An efficient NICE-Schnorr-type signature scheme

Detlef Hühnlein and Johannes Merkle

secunet Security Networks AG
Mergenthalerallee 77-81
D-65760 Eschborn, Germany
{huehnlein,merkle}@secunet.de

Abstract. Recently there was proposed a novel public key cryptosystem [17] based on non-maximal imaginary quadratic orders with *quadratic decryption time*. This scheme was later on called NICE for **N**ew **I**deal **C**oset **E**ncryption [6]. First implementations show that the decryption is as efficient as RSA-encryption with $e = 2^{16} + 1$. It was an open question whether it is possible to construct comparably efficient signature schemes based on non-maximal imaginary quadratic orders. The major drawbacks of the ElGamal-type [7] and RSA/Rabin-type signature schemes [8] proposed so far are the *slow signature generation* and the *very inefficient system setup*, which involves the computation of the class number $h(\Delta_1)$ of the maximal order with a subexponential time algorithm. To avoid this tedious computation it was proposed to use *totally* non-maximal orders, where $h(\Delta_1) = 1$, to set up DSA analogues. Very recently however it was shown in [10], that the discrete logarithm problem in this case can be reduced to finite fields and hence there seems to be no advantage in using DSA analogues based on totally non-maximal orders.

In this work we will introduce an efficient NICE-Schnorr-type signature scheme based on conventional non-maximal imaginary quadratic orders which solves both above problems. It gets its strength from the difficulty of *factoring* the discriminant $\Delta_p = -rp^2$, r, p prime. To avoid the computation of $h(\Delta_1)$, our proposed signature scheme only operates in (a subgroup of) the kernel of the map ϕ_{Cl}^{-1}, which allows to switch from the class group of the non-maximal order to the maximal order. Note that a similar setup is used in NICE. For an efficient signature generation one may use the novel arithmetic [9] for elements of $\mathrm{Ker}(\phi_{Cl}^{-1})$. While the signature generation using this arithmetic is already slightly faster than in the original scheme, we will show in this work that we can even do better by applying the Chinese Remainder Theorem for $(\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^*$. First implementations show that the signature generation of our scheme is *more than twice as fast* as in the original scheme in $\mathbb{F}_p^*$, which makes it very attractive for practical applications.

1 Introduction

Since nobody can guarantee that currently used cryptosystems based on the difficulty of factoring or the computation of discrete logarithms in some group stay secure forever it is important to consider different primitives and groups for the construction of cryptosystems. On the other hand the continously growing popularity of cryptosystems based on elliptic curves emphasize that certain mathematical structures seem to allow more efficient implementation for the same conjectured level of security.

Another recently proposed mathematical structure which allows the construction of very efficient cryptosystems are *non-maximal imaginary quadratic orders*. For a recent survey of cryptosystems based on quadratic orders we refer to the forthcoming [11]. For example it was shown in [17] that there is a public key cryptosystem which has *quadratic decryption time*. To our knowledge this is the only scheme having this property. First implementations show that the *de*cryption is about as efficient as the *en*cryption with RSA with $e = 2^{16} + 1$. Note that this a very important feature, as the decryption often takes place in a device with limited computational power, such as a smart card. It was an open question whether there is also an efficient signature scheme based these non-maximal imaginary quadratic orders. All currently proposed signature schemes based on this structure have different drawbacks: The signature generation of the ElGamal analogue [7] and the RSA/Rabin analogues [8] based on conventional non-maximal orders is fairly inefficient. In fact, except from the Rabin-analogue, one uses the particular structure of the *non-maximal* order only to *set up* the system. The signature generation itself has to be performed in the public non-maximal order, which does not allow very efficient computation. For the system setup one has to compute the class number $h(\Delta_1)$ of the maximal order, where $|\Delta_1| > 2^{200}$ to prevent Δ_p from being factored using the Elliptic Curve Method (ECM). The computation of $h(\Delta_1)$ is done with an analogue of the quadratic sieve with subexponential running time and hence is very inefficient. To avoid this computation it was proposed in [8] to use totally non-maximal orders, where $h(\Delta_1) = 1$. Using the recently developed exponentiation technique [9] one is able to implement DSA analogues in these totally non-maximal orders almost as efficiently as conventional DSA in $\mathbb{F}_p^*$ for the same *conjectured* level of security. However, even more recently, it was shown in [10] that discrete logarithms in the class group of *totally* non-maximal imaginary quadratic orders $Cl(\Delta_p)$ can be reduced to discrete logarithms in finite fields and hence there seems to be no advantage in using this DSA analogue.

