A survey of cryptosystems based on imaginary quadratic orders

Detlef Hühnlein

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

Abstract

Since nobody can *guarantee* that popular public key cryptosystems based on factoring or the computation of discrete logarithms in some group will stay secure forever, it is important to study different primitives and groups which may be utilized if a popular class of cryptosystems gets broken.

A promising candidate for a group in which the DL-problem seems to be hard is the class group $Cl(\Delta)$ of an imaginary quadratic order, as proposed by Buchmann and Williams [BuWi88]. Recently this type of group has obtained much attention, because there was proposed a very efficient cryptosystem based on non-maximal imaginary quadratic orders [PaTa98a], later on called NICE (for **N**ew **I**deal **C**oset **E**ncryption) with *quadratic decryption time*. To our knowledge this is the only scheme having this property. First implementations show that the time for *de*cryption is comparable to RSA *en*cryption with $e = 2^{16} + 1$. Very recently there was proposed an efficient NICE-Schnorr type signature scheme [HuMe99] for which the signature generation is *more than twice as fast* as in the original scheme based on $\mathbb{F}_p^*$.

Due to these results there has been increasing interest in cryptosystems based on imaginary quadratic orders. Therefore it seems necessary to provide an up to date survey to facilitate further work in this direction. Our survey will discuss the history, the state of the art and future directions of cryptosystems based on imaginary quadratic orders.

1 Introduction

Public key cryptography is unquestionable a core technology which is widely applied to secure IT-systems and electronic commerce. However all popular public key schemes have a common problem: Their security is based on *unproven assumptions*, like the conjectured intractability of factoring or the computation of discrete logarithms in some group, like $\mathbb{F}_p^*$ or the group of points on (hyper-) elliptic curves over finite fields.

Thus as long as nobody can *guarantee* that such problems remain intractible for the future it is important to study public key cryptosystems based on different primitives and alternative groups in which the discrete logarithm problem seems to be hard.

A promising candidate for such a group, which was proposed by Buchmann and Williams [BuWi88], is the class group $Cl(\Delta)$ of an imaginary quadratic order $\mathcal{O}_\Delta$. See Section 2 for background and notations. These groups are not only interesting from a theoretical point of view but also served as basis for cryptosystems with very practical properties.

Unlike factoring or the DL problem in $\mathbb{F}_p^*$, there is no $L_\Delta[\frac{1}{3}, c]$ algorithm known for the computation of logarithms in arbitrary $Cl(\Delta)$ and it is known that this DL problem is *at least* as hard as factoring the discriminant Δ. Thus if an $L_\Delta[\frac{1}{3}, c]$ algorithm for the computation of discrete logarithms in $Cl(\Delta)$ would be found this would imply a possibly second asymptotically fast algorithm for factoring, besides the number field sieve. Furthermore these imaginary quadratic orders are closely related to non-supersingular elliptic curves. They happen to be isomorphic to their endomorphism rings. Thus a good understanding of imaginary quadratic orders may shed some light on the real difficulty of the discrete logarithm problem of elliptic curves, which is very important because elliptic curve cryptosystem are increasingly used in practice. See Section 6 for further discussion of this line of thought.

But studying imaginary quadratic orders is not only interesting from a theoretical point of view. Recently there were proposed cryptosystems based on non-maximal imaginary quadratic orders with *very practical properties*. For example in [PaTa98a] there was proposed a public key cryptosystem (later on called NICE) with *quadratic decryption time*, which makes the decryption as efficient as RSA-encryption with $e = 2^{16} + 1$. To our knowledge this is the only public key cryptosystem with this property. More recently there was proposed an efficient NICE-Schnorr-type signature scheme [HuMe99], where the signature generation is more than twice as fast as in the original Schnorr-scheme in $\mathbb{F}_p^*$. It is clear that fast decryption and signature generation are very important features as these operations often take place in a device with limited computational power, like a smartcard.

Due to these results there has been increasing interest in cryptosystems based on imaginary quadratic orders. However there seems to be no comprehensive reference for this topic and therefore it seems necessary to provide an up to date survey of these cryptosystem to facilitate further work in this direction. This work will show the history, the state of the art and future directions of cryptosystems based on imaginary quadratic orders. As the underlying mathematical structures seem to be less well known in the cryptographic community than elliptic curves for example, we will provide a tutorial on the mathematical background in the full paper.

This paper is organized as follows: In Section 2 we will give the necessary background concerning imaginary quadratic orders. The full paper will comprise a more comprehensive tutorial on this subject. In Section 3 we briefly talk about the being of imaginary quadratic orders prior to cryptographic utilization in 1988. In Section 4 we discuss cryptosystems which are based on class groups of maximal orders. The recently proposed cryptosystems based on non-maximal orders are discussed in Section 5. In Section 6 we will point out some future directions.

