Reducing Logarithms in Totally Non-maximal Imaginary Quadratic Orders to Logarithms in Finite Fields

Detlef Hühnlein[1] and Tsuyoshi Takagi[2]

[1] Security Networks GmbH
Mergenthalerallee 77-81, D-65760 Eschborn, Germany
huehnlein@secunet.de
[2] NTT Information Sharing Platform Laboratories
Immermannstr. 40, D-40210 Düsseldorf, Germany
ttakagi@ntt.de

Abstract. We discuss the discrete logarithm problem over the class group $Cl(\Delta)$ of an imaginary quadratic order $\mathcal{O}_\Delta$, which was proposed as a public-key cryptosystem by Buchmann and Williams [8]. While in the meantime there has been found a subexponential algorithm for the computation of discrete logarithms in $Cl(\Delta)$ [16], this algorithm only has running time $L_\Delta[\frac{1}{2}, c]$ and is far less efficient than the number field sieve with $L_p[\frac{1}{3}, c]$ to compute logarithms in $\mathbb{F}_p^*$. Thus one can choose smaller parameters to obtain the same level of security. It is an open question whether there is an $L_\Delta[\frac{1}{3}, c]$ algorithm to compute discrete logarithms in arbitrary $Cl(\Delta)$.
In this work we focus on the special case of *totally non-maximal* imaginary quadratic orders $\mathcal{O}_{\Delta_p}$ such that $\Delta_p = \Delta_1 p^2$ and the class number of the maximal order $h(\Delta_1) = 1$, and we will show that there is an $L_{\Delta_p}[\frac{1}{3}, c]$ algorithm to compute discrete logarithms over the class group $Cl(\Delta_p)$. The logarithm problem in $Cl(\Delta_p)$ can be reduced in (expected) $O(\log^3 p)$ bit operations to the logarithm problem in $\mathbb{F}_p^*$ (if $(\frac{\Delta_1}{p}) = 1$) or $\mathbb{F}_{p^2}^*$ (if $(\frac{\Delta_1}{p}) = -1$) respectively. This result implies that the recently proposed efficient DSA-analogue in totally non-maximal imaginary quadratic order $\mathcal{O}_{\Delta_p}$ [21] are only as secure as the original DSA scheme based on finite fields and hence loose much of its attractiveness.

1 Introduction

A general and possible inherent problem of all currently known public key cryptosystems is that their intractability is based on certain unproven assumptions. Thus nobody can guarantee that popular cryptosystems based on factoring integers or computing discrete logarithms in some group will remain secure in the future. Therefore it is important to study alternative primitives and different groups to have a backup if one assumption such as the intractability of factoring or computation of discrete logarithms in one group turns out to be false. Beside

K. Y. Lam, E. Okamoto and C. Xing (Eds.): ASIACRYPT'99, LNCS 1716, pp. 219–231, 1999.

the multiplicative group of finite fields and the group of points on (hyper-) elliptic curves over finite fields, a very promising candidate for a group in which the discrete logarithm is hard is the class group $Cl(\Delta)$ of imaginary quadratic orders, such as proposed by Buchmann and Williams [8] in 1988. For example the discrete logarithm problem in $Cl(\Delta)$ has the interesting property that it is at least as hard as factoring the discriminant Δ. Another reason which makes studying imaginary quadratic orders $\mathcal{O}_\Delta$ very important today, is that these rings are isomorphic to the *endomorphism rings* of non-supersingular elliptic curves over finite fields. Thus a good understanding of these rings can shed some light on the real difficulty of the discrete logarithm problem in elliptic curves. While Hafner and McCurley discovered a subexponential algorithm one year later [16] to compute discrete logarithms in $Cl(\Delta)$, this algorithm has a running time $L_\Delta[\frac{1}{2}, 1]$ and is far less efficient than the number field sieve to compute discrete logarithms in $\mathbb{F}_p^*$ or factoring integers with $L_n[\frac{1}{3}, (\frac{64}{9})^{1/3}]$. The precise definition of $L_n[e, c]$ will be given in Section 3. Thus one may choose smaller parameters, and still obtain the same level of security. It is an open question whether there is an $L_\Delta[\frac{1}{3}, c]$ algorithm to compute discrete logarithms in arbitrary imaginary quadratic class groups $Cl(\Delta)$. Note that as mentioned above this would imply another asymptotically fast algorithm for factoring integers, because factoring the discriminant Δ is reduced to the computation of discrete logarithms in $Cl(\Delta)$.

Furthermore these cryptosystems based on imaginary quadratic class groups are not only interesting from a theoretical point of view. Recently cryptosystems have been proposed with very *practical properties*. We will only name a few cryptosystems based on imaginary quadratic orders here and refer to Section 2 for a more comprehensive survey . In [26] a public key cryptosystem was proposed with *quadratic decryption time*. To our knowledge this is the only known cryptosystem having this property. First implementations show that the decryption is as efficient as RSA-encryption with $e = 2^{16}+1$. While this cryptosystem is based on factoring, it is also possible to set up interesting DL-based cryptosystems using non-maximal imaginary quadratic orders. If one uses the recently developed exponentiation technique for *totally* non-maximal orders [21] it is possible to implement efficient DSA-analogues. The running time is roughly comparable to DSA in $\mathbb{F}_p^*$ and there is certainly much space for further improvements. The major property of these totally non-maximal orders is that the class number of the maximal order $h(\Delta_1) = 1$ and thus the class number of the non-maximal order $h(\Delta_p) = p - (\frac{\Delta_1}{p})$, where the conductor p is prime and $(\frac{\Delta_1}{p})$ is the Kronecker-Symbol, is known immediately. Note that these totally non-maximal quadratic orders are therefore analogous to *supersingular elliptic curves*, where one also knows the group order in advance.

