Faster generation of NICE-Schnorr-type signatures

Detlef Hühnlein

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

Abstract. In [7] there was proposed a Schnorr-type signature scheme based on non-maximal imaginary quadratic orders, which signature generation is – for the same conjectured level of security – about twice as fast as in the original scheme [15].
In this work we will significantly improve upon this result, by speeding up the generation of NICE-Schnorr-type signatures by another factor of two. While in [7] one used the surjective homomorphism $\mathbb{F}_p^* \otimes \mathbb{F}_p^* \to \mathrm{Ker}(\phi_{Cl}^{-1})$ to generate signatures by two modular exponentiations, we will show that there is an efficiently computable isomorphism $\mathbb{F}_p^* \stackrel{\sim}{=} \mathrm{Ker}(\phi_{Cl}^{-1})$ in this case, which makes the signature generation about four times as fast as in the original Schnorr scheme [15].

1 Introduction

In todays electronic commerce applications it is necessary to apply digital signatures to provide integrity, authentication and non-repudiation services. Especially for the latter goal(s) it seems to be crucial to store and apply the secret keys in a secure environment, like a smartcard or any other tamper-resistant device. While hardware-technology is continously improving, the computing power of such devices – compared to stationary equipment – is still rather limited. Therefore it is important to search for new signature schemes which allow more efficient signature generation or improve the efficiency of exisiting ones.

In [7] there was proposed a Schnorr-type signature scheme based on non-maximal imaginary quadratic orders. In this scheme one basically replaces the group $\mathbb{F}_p^*$ by the group $\mathrm{Ker}(\phi_{Cl}^{-1})$, which is a subgroup of the class group $Cl(\Delta p^2)$ of the non-maximal imaginary quadratic order $\mathcal{O}_{\Delta p^2}$. For the necessary basics of imaginary quadratic orders we refer to section 2. In contrary to the original scheme [15], this scheme essentially relies on the hardness of factoring the public discriminant $\Delta p^2 < 0$, where $|\Delta|$ and p are primes with (say) 300 bits.

As the signature generation in this scheme is – for the same conjectured level of security – more than twice as fast as in the original scheme [15], this seems to be a good candidate for applications in which fast signature generation in

constrained environment is crucial. The signature generation in this scheme, i.e. essentially one exponentiation in the group $\mathrm{Ker}(\phi_{Cl}^{-1})$, is reduced to *two modular exponentiations* modulo the conductor p. This reduction is possible by applying the efficiently computable surjective homomorphism

$$\mathbb{F}_p^* \otimes \mathbb{F}_p^* \longrightarrow \mathrm{Ker}(\phi_{Cl}^{-1}), \tag{1}$$

which follows from [7, Proposition 4 and Theorem 3].

In this work we will show how the – already remarkably efficient – signature generation in this scheme can be speeded up by another factor of two. More precisely we will prove the following:

Theorem 1 (Main result). *Let $\mathcal{O}_\Delta$ be an imaginary quadratic maximal order of discriminant $\Delta < -4$, p prime, $\left(\frac{\Delta}{p}\right) = 1$, $\phi_{Cl}^{-1} : Cl(\Delta p^2) \to Cl(\Delta)$ like in Proposition 2 and the two roots $\rho, \bar{\rho} \in \mathbb{F}_p^*$ of the polynomial $f(X)$, like in (6), be given. Then it is possible to compute the isomorphism*

$$\psi : \mathbb{F}_p^* \xrightarrow{\sim} \mathrm{Ker}(\phi_{Cl}^{-1})$$

and its inverse ψ^{-1} in $O(\log(p)^2)$ bit operations.

Using this theorem, the signature generation is obviously reduced to *only one modular exponentiation* modulo the conductor p. As the bitlength of p (and $|\Delta|$) is only about one third of the bitlength of the modulus in the original scheme, our signature generation is more than four times as fast. Note that – as shown in [7, Section 4] – a direct analogue in $(\mathbb{Z}/n\mathbb{Z})^*$, n composite, would be totally insecure.