In this work we will introduce an efficient NICE-Schnorr-type signature scheme based on non-maximal imaginary quadratic orders which solves both above problems:

At first the *system-setup* is very fast, because we do not have to compute the class number of the maximal order $h(\Delta_1)$, but only compute in (a subgroup of) the *kernel* of ϕ_{Cl}^{-1} instead, which cardinality is known in advance. This is a similar situation as for the NICE cryptosystem. As noted in [17], the restriction

to elements of the kernel does not seem to introduce any weakness as long as the conductor p is kept secret and hence our scheme is based on the difficulty of factoring $\Delta_p = \Delta_1 p^2$.

Second the *signature generation* of our proposed scheme is also very fast. To perform the exponentiation of a generator $\mathfrak{g}$ of a 160 bit subgroup of order q of $\mathrm{Ker}(\phi_{Cl}^{-1})$ one can use the recently developed arithmetic [9], which is about *twenty* times as fast as standard ideal arithmetic. This arithmetic allows the signer to replace the fairly inefficient ideal arithmetic in the non-maximal order by computations in $(\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^*$.

In this work we will show that one can even do better by application of the Chinese Remainder Theorem for $(\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^*$. If $\left(\frac{\Delta_1}{p}\right) = 1$ then there is an isomorphism $(\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^* \simeq \mathbb{F}_p^* \otimes \mathbb{F}_p^*$. Thus the signature generation in our scheme essentially consists of two exponentiations in $\mathbb{F}_p^*$. Considering the best algortihms (NFS and ECM) it is reasonable to assume that factoring $\Delta_p = -rp^2$, $p, r \approx 2^{340}$ prime, is "about as hard" as computing discrete logarithms in $\mathbb{F}_{p'}^*$ with p' about 1000 bits. Note that while it is *conjectured* that factoring numbers of the form rp^2 is considerably easier than factoring $n = pq$ there is only an ECM-variant [18] known which is able to make use of this special structure and if $r, p > 2^{240}$ this method is clearly infeasible. Thus the bitlength of the modulus p in our exponentiations is only *about one third* of the bitlength of the modulus in the original Schnorr scheme. Hence we end up with a signature generation which is *more than twice as fast* as for the original Schnorr scheme [20], which in turn is much faster than that of RSA for example.

Note that for possible Schnorr analogues working in subgroups of $(\mathbb{Z}/n\mathbb{Z})^*$ for composite n, one needs to be *very careful* as pointed out in [14]. This issue and the *entirely different* situation here is discussed in Section 4.

The paper is organized as follows: Section 2 will provide the necessary background and notations of non-maximal imaginary quadratic orders used in this work. In Section 3 we will explain the proposed signature scheme. In Section 4 we will consider the security of our scheme. In Section 5 we will introduce the novel exponentiation technique using CRT in $(\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^*$ and give timings of a first implementation. This will show that the signature generation of our scheme is more than twice as fast in the original Schnorr scheme, which makes our scheme very attractive for practical application.

2 Necessary preliminaries and notations of imaginary quadratic orders

The basic notions of imaginary quadratic number fields may be found in [2, 3]. For a more comprehensive treatment of the relationship between maximal and non-maximal orders we refer to [4, 7, 9, 10].

Let $\Delta \equiv 0,1 \pmod 4$ 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

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

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 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 $\mathcal{O}_\Delta$, are 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 $\mathcal{O}_\Delta$. Algorithms for the group operation (multiplication and reduction of ideals) can be found in [3]. The order of the class group is called the *class number* of $\mathcal{O}_\Delta$ and is denoted by $h(\Delta)$.

Our cryptosystem makes use of the relation between the maximal and non-maximal orders. Any non-maximal order may be represented as $\mathcal{O}_{\Delta_p} = \mathbb{Z} + p\mathcal{O}_{\Delta_1}$. If $h(\Delta) = 1$ then $\mathcal{O}_{\Delta_p}$ is called a *totally non-maximal* imaginary quadratic order of conductor p. 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. In every class there is an ideal which is prime to any given number. The algorithm FindIdealPrimeTo in [7] will compute such an ideal. If we denote the (principal) $\mathcal{O}_{\Delta_p}$-ideals, which are prime to p by $\mathcal{P}_{\Delta_p}(p)$ and $\mathcal{I}_{\Delta_p}(p)$ respectively then there

is an isomorphism

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

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 $\mathcal{I}_{\Delta_1}(p) \tilde{\to} \mathcal{I}_{\Delta_p}(p)$. The inverse of this map is $\varphi^{-1} : \mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_{\Delta_1}$.*

Proof: See [4, Proposition 7.20, page 144] . □

Thus we are able to switch to and from the maximal order. 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 [7].