In this work we will show that the discrete logarithm problem in totally non-maximal imaginary quadratic orders can be reduced to the discrete logarithm problem in $\mathbb{F}_p^*$ (if $(\frac{\Delta_1}{p}) = 1$) or $\mathbb{F}_{p^2}^*$ (if $(\frac{\Delta_1}{p}) = -1$) respectively. The reduction is very efficient and can be performed in (expected) $O(\log^3 p)$ bit operations. Thus the situation for cryptosystems based on imaginary quadratic orders is

somewhat analogous to the situation for cryptosystems based on elliptic curves. This may be summarized as follows:

> *While there is no known algorithm with* $L_{\Delta}[\frac{1}{3}, c]$ *for the computation of discrete logarithms in imaginary quadratic class groups in general, there are problem classes for which such an algorithm is known. This is no general problem however, because it is easy to avoid these weak classes in practice.*

It is clear that an analogous statement for elliptic curves would be somewhat sharper and consider algorithms with subexponential running time $L_p[e, c]$, $e < 1$.

This paper is organized as follows: In Section 2 we will give a brief survey of cryptosystems based on imaginary quadratic orders, because many results appeared very recently and are sometimes not yet published. Section 3 gives the necessary background and notations of imaginary quadratic orders. In Section 4 we will provide the main result of this paper which consists of the reduction of the discrete logarithm problem in totally non-maximal imaginary quadratic orders to the discrete logarithm problem in finite fields. Finally, in Section 5, we will conclude this work by discussing the cryptographic implications of our result.

2 A Brief Survey of Cryptosystems Based on Imaginary Quadratic Orders

We will only highlight the most important works in this direction. As mentioned above it is a general problem that the security of popular cryptosystems is based on *unproven assumptions*. Nobody can guarantee that DL-type cryptosystems based on finite fields or elliptic curves over finite fields will stay secure forever. Thus it is important to study alternative groups which can be used if an efficient algorithm for the computation of discrete logarithms in one particular type of group is discovered.

2.1 The Early Days - Maximal Orders

With this motivation Buchmann and Williams [8] proposed to use imaginary quadratic class groups $Cl(\Delta)$ for the construction of cryptosystems. A nice property of this approach is that breaking this scheme is at least as difficult as factoring the fundamental discriminant Δ of the *maximal order*. Furthermore it should be mentioned that imaginary quadratic orders are closely related to non-supersingular elliptic curves over finite fields. They happen to be isomorphic to their endomorphism ring. Thus a sound understanding of imaginary quadratic orders may lead to a better understanding of the real security of elliptic curve cryptosystems. In 1988, when they proposed these groups for cryptographic purposes, the best algorithms to compute the class number $h(\Delta)$ and discrete logarithms in $Cl(\Delta)$ were *exponential time algorithms* with $L_{\Delta}[1, \frac{1}{5}]$ [23,30] assuming

the truth of the Generalized Riemann Hypothesis (GRH) or $L_{\Delta}[1, \frac{1}{4}]$ without this assumption. In [6] the first implementation was reported along with a complexity analysis of this key agreement scheme. For example it was shown that the complexity of an exponentiation in $Cl(\Delta)$ needs $O(\log^4 |\Delta|)$ bit operations, which is fairly inefficient compared to the original scheme [13] which is of cubic complexity. Another problem of cryptosystems based on class group $Cl(\Delta)$ of the maximal order, was that the computation of the class number $h(\Delta)$ is almost as difficult as the computation of discrete logarithms. Thus it seemed impossible to set up signature schemes analogous to DSA [25] or RSA [28].

Even worse for this approach was the discovery of a subexponential time algorithm [16] by Hafner and McCurley in 1989. This algorithm has running time $L_{\Delta}[\frac{1}{2}, c]$ and can be used to compute the class number $h(\Delta)$ and with some modifications to the computation of discrete logarithms in $Cl(\Delta)$ as shown in [5]. Note that at this time the asymptotically best algorithm for factoring integers was the quadratic sieve [29] with running time $L_n[\frac{1}{2}, 1]$ if one makes certain plausible assumptions. The situation for discrete logarithms in $\mathbb{F}_p^*$ was similar these days. The algorithm due to Coppersmith, Odlyzko and Schroeppel (COS) [11] to compute discrete logarithms in prime fields also has running time $L_p[\frac{1}{2}, 1]$.

Thus, it was inclined to consider cryptosystems based on imaginary quadratic class groups $Cl(\Delta)$ to be unsuitable for practical application.

2.2 The Recent Revival - Non-maximal Orders

In the meantime however an idea of Pollard lead to today's asymptotically best algorithm for factoring integers - the number field sieve (see [24]). This algorithm has (expected) running time $L_n[\frac{1}{3}, (\frac{64}{9})^{1/3}]$ and was used in 1996 for the factorization of RSA-130 [9] and recently for the factorization of RSA-140 [27] for example. The number field sieve can also be used to compute discrete logarithms in finite fields (see e.g. [15,31]), where the (expected) running time is $L_p[\frac{1}{3}, (\frac{64}{9})^{1/3}]$ as well. In contrast to this development there is still no $L_{\Delta}[\frac{1}{3}, c]$ algorithm known for the computation of discrete logarithms in arbitrary $Cl(\Delta)$. The asymptotically best algorithm for this task still is an analogue of the multiple polynomial quadratic sieve [22] with $L_{\Delta}[\frac{1}{2}, 1]$.

It is clear that this development alone would not justify the term "revival". In 1998 it was shown in [19] that by using class groups $Cl(\Delta_p)$, $\Delta_p = \Delta_1 p^2$, of *non-maximal* orders one solves the problem that the class number $h(\Delta_p)$ can not be determined and that one is able to implement an ElGamal-type cryptosystem with comparably fast decryption. While the performance of this scheme still was too bad to be used in practice this result may be considered as the *birth of a new generation* of cryptosystems based on quadratic orders.