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 will carry together the relevant work concerning the efficient implementation of cryptosystems working in $\mathrm{Ker}(\phi_{Cl}^{-1})$. In Section 4 we will prove Theorem 1 and show how this result can be applied for fast signing. In Section 5 we will provide timings of a first implementation, which shows that the signature generation in this scheme is – for the same conjectured level of security – more than four times as fast as in the original scheme [15].

2 Necessary preliminaries and notations of imaginary quadratic orders

The basic notions of imaginary quadratic number fields may be found in [1, 2]. For a more comprehensive treatment of the relationship between maximal and non-maximal orders we refer to [3–6, 9].

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

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

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

If Δ is squarefree, then $\mathcal{O}_\Delta$ is the *maximal order* of the quadratic number field $\mathbb{Q}(\sqrt{\Delta})$ and Δ is called a fundamental discriminant. The *non-maximal order* of conductor $p > 1$ with (non-fundamental) discriminant Δp^2 is denoted by $\mathcal{O}_{\Delta p^2}$. We will always assume in this work that the conductor p is prime.

The standard representation of an $\mathcal{O}_\Delta$-ideal is

$$\mathfrak{a} = q\left(\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2a}\mathbb{Z}\right) = q(a,b), \tag{3}$$

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 $\rho(\cdot)$ and write $\rho_p(\cdot)$ 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 $Cl(\Delta)$. We denote the equivalence class of an ideal $\mathfrak{a}$ by $[\mathfrak{a}]$. $Cl(\Delta)$ 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 [2]. The order of the class group is called the *class number* of $\mathcal{O}_\Delta$ and is denoted by $h(\Delta)$.

The signature scheme in [7] makes use of the relation between the maximal and non-maximal orders. Any non-maximal order may be represented as $\mathcal{O}_{\Delta p^2} = \mathbb{Z} + p\mathcal{O}_\Delta$. If $h(\Delta) = 1$ then $\mathcal{O}_{\Delta p^2}$ 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 $\mathcal{O}_{\Delta p^2}$-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 [4] will compute such an ideal. Let $\mathcal{I}_{\Delta p^2}(p)$ be the set of all $\mathcal{O}_{\Delta p^2}$-ideals prime to p and let $\mathcal{P}_{\Delta p^2}(p)$ be the principal $\mathcal{O}_{\Delta p^2}$-ideals prime to p. Then there is an isomorphism

$$\mathcal{I}_{\Delta p^2}(p) \Big/ \mathcal{P}_{\Delta p^2}(p) \cong \mathcal{I}_{\Delta p^2} \Big/ \mathcal{P}_{\Delta p^2} = Cl(\Delta p^2). \tag{4}$$

Thus we may 'neglect' the ideals which are not prime to the conductor, if we are only interested in the class group $Cl(\Delta p^2)$. There is an isomorphism between the group of $\mathcal{O}_{\Delta p^2}$-ideals which are prime to p and the group of $\mathcal{O}_\Delta$-ideals, which are prime to p, denoted by $\mathcal{I}_\Delta(p)$ respectively:

Proposition 1. *Let $\mathcal{O}_{\Delta p^2}$ be an order of conductor p in an imaginary quadratic field $\mathbb{Q}(\sqrt{\Delta})$ with maximal order $\mathcal{O}_\Delta$.*

(i.) *If $\mathfrak{A} \in \mathcal{I}_\Delta(p)$, then $\mathfrak{a} = \mathfrak{A} \cap \mathcal{O}_{\Delta p^2} \in \mathcal{I}_{\Delta p^2}(p)$ and $\mathcal{N}(\mathfrak{A}) = \mathcal{N}(\mathfrak{a})$.*
(ii.) *If $\mathfrak{a} \in \mathcal{I}_{\Delta p^2}(p)$, then $\mathfrak{A} = \mathfrak{a}\mathcal{O}_\Delta \in \mathcal{I}_\Delta(p)$ and $\mathcal{N}(\mathfrak{a}) = \mathcal{N}(\mathfrak{A})$.*
(iii.) *The map $\varphi : \mathfrak{A} \mapsto \mathfrak{A} \cap \mathcal{O}_{\Delta p^2}$ induces an isomorphism $\mathcal{I}_\Delta(p) \tilde{\to} \mathcal{I}_{\Delta p^2}(p)$. The inverse of this map is $\varphi^{-1} : \mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_\Delta$.*

Proof: See [3, 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 [4].

