Rabin and RSA analogues based on non-maximal imaginary quadratic orders

Detlef Hühnlein[1], Andreas Meyer[2], and Tsuyoshi Takagi[3]

[1] secunet Security Networks GmbH, Mergenthalerallee 77-81, D-65760 Eschborn, Germany, huehnlein@secunet.de
[2] University of Technology Darmstadt, Alexanderstr. 10, D-64283 Darmstadt, Germany, amy@cdc.informatik.tu-darmstadt.de
[3] NTT Software Laboratories Düsseldorf Branch, Immermannstraße 40, 40210 Düsseldorf, Germany, ttakagi@ntt.de

Abstract. In [14] and [21] there are proposed ElGamal-type cryptosystems based on non-maximal imaginary quadratic orders with fast trapdoor decryption. The trapdoor information is the factorization of the non-fundamental discriminant $\Delta_q = \Delta q^2$. We will extend the ideas given there to set up Rabin and RSA analogues based on non-maximal imaginary quadratic orders.
To implement the Rabin analogue we will introduce a new algorithm, which reduces the computation of square roots in $Cl(\Delta_q)$ to the computation of square roots in $Cl(\Delta)$. This is more efficient than the classical Gaussian algorithm. If the class number $h(\Delta)$ for $\Delta = -p$, $p \equiv 3 \ mod \ 4$ prime, is known, it is possible to extract square roots by a simple exponentiantion. In this case it is easy to set up RSA analogues as well. It will be shown, that breaking the Rabin analogue is as hard as factoring, just like the original scheme in $(\mathbb{Z}/n\mathbb{Z}^*)$.
The major advantage of our schemes compared to the original Rabin and RSA schemes is that they are immune against the currently known low exponent attacks and the chosen ciphertext attack from [10].

Keywords: Rabin, RSA, non-maximal imaginary quadratic order, factorization, low exponent attack, chosen ciphertext attack

1 Introduction

The utilization of imaginary quadratic class groups in cryptography is due to Buchmann and Williams [4], who proposed a key agreement protocol analogue to [7] based on class groups of imaginary quadratic fields, i.e. the class group of the *maximal order*. Since the computation of discrete logarithms in the class group of the imaginary quadratic number field is at least as difficult as factoring the corresponding discriminant (see [4, 26]) these cryptosystems are very interesting from a theoretical point of view. In practice however these cryptosystems have as yet not gained very much attention, because they seemed to be less efficient than

popular cryptosystems based on computing discrete logarithms in $(\mathbb{Z}/p\mathbb{Z}^*)$, like [7, 9] or factoring integers, like [23, 22]. Another issue is that the computation of the group order, i.e. the class number, is in general almost as hard as computing discrete logarithms itself by application of the algorithm of Hafner / McCurley [11] or more practical variants like [8], which is subexponential with $L[\frac{1}{2}]$ and hence it seemed to be impossible to set up signature schemes analogue to [9, 25, 19, 20] or [23]. In [14] however it was shown how the application of *non-maximal* imaginary quadratic orders may be used to construct an ElGamal-type cryptosystem with faster decryption and that it is in principle possible to set up ElGamal and RSA-type signature schemes. In [21] it was shown how imaginary quadratic orders can be used to construct public key cryptosystems with *quadratic decryption time*.

In this work we will extend these ideas and propose a cryptosystem analogue to Rabin's [22]. We will show, that breaking the proposed Rabin analogue based on the difficulty of computing square roots in the class group of imaginary quadratic orders is equivalent to factoring, just like the original scheme over $(\mathbb{Z}/n\mathbb{Z}^*)$. We will outline the classical Gaussian algorithm, based on reduction of ternary quadratic forms, to compute square roots in arbitrary imaginary quadratic class groups. Then we introduce an entirely new algorithm, which reduces the computation of square roots in $Cl(\Delta_q)$ to the computation of square roots in $Cl(\Delta)$, which is much more efficient than Gauss' algorithm in $Cl(\Delta_q)$, because the size of the coefficients in the class group of the maximal order $Cl(\Delta)$ is much smaller. In this case one may choose a prime discriminant $\Delta = -p \equiv 1 \ mod\, 4$ and extract square roots in $Cl(\Delta)$ by suitable exponentiation. Note, that this is possible, because the class number $h(\Delta) = h(-p)$ is *odd* by genus theory (see e.g. [30]).