Recently, a very efficient successor [26] with *quadratic decryption time* was proposed. This scheme was later on called NICE for New Ideal Coset Encryption. First implementations show that the time for decryption is comparable to RSA - encryption with $e = 2^{16} + 1$. The central idea is to use an element $\mathfrak{g} \in \ker(\varphi^{-1})$ to mask the message in the ElGamal-type encryption scheme by multiplication

with $\mathfrak{g}^k$ for random k. Here φ^{-1} is the isomorphism introduced in [19] which allows switching from the public non-maximal order to the secret maximal order. Thus during the decryption step, which essentially consists of the computation of φ^{-1}, the mask $\mathfrak{g}^k$ simply disappears and the message is recovered. Note that the computation of φ^{-1} is essentially one modular inversion with the Extended Euclidean Algorithm which takes quadratic time. It is clear that this cryptosystem is very well suited for applications in which a central server has to decrypt a large amount of ciphertext in a short time. For this scenario one may use the recently developed NICE-batch-decryption method [21], which speeds up the already very efficient decryption process by another 30% for a batch size of 100 messages. An efficient undeniable signature scheme based on the NICE-structure was also proposed [3].

In 1998 the first conventional signature schemes based on non-maximal imaginary quadratic orders were also proposed. In [20] RSA- and Rabin analogues were proposed. The corresponding encryption schemes have the major advantage that they are immune against low-exponent- and chosen-ciphertext attacks. Moreover a novel algorithm to compute square roots in $Cl(\Delta_p)$ was proposed, which replaces the fairly inefficient Gaussian algorithm using ternary quadratic forms. To avoid the computation of $h(\Delta_1)$, where $|\Delta_1|$ should have at least 200 bits to prevent the factorization of Δ_p using ECM (see [4] for a recent finding of a 53 digit factor), it was proposed to use *totally* non-maximal imaginary quadratic orders. Note that the above cryptosystems are based on *completely* factoring the non-fundamental discriminant Δ_p or Δ_{pq} in the case of totally non-maximal orders respectively. While the utilization of totally non-maximal orders for RSA-analogues is only interesting from a theoretical point of view, it is clear that this structure may well be used to set up DSA analogues. The discriminant $\Delta_p = \Delta_1 p^2$, with $\Delta_1 = -163$ and hence $h(\Delta) = 1$ for example, can be chosen with about 800 bits to obtain the same level of security as for DSA in $\mathbb{F}_p^*$ with p about 1000 bits. Note that this comparison, i.e. 400 bit p for $Cl(\Delta_p)$ compared to 1000 bit p for $\mathbb{F}_p^*$, is a rather pessimistic one. Nevertheless this DSA analogue *seemed* to be too inefficient to be used in practice.

Very recently however a new arithmetic for these totally non-maximal orders was proposed [21]. The central idea is to replace the fairly inefficient conventional *ideal*-arithmetic, i.e. multiplication and reduction of ideals, by simple manipulations on the corresponding generator in the maximal order. This means that instead of (multiple) applications of the comparably costly Extended Euclidean Algorithm one only has a few modular multiplications. This strategy turns out to be *thirteen* times as fast and ends up with a DSA analogue based on totally non-maximal orders, in which the running time for the signature generation is roughly comparable to the conventional DSA in $\mathbb{F}_p^*$. Furthermore there still seems to be much space for further improving this scheme.

However beside the possibility to *speed up* the DSA analogues, there is yet another and even more important effect of the very recent result [21]:

> *It was precisely the way in which one considers the arithmetic of ideals in totally non-maximal orders, which led to the (previously conjectured)*

constructive version of the reduction proof presented in Section 4 of this work.

3 Some Background and Notations Concerning Imaginary Quadratic Orders

We first define the function $L_n[e,c]$ which is used to describe the asymptotic running time of subexponential algorithms. Let $n,e,c \in \mathbb{R}$ with $0 \leq e \leq 1$ and $c > 0$. Then we define

$$L_n[e,c] = \exp\left(c \cdot (\log|n|)^e \cdot (\log\log|n|)^{1-e}\right).$$

Thus the running time for subexponential algorithms is between polynomial time ($L_n[0,c]$) and exponential time ($L_n[1,c]$).

Now we will give some basics concerning quadratic orders. The basic notions of imaginary quadratic number fields may be found in [7,10]. For a more comprehensive treatment of the relationship between maximal and non-maximal orders we refer to [12,19].

Let $\Delta \equiv 0,1 \bmod 4$ be a negative integer, which is not a square. The quadratic order of discriminant Δ is defined to be

$$\mathcal{O}_\Delta = \mathbb{Z} + \omega\mathbb{Z},$$

where

$$\omega = \begin{cases} \sqrt{\frac{\Delta}{4}}, & \text{if } \Delta \equiv 0 \pmod 4, \\ \frac{1+\sqrt{\Delta}}{2}, & \text{if } \Delta \equiv 1 \pmod 4. \end{cases} \tag{1}$$

The standard representation of some $\alpha \in \mathcal{O}_\Delta$ is $\alpha = x + y\omega$, where $x,y \in \mathbb{Z}$.

If Δ_1 is squarefree, then $\mathcal{O}_{\Delta_1}$ is the *maximal order* of the quadratic number field $\mathbb{Q}(\sqrt{\Delta_1})$ and Δ_1 is called a fundamental discriminant. The *non-maximal order* of conductor $p > 1$ with (non-fundamental) discriminant $\Delta_p = \Delta_1 p^2$ is denoted by $\mathcal{O}_{\Delta_p}$. We will always assume in this work that the conductor p is prime. Furthermore we will omit the subscripts to reference arbitrary (fundamental or non-fundamental) discriminants. Because $\mathbb{Q}(\sqrt{\Delta_1}) = \mathbb{Q}(\sqrt{\Delta_p})$ we also omit the subscripts to reference the number field $\mathbb{Q}(\sqrt{\Delta})$. The standard representation of an $\mathcal{O}_\Delta$-ideal is

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

where $q \in \mathbb{Q}_{>0}, a \in \mathbb{Z}_{>0}$, $c = (b^2-\Delta)/(4a) \in \mathbb{Z}$, $\gcd(a,b,c) = 1$ and $-a < b \leq a$. The norm of this ideal is $\mathcal{N}(\mathfrak{a}) = aq^2$. An ideal is called primitive if $q = 1$. A primitive ideal is called *reduced* if $|b| \leq a \leq c$ and $b \geq 0$, if $a = c$ or $|b| = a$. It can be shown, that the norm of a reduced ideal $\mathfrak{a}$ satisfies $\mathcal{N}(\mathfrak{a}) \leq \sqrt{|\Delta|/3}$ and conversely that if $\mathcal{N}(\mathfrak{a}) \leq \sqrt{|\Delta|/4}$ then the primitive ideal $\mathfrak{a}$ is reduced. We denote the reduction operator in the maximal order by $\rho_1()$ and write $\rho_p()$ for the reduction operator in the non-maximal order of conductor p.

