quad .$$

Proof. Since $p, q > 4$, the group of units $\mathcal{O}^*_\Delta = \mathcal{O}^*_{\Delta q^2} = \{\pm 1\}$. Thus $[\mathcal{O}^*_{\Delta_1} : \mathcal{O}^*_{\Delta_q}]$ in Theorem 13 equals 1. Noting that q is prime concludes the proof. □

Knowledge of $h(\Delta_q)$ allows us to set up DL-based signature schemes in $Cl(\Delta_q)$ very easily. Moreover, computing $h(\Delta_q)$ using the sub-exponential algorithm of Hafner-McCurley [12] or its more practical versions from [10] and [14] are still impractical for suitable choices of Δ_q. Unfortunately, these signature schemes have the disadvantage that the signature generation and verification both take place in the non-maximal order, so no extra efficiency is gained using this approach. Also, the security of these schemes is also computationally equivalent to factoring, so they probably have no significant advantages over regular ElGamal or RSA signature schemes.

An interesting side-effect of our scheme is that it is possible to set up a key escrow cryptosystem using the classical imaginary quadratic field cryptosystem. Instead of a fundamental discriminant, the key provider simply issues a non-fundamental discriminant of which only he knows the conductor to the users of the protocol. The users have no way of knowing that they are encrypting and decrypting in a non-maximal order, but the key provider can easily read their messages by solving the DLP in the maximal order. Hence it is important for any users of such protocols to ensure that they only use fundamental discriminants, and to have their key provider prove that the discriminant he issues is indeed fundamental. This could be done as follows:

Assume that Bob wants to prove to Alice that Δ is squarefree. Remark that if Δ and $\phi(\Delta)$ are coprime, then Δ is squarefree. Alice chooses a random integer x, computes $y = x^\Delta$ and sends it to Bob. If Δ and $\phi(\Delta)$ are indeed coprime, then Bob can compute an integer e such that $e \cdot \Delta \equiv 1 \pmod{\phi(\Delta)}$ using the extended Euclidean algorithm. So Bob computes $z = y^e$ and sends it to Alice. Alice compares x and z; if they are not equal, Alice rejects Δ. If Δ is not squarefree, then Bob can cheat with probability at most $1/q$, where $q^2 \mid \Delta$. Thus after several iterations without rejecting, Alice will believe that Δ and $\phi(\Delta)$ are coprime, and hence Δ is squarefree.

Note that this method fails to prove squarefreeness for integers of the form pq where $q \mid (p-1)$, for example. However, a key provider can easily select a squarefree discriminant Δ coprime to $\phi(\Delta)$ which he can prove is squarefree using the protocol given above.

5 Acknowlegdements

We thank Johannes Buchmann and Volker Müller for several helpful remarks, and Volker's interactive proof of the squarefreeness of a given number.

References

1. I. Biehl, J. Buchmann, and T. Papanikolaou. *LiDIA - A library for computational number theory.* The LiDIA Group, Universität des Saarlandes, Saarbrücken, Germany, 1995.
2. Z.I. Borevich and I.R. Shafarevich. *Number Theory.* Academic Press, New York, 1966.
3. J. Buchmann and S. Düllmann. On the computation of discrete logarithms in class groups. In *Advances in Cryptology - CRYPTO '90*, volume 537 of *Lecture Notes in Computer Science*, pages 134–139, 1991.
4. J. Buchmann, S. Düllmann, and H.C. Williams. On the complexity and efficiency of a new key exchange system. In *Advances in Cryptology - EUROCRYPT '89*, volume 434 of *Lecture Notes in Computer Science*, pages 597–616, 1990.
5. J. Buchmann and H.C. Williams. A key-exchange system based on imaginary quadratic fields. *Journal of Cryptology*, 1:107–118, 1988.
6. J.P. Buhler, H.W. Lenstra, Jr., and C. Pomerance. Factoring integers with the number fields sieve. In A.K. Lenstra and H.W. Lenstra, Jr., editors, *The Develoepement of the Number Field Sieve*, volume 1554 of *Lecture Notes in Math.*, pages 50–94. Springer, Berlin, 1993.
7. H. Cohen. *A Course in Computational Algebraic Number Theory.* Springer-Verlag, Berlin, 1993.
8. D.A. Cox. *Primes of the form $x^2 + ny^2$.* John Wiley & Sons, New York, 1989.
9. W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22:472–492, 1976.
10. S. Düllmann. *Ein Algorithmus zur Bestimmung der Klassengruppe positiv definiter binärer quadratischer Formen.* PhD thesis, Universität des Saarlandes, Saarbrücken, Germany, 1991.
11. T. El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31:469–472, 1985.
12. J.L. Hafner and K.S. McCurley. A rigorous subexpoential algorithm for computation of class groups. *J. Amer. Math. Soc.*, 2:837–850, 1989.
13. L.K. Hua. *Introduction to Number Theory.* Springer-Verlag, New York, 1982.
14. M.J. Jacobson, Jr. Applying sieving to the computation of quadratic class groups. To appear in Math. Comp., 1997.
15. N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48:203–209, 1987.
16. N. Koblitz. Hyperelliptic cryptosystems. *Journal of Cryptology*, 1:139–150, 1989.
17. H.W. Lenstra, Jr. Factoring integers with elliptic curves. *Annals of Math. (2)*, 126:649–673, 1987.

18. K.S. McCurley. Cryptographic key distribution and computation in class groups. In R.A. Mollin, editor, *Proc. NATO ASI on Number Theory and Applications*, pages 459–479. Kluwer Academic Press, 1989.
19. K.S. McCurley. A key distribution system equivalent to factoring. *Journal of Cryptology*, 1:95–105, 1989.
20. V. Miller. Use of elliptic curves in cryptography. In *Advances in Cryptology - CRYPTO '85*, volume 218 of *Lecture Notes in Computer Science*, pages 417–426, 1986.
21. J. Neukirch. *Algebraische Zahlentheorie*. Springer, Berlin, 1992.
22. K. Nyberg and R. Rüppel. A new signature scheme based on the DSA giving message recovery. In *1st ACM Conference on Computer and Communications Security*, Fairfax, Virginia, Nov. 3-5, 1993.
23. National Institute of Standards and Technology (NIST). Digital signature standard (DSS). *Federal Information Processing Standards Publication*, 186, May 19, 1994.
24. C. Pomerance. Analysis and comparison of some integer factoring algorithms. In H.W. Lenstra, Jr. and R. Tijdeman, editors, *Computational Methods in Number Theory*, pages 89–139. Math. Centre Tracts, Amsterdam, 1983. Number 154, Part I.
25. R.J. Schoof. Quadratic fields and factorization. In H.W. Lenstra, Jr. and R. Tijdeman, editors, *Computational Methods in Number Theory*, pages 235–286. Math. Centre Tracts, Amsterdam, 1983. Number 155, Part II.
26. D. Shanks. On Gauss and composition I, II. In R.A. Mollin, editor, *Proc. NATO ASI on Number Theory and Applications*, pages 163–179. Kluwer Academic Press, 1989.