It is important to note that the isomorphism φ is between the ideal groups $\mathcal{I}_{\Delta_1}(p)$ and $\mathcal{I}_{\Delta_p}(p)$ and *not the class groups.*

If, for $\mathfrak{A}, \mathfrak{B} \in \mathcal{I}_{\Delta_1}(p)$ 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}. More precisely we have the following:

Proposition 2. *The isomorphism φ^{-1} induces a* surjective homomorphism $\phi_{Cl}^{-1} : Cl(\Delta_p) \to Cl(\Delta_1)$, *where $\mathfrak{a} \mapsto \rho_1(\varphi^{-1}(\mathfrak{a}))$.*

Proof: This immediately follows from the short exact sequence:

$$Cl(\Delta_p) \longrightarrow Cl(\Delta_1) \longrightarrow 1$$

(see [16, Theorem 12.9, p. 82]). □

In the following we will study the kernel $\mathrm{Ker}(\phi_{Cl}^{-1})$ of the above map ϕ_{Cl}^{-1} and hence the relation between a class in the maximal order and the associated classes in the non-maximal order in more detail. We start with yet another interpretation of the class group $Cl(\Delta_p)$.

Proposition 3. *Let $\mathcal{O}_{\Delta_p}$ be an order of conductor p in a quadratic field. Then there are natural isomorphisms*

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

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 $\alpha \equiv a \pmod{p\mathcal{O}_{\Delta_1}}$ for some $a \in \mathbb{Z}$ such that $gcd(a,p) = 1$.

Proof: See [4, Proposition 7.22, page 145]. □

The following corollary is an immediate consequence.

Corollary 1. *With notations as above we have the following isomorphism*

$$\mathrm{Ker}(\phi_{Cl}^{-1}) \simeq {}^{\mathcal{P}_{\Delta_1}(f)}\Big/_{\mathcal{P}_{\Delta_1,\mathbb{Z}}(f)}.$$

The next result explains the relation between $\mathrm{Ker}(\phi_{Cl}^{-1})$ and $(\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^*$.

Proposition 4. *The map $(\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^* \to \mathrm{Ker}(\phi_{Cl}^{-1})$, where $\alpha \mapsto \varphi(\alpha\mathcal{O}_{\Delta_1})$ is a surjective homomorphism.*

Proof: This is shown in the more comprehensive proof of Theorem 7.24 in [4] (page 147). □

Thus one may reduce the arithmetic in $\mathrm{Ker}(\phi_{Cl}^{-1})$ to more efficient computation in $(\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^*$. This is precisely what was proposed in [9]. Using the naive "generator-arithmetic" as introduced there one is able to perform an exponentiation in $\mathrm{Ker}(\phi_{Cl}^{-1})$ about twenty times as fast as by using standard ideal arithmetic. In Section 5 we will show that one can even do much better by applying the CRT in $(\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^*$.

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

Proposition 5. *Let $\Delta_1 < -4$, $\Delta_1 \equiv 0, 1 \pmod 4$ and p prime. Then $h(\Delta_p) = h(\Delta_1)\left(p - \left(\frac{\Delta_1}{p}\right)\right)$ and $\left|\mathrm{Ker}(\phi_{Cl}^{-1})\right| = \left(p - \left(\frac{\Delta_1}{p}\right)\right)$, where $\left(\frac{\Delta_1}{p}\right)$ is the Kronecker-symbol.*

Proof: Because $\mathcal{O}^*_{\Delta_1} = \mathcal{O}^*_{\Delta_p} = \{\pm 1\}$, for $\Delta_p = \Delta_1 p^2$, p prime and $\Delta_1 < -4$ this is an immediate corollary [4, Theorem 7.24, page 146]. □

Thus we are able to control the order of the kernel and consequently set up a Schnorr analogue using the group $\mathrm{Ker}(\phi_{Cl}^{-1})$ instead of $\mathbb{F}_p^*$.

3 The new signature scheme

In this section we will show how one can set up a NICE-Schnorr-type signature scheme using $\mathrm{Ker}(\phi_{Cl}^{-1})$ instead of $\mathbb{F}_p^*$.

The *system setup* for Alice consists of the following steps:

1. Choose a random prime r and set $\Delta_1 = -r$ if $r \equiv 3 \pmod 4$ or $\Delta = -4r$ otherwise.
2. Choose a random prime q, which will later on serve as the order of the used subgroup of $\mathrm{Ker}(\phi_{Cl}^{-1}) \subset Cl(\Delta_p)$.
3. Choose a random prime p, such that $\left(\frac{\Delta_1}{p}\right) = 1, q|(p-1)$ and set $\Delta_p = \Delta_1 p^2$.
4. Choose a random $\alpha = x + y\omega$ such that $\varphi(\alpha\mathcal{O}_{\Delta_1})$ is of order q in $Cl(\Delta_p)$. This may be done by choosing a random $\beta = x' + y'\omega$ and computing $\alpha = \beta^{(p-1)/q}$ until $\mathfrak{g} = \rho_p(\varphi(\alpha\mathcal{O}_{\Delta_1})) \neq \mathcal{O}_{\Delta_1}$ using the algorithm Gen-Exp from [9] or the more efficient CRT variant introduced in Section 5.
5. Choose a random integer $a < q$ and compute the public key $\mathfrak{a} = \rho_p(\mathfrak{g}^a)$.
6. The secret key of Alice is the triple x, y, a.