The group of invertible $\mathcal{O}_\Delta$-ideals is denoted by $\mathcal{I}_\Delta$. Two ideals $\mathfrak{a}, \mathfrak{b}$ are equivalent, if there is a $\gamma \in \mathbb{Q}(\sqrt{\Delta})$, such that $\mathfrak{a} = \gamma\mathfrak{b}$. This equivalence relation is denoted by $\mathfrak{a} \sim \mathfrak{b}$. The set of principal $\mathcal{O}_\Delta$-ideals, i.e. which are equivalent to $\mathcal{O}_\Delta$, is denoted by $\mathcal{P}_\Delta$. The factor group $\mathcal{I}_\Delta/\mathcal{P}_\Delta$ is called the *class group* of $\mathcal{O}_\Delta$ denoted by $Cl(\Delta)$. $Cl(\Delta)$ is a finite abelian group with neutral element $\mathcal{O}_\Delta$. In every equivalence class there is one and only one reduced ideal, which represents its class. Algorithms for the group operation (multiplication and reduction of ideals) can be found in [10]. The order of the class group is called the *class number* of $\mathcal{O}_\Delta$ and is denoted by $h(\Delta)$.

All cryptosystems from Section 2.2 make use of the relation between the maximal and some non-maximal order. Any non-maximal order of conductor p may be represented as $\mathcal{O}_{\Delta_p} = \mathbb{Z} + p\mathcal{O}_{\Delta_1}$. A special type of non-maximal order, which is of central importance in this work, is given if $h(\Delta) = 1$. In this case $\mathcal{O}_{\Delta_p}$ is called a *totally non-maximal* imaginary quadratic order. An $\mathcal{O}_\Delta$-ideal $\mathfrak{a}$ is called prime to p, if $\gcd(\mathcal{N}(\mathfrak{a}), p) = 1$. It is well known, that all $\mathcal{O}_{\Delta_p}$-ideals prime to the conductor are invertible.

Denote by $\mathcal{I}_{\Delta_p}(p)$ (respectively, $\mathcal{P}_{\Delta_p}(p)$) the $\mathcal{O}_{\Delta_p}$-ideals prime to p (respectively, the principal $\mathcal{O}_{\Delta_p}$-ideals prime to p). There is an isomorphism (See [12, Proposition 7.22,page 145])

$$\mathcal{I}_{\Delta_p}(p)\Big/\mathcal{P}_{\Delta_p}(p) \simeq \mathcal{I}_{\Delta_p}\Big/\mathcal{P}_{\Delta_p} = Cl(\Delta_p). \tag{3}$$

Thus we may 'neglect' the ideals which are not prime to the conductor, if we are only interested in the class group $Cl(\Delta_p)$. There is an isomorphism between the group of $\mathcal{O}_{\Delta_p}$-ideals which are prime to p and the group of $\mathcal{O}_{\Delta_1}$-ideals, which are prime to p, denoted by $\mathcal{I}_{\Delta_1}(p)$ respectively:

Proposition 1. *Let $\mathcal{O}_{\Delta_p}$ be an order of conductor p in an imaginary quadratic field $\mathbb{Q}(\sqrt{\Delta})$ with maximal order $\mathcal{O}_{\Delta_1}$.*

(i.) *If $\mathfrak{A} \in \mathcal{I}_{\Delta_1}(p)$, then $\mathfrak{a} = \mathfrak{A} \cap \mathcal{O}_{\Delta_p} \in \mathcal{I}_{\Delta_p}(p)$ and $\mathcal{N}(\mathfrak{A}) = \mathcal{N}(\mathfrak{a})$.*
(ii.) *If $\mathfrak{a} \in \mathcal{I}_{\Delta_p}(p)$, then $\mathfrak{A} = \mathfrak{a}\mathcal{O}_{\Delta_1} \in \mathcal{I}_{\Delta_1}(p)$ and $\mathcal{N}(\mathfrak{a}) = \mathcal{N}(\mathfrak{A})$.*
(iii.) *The map $\varphi : \mathfrak{A} \mapsto \mathfrak{A} \cap \mathcal{O}_{\Delta_p}$ induces an isomorphism $\mathcal{I}_{\Delta_1}(p) \xrightarrow{\sim} \mathcal{I}_{\Delta_p}(p)$. The inverse of this map is $\varphi^{-1} : \mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_{\Delta_1}$.*

Proof. See [12, Proposition 7.20, page 144] . □

Thus we are able to switch to and from the maximal order as applied in the cryptosystems of Section 2.2. The algorithms $\mathsf{GoToMaxOrder}(\mathfrak{a}, p)$ to compute φ^{-1} and $\mathsf{GoToNonMaxOrder}(\mathfrak{A}, p)$ to compute φ respectively may be found in [19]. Note, that the above map is defined on ideals themselves, rather than equivalence classes. The class group $Cl(\Delta_p)$ of a non-maximal order can be described as follows:

Proposition 2. *There is an isomorphism*

$$Cl(\Delta_p) \simeq \mathcal{I}_{\Delta_1}(p)\Big/\mathcal{P}_{\Delta_1,\mathbb{Z}}(p),$$

where $\mathcal{P}_{\Delta_1,\mathbb{Z}}(p)$ *denotes the subgroup of* $\mathcal{I}_{\Delta_1}(p)$ *generated by the principal ideals of the form* $\alpha\mathcal{O}_{\Delta_1}$ *where* $\alpha \in \mathcal{O}_{\Delta_1}$ *satisfies* $\alpha \equiv a \bmod p\mathcal{O}_{\Delta_1}$ *for some* $a \in \mathbb{Z}$ *such that* $\gcd(a,p)=1$. *This isomorphism is induced by isomorphism* φ *between* $\mathcal{I}_{\Delta_1}(p)$ *and* $\mathcal{I}_{\Delta_p}(p)$.