2 Some background and notations concerning imaginary quadratic orders

We first recall 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 [BoSh66, Cohe93]. For a more comprehensive treatment of the relationship between maximal and non-maximal orders we refer to [Cox89, HJPT98].

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

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

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 $f > 1$ with (non-fundamental) discriminant $\Delta_f = \Delta_1 f^2$ is denoted by $\mathcal{O}_{\Delta_f}$. We will omit the subscripts to reference arbitrary (fundamental or non-fundamental) discriminants. Because $\mathbb{Q}(\sqrt{\Delta_1}) = \mathbb{Q}(\sqrt{\Delta_f})$ 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 ideal $\mathfrak{a}$ is reduced. We denote the reduction operator in the maximal order by $\rho_1()$ and write $\rho_f()$ for the reduction operator in the non-maximal order of conductor f.

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 [Cohe93]. 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 5 make use of the relation between the maximal and some non-maximal order. Any non-maximal order of conductor f may be represented as $\mathcal{O}_{\Delta_f} = \mathbb{Z} + f\mathcal{O}_{\Delta_1}$. A special type of non-maximal order is given if $h(\Delta_1) = 1$. In this case $\mathcal{O}_{\Delta_f}$ is called a *totally non-maximal* imaginary quadratic order. An $\mathcal{O}_\Delta$-ideal $\mathfrak{a}$ is called prime to f, if $gcd(\mathcal{N}(\mathfrak{a}), f) = 1$. It is well known, that all $\mathcal{O}_{\Delta_f}$-ideals prime to the conductor are invertible.

Let $\mathcal{I}_{\Delta_f}(f)$ be the group of invertible ideals, which are prime to f, and $\mathcal{P}_{\Delta_f}(f)$ be the invertible principal ideals, which are prime to f then there is an isomorphism

$$\mathcal{I}_{\Delta_f}(f)\big/\mathcal{P}_{\Delta_f}(f) \simeq \mathcal{I}_{\Delta_f}\big/\mathcal{P}_{\Delta_f} = Cl(\Delta_f). \tag{3}$$

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

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

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

Proof: See [Cox89, Proposition 7.20, page 144] . □

Thus we are able to switch to and from the maximal order. This mapping is of central importance for all cryptosystems in Section 5. The algorithms GoToMaxOrder($\mathfrak{a}, f$) to compute φ^{-1} and GoToNonMaxOrder($\mathfrak{A}, f$) to compute φ respectively may be found in [HJPT98]. Note that for the most important case, where f is prime, one knows that all reduced ideals in $Cl(\Delta_f)$ (and then of course also $Cl(\Delta_1)$) are prime to f if one chooses $f > \sqrt{|\Delta_1|}$.

Note that the above map is defined on ideals itself, rather than equivalence classes. For $\mathfrak{A}, \mathfrak{B} \in \mathcal{I}_{\Delta_1}(f)$ such that $\mathfrak{A} \sim \mathfrak{B}$, it is not necessarily true that $\varphi(\mathfrak{A}) \sim \varphi(\mathfrak{B})$. On the other hand, equivalence *does* hold under φ^{-1} and we have (by [Neuk92, Theorem 12.9, p. 82]) the following short exact sequence:

$$Cl(\Delta_f) \xrightarrow{\phi_{Cl}^{-1}} Cl(\Delta_1) \longrightarrow 1, \tag{4}$$

where the (surjective) homomorphism ϕ_{Cl}^{-1} is explicitely given by $\mathfrak{a} \mapsto \rho_1(\varphi^{-1}(\mathfrak{a}))$.

The kernel $\operatorname{Ker}(\phi_{Cl}^{-1})$ of the map ϕ_{Cl}^{-1} plays an important role in the construction of the NICE-type cryptosystems [PaTa98a, HuMe99], as it replaces the group $\mathbb{F}_p^*$ in classical DL-based cryptosystems.

Moreover by [Cox89, Theorem 7.24, page 146] one knows that the map

$$(\mathcal{O}_{\Delta_1}/f\mathcal{O}_{\Delta_1})^* \to \operatorname{Ker}(\phi_{Cl}^{-1}), \tag{5}$$

where $\alpha \mapsto \alpha\mathcal{O}_{\Delta_1}$ is a surjective homomorphism and the exact relation between the class numbers $h(\Delta_1)$ and $h(\Delta_f)$ is given as

$$h(\Delta_f) = \frac{h(\Delta_1)f}{[\mathcal{O}_{\Delta_1}^* : \mathcal{O}_{\Delta_f}^*]} \prod_{p\,|\,f} \left(1 - \frac{\left(\frac{\Delta_1}{p}\right)}{p}\right) = nh(\Delta_1), \tag{6}$$

where $n \in \mathbb{N}$ and $\left(\frac{\Delta_1}{p}\right)$ is the Kronecker-symbol.