Note that Alice will keep secret p, q, r, x, y, a and only publishes $\Delta_p, \mathfrak{g}, \mathfrak{a}$. Now the signature generation and verification procedure is analogous to the original Schnorr-scheme [20]. The only difference is that Alice may speed up the signature generation process by using the knowledge of $\alpha = x + y\omega$ and performing the computation in $(\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^*$ instead of using the fairly inefficient ideal arithmetic.

More precisely Alice performs the following steps to sign a message $m \in \mathbb{Z}$:

1. Choose a random integer $1 < k < q$ and compute $\mathfrak{k} =$Gen-CRT(x, y, p, k), where the algorithm Gen-CRT() is given in Section 5.
2. Compute $e = h(m||\mathfrak{k})$ and $s \equiv ae + k \ mod\, q$.
3. Alice's signature for m is the pair (e, s).

The verification is completely analogous to the original scheme [20] using standard ideal arithmetic (see e.g. [3]) in the *non-maximal* order:

1. Compute $\mathfrak{v} = \rho_p(\mathfrak{g}^s\mathfrak{a}^{-e})$ and $e' = h(m||\mathfrak{v})$.
2. The signature is valid if and only if $e' = e$.

It is clear that the verification works if the signature was generated by Alice, because $\mathfrak{v} \sim \mathfrak{g}^s\mathfrak{a}^{-e} \sim \mathfrak{g}^s\mathfrak{g}^{-ae} \sim \mathfrak{g}^k \sim \mathfrak{k}$. Thus $h(m||\mathfrak{k}) = h(m||\mathfrak{v})$ and hence $e' = e$.

While the procedures for signature generation and verification are completely analogous to the original scheme there is a big difference in the overall scheme which has to be considered more closely. Our scheme is (beside other difficulties which are explained below) based on the intractability of factoring Δ_p. In step 2. the s-part of of the signature is unique modulo q, which is kept secret. Thus by collecting a lot of signatures with different s's one may hope to learn the magnitude of q, which divides $p - 1$. This information *might* be useful to factor Δ_p. In the next section however we will show that such an attack is no real threat.

4 Security issues of the proposed scheme

In this section we will discuss the security and appropriate parameter sizes of our proposed scheme. As it relies on the difficulty of computing discrete logarithms in (a subgroup of) the kernel of ϕ_{Cl}^{-1} we will start with relating this problem to more conventional problems such as factoring and computing logarithms in finite fields.

The following result shows that "in practice" the DL-problem in $\mathrm{Ker}(\phi_{Cl}^{-1})$ is "about as hard" as factoring Δ_p.

Theorem 1. *With notations as in the previous section we have the following two probabilistic polynomial time reductions:*

1. *Factoring the discriminant Δ_p can be reduced to the DL-problem in* $\mathrm{Ker}(\phi_{Cl}^{-1})$.
2. *If the factorization of $\Delta_p = \Delta_1 p^2$ is known, then one can reduce the DL-problem in* $\mathrm{Ker}(\phi_{Cl}^{-1})$ *to the DL-problem in $\mathbb{F}_p^*$.*

Proof:(Sketch) To show 1. we assume that some oracle is able to compute discrete logarithms in $\mathrm{Ker}(\phi_{Cl}^{-1})$. That is given a fixed generator $\mathfrak{g}$ of $\mathrm{Ker}(\phi_{Cl}^{-1})$ it returns on input of some element $\mathfrak{g}^e \in \mathrm{Ker}(\phi_{Cl}^{-1})$ the smallest possible exponent e. It is easy to see that this oracle can be used to determine $|\mathrm{Ker}(\phi_{Cl}^{-1})| = p \pm 1$, where the '+' occurs for our concrete setup. This is done by choosing some e' and handing over $\mathfrak{g}^{e'}$ to the oracle. Then $e' > |\mathrm{Ker}(\phi_{Cl}^{-1})|$ implies that $e' > e$ and then $e' - e = k|\mathrm{Ker}(\phi_{Cl}^{-1})|$ for some integer k. If we repeat this step multiple times then the gcd of the obtained differences will be $|\mathrm{Ker}(\phi_{Cl}^{-1})|$ with high probability. The reduction 2. is shown in [10]. □

Note that as in the original Schnorr-setup our scheme operates in a *subgroup* of the kernel. While it is not rigorously proven it is commonly assumed that the DL-problem in the subgroup is indeed as hard as the "full" DL-problem. Thus the assumption that the DL-problem in a subgroup of $\mathrm{Ker}(\phi_{Cl}^{-1})$ is computational equivalent to the DL-problem in $\mathrm{Ker}(\phi_{Cl}^{-1})$ itself is denoted by (subgroup-DL).