Proof. See the details in [12, Proposition 7.22,page 145]. For the sake of convenience we describe the outline of proof. Recall $\mathcal{I}_{\Delta_p}(p)/\mathcal{P}_{\Delta_p}(p) \simeq Cl(\Delta_p)$. Isomorphism $\varphi^{-1} : \mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_{\Delta_1}$ maps $\mathcal{P}_{\Delta_p}(p)$ to a subgroup $\mathcal{P}'$ of $\mathcal{I}_{\Delta_1}(p)$. We can prove that $\mathcal{P}' = \mathcal{P}_{\Delta_1,\mathbb{Z}}(p)$ using relation

$$\alpha \equiv a \bmod p\mathcal{O}_{\Delta_1}, a \in \mathbb{Z}, \gcd(a,p)=1 \Longleftrightarrow \alpha \in \mathcal{O}_{\Delta_p}, \gcd(N(\alpha),p)=1.$$

□

This interpretation of $Cl(\Delta_p)$ will be used in Section 4 to reduce the computation of discrete logarithms in totally non-maximal imaginary quadratic orders to the computation of discrete logarithms in finite fields.

Definition 1. *Let* $\Delta_1 < 0$ *and* $\Delta_1 \equiv 0,1 \bmod 4$, *such that* $h(\Delta_1)=1$ *and* p *prime. Furthermore let* $\mathfrak{g}$ *and* $\mathfrak{a}$ *be reduced* $\mathcal{O}_{\Delta_p}$*-ideals in standard-representation (2), which represent classes of the class group* $Cl(\Delta_p)$ *of the totally non-maximal order. Then the* discrete logarithm problem *DLP in* $Cl(\Delta_p)$ *is given as follows: Determine an* $a \in \mathbb{Z}$ *such that* $\mathfrak{g}^a \sim \mathfrak{a}$, *or show that no such* a *exists.*

Furthermore the class number of a totally non-maximal order of conductor p is given as follows:

Proposition 3. *Let* $\Delta_1 < -4$, $\Delta_1 \equiv 0,1 \bmod 4$ *such that* $h(\Delta_1)=1$ *and* p *prime. Then* $h(\Delta_p) = p - (\frac{\Delta_1}{p})$, *where* $(\frac{\Delta_1}{p})$ *is the Kronecker-symbol.*

Proof. This follows immediately from [12, Theorem 7.24, page 146]. □

Finally we will make use of the following interpretation of the ring $(\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^*$:

Proposition 4. *Let* $\mathcal{O}_{\Delta_1}$ *be the maximal order and* p *be the prime conductor. Then there is an isomorphism between*

$$(\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^* \simeq \mathbb{F}_p[X]\Big/(f(X)),$$

where $(f(X))$ *is the ideal generated by* $f(X) \in \mathbb{F}_p[X]$ *and*

$$f(X) = \begin{cases} X^2 - \frac{\Delta_1}{4}, & \text{if } \Delta \equiv 0 \pmod 4, \\ X^2 - X + \frac{1-\Delta_1}{4}, & \text{if } \Delta \equiv 1 \pmod 4. \end{cases} \tag{4}$$

Proof. Let $\rho \in \mathbb{F}_p$ be a root of $f(X) \in \mathbb{F}_p[X]$, where $f(X)$ is as given above. Then an element $\alpha \in \mathbb{F}_p[X]/(f(X))$ has a representation $\alpha = x + y\rho$, where $x, y \in \mathbb{F}_p$. On the other hand an element $\beta \in (\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^*$ has a representation $\beta = \bar{x} + \bar{y}\omega$, where ω given as in (1) and $\bar{x}, \bar{y} \in \mathbb{F}_p$. If we set $x \equiv \bar{x} \bmod p$ and $y \equiv \bar{y} \bmod p$ we immediately have the desired bijective correspondence. Furthermore it can be easily shown by straight forward calculation that this bijective correspondence is indeed an isomorphism. □

Note that this isomorphism implicitly was used in [21] to speed up the arithmetic in totally-non-maximal orders.

4 Reducing Logarithms in Totally Non-maximal Orders to Logarithms in Finite Fields

In this section we will show that the discrete logarithm problem in $Cl(\Delta_p)$ as given in Definition 1 can be reduced to the discrete logarithm problem in finite fields. More precisely we will show the following

Theorem 1. *The DLP in the class group $Cl(\Delta_p)$ of a* totally *non-maximal order $\mathcal{O}_{\Delta_p}$, where $\Delta_p = \Delta_1 p^2$ for prime p, can be reduced in (expected) $O(\log^3 p)$ bit operations*

1. *to the DLP in $\mathbb{F}_{p^2}^*$ if $(\frac{\Delta_1}{p}) = -1$ or*
2. *to the DLP in $\mathbb{F}_p^*$ if $(\frac{\Delta_1}{p}) = 1$.*