It is important to note that the isomorphism φ is between the ideal groups $\mathcal{I}_\Delta(p)$ and $\mathcal{I}_{\Delta p^2}(p)$ and *not the class groups*.

If, for $\mathfrak{A}, \mathfrak{B} \in \mathcal{I}_\Delta(p)$ 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 $\phi_{Cl}^{-1} : Cl(\Delta p^2) \to Cl(\Delta)$, *where $\mathfrak{a} \mapsto \rho(\varphi^{-1}(\mathfrak{a}))$.*

Proof: This immediately follows from the short exact sequence:

$$Cl(\Delta p^2) \longrightarrow Cl(\Delta) \longrightarrow 1$$

(see [12, Theorem 12.9, p. 82]). □

It is easy to show that the kernel $\mathrm{Ker}(\phi_{Cl}^{-1})$ of this map is a subgroup of $Cl(\Delta p^2)$.

If $\Delta < -4$ and p is prime, then it follows from [3, Theorem 7.24, page 146] that the order of this kernel is given as

$$\left|\mathrm{Ker}(\phi_{Cl}^{-1})\right| = p - \left(\frac{\Delta}{p}\right). \tag{5}$$

3 Related work

As many results concerning (the implementation of) cryptosystems based on non-maximal imaginary quadratic orders appeared fairly recently, it seems worthwile to recall the most important results which are relevant in our context.

In Section 3.1 we will briefly introduce the available cryptosystems operating in the kernel $\mathrm{Ker}(\phi_{Cl}^{-1})$ of the above map $\phi_{Cl}^{-1} : Cl(\Delta p^2) \to Cl(\Delta)$. In Section 3.2 we will focus on fast arithmetic in $\mathrm{Ker}(\phi_{Cl}^{-1})$, as it is applied for generating Schnorr-like signatures.

3.1 Cryptosystems utilizing $\mathrm{Ker}(\phi_{Cl}^{-1})$

In the following we will briefly recall some cryptosystems working in $\mathrm{Ker}(\phi_{Cl}^{-1})$. We will distinguish between encryption- and signature-schemes.

NICE-encryption-scheme The first – and probably most popular – cryptosystem, which utilizes $\mathrm{Ker}(\phi_{Cl}^{-1})$ in a crucial way is the NICE[1]-cryptosystem [13]. This cryptosystem is essentially an ElGamal-encryption scheme, where the message is embedded in an element of $Cl(\Delta p^2)$ and the mask which hides this message is a random power of an element of $\mathrm{Ker}(\phi_{Cl}^{-1})$. Therefore the decryption essentially consists of computing ϕ_{Cl}^{-1}, which only takes quadratic time. It should be noted, that the chosen ciphertext attack [10] is no real threat in practice, as it is easily prevented by appending a hash-value of the plaintext to the ciphertext.

NICE-signature-schemes While it would be easy to set up a DSA-like signature scheme in the classgroup $Cl(\Delta p^2) = \mathrm{Ker}(\phi_{Cl}^{-1})$ of a *totally* non-maximal imaginary quadratic order, e.g. in $\mathcal{O}_{-8p^2}$ where $h(\Delta) = 1$, it was shown in [6] that the discrete logarithm problem in this case can be reduced from $Cl(-8p^2)$ to either $\mathbb{F}_p^*$ or $\mathbb{F}_{p^2}^*$ – depending on $\left(\frac{\Delta}{p}\right)$. Because of this reduction, there is no advantage in using NICE-DSA instead of the regular DSA in finite fields.

A crucial difference between DSA and the original Schnorr-scheme [15] is, that in the latter scheme it is not necessary that the verifying party knows the group order q.