If we furthermore assume that our hash function acts like a random oracle [1], denoted by (ROM), then it is easy to prove the following result in complete analogy to [19, Theorem 5]:

Theorem 2. *Assume (ROM). If an existential forgery of the NICE-Schnorr signature scheme, under an adaptively chosen message attack, has non-negligible probability of success, then the discrete logarithm in subgroups of* $\mathrm{Ker}(\phi_{Cl}^{-1})$ *can be solved in polynomial time.*

Thus we may combine the above results to obtain the following:

Corollary 2. *Assume (ROM) and (subgroup-DL). Furthermore assume that one is able to compute discrete logarithms in $\mathbb{F}_p^*$, which is feasible for the proposed parameter sizes. Then forging of signatures in our NICE-Schnorr-scheme is equivalent to factoring $\Delta_p = \Delta_1 p^2$.*

Thus our scheme is secure as long as we choose the parameters as follows:

- That one cannot compute discrete logarithms in $Cl(\Delta_p) \supset \mathrm{Ker}(\phi_{Cl}^{-1})$ using a subexponential algorithm [12] we require $\Delta_p > 2^{400}$.
- That one cannot use a generic technique to compute discrete logarithms in the subgroup of the kernel, such as Pollard's ρ-method, we require $q > 2^{160}$.
- If one is able to factor Δ_p then one can reduce the discrete logarithm problem in the kernel to the discrete logarithm problem in $\mathbb{F}_p^*$ using the recent reduction from [10]. Thus we need to ensure that Δ_p cannot be factored. With current algorithms (NFS and optimized ECM [18]) this should be impossible if we require $\Delta_p > 2^{720}$ and $p, r > 2^{240}$.
- As we do not disclose q, where $q|(p-1)$, we need to take care that the knowledge of many signatures does not help to find q, and hence breaking the scheme by factoring Δ_p, easier.

In the following we will discuss the potential threat of estimating q with the knowledge of many signatures more thoroughly. We will only sketch the main ideas here.

Estimating q by the maximal value of s

It is clear that $q|(p-1)$ and our scheme can be easily broken if $\Delta_p = \Delta_1 p^2$ is factored, because in this case one uses the result of [10] and is just faced with the computation of discrete logarithms in $\mathbb{F}_p^*$, which is possible for the proposed size of p. While it is not clear at the moment whether knowledge of q will immediately imply the knowledge of p, we will show that collecting signatures and taking care of the maximum s-value does not even help to come very close to q.

Since for all signatures (e_i, s_i) it holds that $s_i \in [0, q-1]$ an attacker could try to estimate q by the $\max_i(s_i)$ and then to use this gained information to factor Δ_p. The following argument shows that with overwhelming probability $\max_i(s_i)$ is not close enough to q.

Since h is a strong hash function we may assume that $e = h(m||\mathfrak{k})$ and k are not significantly correlated for randomly chosen m and k. For simplicity we assume that e and k are statistically independent. Then $s \equiv ae + k \bmod q$ is uniform distributed in $[0, q-1]$. Therefore, for fixed $0 \leq \alpha \leq 1$ and for randomly chosen messages $m_1, \ldots, m_n$ and randomly chosen $k_1, \ldots, k_n$ with probability α^n the inequality $s_i \leq \alpha(q-1)$ holds for all $i \leq n$. Thus for $n \ll m$ the probability that $s_i \leq (1 - 1/m)q$ holds for all $i \leq n$ is approximately $(1 - n/m)$.

If we assume that the number n of signatures is limited by 2^{20} we can estimate that for all, say $\ell > 20$ at most with probablity $2^{20-\ell}$ there is an $i \leq n$ with $s_i > (1 - 2^{-\ell})q$. On the other hand if $q \approx 2^{160}$ an attacker using the estimation

$$\max_i(s_i) \leq \alpha q \tag{4}$$

with $\alpha < (1 - 2^{-\ell})$ still has a search space of $2^{-\ell}\max_i(s_i) \approx 2^{160-\ell}$ many possible values q satisfying (4). Now if we assume that the time needed for finding q is about the square root of the size of the search space (i.e. $2^{80-\ell/2}$) we can estimate

the expected workload of this attack by $2^{80-\ell/2}/2^{20-\ell} = 2^{60+\ell/2} > 2^{70}$ which would be a formidable task. Note that to our knowledge there is no way to use that q is prime if one applies a "square root" algorithm such as Pollard-ρ to determine q.

Security problem of Schnorr-analogue in prime order subgroups of $(\mathbb{Z}/n\mathbb{Z})^*$ - Immunity of our scheme

The main practical advantage of our proposed scheme compared to the original one is its very efficient signature generation due to application of CRT for $(\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^*$. Thus one may think about a Schnorr-analogue operating in a prime order subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$ rather than $\mathbb{F}_p^*$, which would allow the same speedup by using CRT for $(\mathbb{Z}/n\mathbb{Z})^*$ in this case.