3 The being of imaginary quadratic orders prior to cryptosystems

The history of what we call imaginary quadratic orders today actually started with the study of diophantine equations by the ancient greeks. While famous mathematicians like Fermat, Euler, Lagrange and Legendre had important contributions to the development it seems that Carl Friedrich Gauss were the first who provided a systematically treatment of this subject in the language of positive definite binary quadratic forms [Gaus01] about 200 years ago. See [Buel89] for a modern treatment of binary quadratic forms. Note that it is well known that the class group of binary quadratic forms is isomorphic to the class group $Cl(\Delta)$ of a quadratic order and hence we do not distinguish here. Before using imaginary quadratic orders to construct cryptosystems they were used for *factoring the discriminant* by searching for ambigue classes in $Cl(\Delta)$, i.e. classes of order 2. Algorithms for factoring with this strategy with exponential running time may be found in [Shan71b, Lens82, Scho83] for example. What seems to be well less known today is that the idea to use other groups in Pollards $p-1$-factoring method, which lead to the Elliptic Curve Method [Lens87], actually is due to Schnorr and Lenstra [ScLe84] who used imaginary quadratic class groups, because the probabiltiy for the group order $h(\Delta)$ to be smooth is significantly higher than for random integers of comparable size. The concept of factor bases for factoring with imaginary quadratic orders, which leads to a subexponential algorithm, was first used by Seysen in [Seys87].

4 The early days of cryptographic utilization - maximal orders

As mentioned in the introduction 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.

With this motivation Buchmann and Williams [BuWi88] 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*. This is done via finding the ambigous classes, as mentioned above. Furthermore note 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. We will return to this issue in Section 6. 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 $L_\Delta[1, \frac{1}{5}]$ [Lens82, Scho83] assuming the truth of the Generalized Riemann Hypothesis (GRH) or $L_\Delta[1, \frac{1}{4}]$ without this assumption. In [Duel88, BuDW90] there were reported the first implementations and a complexity analysis of this key agreement scheme. While it was shown fairly recently [BiBu98] that these cryptosystems are *asymptotically* as efficient as classical cryptosystems, i.e. encryption and decryption needs $O(\log^3 |\Delta|)$ bit operations, they are still far less efficient in practice.

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 [NIST94] or RSA [RiSA78].

Therefore in [Meye97] there was proposed a Fiat-Shamir-like signature- and identification scheme based on $Cl(\Delta)$, where one clearly does not need to know $h(\Delta)$. While an algorithm for the computation of square roots in $Cl(\Delta)$ obviously can be used to find ambigue classes and hence to factor Δ, it was initially doubted that the knowledge of the factorization of Δ can be used to compute square roots in $Cl(\Delta)$. Finally however there was found an algorithm to compute square roots in $Cl(\Delta)$ due to Gauss [Gaus01, Art. 286, p. 328] which uses ternary quadratic forms and computes square roots in $Cl(\Delta)$ on input of the factorization of Δ. Hence this scheme is 'only equivalent' to factoring Δ and thus there is no advantage in using this scheme compared to the original one [FiSh86].

Even worse for cryptosystems based on imaginary quadratic orders was the discovery of a subexponential time algorithm [HaMC89, McCu89] by Hafner and McCurley in 1989. This algorithm has running time $L_\Delta[\frac{1}{2}, \sqrt{2}]$ 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 [BuDu91]. Note that at this time the asymptotically best algorithm for factoring integers was the quadratic sieve [Silv87] 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) [CoOS86] to compute discrete logarithms in prime fields also has running time $L_p[\frac{1}{2}, 1]$.

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

5 The recent revival - non-maximal orders

In the meantime however an idea of Pollard lead to todays asymptotically best algorithm for factoring integers - the number field sieve (see [LeLe93]). 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 [CDE+96] and recently for the factorization of RSA-140 [CDL+99] and RSA-155 [TeR+99] for example. The number field sieve can also be used to compute discrete logarithms in finite fields (see e.g. [Gord93, Webe98]), 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 [Jaco99] with $L_\Delta[\frac{1}{2}, 1]$.

It is clear that this development alone would not justify the term 'revival' in the heading. In 1998 it was shown in [HJPT98] 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. The central idea is to use a non-fundamental discriminant $\Delta_p = -qp^2$, p, q prime. Thus, because p is part of the secret key one can apply the isomorphic map φ^{-1} from Proposition 1, to switch to the secret maximal order, with much smaller coefficients, and perform the ElGamal-decryption there. While the overall performance of this scheme still was too bad to be used in practice this result stimulated much research in this direction.