Therefore it was proposed in [7] to use conventional non-maximal orders to set up a NICE-Schnorr-type signature scheme, which primarily gets its security from the hardness of factoring Δp^2 instead of solely from the DL-problem in $\mathrm{Ker}(\phi_{Cl}^{-1}) \subset Cl(\Delta p^2)$. Thus an attacker is only able to apply the reduction from [6] *after factoring* the public discriminant Δp^2, which is considered to be infeasible for the proposed parameter sizes.

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

1. Choose a random prime r and set $\Delta = -r$ 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 $\mathrm{Ker}(\phi_{Cl}^{-1}) \subset Cl(\Delta p^2)$.
3. Choose a random prime p, such that $\left(\frac{\Delta}{p}\right) = 1, q|(p-1)$ and compute Δp^2.
4. Choose a random $\alpha = x + y\omega$ such that $\mathfrak{g} = \varphi(\alpha\mathcal{O}_\Delta)$ is of order q in $Cl(\Delta p^2)$.
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 tuple (x, y, a, p, q, r).

Note that Alice will keep these values secret and only publishes $\Delta p^2, \mathfrak{g}, \mathfrak{a}$. Now the signature generation and verification procedure is analogous to the

[1] **N**ew **I**deal **C**oset **E**ncryption

original Schnorr-scheme [15]. The only difference is that Alice may speed up the signature *generation* process using some more sophisticated arithmetic for $\mathrm{Ker}(\phi_{Cl}^{-1})$, which utilizes the knowledge of x, y and p. In Section 3.2 we will return to this issue and recall what has been known so far. In Section 4 we show that these results can be significantly improved.

To sign a message $m \in \mathbb{Z}$, Alice performs the following steps:

1. Choose a random integer $1 < k < q$ and compute $\mathfrak{k} = \mathsf{Gen\text{-}ISO}(x, y, p, k)$, where the algorithm $\mathsf{Gen\text{-}ISO}()$ is given in Section 4.
2. Compute[2] $e = h(m||\mathfrak{k})$ and $s = ae + k$.
3. Alice's signature for m is the pair (e, s).

The verification is completely analogous to the original scheme [15] using standard ideal arithmetic (see e.g. [2]) 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 $e' = e$.

For security issues of this scheme and the proposed parameter sizes we refer to [7, Section 4] and [14].

3.2 Fast arithmetic in $\mathbf{Ker}(\phi_{Cl}^{-1})$

In this section we will study the kernel $\mathrm{Ker}(\phi_{Cl}^{-1})$ of the above map ϕ_{Cl}^{-1}, i.e. the relation between a class in the maximal order and the associated classes in the non-maximal order, in more detail. A thorough understanding of this relation is crucial for the development of a fast arithmetic for the group $\mathrm{Ker}(\phi_{Cl}^{-1})$, like proposed in [5–7] and Section 4.

We start with yet another interpretation of the class group $Cl(\Delta p^2)$.

Proposition 3. *Let $\mathcal{O}_{\Delta p^2}$ be an order of conductor p in a quadratic field. Then there are natural isomorphisms*

$$Cl(\Delta p^2) \simeq {\mathcal{I}_{\Delta p^2}(p)}\Big/{\mathcal{P}_{\Delta p^2}(p)} \simeq {\mathcal{I}_{\Delta}(p)}\Big/{\mathcal{P}_{\Delta,\mathbb{Z}}(p)},$$

where $\mathcal{P}_{\Delta,\mathbb{Z}}(p)$ denotes the subgroup of $\mathcal{I}_{\Delta}(p)$ generated by the principal ideals of the form $\alpha\mathcal{O}_{\Delta}$ where $\alpha \in \mathcal{O}_{\Delta}$ satisfies $\alpha \equiv a \pmod{p\mathcal{O}_{\Delta}}$ for some $a \in \mathbb{Z}$ such that $\gcd(a, p) = 1$.

[2] Note that in [7] it was proposed to return the residue of s modulo q, which makes the signature slightly smaller and saves some time for the verifying party. While in [7] there were given ad-hoc-arguments that this is no security threat, it might be more satisfying to return $s = ae + k$, as the detailed security analysis of [14] applies in this case.