However we will briefly show in the following that, in contrary to our scheme, the breaking of such an analogue in $(\mathbb{Z}/n\mathbb{Z})^*$, is surprisingly easy.

Let $n = p_1p_2$, p_1, p_2 prime and g be of order q in $(\mathbb{Z}/n\mathbb{Z})^*$, where q is prime. Because, $g^q \equiv 1 \pmod{n}$ we know by the CRT that $g^q \equiv 1 \pmod{p_1}$ and $g^q \equiv 1 \pmod{p_2}$. Thus it is clear that q must divide at least one of the numbers $p_1 - 1$ or $p_2 - 1$. W.l.o.g. we may assume that

$$q|(p_1 - 1) \tag{5}$$

Now there are two different cases to consider:

1. $q \not| (p_2 - 1)$:
   Because g is of order q in $(\mathbb{Z}/n\mathbb{Z})^*$ (and by (5) also in $\mathbb{F}_{p_1}^*$), we have $g \not\equiv 1 \pmod{p_1}$.
   But $g^q \equiv 1 \pmod{p_2}$ together with $q \not| (p_2 - 1)$ and the primeness of q implies that $g \equiv 1 \pmod{p_2}$ and hence $g - 1 = p_2k$ for some integer k. Thus n is easily factored by computing $p_2 = \gcd(g - 1, n)$. Note that in this case one does not even need to know q and this case is very likely if p_2 is chosen randomly.
2. $q|(p_2 - 1)$:
   In this case the scheme is similar to [5] and as shown in [14] is not immediately broken, but factoring n is made much easier, if one knows q.
   We have $n = (2qp_1' + 1)(2qp_2' + 1)$, for some (in the worst case prime) numbers p_1', p_2'.
   Then by [14, Proposition 2] one can factor n in $O(\frac{p_1' + p_2'}{q})$ steps. Thus if p_1', p_2', q are the same order of magnitude this is a trivial task. Hence one must take great care, when working with subgroups of $(\mathbb{Z}/n\mathbb{Z})^*$.

The situation for our proposed scheme in $\mathrm{Ker}(\phi_{Cl}^{-1}) \subset Cl(\Delta_p)$ is *entirely different*, because there is *no* gcd-*analogue* known for imaginary quadratic class groups, which could be applied to mount an "attack" like explained in the first situation above. Note that the existence of such a gcd-analogue would also imply the insecurity of NICE. The situation that $q|h(\Delta_1)$, which corresponds to the second situation above, is *very unlikely* if q, Δ_1 are chosen at random.

5 More efficient exponentiation using CRT in $(\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^*$ and timings

In Section 2 and [9] we saw that the arithmetic in $\mathrm{Ker}(\phi_{Cl}^{-1})$ can be reduced to arithmetic in $(\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^*$, which is much more efficient. In this section we will introduce a method which again speeds up the signing process considerably.

We will start with an auxilliary result.

Lemma 1. *Let $\mathcal{O}_{\Delta_1}$ be the maximal order and p be prime. Then there is an isomorphism between rings*

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

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

$$f(X) = \begin{cases} X^2 - \frac{\Delta_1}{4}, & \text{if } \Delta_1 \equiv 0 \pmod 4, \\ X^2 - X + \frac{1-\Delta_1}{4}, & \text{if } \Delta_1 \equiv 1 \pmod 4. \end{cases} \tag{6}$$

Proof: See [10, Proposition 5]. □

This isomorphism between rings clearly implies an isomorphism between the multiplicative groups and with a little more effort we can show the central result of this section.

Theorem 3. *Assume that $\left(\frac{\Delta_1}{p}\right) = 1$ and the roots $\rho, \bar{\rho} \in \overline{\mathbb{F}}_p$ of $f(X) \in \mathbb{F}_p[X]$ as given in* (6) are known. Then the following isomorphism can be computed in time $O((\log p)^2)$:

$$(\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^* \simeq \mathbb{F}_p^* \otimes \mathbb{F}_p^*$$

Proof: From Lemma 1 we know that there is an isomorphic map $(\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^* \to \mathbb{F}_p[X]/(f(X))^*$, where $f(X) \in \mathbb{F}_p[X]$ is given in (6). And that this isomorphism is trivial to compute.