Recently, a very efficient successor [PaTa98a] with *quadratic decryption time* was proposed. This scheme was later on called NICE (for **N**ew **I**deal **C**oset **E**ncryption) [HaPT99]. First software implementations show that the time for decryption is comparable to RSA - encryption with $e = 2^{16} + 1$. The central idea of NICE is to use an element $\mathfrak{g} \in \operatorname{Ker}(\phi_{Cl}^{-1})$, to mask the message in the ElGamal-type encryption scheme by multiplication the message ideal $\mathfrak{m}$ with $\mathfrak{g}^k$ for random k. Thus during the decryption step, which consists of the computation of φ^{-1} and reducing the resulting ideal in the maximal order, the mask $\mathfrak{g}^k$ simply disappears and the message $\mathfrak{m}$ is recovered. Note that the computation of φ^{-1} is essentially one modular inversion with the Extended Euclidean Algorithm which takes quadratic time. A first smartcard implementation on a Siemens SLE66CX80S [HaPT99] however shows that standard chips, which are highly optimized for RSA, do not allow such an efficient implementation. Thus to obtain the same big advantage as in software one needs to consider the underlying architecture more carefully.

On the other hand it is clear that this cryptosystem is very well suited for applications in which a central server has to decrypt a large number of ciphertext in a short time. For this scenario one may use the recently developed NICE-batch-decryption method [Hueh99], which even speeds up the already very efficient decryption process by another 30% for a batch size of 100 messages.

The implementation was done using the LiDIA-package [LiDI99] on a Pentium 133 MHz choosing random primes p, q of the respective bit-length. The timings are given in microseconds, averaged over a number of 100 randomly chosen messages. The first row shows how many modular multiplications are as costly as one inversion in LiDIA. The

bitlength p, q	200		300		400		500	
mult / inv	13.9		15.4		16.2		15.6	
	ms	%	ms	%	ms	%	ms	%
NICE Enc. (binary)	1861.7	100	4065.2	100	7368.9	100	12182.1	100
NICE Enc. (BGMW)	669.7	35.97	1786.6	43.95	3556.5	48.26	6461.9	53.04
NICE Enc. (±-BGMW)	640.9	34.43	1732.6	42.62	3493.6	47.41	6315.5	51.84
NICE Dec. (1 mess.)	9.50	100	16.75	100	26.30	100	35.66	100
NICE Dec. (5 mess.)	8.20	86.32	13.16	78.57	20.00	76.05	26.93	75.52
NICE Dec. (10 mess.)	7.45	78.42	12.34	73.67	19.11	72.66	25.61	71.82
NICE Dec. (100 mess.)	6.70	70.53	11.64	69.49	18.30	69.58	24.61	69.01

Table 1: Timings for NICE with sequential and batch decryption

next rows give the time for a NICE-encryption using 80 bit exponents and the binary, usual BGMW-, and the signed BGMW-method [BGMW93] for exponentiation. Note that unlike the classical ElGamal cryptosystem, where one can apply generic methods to compute discrete logarithms, it is sufficient to have 80 bit exponents here, as the only way to attack NICE apart from factoring Δ_p seems to be brute force. Note that the timings here include the time for the message-embedding. The last four rows give the decryption time (per message) for batch sizes of 1, 5, 10 and 100 messages respectively.

There was also proposed an efficient undeniable signature scheme [BiPT99] based on the NICE-structure. The central idea is to use a zero-knowledge-proof for the knowledge of the ideal with the smallest norm among all 'kernel-equivalent' classes for a given class in the non-maximal order $Cl(\Delta_p)$. Kernel-equivalence here means that classes in $Cl(\Delta_p)$ only differ by a class in the kernel of ϕ_{Cl}^{-1}. Given a reduced ideal $\mathfrak{m}$ in the non-maximal order and the conductor p, the class with the smallest norm among all kernel-equivalence classes can easily be computed as $\varphi(\rho_1(\varphi^{-1}(\mathfrak{m})))$. Thus one simply steps down to the maximal order, reduces the ideal and lifts the result up again. Note that it was shown in [PaTa98a, Theorem 1] that $\varphi^{-1}(\mathfrak{m})$ can be computed if and only if the conductor p, i.e. the factorization of Δ_p, is known.

Note that the central idea of NICE, i.e. computing in the *secret* kernel of a surjective map, can be used in other groups as well [PaTa98b]. However non-maximal imaginary quadratic orders seem to be the only known instance where this coset problem is intractable.