Proof: See [3, Proposition 7.22, page 145]. □

The following corollary is an immediate consequence.

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

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

Now we will turn to the relation between $(\mathcal{O}_\Delta/p\mathcal{O}_\Delta)^*$ and $\mathrm{Ker}(\phi_{Cl}^{-1})$:

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

Proof: This is shown in the more comprehensive proof of Theorem 7.24 in [3] (page 147). □

From these results it is clear that for all ideal classes $[\mathfrak{a}] \in \mathrm{Ker}(\phi_{Cl}^{-1}) \subseteq Cl(\Delta p^2)$ there is a *generator representation*:

Definition 1. *Let* $\alpha = x + \omega y \in (\mathcal{O}_\Delta/p\mathcal{O}_\Delta)^*$, *such that* $[\mathfrak{a}] \sim \varphi(\alpha)$. *Then* (x, y) *is called a* generator representation *of the class* $[\mathfrak{a}] \in \mathrm{Ker}(\phi_{Cl}^{-1})$.

For simple conversion routines between the standard representation (3) and this generator representation we refer to [9, Algorithmus 16 (Gen2Std) and Algorithmus 17 (Std2Gen)]. These algorithms require the conductor p as input and run in $O(\log(p)^2)$ bit operations.

Remark 1. It should be noted that this generator representation (x, y) for a class $[\mathfrak{a}]$ is *not unique*. From Proposition 3 we see that (sx, sy), where $s \in \mathbb{F}_p^*$, is yet another generator representation of the class $[\mathfrak{a}]$. We will return to this issue in the proof of Theorem 1.

The central point in using this generator representation instead of the standard ideal representation (3) is that one may reduce the arithmetic in $\mathrm{Ker}(\phi_{Cl}^{-1})$ to much more efficient computations in $(\mathcal{O}_\Delta/p\mathcal{O}_\Delta)^*$. This is precisely what was proposed in [5]. Using the naive "generator-arithmetic", i.e. naive computation in $(\mathcal{O}_\Delta/p\mathcal{O}_\Delta)^*$, as proposed 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, like given in [2] for example.

But, as shown in [6, 7], one can even do better; in Section 5 we will provide concrete timings of a first implementation.

The following simple result explains the structure of the ring $(\mathcal{O}_\Delta/p\mathcal{O}_\Delta)$:

Proposition 5. *Let* $\mathcal{O}_\Delta$ *be the maximal order and* p *be prime. Then there is an isomorphism between rings*

$$(\mathcal{O}_\Delta/p\mathcal{O}_\Delta) \cong {}^{\mathbb{F}_p[X]}\!/_{(f(X))},$$

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

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

Proof: See [6, Proposition 5]. □

Using this auxilliary result one obtains the following Proposition 6, which – together with Proposition 2 – is responsible for the fast signature generation in [7].

Proposition 6. *Assume that* $\left(\frac{\Delta}{p}\right) = 1$ *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 isomorphism

$$\psi_{\mathbb{F}} : (\mathcal{O}_\Delta / p\mathcal{O}_\Delta)^* \xrightarrow{\sim} \mathbb{F}_p^* \otimes \mathbb{F}_p^*$$

can be computed with $O(\log(p)^2)$ bit operations.

Note that this result essentially uses the chinese remainder theorem in the ring $(\mathcal{O}_\Delta/p\mathcal{O}_\Delta)$ to speed up the computation. Compared to the standard ideal arithmetic (e.g. in [2]), this approach yields an approximately forty-fold speedup.

While this arithmetic is already remarkable efficient, we will show in the next section that one can even do better.

4 The main result and its application to fast signing

In this section we will show that for an exponentiation in $\mathrm{Ker}(\phi_{Cl}^{-1})$, where $\left(\frac{\Delta}{p}\right) = 1$, it is sufficient to perform *a single modular exponentiation* modulo the conductor p.