To show the above result we will first consider the structure of the class group $Cl(\Delta_p)$ of the totally non-maximal order. By the definition of a *totally* non-maximal order, we know that the class number of the maximal order $h(\Delta_1) = 1$. This means that in $\mathcal{O}_{\Delta_1}$ there are only principal ideals and hence $\mathcal{I}_{\Delta_1} = \mathcal{P}_{\Delta_1}$. Recall from Proposition 2 that $Cl(\Delta_p) \simeq \mathcal{I}_{\Delta_1}(p)/\mathcal{P}_{\Delta_1,\mathbb{Z}}(p)$, where $\mathcal{P}_{\Delta_1,\mathbb{Z}}(p)$ denotes the principal ideals $\alpha\mathcal{O}_{\Delta_1}$ of the form $\alpha \equiv a \bmod p\mathcal{O}_{\Delta_1}$, with $a \in \mathbb{Z}$ and $\gcd(a, p) = 1$. Thus in our case we obtain the following isomorphism:

$$Cl(\Delta_p) \simeq {\mathcal{P}_{\Delta_1}(p)}\Big/{\mathcal{P}_{\Delta_1,\mathbb{Z}}(p)}.$$

Hence the group structure of the class group $Cl(\Delta_p)$ can be explained exclusively by a relation of principal ideals in the maximal order $\mathcal{O}_{\Delta_1}$. With this knowledge we are able to relate the ring $(\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^*$ to our class group $Cl(\Delta_p)$.

Lemma 1. *The map $(\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^* \to \mathcal{P}_{\Delta_1}(p)/\mathcal{P}_{\Delta_1,\mathbb{Z}}(p)$, which $\alpha \in (\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^*$ maps to $\alpha\mathcal{O}_{\Delta_1} \in \mathcal{P}_{\Delta_1}(p)/\mathcal{P}_{\Delta_1,\mathbb{Z}}(p)$, is a well-defined group homomorphism and surjective.*

Proof. This is shown in the more comprehensive proof of Theorem 7.24 in [12] (page 147). □

The "running time" to compute this map is trivially constant time. Note that this map cannot be injective, just because there are (depending on (Δ_1/p)) either $p^2 - 1$ or $(p-1)^2$ elements in $(\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^*$ and by Proposition 3 only $p - (\Delta_1/p) = p \pm 1$ elements in $Cl(\Delta_p)$. It would be an isomorphism if we would restrict it to appropriate subgroups of $(\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^*$. The precise relation is given in Lemma 2.

In the next step we show that there is an isomorphism ψ between the ring $(\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^*$ and the multiplicative group of a finite field of degree at most 2, which can be computed in (expected) $O(\log^3 p)$ bit operations.

Lemma 2. *We have to distinguish two cases:*

1. *If* $(\frac{\Delta_1}{p}) = -1$ *then there exists an isomorphism* $\psi : (\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^* \to \mathbb{F}_{p^2}^*$, *which can be computed in constant time.*
2. *If* $(\frac{\Delta_1}{p}) = 1$ *then there exits a surjective homomorphism* $\psi : (\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^* \to \mathbb{F}_p^*$, *which can be computed with (expected)* $O(\log^3 p)$ *bit operations.*

Proof. From Proposition 4 we know that there is an isomorphism $(\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^* \to \mathbb{F}_p[X]/(f(X))$, where $f(X) \in \mathbb{F}_p[X]$ is given as in (4). Now we need to separate the two cases.

(1) $(\frac{\Delta_1}{p}) = -1$: In this case the polynomial $f(X)$ is irreducible in $\mathbb{F}_p[X]$ and therefore we have $\mathbb{F}_p[X]/(f(X)) \simeq \mathbb{F}_{p^2}$. Therefore we get the bijective map $\psi : (\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^* \to \mathbb{F}_{p^2}^*$ as follows: Let $\alpha = a + b\omega \in (\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^*$. Then $\psi(\alpha) = a + bX \in \mathbb{F}_{p^2}$. This map can be trivially computed in constant time. Furthermore it is easy to show that this map is indeed an isomorphism.

(2) $(\frac{\Delta_1}{p}) = 1$: In this case the polynomial $f(X)$ is *not* irreducible, but can be decomposed as $f(X) = (X - \rho)(X - \bar{\rho}) \in \mathbb{F}_p[X]$ where $\rho \in \mathbb{F}_p$ is a root of $f(X)$ and $\bar{\rho}$ is conjugate to ρ. Thus if $\Delta_1 \equiv 0 \bmod 4$ and $D = \Delta_1/4$ we have $\rho \in \mathbb{F}_p$ such that $\rho^2 \equiv D \bmod p$ and $\bar{\rho} = -\rho$. In the other case $\Delta_1 \equiv 1 \bmod 4$ we have $\rho = (1 + b)/2$, where $b^2 \equiv \Delta_1 \bmod p$ and $\bar{\rho} = (1 - b)/2 \in \mathbb{F}_p$. Thus in our case $(\Delta_1/p) = 1$ we have $\mathbb{F}_p[X]/(f(X)) \simeq \mathbb{F}_p[X]/(X - \rho) \otimes \mathbb{F}_p[X]/(X - \bar{\rho})$. In both cases ($\Delta_1$ even or odd) we have to compute a square root in $\mathbb{F}_p$ to find ρ and $\bar{\rho}$. This takes random polynomial time using the algorithm of Cipolla. More precisely we know from [1, Theorem 7.2.3, page 158] that this algorithm takes (expected) time $O(\log^3 p)$. In this case we have the map between $\alpha = a + b\omega \in (\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^*$ and $\psi(\alpha) = a + b\rho \in \mathbb{F}_p^*$. Finally one can easily show that this map is indeed a surjective homomorphism. □

Now we only have one more *minor* problem. The DLP in Definition 1 is formulated for reduced ideals in the standard representation such that $\mathfrak{a} = a\mathbb{Z} + \frac{b+\sqrt{\Delta_1}}{2}\mathbb{Z}$ in $Cl(\Delta_p)$. We have to convert this standard representation in $Cl(\Delta_p)$ to that in $\mathcal{P}_{\Delta_1}(p)/\mathcal{P}_{\Delta_1,\mathbb{Z}}(p)$ using Proposition 2. The following simple lemma indicates that we can efficiently switch to the desired generator-representation (and back).