In 1998 there were also proposed first conventional signature schemes based non-maximal imaginary quadratic orders. In [HuMT98] there were proposed RSA- and Rabin analogues. To set up an RSA analogue it is sufficient to know the group order $h(\Delta_f)$. Thus by (6) one can easily perform this if $h(\Delta_1)$ is known. Thus one possibility to set up an RSA analogue is to choose some prime $q \equiv 3 \pmod 4$ and another large prime p, set $\Delta_1 = -q$, compute $h(\Delta_1)$ using the subexponential algorithm from [Jaco99] and finally computing $h(\Delta_p) = h(\Delta_1)\left(p - \left(\frac{\Delta_1}{p}\right)\right)$. Then one chooses some public exponent e which is prime to $h(\Delta_p)$ and computes the secret exponent d such that $ed \equiv 1 \pmod{h(\Delta_p)}$. The corresponding encryption schemes have the major advantage that they are immune against low-exponent- and chosen-ciphertext attacks. That such an attack is not only of academic interest is demonstrated by the recent attack on the Rabin cryptosystem due to Joye and Quisquater [JoQu99]. This attack makes the revision of the ISO-9796-1 standard (with padding) necessary, as the signature of *only one* suitably chosen message will reveal the factorization of the modulus n. Note that the Rabin analogue in non-maximal imaginary quadratic orders, is inherently immune against this kind of attack, as no analogue of the $\gcd$-algorithm is know to exist. As in the original scheme it can be shown that breaking the Rabin scheme is equivalent to factoring. Moreover there was proposed a novel algorithm to compute square roots in $Cl(\Delta_p)$, which replaces the fairly inefficient Gaussian algorithm using ternary quadratic forms. To avoid the computation of $h(\Delta_1)$, where $|\Delta_1| = q$ should have at least 200 bit to prevent the factorization of Δ_p using ECM[1], it was proposed to use *totally* non-maximal imaginary quadratic orders, where $h(\Delta_1) = 1$ and a *composite* conductor pq. Thus one may set up an RSA-analogue in $Cl(\Delta_{pq})$, where $\Delta_{pq} = -8p^2q^2$ for example and knows $h(\Delta_{pq}) = (p - (-8/p))(q - (-8/q))$ immediately after computing the Kronecker symbols $(-8/\cdot)$. 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. In this case one can choose $p \approx 2^{400}$ and set up DSA analogues in $Cl(\Delta_p)$, where $\Delta_p = -8p^2$. By a conservative estimate this cryptosystem *was* considered to be as hard to break as DSA in $\mathbb{F}_p^*$ with $p \approx 2^{1024}$. In fact it was heuristically shown in [Hamd99] that the computation of discrete logarithms in $Cl(\Delta)$ for $\Delta \approx -2^{700}$, using the subexponential algorithm from [Jaco99], should be comparable with factoring a 1024 bit number with the number field sieve. Nevertheless this DSA analogue *seemed* to be too inefficient to be used in practice.

Very recently in [Hueh99] however there was proposed an entirely new arithmetic for these totally non-maximal orders and more generally for elements in $\mathrm{Ker}(\phi_{Cl}^{-1})$, which happens to coincide with the entire class group in the case of totally non-maximal orders. 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. One uses the (trivially computable) surjective homomorphism $(\mathcal{O}_{\Delta_1}/f\mathcal{O}_{\Delta_1})^* \to \mathrm{Ker}(\phi_{Cl}^{-1})$ to replace the inefficient arithmetic in $\mathrm{Ker}(\phi_{Cl}^{-1}) \subseteq Cl(\Delta_p)$ by the more efficient arithmetic in $(\mathcal{O}_{\Delta_1}/f\mathcal{O}_{\Delta_1})^*$. This means that instead of (multiple) applications of the comparably costly Extended Euclidean Algorithm one only has a few modular multiplications. For totally non-maximal orders (i.e. $\Delta_p \approx -p^2$) this strategy turns out to be *thirteen* times as fast and one ends up with a DSA analogue, which is almost as efficient as conventional DSA in $\mathbb{F}_p^*$.

Without the even more recent result in [HuTa99] the DSA analogue based on totally non-maximal imaginary quadratic orders *would have been* a very interesting alternative.

As it often happens in cryptology there is a sharp edge between good and bad news.

In [HuTa99] it was shown that using similar ideas like in [Hueh99] (for speeding up the system) one can reduce the discrete logarithm problem in these totally non-maximal imaginary quadratic orders in (expected) $O(\log^3 p)$ bit operations to the discrete logarithm problem in finite fields. One uses the surjective homomorphism ψ and constructs an

[1] See [Bren99] for a recent finding of a 53 digit factor using ECM.

additional isomorphism between (a subgroup of) $(\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^*$ and the multiplicative group of a finite field. This clearly implies that that this scheme is only as hard to break as the original scheme and hence there seems to be no reason for using it in practice.