This significant improvement essentially follows from the fact that in our case we have $\left(\frac{\Delta}{p}\right) = 1$ and there is an isomorphism $\mathbb{F}_p^* \tilde{=} \mathrm{Ker}(\phi_{Cl}^{-1})$, which can be computed efficiently.

While, because of $\left|\mathrm{Ker}(\phi_{Cl}^{-1})\right| = p - 1$, the existence of such an isomorphism was already suspected earlier – and in fact follows immediately from [3, (7.27), page 147] – the crucial point for our application is that this isomorphism can be computed in $O(\log(p)^2)$ bit operations.

Proof (of Theorem 1). Let $\left(\frac{\Delta}{p}\right) = 1$. Then Proposition 6 shows that $(\mathcal{O}_\Delta/p\mathcal{O}_\Delta)^* \tilde{=} \mathbb{F}_p^* \otimes \mathbb{F}_p^*$ and our claimed isomorphism $\mathrm{Ker}(\phi_{Cl}^{-1}) \tilde{=} \mathbb{F}_p^*$ follows immediately from the exact sequence [3, (7.27), page 147]

$$1 \longrightarrow \mathbb{F}_p^* \longrightarrow (\mathcal{O}_\Delta/p\mathcal{O}_\Delta)^* \tilde{=} \mathbb{F}_p^* \otimes \mathbb{F}_p^* \longrightarrow \mathrm{Ker}(\phi_{Cl}^{-1}) \longrightarrow 1.$$

It remains to give a constructive version of this isomorphism and show that the runtime is bound by $O(\log(p)^2)$ bit operations.

Let (x, y) be a generator representation of the ideal class $[\mathfrak{a}] \sim \varphi(\alpha) \in \mathrm{Ker}(\phi_{Cl}^{-1})$, where $\alpha = x + y\omega \in (\mathcal{O}_\Delta/p\mathcal{O}_\Delta)^*$, and $\rho, \bar{\rho}$ are the roots of $f(X)$ like in (6). Then the isomorphism $\psi_{\mathbb{F}} : (\mathcal{O}_\Delta/p\mathcal{O}_\Delta)^* \to \mathbb{F}_p^* \otimes \mathbb{F}_p^*$ from Proposition 6 maps $\alpha = x + y\omega \in (\mathcal{O}_\Delta/p\mathcal{O}_\Delta)^*$ to $(x_1, x_2) \in \mathbb{F}_p^* \otimes \mathbb{F}_p^*$, $x_1 = x + y\rho$ and $x_2 = x + y\bar{\rho}$.

Let $s \in \mathbb{F}_p^*$, such that $s(x + y\bar{\rho}) \equiv 1 \pmod{p}$. From Proposition 3 (see also Remark 1) it follows, that $\varphi(\alpha) \sim \varphi(s \cdot \alpha)$ and (sx, sy) is another generator representation of the class $[\mathfrak{a}] \sim \varphi(\alpha) \sim \varphi(s \cdot \alpha)$. Using $\psi_{\mathbb{F}}$ we map $s \cdot \alpha$ to the pair $(s(x + y\rho), 1)$, which induces the desired isomorphism $\psi^{-1} : \mathrm{Ker}(\phi_{Cl}^{-1}) \xrightarrow{\sim} \mathbb{F}_p^* \otimes \mathbf{1} \stackrel{\sim}{=} \mathbb{F}_p^*$,

$$\begin{aligned}
\mathfrak{a} &= \varphi(x + y\omega) \\
&\sim \varphi\left(\frac{x + y\omega}{x + \bar{\rho}y}\right) \\
&\mapsto \psi^{-1}\left(\varphi\left(\frac{x + y\omega}{x + \bar{\rho}y}\right)\right) \\
&= \left(\frac{x + \rho y}{x + \bar{\rho}y}, \frac{x + \bar{\rho}y}{x + \bar{\rho}y}\right) \\
&= \left(\frac{x + \rho y}{x + \bar{\rho}y}, 1\right) \\
&\simeq \frac{x + \rho y}{x + \bar{\rho}y}.
\end{aligned} \tag{7}$$