Because $\left(\frac{\Delta_1}{p}\right) = 1$ 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 $\rho, \bar{\rho} \in \mathbb{F}_p$ are the roots of $f(X)$. Thus if $\Delta_1 \equiv 0 \pmod 4$ and $D = \Delta_1/4$ we have $\rho \in \mathbb{F}_p$ such that $\rho^2 \equiv D \pmod p$ and $\bar{\rho} = -\rho$. In the other case $\Delta_1 \equiv 1 \pmod 4$ we have $\rho = (1 + b)/2$, where $b^2 \equiv \Delta_1 \pmod p$ and $\bar{\rho} = (1 - b)/2 \in \mathbb{F}_p$. Thus we have the isomorphisms

$$(\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^* \simeq \left({\mathbb{F}_p[X]}\Big/{(X - \rho)}\right)^* \otimes \left({\mathbb{F}_p[X]}\Big/{(X - \bar{\rho})}\right)^* \simeq \mathbb{F}_p^* \otimes \mathbb{F}_p^*.$$

Let $\alpha = a + b\omega \in (\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^*$ then the mapping $\psi : (\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^* \to \mathbb{F}_p^* \otimes \mathbb{F}_p^*$ is given as $x_1 = \psi_1(\alpha) = a + b\rho \in \mathbb{F}_p^*$ and $x_2 = \psi_2(\alpha) = a + b\bar{\rho} \in \mathbb{F}_p^*$. The inverse map ψ^{-1} is computed by solving the small system of linear equations.

I.e. one will recover $a, b \in \mathbb{F}_p^*$ by computing $b = \frac{x_2 - x_1}{\bar{\rho} - \rho}$ and $a = x_1 - b\rho$. Thus both transformations ψ and ψ^{-1} need time $O((\log p)^2)$. □

With this result we immediately obtain the of the following algorithm.

Algorithm 4 *(Gen-CRT)*

Input: $\alpha = x + y\omega \in \mathcal{O}_{\Delta_1}$, *the conductor* p, *such that* $\gcd(\mathcal{N}(\alpha), p) = 1$, $\left(\frac{\Delta_1}{p}\right) = 1$, *the roots* $\rho, \bar{\rho} \in \mathbb{F}_p^*$ *of* $f(X)$ *as given in (6) and the exponent* $n \in \mathbb{Z}$.

Output: $\mathfrak{a} = (a, b) = \rho_p(\varphi((\alpha\mathcal{O}_{\Delta_1})^n))$.

1. *IF* $n = 0$ *THEN OUTPUT*$(1, \Delta_1 \pmod 2)$
2. *IF* $n < 0$ *THEN* $n \leftarrow -n$, $y \leftarrow -y$
3. $x_1 \leftarrow (x + \rho y)^n \pmod p$
4. $x_2 \leftarrow (x + \bar{\rho} y)^n \pmod p$
5. $r \leftarrow (\bar{\rho} - \rho)^{-1} \pmod p$
6. $y_h \leftarrow (x_2 - x_1) r \pmod p$
7. $x_h \leftarrow x_1 - y_h \rho \pmod p$
8. /* *Compute the standard representation* $\mathfrak{A} = d(a, b) = \alpha_h \mathcal{O}_{\Delta_1}$ */
   - 8.1 /* *Use* $\frac{x + y\sqrt{\Delta_1}}{2}$*-form* */
     $x_h \leftarrow 2x_h$
     IF $\Delta_1 \equiv 1 \pmod 4$ *THEN* $x_h \leftarrow x_h + y_h$
   - 8.2 *Compute* $d \leftarrow \gcd(y_h, (x_h + y_h\Delta_1)/2) = \lambda y_h + \mu(x_h + y_h\Delta_1)/2$, *for* $\lambda, \mu \in \mathbb{Z}$
   - 8.3 $A \leftarrow |x_h^2 - \Delta_1 y_h^2|/(4d^2)$
   - 8.4 $B \leftarrow (\lambda x_h + \mu(x_h + y_h)\Delta_1/2)/d \pmod{2A}$
9. /* *Lift* $\mathfrak{A}' = (1/d)\mathfrak{A}$ *to the non-maximal order and reduce it* */
   $b \leftarrow Bf \pmod{2A}$
   $(a, b) \leftarrow \rho_p(A, b)$
10. *OUTPUT*(a, b)

Correctness: The correctness of the exponentiation part is immediate, because we just compute the isomorphism ψ as given in the proof of Theorem 3, perform two exponentiations in $\mathbb{F}_p^*$ and compute ψ^{-1}. The rest of the algorithm is equal to this part in Gen-Exp [9, Algorithm 19]. □

Note that the computation of r in Step 5 can be done in a precomputation phase, as is it independent of the current α.

Finally we will give the timings of a first implementation using the LiDIA - package [13]. The timings of the exponentiation are given in microseconds on a Pentium 133 MHz. We used a random exponent $k < 2^{160}$ and $\Delta_p = \Delta_1 p^2$ where $\Delta_1 = -q$ (or $\Delta_1 = -4q$ if $q \equiv 1 \pmod 4$ respectively) and p, q with equal bitlength. This may be compared with the timings for an exponentiation in $\mathbb{F}_{p'}^*$, where p' has the same bitlength as Δ_p. We neglected the time for hashing and computing the s-value.