But these bad news also initiated the development of a new, more efficient and (under standard assumptions) provable secure signature scheme. In [HuMe99] it was shown how one can construct an efficient NICE-Schnorr-signature scheme, which operates in the *secret* kernel of ϕ_{Cl}^{-1} instead of $\mathbb{F}_p^*$. This is a similar situation as in NICE. First implementations showed that the signature generation using the arithmetic from [Hueh99] is even a little bit faster than the original scheme in $\mathbb{F}_p^*$. And using the isomorphism from [HuTa99], which was used to 'break' the DSA-analogue in *totally* non-maximal orders to *speed up* the signing process in the NICE-Schnorr-scheme by a factor of two using the Chinese Remainder Theorem in $(\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^*$. Thus the entire signature generation is *more than twice as fast* as in the original scheme in $\mathbb{F}_p^*$. The timings in the following table are given in microseconds on a Pentium 133 using LiDIA [LiDI99].

cryptosystem	Schnorr / DSA					RSA		
arithmetic	mod.	ideal	Gen-exp	Gen-exp	Gen-CRT	mod.	ideal	Gen-exp
bitlength of	p	Δ_p	$\Delta_p = -163p^2$	$\Delta_p = -qp^2$	$\Delta_p = -qp^2$	$n = pq$	$n = pq$	$n = pq$
600	188	3182	240	159	83	258	10490	994
800	302	4978	368	234	123	583	22381	2053
1000	447	7349	542	340	183	886	35231	3110
1200	644	9984	724	465	249	1771	68150	6087
1600	1063	15751	1156	748	409	3146	125330	10864
2000	1454	22868	1694	1018	563	5284	224799	18067

Table 2: Timings for exponentiation with different arithmetics

In [HuMe99] it was also shown that an existential forgery for this scheme under an adaptively chosen message attack can be proven to be equivalent to factoring Δ_p in the random oracle model if one furthermore assumes that the computation of discrete logarithms in a subgroup of $\mathrm{Ker}(\phi_{Cl}^{-1})$ is equivalent to the DL-problem in $\mathrm{Ker}(\phi_{Cl}^{-1})$ itself.

6 Future path

Finally we will point out a few areas of further work. Since there are already very promising schemes based on imaginary quadratic orders, it will become increasingly important to study implementation and standardization issues of these schemes. As the recent result [HuTa99] however indicates we need to study the security of such schemes with even more scrutiny. One point is to further research special purpose factoring algorithms for numbers of the form qp^2, as was done in [PeOk96] for example. Since nobody knows whether factoring itself will stay intractable forever it is also important to study cryptosystems based on *maximal* orders, like in [BBHM99] for example.

Since imaginary quadratic orders appear as endomorphism rings of elliptic curves one should also investigate possible implications of recent results, concerning imaginary quadratic orders like [HuTa99], to the security of elliptic curve cryptosystems.

We will spend a few more words to clarify this issue. Let $p > 3$ be prime and $E(\mathbb{F}_p)$ be an elliptic curve over the prime field $\mathbb{F}_p$ with group order $n = |E(\mathbb{F}_p)|$.

Furthermore assume that:

- n and its prime factorization is known.
  This is reasonable, as n can be computed using the (improved) Schoof Algorithm in polynomial time. In practice one uses curves such that n is ('almost') prime.
- $E(\mathbb{F}_p)$ is non-supersingular.
  To prevent the MOV / Frey-Rück - attack.
- $n \neq p$
  To prevent the anomalous attack by Smart.
- $n \neq r^2$ for some $r \in \mathbb{Z}$.
  This is ensured in practice as n is chosen to be 'almost prime'.

Note that such curves are believed to provide most security. As $E(\mathbb{F}_p)$ is assumed to be non-supersingular we know, by the theory of complex multiplication, that the ring of endomorphisms $\mathrm{End}(E(\mathbb{F}_p))$ of our curve is isomorphic to an imaginary quadratic order $\mathcal{O}_\Delta$. Let $\pi \in \mathcal{O}_\Delta$ be the Frobenius endomorphism. Note that Δ and π can be efficiently determined given n.

H.W. Lenstra has shown in [Lens96] that there is an isomorphism

$$E(\mathbb{F}_p) \simeq {}^{\mathcal{O}_\Delta}\!\big/_{(\pi - 1)\mathcal{O}_\Delta}, \tag{7}$$

taken additively. It should be mentioned that for this isomorphism to hold one needs to assume that $\pi \notin \mathbb{Z}$, which follows directly from the assumption that n is no square. The discrete logarithm problem in $(\mathcal{O}_\Delta/(\pi - 1)\mathcal{O}_\Delta)^+$ can be reduced, using the results from [HuTa99], to discrete logarithms in *additive* groups of a small number of finite fields, which can be solved in polynomial time. Thus the remaining - presumably very hard - task would be to find a *constructive map* for the isomorphism (7).