The inverse map $\psi : \mathbb{F}_p^* \xrightarrow{\sim} \mathrm{Ker}(\phi_{Cl}^{-1})$ is – like shown in the proof of Proposition 6 and [7, Gen-CRT (Algorithm 4)] – given by

$$\begin{aligned}
x &\mapsto \psi(x) \\
&\simeq \psi_{p^2}(x, 1) \\
&= \varphi\left(x - \frac{1 - x}{\bar{\rho} - \rho}\rho + \frac{1 - x}{\bar{\rho} - \rho}\omega\right) \\
&= \varphi\left(\frac{x(\bar{\rho} - \rho) - (1 - x)\rho}{\bar{\rho} - \rho} + \frac{1 - x}{\bar{\rho} - \rho}\omega\right) \\
&= \varphi\left(\frac{x\bar{\rho} - x\rho - \rho + x\rho}{\bar{\rho} - \rho} + \frac{1 - x}{\bar{\rho} - \rho}\omega\right) \\
&= \varphi\left(\frac{x\bar{\rho} - \rho}{\bar{\rho} - \rho} + \frac{1 - x}{\bar{\rho} - \rho}\omega\right) \\
&\sim \varphi\left(x\bar{\rho} - \rho + (1 - x)\omega\right).
\end{aligned} \tag{8}$$

Because we assume that the two roots $\rho, \bar{\rho} \in \mathbb{F}_p^*$ of $f(X)$, like in (6), are known, we immediately see that the isomorphism ψ and its inverse can be computed in $O(\log(p)^2)$ bit operations. □

Using the constructive version of this isomorphism in (7) and (8), it is straightforward to construct an efficient exponentiation algorithm for elements in $\mathrm{Ker}(\phi_{Cl}^{-1})$.

Algorithm 1 Gen-Iso

Input: A generator representation (x, y) of the class $[\mathfrak{a}] \sim \varphi(x+y\omega) \in \mathrm{Ker}(\phi_{Cl}^{-1})$, where $x + y\omega \in (\mathcal{O}_\Delta / p\mathcal{O}_\Delta)^*$, the conductor p, where $\left(\frac{\Delta}{p}\right) = 1$, the roots $\rho, \bar{\rho} \in \mathbb{F}_p^*$ of $f(X)$, like in (6), and the exponent $n \in \mathbb{Z}_{>0}$.

Output: The standard representation (a, b) of the reduced representative of the class of $[\mathfrak{a}^n] = a\mathbb{Z} + \frac{b+\sqrt{\Delta p^2}}{2}\mathbb{Z} \in \mathrm{Ker}(\phi_{Cl}^{-1})$.

{Compute $\psi^{-1}(\varphi(x + y\omega))$, like in (7)}
$g \leftarrow \frac{x+\rho y}{x+\bar{\rho} y} \pmod p$
{Exponentiation in $\mathbb{F}_p^*$}
$g \leftarrow g^n \pmod p$
{Compute $\psi(g)$, like in(8)}
$x \leftarrow g\bar{\rho} - \rho \pmod p$
$y \leftarrow 1 - g \pmod p$
$(a, b) \leftarrow$ Gen2Std(x, y)
return(a, b)

Furthermore it is clear that a complete signing routine would use this algorithm to compute $\mathfrak{k} = \rho_p(\mathfrak{g}^k)$ and then compute the signature (e, s) by $e = h(m||\mathfrak{k})$ and $s = ae + k$. For a rough estimate of the signing efficiency, we may savely ignore the time for computing the values e and s and only take care of the exponentiation time.

5 Timings

We conclude this work by providing the timings of a first implementation.

The timings are given in microseconds on a Pentium with 133 MHz using the LiDIA-library [11]. It should be noted that in all algorithms there is used a naive square and multiply strategy. It is clear that in real world applications one would use some more sophisticated (e.g. window-) exponentiation strategy – possibly using precomputed values. All timings correspond to random 160 bit exponents.