Lemma 3. *Let* $\Delta_1 < 0$ *and* $\Delta_1 \equiv 0, 1 \bmod 4$ *such that* $h(\Delta_1) = 1$ *and* p *prime. Then*

1. *there is a deterministic algorithm which computes ideal* $\alpha\mathcal{O}_{\Delta_1} = \varphi^{-1}(\mathfrak{a}) \in \mathcal{P}_{\Delta_1}(p)$ *for a given reduced ideal* $\mathfrak{a} \in Cl(\Delta_p)$ *prime to* p *in* $O(\log^2 p)$ *bit operations and*
2. *there is a deterministic algorithm which computes reduced ideal* $\mathfrak{a}$ *which is equivalent to* $\varphi(\alpha\mathcal{O}_{\Delta_1}) \in Cl(\Delta_p)$ *for a given ideal* $\alpha\mathcal{O}_{\Delta_1} \in \mathcal{P}_{\Delta_1}(p)/\mathcal{P}_{\Delta_1,\mathbb{Z}}(p)$ *in* $O(\log^2 p)$ *bit operations.*

Proof. Note that algorithm φ and φ^{-1} can be computed in $O(\log^2 p)$ bit operations [26]. We denote by $\mathfrak{a} = a\mathbb{Z} + \frac{b+\sqrt{\Delta_q}}{2}\mathbb{Z}$ a reduced ideal in $Cl(\Delta_p)$.

From Proposition 1 all reduced ideals $\mathfrak{a} \in Cl(\Delta_p)$ prime to p are of the form $\mathfrak{a} = \varphi(\alpha\mathcal{O}_{\Delta_1})$ for some $\alpha \in \mathcal{O}_{\Delta_1}$. We can find the generator α by reducing $\varphi^{-1}(\mathfrak{a})$. Let $\mathfrak{A} = \varphi^{-1}(\mathfrak{a}) = A\mathbb{Z} + \frac{B+\sqrt{\Delta_1}}{2}\mathbb{Z}$. From [2] one can reduce ideal $\mathfrak{A}$ of $\mathcal{O}_{\Delta_1}$ and find element $\alpha \in \mathcal{O}_{\Delta_1}$ such that $\alpha\mathcal{O}_{\Delta_1} \sim \mathfrak{A}$ in $O((\log A)^2)$ bit operations. The norm of ideal $\mathfrak{a} \in Cl(\Delta_p)$ is a. Because $\mathfrak{a}$ is reduced we have $a < \sqrt{|\Delta_p|/3}$ and $a = O(p)$. Note that the norm a of ideals does not change while switching the orders by map φ, thus $A = a$ holds. Therefore one can compute the generator $\alpha\mathcal{O}_{\Delta_1} = \varphi^{-1}(\mathfrak{a})$ in $O(\log^2 p)$ bit operations. On the contrary, let $\mathfrak{A}$ be the standard representation of ideal $\alpha\mathcal{O}_{\Delta_1} \in \mathcal{P}_{\Delta_1}(p)/\mathcal{P}_{\Delta_1,\mathbb{Z}}(p)$. From [21] one can compute ideal $\mathfrak{A}$ in $O((\log \Delta_1)^2)$ bit operations. Then to compute the reduced ideal equivalent to $\varphi(\mathfrak{A})$ in $Cl(\Delta_p)$ requires map φ and one reduction algorithm, and they are in $O(\log^2 p)$ bit operations. This proofs the assertion of Lemma 3. □

Thus we are now able to put together our auxiliary lemma to prove the main result of this work.

Proof (Proof of Theorem 1). If one is given $\mathfrak{g}, \mathfrak{a}$ as given in Definition 1 to compute the discrete logarithm in the class group $Cl(\Delta_p)$ then one can compute the corresponding generators $\gamma, \alpha \in \mathcal{O}_{\Delta_1}$ such that $\gamma\mathcal{O}_{\Delta_1} = \varphi^{-1}(\mathfrak{g}), \alpha\mathcal{O}_{\Delta_1} = \varphi^{-1}(\mathfrak{a})$ by Lemma 1 and Lemma 3. Using the isomorphism ψ from Lemma 2 one can compute the corresponding elements $a = \psi(\alpha)$ and $g = \psi(\gamma)$ in the finite field $\mathbb{F}_p^*$ (if $(\Delta_1/p) = 1$) or $\mathbb{F}_{p^2}^*$ (if $(\Delta_1/p) = -1$) respectively. Then one is able to compute the discrete logarithm there or determine that it does not exist. It is clear that the entire reduction does only take (expected) $O(\log^3 p)$ bit operations. □

5 Conclusion

In this work we have shown that the discrete logarithm problem in the class group $Cl(\Delta_p)$ of a *totally* non-maximal imaginary quadratic order can be reduced to the discrete logarithm problem in finite fields using (expected) $O(\log^3 p)$ bit-operations. This result clearly implies that the formerly proposed bitlength of 800 for Δ_p does *not* provide sufficient security, because one could simply compute discrete logarithms in $\mathbb{F}_{p^k}^*$, where $k \in \{1, 2\}$ which should be possible in the near future if $p \approx 2^{400}$. The algorithm which is used in $\mathbb{F}_{p^k}^*$ is the number field sieve with $L[\frac{1}{3}]$. This would imply that p (at least in the case that $(\Delta_1/p) = 1$) should be about 1024 bit to yield (expected) long term security. Hence cryptosystems based on totally non-maximal imaginary quadratic orders seem to lose much of their attractiveness.

Analogous to the situation for Elliptic Curves, where the DLP in supersingular curves can efficiently be solved in finite fields with small extension degree, we discovered that there is also a *weak class for class groups* of imaginary quadratic orders. It remains an open question whether it is possible to find an $L[\frac{1}{3}]$ algorithm to compute discrete logarithms in arbitrary class groups. Another

interesting question is whether these results have any relevance to the elliptic curves discrete logarithm problem for elliptic curves whose endomorphism ring is a *totally non-maximal* order. These issues will be subject of further research. To avoid miss-interpretation of these result it should be noted that non-maximal orders, such as those applied in [19,26], where the factorization of Δ_p is kept secret, are *not effected* by this result.