References

[BiBu98] I. Biehl and J. Buchmann: *An analysis of the reduction algorithms for binary quadratic forms*, in P. Engel, H. Syta (eds.), 'Voronoi's Impact on Modern Science', vol. **1**, Institute of Mathematics of National Academy of Sciences, Kyiv, Ukraine, 1998

[BBHM99] I. Biehl, J. Buchmann, S. Hamdy and A. Meyer: *Cryptographic Protocols Based on the Intractibility of Extracting Roots and Computing Discrete Logarithms*, Technical Report, University of Technology, Darmstadt, 1999, via

http://www.informatik.tu-darmstadt.de/TI/Veroeffentlichung/TR/Welcome.html

[BiPT99] I. Biehl, S. Paulus and T. Takagi: *An efficient undeniable signature scheme based on non-maximal imaginary quadratic orders*, Technical Report, University of Technology, Darmstadt, 1999, via

http://www.informatik.tu-darmstadt.de/TI/Veroeffentlichung/TR/Welcome.html

[BoSh66] Z.I. Borevich and I.R. Shafarevich: *Number Theory* Academic Press: New York, 1966

[Bren99] R. Brent: *ECM champs*, ftp.comlab.ox.ac.uk/ pub/Documents/techpapers/Richard.Brent/champs.ecm

[BGMW93] E. Brickell, D. Gordon, K. McCurley, D. Wilson: *Fast Exponentiation with Precomputation*, Proceedings of Eurocrypt 1992, LNCS **658**, Springer, 1993, pp. 200-207

[BuDu91] 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

[BuDW90] 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

[BuWi88] J. Buchmann and H.C. Williams: *A key-exchange system based on imagninary quadratic fields*. Journal of Cryptology, **1**, 1988, pp. 107-118

[Buel89] D.A. Buell: *Binary Quadratic Forms - Classical Theory and Modern Computations*, Springer: Berlin, 1989.

[CDE+96] 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*, proceedings of ASIACRYPT'96, Springer, LNCS **1163**, 1996, pp. 382-394

[Cohe93] H. Cohen: *A Course in Computational Algebraic Number Theory*. Graduate Texts in Mathematics **138**. Springer: Berlin, 1993.

[CoOS86] D. Coppersmith, A.M. Odlyzko and R. Schroeppel: *Discrete logarithms in* $GF(p)$, Algorithmica, **1**, 1986, pp. 1-15

[Cox89] D.A. Cox: *Primes of the form* $x^2 + ny^2$, John Wiley & Sons, New York, 1989

[DiHe76] W. Diffie and M. Hellman: *New directions in cryptography*, IEEE Transactions on Information Theory **22**, 1976, pp. 472-492

[Duel88] S. Düllmann: *Ein neues Verfahren zum öffentlichen Schlüsselaustausch*, Master-thesis (in german), University of Düsseldorf, 1988

[Duel91] S. Düllmann: *Ein Algorithmus zur Bestimmung der Klassenzahl positiv definiter binärer quadratischer Formen*, PHD-thesis (in german), University of Saarbrücken, 1991

[FiSh86] A. Fiat and A. Shamir: *How to prove yourself: Practical solutions to identification and signature problems*, Advances in Cryptology, Proceedings of CRYPTO '86, Springer, LNCS 263, 1987, pp. 186-194

[Gaus01] C.F. Gau: *Disquisitiones Arithmeticae*, 1801, reprinted 1986 by Springer, ISBN 0-387-96254-9

[Gord93] D.M. Gordon: *Discrete logarithms in* $GF(p)$ *using the number field sieve*, SIAM Journal on Discrete Mathematics, **6**, 1993, pp. 124-138

[Hamd99] S. Hamdy: *The key-length of DL-based cryptosystems in class groups*, available upon request from hamdy@cdc.informatik.tu-darmstadt.de, 1999

[HaMC89] J.L. Hafner and K.S. McCurley: *A rigorous subexponential algorithm for computation of class groups*, Journal of the American Mathematical Society, **2**, 1989, 837-850

[HaPT99] M. Hartmann, S. Paulus and T. Takagi: *NICE - New Ideal Coset Encryption*, appeared at CHES, to appear in Springer LNCS, 1999, preprint via

http://www.informatik.tu-darmstadt.de/TI/Veroeffentlichung/TR/Welcome.html

[Hua82] L.K. Hua: *Introduction to Number Theory*. Springer-Verlag, New York, 1982.