One should note that the implementation of neither variant is optimized. This is no problem, because we are interested in the comparison, rather than the absolute timings.

group	$\mathbb{F}_p^*$	$\mathrm{Ker}(\phi_{Cl}^{-1})$	
arithmetic	modular	Gen-exp [9]	Gen-CRT
bitlength of	p	Δ_p	Δ_p
600	188	159	83
800	302	234	123
1000	447	340	183
1200	644	465	249
1600	1063	748	409
2000	1454	1018	563

Table 1. Timings for Schnorr-signature generation

These timings show that the signature generation of our proposed scheme using the novel CRT variant for exponentiation is *more than twice as fast as the original scheme*. While the signature verification is much less efficient than in the original scheme, this should be no problem, as the verification is usually not performed in a device with limited computational power, such as a smartcard.

6 Conclusion and future work

We have introduced a new signature scheme based on non-maximal imaginary quadratic orders, which features very fast signature generation. The security analysis shows that using standard assumptions the forging of signatures is equivalent to factoring $\Delta_p = \Delta_1 p^2$. Thus beside further studying implementation issues of cryptosystems based on non-maximal imaginary quadratic orders it will be an important task for the future to consider the factorization problem for this type of non-fundamental discriminant more closely.

References

1. M. Bellare, P. Rogaway: *Random Oracles are Practical: a Paradigm for Designing Efficient Protocols* in Proceedings of the 1st ACM Conference on Computer and Communcations Security, Fairfax, Virginia, USA, ACM press, 1993, pp. 62-73
2. Z.I. Borevich and I.R. Shafarevich: *Number Theory* Academic Press: New York, 1966
3. H. Cohen: *A Course in Computational Algebraic Number Theory*. Graduate Texts in Mathematics **138**. Springer: Berlin, 1993.
4. D.A. Cox: *Primes of the form* $x^2 + ny^2$, John Wiley & Sons, New York, 1989
5. M. Girault: *An identity based identification scheme based on discrete logarithms modulo a composite number*, Advances in Cryptology - Proceedings of Eurocrypt '90, LNCS 473, Springer, pp. 481-486

6. M. Hartmann, S. Paulus and T. Takagi: *NICE - New Ideal Coset Encryption*, to appear in proceedings of CHES, LNCS, Springer, 1999
7. 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
8. 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
9. D. Hühnlein: *Efficient implementation of cryptosystems based on non-maximal imaginary quadratic orders*, to appear in proceedings of SAC'99, LNCS, Springer, 1999, preprint via http://www.informatik.tu-darmstadt.de/TI/Veroeffentlichung/TR/Welcome.html
10. D. Hühnlein, T. Takagi: *Reducing logarithms in totally non-maximal imaginary quadratic orders to logarithms in finite fields*, to appear in proceedings of ASIACRYPT'99, Springer, LNCS, 1999, preprint via http://www.informatik.tu-darmstadt.de/TI/Veroeffentlichung/TR/Welcome.html
11. D. Hhnlein: *A survey of cryptosystems based on imaginary quadratic orders*, forthcoming, 1999
12. M.J. Jacobson Jr.: *Subexponential Class Group Computation in Quadratic Orders*, PhD thesis, TU Darmstadt, to apear, 1999
13. LiDIA: *A c++ library for algorithmic number theory*, via http://www.informatik.tu-darmstadt.de/TI/LiDIA
14. W. Mao: *Cryptoanalysis in Prime Order Subgroups of $\mathbb{Z}_n^*$*, contribution to IEEE-P1363, manuscript via http://www.ieee.org, 1998
15. National Institute of Standards and Technology (NIST): *Digital Signature Standard (DSS)*. Federal Information Processing Standards Publication 186, **FIPS-186**, 19th May, 1994
16. J. Neukirch: *Algebraische Zahlentheorie*, Springer, Berlin, 1992
17. S. Paulus and T. Takagi: *A completely new public key cryptosystem with quadratic decryption time* , to appear in Journal of Cryptology, 1998, preprint via http://www.informatik.tu-darmstadt.de/TI/Mitarbeiter/sachar.html
18. R. Peralta and E. Okamoto: *Faster factoring of integers of a special form*, IEICE Trans. Fundamentals, Vol. E-79-A, No. 4, 1996, pp. 489-493
19. D. Pointcheval, J. Stern: *Security Proofs for Signature Schemes*, Proceedings of Eurocrypt '96, Springer-Verlag, LNCS **1070**, 1996, pp. 387-398
20. C.P. Schnorr: *Efficient identification and signatures for smart cards*, Advances in Cryptology - CRYPTO '89, LNCS **435**, 1990, pp. 239-252