Arithmetic	modular	ideal	Gen-Exp, [5]	Gen-CRT, [7]	Gen-ISO
bitlength of	p	$\Delta p^2 = -rp^2$	$\Delta p^2 = -rp^2$	$\Delta p^2 = -rp^2$	$\Delta p^2 = -rp^2$
600	188	3182	159	83	42
800	302	4978	234	123	60
1000	447	7349	340	183	93
1200	644	9984	465	249	123
1600	1063	15751	748	409	206
2000	1454	22868	1018	563	280

Table 1. Timings for exponentiations in $\mathrm{Ker}(\phi_{Cl}^{-1})$

The timings in Table 1 show the impressive improvement. Compared to an exponentiation in $\mathrm{Ker}(\phi_{Cl}^{-1}) \subset Cl(\Delta p^2)$ using the standard ideal arithmetic (see e.g. [2]), the generator arithmetic from [5, Gen-Exp] is already about twenty times as fast. This arithmetic makes the signature generation in the NICE-Schnorr-scheme [7] – considering the different algoritms for solving the underlying problem, like in [8] – about as efficient as in the original scheme [15]. The application of the chinese remainder theorem in $(\mathcal{O}_\Delta/p\mathcal{O}_\Delta)$ in [7, Gen-CRT] roughly leads to a two-fold speedup. Finally, using the isomorphism $\mathbb{F}_p^* \tilde{=} \mathrm{Ker}(\phi_{Cl}^{-1})$ leads to yet another two-fold speedup. This arithmetic is about eighty times as fast as the conventional ideal arithmetic.

Most importantly, the signature generation in the NICE-Schnorr-scheme [7] now is about *four times* as fast as the signing in the original scheme [15].

References

1. Z.I. Borevich and I.R. Shafarevich: *Number Theory* Academic Press: New York, 1966
2. H. Cohen: *A Course in Computational Algebraic Number Theory*. Graduate Texts in Mathematics **138**. Springer: Berlin, 1993.
3. D.A. Cox: *Primes of the form* $x^2 + ny^2$, John Wiley & Sons, New York, 1989
4. 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
5. D. Hühnlein: *Efficient implementation of cryptosystems based on non-maximal imaginary quadratic orders*, Proceedings of SAC'99, LNCS **1758**, Springer, 2000, pp. 150–167
6. D. Hühnlein, T. Takagi: *Reducing logarithms in totally non-maximal imaginary quadratic orders to logarithms in finite fields*, Advances in Cryptology - ASIACRYPT'99, Springer, LNCS **1716**, 1999, pp. 219–231
7. D. Hühnlein, J. Merkle: *An efficient NICE-Schnorr-type signature scheme*, Proceedings of PKC 2000, LNCS **1751**, Springer, 2000, pp. 14–27
8. D. Hühnlein: *Quadratic orders for NESSIE - Overview and parameter sizes of three public key families*, Technical Report, TI 3/00, TU-Darmstadt, 2000

9. D. Hühnlein: *Cryptosystems based on quadratic orders*, (in German), PhD-thesis, TU-Darmstadt, Germany, forthcoming, 2000
10. É. Jaulmes, A. Joux: *A NICE Cryptoanalysis*, Advances in Cryptology - EUROCRYPT '00, LNCS **1807**, Springer, 2000, pp. 382 – 391
11. LiDIA: *A c++ library for algorithmic number theory*, via http://www.informatik.tu-darmstadt.de/TI/LiDIA
12. J. Neukirch: *Algebraische Zahlentheorie*, Springer, Berlin, 1992
13. S. Paulus and T. Takagi: *A new public-key cryptosystem over quadratic orders with quadratic decryption time* Journal of Cryptology, vol. **13**, no. 2, 2000, pp. 263–272
14. G. Poupard, J. Stern: *Security Analysis of a Practical "on the fly" Authentication and Signature Generation*, Advances in Cryptology – EUROCRYPT '98, LNCS **1403**, Springer, 1998, pp. 422 – 436
15. C.P. Schnorr: *Efficient identification and signatures for smart cards*, Advances in Cryptology - CRYPTO '89, LNCS **435**, 1990, pp. 239-252