[HJPT98] 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

[HuMT98] 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

[Hueh99] D. Hühnlein: *Efficient implementation of cryptosystems based on non-maximal imaginary quadratic orders*, to appear in Proceedings of SAC'99, Springer, LNCS **1758**, 2000, pp. 150-167, preprint via

http://www.informatik.tu-darmstadt.de/TI/Veroeffentlichung/TR/Welcome.html

[HuMe99] D. Hühnlein, J. Merkle: *An efficient NICE-Schnorr-type cryptosystem*, to appear at PKC2000, Melbourne, January 2000 and Springer LNCS preprint via

http://www.informatik.tu-darmstadt.de/TI/Veroeffentlichung/TR/Welcome.html

[HuTa99] D. Hühnlein, T. Takagi: *Reducing logarithms in totally non-maximal imaginary quadratic orders to logarithms in finite fields*, Advances in Cryptology - Asiacrypt'99, LNCS **1716**, Springer, 1999, pp. 219

[Jaco99] M.J. Jacobson Jr.: *Subexponential Class Group Computation in Quadratic Orders*, Berichte aus der Informatik, Shaker, ISBN 3-8265-6374-3, 1999

[JoQu99] M. Joye, J.J. Quisquater: *On Rabin-type signatures*, Research contribution to IEEE-P1363, 1999, via

http://grouper.ieee.org/groups/1363/contrib.html

[Lens82] H.W. Lenstra: *On the computation of regulators and class numbers of quadratic fields*, London Math. Soc. Lecture Notes, **56**, 1982, pp. 123-150

[Lens87] H.W. Lenstra: *Factoring integers with elliptic curves*, Annals of Mathematics, **126**, 1987, pp. 649-673

[LeLe93] A.K. Lenstra and H.W. Lenstra Jr. (eds.): *The development of the number field sieve*, Lecture Notes in Mathematics, Springer, 1993

[Lens96] H.W. Lenstra: *Complex Multiplication Structure of Elliptic Curves*, Journal of Number Theory, Vol. **56**, No. **2**, 1996, pp. 227-241

[LiDI99] LiDIA: *A c++ library for algorithmic number theory*,

via http://www.informatik.tu-darmstadt.de/TI/LiDIA

[MaYa96] U. Maurer, Y. Yacobi: *A non-interactive public-key distribution system*, Design Codes and Cryptography, No. **9**, 1996, pp. 305-316

[McCu89] K.S. McCurley: *Cryptographic key distribution and computation in class groups*, Number Theory and applications (R.A. Mollin, ed.), NATO ASI series, Series C, vol. **265**, Dordrecht, 1989, pp. 459-479

[Meye97] A. Meyer: *Ein neues Identifikations- und Signaturverfahren über imaginär-quadratischen Zahlkörpern*, Master-thesis (in german), University of Saarbrücken, Germany, 1997
via

ftp://ftp.informatik.tu-darmstadt.de/pub/TI/reports/amy.diplom.ps.gz

[NIST94] National Institute of Standards and Technology (NIST): *Digital Signature Standard (DSS)*. Federal Information Processing Standards Publication 186, **FIPS-186**, 19th May, 1994

[Neuk92] J. Neukirch, *Algebraische Zahlentheorie*, Springer, Berlin, 1992

[PaTa98a] S. Paulus and T. Takagi: *A 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

[PaTa98b] S. Paulus and T. Takagi: *A generalization of the Diffie-Hellman problem based on the coset problem allowing fast decryption*, Proceedings of ICICS '98, ISBN 89-85305-14-X, 1998

[PeOk96] 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

[CDL+99] S. Cavallar, B. Dodson, A. Lenstra, P. Leyland, W. Lioen, P.L. Montgomery, B. Murphy, H. te Riele, P. Zimmerman: *Factorization of RSA-140 Using the Number Field Sieve*, Proceedings of ASIACRYPT'99, LNCS **1716**, Springer, 1999, pp. 195-207

[TeR+99] H. te Riele & al: *Factorization of RSA-155 with the Number Field Sieve*, posting in sci.crypt.research, August 1999

[RiSA78] 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

[Seys87] M. Seysen: *A probabilistic factoring algorithm with quadratic forms of negative discriminant*, Math. Comp.,**48**, 1987, pp. 737-780

[Silv87] R.D. Silverman: *The multiple polynomial quadratic sieve*, Math. Comp. **48**, 1987, pp. 329-229

[Scho83] R.J. Schoof: *Quadratic Fields and Factorization*. In: H.W. Lenstra, R. Tijdeman, (eds.): *Computational Methods in Number Theory*. Math. Centrum Tracts **155**. Part II. Amsterdam, 1983. pp. 235-286.

[ScLe84] C.P. Schnorr, H.W. Lenstra: *A Monte Carlo factoring algorithm with linear storage*, Mathematics of Computation, v. **43**, 1984, pp. 289-312

[Shan71a] D. Shanks: *Gauss' ternary form reduction and the 2-Sylow subgroup*, Math. Comp. **25**, 1971, pp. 837-853.

[Shan71b] D. Shanks: *Class number, a theory of factorization and genera*, Proc. Symposium Pure Mathematics, American Mathematical Society, **20**, 1971, pp. 415-440

[Webe98] D. Weber: *Computing discrete logarithms with quadratic number rings*, Advances in Cryptology - EUROCRYPT '98, LNCS **1403**, Springer, 1998, pp. 171-183