References

1. E. Bach, J. Shallit: *Algorithmic number theory*, vol. 1 - Efficient Algorithms, Foundations of computing, MIT press, ISBN 0-262-02405-5, (1996) 228
2. I. Biehl and J. Buchmann: "An analysis of the reduction algorithms for binary quadratic forms," Voronoi's Impact on Modern Science, vol. **1**, Institute of Mathematics of National Academy of Sciences, Kyiv, Ukraine, (1998) 229
3. I. Biehl, S. Paulus and T. Takagi: "An efficient undeniable signature scheme based on non-maximal imaginary quadratic orders," Proceedings of Mathematics of Public Key Cryptography, Toronto, (1999) 223
4. R. Brent: *ECM champs*, ftp.comlab.ox.ac.uk/pub/Documents/techpapers/Richard.Brent/champs.ecm 223
5. J. Buchmann and S. Düllmann: "On the computation of discrete logarithms in class groups," Advances in Cryptology - CRYPTO '90, Springer, LNCS 773, (1991), pp.134-139 222
6. J. Buchmann, S. Düllmann, and H.C. Williams: "On the complexity and efficiency of a new key exchange system," Advances in Cryptology - EUROCRYPT '89, Springer, LNCS 434, (1990), pp.597-616 222
7. Z.I. Borevich and I.R. Shafarevich: *Number Theory*, Academic Press, New York, (1966) 224
8. J. Buchmann and H.C. Williams: "A key-exchange system based on imaginary quadratic fields," Journal of Cryptology, **1**, (1988), pp.107-118 219, 220, 221
9. J. Cowie, B. Dodson, M. Elkenbracht-Huizing, A.K. Lenstra, P.L. Montgomery and J. Zayer: "A worldwide number field sieve factoring record: on to 512 bits," Advances in Cryptology - ASIACRYPT'96, Springer, LNCS 1163, (1996), pp.382-394 222
10. H. Cohen: *A Course in Computational Algebraic Number Theory*. Graduate Texts in Mathematics **138**. Springer: Berlin, (1993) 224, 225
11. D. Coppersmith, A.M. Odlyzko and R. Schroeppel: "Discrete logarithms in $GF(p)$," Algorithmica, **1**, (1986), pp.1-15 222
12. D.A. Cox: *Primes of the form* $x^2 + ny^2$, John Wiley & Sons, New York, (1989) 224, 225, 226, 227
13. W. Diffie and M. Hellman: "New directions in cryptography," IEEE Transactions on Information Theory **22**, (1976), pp.472-492 222
14. S. Düllmann: *Ein Algorithmus zur Bestimmung der Klassenzahl positiv definiter binärer quadratischer Formen*, PHD-thesis, University of Saarbrücken, (1991)
15. D.M. Gordon: "Discrete logarithms in $GF(p)$ using the number field sieve," SIAM Journal on Discrete Mathematics, **6**, (1993), pp.124-138 222
16. J.L. Hafner and K.S. McCurley: "A rigorous subexponential algorithm for computation of class groups," Journal of the American Mathematical Society, **2**, (1989), pp.837-850 219, 220, 222
17. L.K. Hua: *Introduction to Number Theory*. Springer-Verlag, New York, (1982)

18. M. Hartmann, S. Paulus and T. Takagi: "NICE - New Ideal Coset Encryption -," to appear in Workshop on Cryptographic Hardware and Embedded Systems.
19. D. Hühnlein, M.J. Jacobson, S. Paulus and T. Takagi: "A cryptosystem based on non-maximal imaginary quadratic orders with fast decryption," Advances in Cryptology - EUROCRYPT'98, LNCS 1403, Springer, (1998), pp.294-307 222, 223, 224, 225, 230
20. D. Hühnlein, A. Meyer and T. Takagi: "Rabin and RSA analogues based on non-maximal imaginary quadratic orders," Proceedings of ICICS '98, ISBN 89-85305-14-X, (1998), pp.221-240 223
21. D. Hühnlein: "Efficient implementation of cryptosystems based on non-maximal imaginary quadratic orders," T.R. TI-6, Technische Universtät Darmstadt, (1999), available at http://www.informatik.tu-darmstadt.de/TI/Veroeffentlichung/TR/Welcome.html#1999 219, 220, 223, 226, 229
22. M.J. Jacobson Jr.: *Subexponential Class Group Computation in Quadratic Orders*, PhD thesis, Technische Universtät Darmstadt, to appear, (1999) 222
23. H.W. Lenstra: "On the computation of regulators and class numbers of quadratic fields," London Math. Soc. Lecture Notes, **56**, (1982), pp.123-150 221
24. A.K. Lenstra and H.W. Lenstra Jr. (eds.): *The development of the number field sieve*, Lecture Notes in Mathematics, Springer, (1993) 222
25. National Institute of Standards and Technology (NIST): Digital Signature Standard (DSS). Federal Information Processing Standards Publication 186, **FIPS-186**, 19th May, (1994) 222
26. S. Paulus and T. Takagi: "A new public-key cryptosystem over the quadratic order with quadratic decryption time," to appear in Journal of Cryptology. 220, 222, 228, 230
27. H.J.J. te Riele: Factorization of RSA-140 with the Number Field Sieve, posting in sci.crypt.research, February (1999) 222
28. R. Rivest, A. Shamir and L. Adleman: "A method for obtaining digital signatures and public key-cryptosystems," Communications of the ACM,**21**, (1978), pp.120-126 222
29. R.D. Silverman: "The multiple polynomial quadratic sieve," Math. Comp. **48**, (1987), pp.329-229 222
30. R.J. Schoof: "Quadratic Fields and Factorization," *Computational Methods in Number Theory*. Math. Centrum Tracts **155**. Part II. Amsterdam, (1983), pp.235-286. 221
31. D. Weber: "Computing discrete logarithms with quadratic number rings," Advances in Cryptology - EUROCRYPT '98, LNCS **1403**, Springer, 1998, pp. 171-183 222