If $h(\Delta)$ and therefore $h(\Delta_q)$ is known it is a natural generalisation to allow arbitrary public exponents e as long as $gcd(e, h(\Delta_q)) = 1$, which yields schemes analogue to RSA. We will give strong evidence, that the proposed schemes are *immune against currently known low exponent attacks and the chosen ciphertext attack* proposed in [10].

For this RSA-type setup however the knowledge of $h(\Delta)$ is essential. Therefore one may choose discriminants of the form $\Delta_{pq} = \Delta p^2 q^2$, where $\Delta = -8$ and p and q are large odd primes. In this case it is very easy to compute the class number $h(\Delta_{pq})$ and set up RSA analogues. Since we have to deal with larger numbers however, this approach seems to loose much of its attractiveness.

This paper is organized as follows: In Section 2 we will provide the necessary basics on imaginary quadratic orders emphasizing the relation between the maximal order and non-maximal orders. In Section 3 we will discuss the system setup for the proposed Rabin- and RSA analogues considering different formed discriminants. In Section 4 we will give algorithms to compute square roots in imaginary quadratic class groups. This will include a new approach, which reduces the computation of square roots in $Cl(\Delta_q)$ to the compuation of square roots in $Cl(\Delta)$. Section 5 is concerned with the security of the proposed schemes.

This will show, that breaking the Rabin analogues is equivalent to factoring the corresponding public discriminants $\Delta_1 = -pq, \Delta_q = -pq^2$ or $\Delta_{pq} = -8p^2q^2$ respectively. Furthermore we will give strong evidence, that our schemes are immune against currently known low exponent attacks and the chosen ciphertext attack [10] against the unbalanced RSA scheme [27]. For convenience we will give the details of the Gaussian square root extraction algorithm in the appendix.

2 Imaginary quadratic orders

The basic notions of imaginary quadratic number fields may be found in [1, 13] or [5]. For a more comprehensive treatment of the relationship between maximal and non-maximal orders we refer to [6] or [14].

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

$$\mathcal{O}_\Delta = \mathbb{Z} + \frac{\Delta + \sqrt{\Delta}}{2}\mathbb{Z}. \tag{1}$$

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 $\mathcal{O}_{\Delta_f}$. In this work 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 a primitive $\mathcal{O}_\Delta$-ideal is

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

where $a \in \mathbb{Z}_{>0}$, $c = (b^2 - \Delta)/(4a) \in \mathbb{Z}$, $gcd(a, b, c) = 1$ and $-a < b \leq a$. The norm of this ideal is $\mathcal{N}(\mathfrak{a}) = a$. 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. Note that this fact will be essential for the immunity of our scheme against the chosen ciphertext attack [10]. 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 $\mathcal{O}_\Delta$, 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 $\mathcal{O}_\Delta$. The order of the class group is called the *class number* of $\mathcal{O}_\Delta$ and is denoted by $h(\Delta)$.

Our cryptosystems make use of the relation between the maximal and non-maximal orders. Any non-maximal order may be represented as $\mathcal{O}_{\Delta_f} = \mathbb{Z} + f\mathcal{O}_{\Delta_1}$. 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. In every class there is an ideal which is prime to any given number. The algorithm FindIdealPrimeTo in [14] will compute such an ideal. If we denote the (principal) $\mathcal{O}_{\Delta_f}$-ideals, which are prime to f by $\mathcal{P}_{\Delta_f}(f)$ and $\mathcal{I}_{\Delta_f}(f)$ respectively 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:

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

Proof: See [6, Proposition 7.20, page 144] . □

Thus we are able to switch to and from the maximal order. The algorithms GoToMaxOrder$(\mathfrak{a}, f)$ to compute φ^{-1} and GoToNonMaxOrder$(\mathfrak{A}, f)$ to compute φ respectively and the proofs for the following propositions may be found in [14].

Note, that the above map is defined on ideals itself, rather than equivalence classes. But it is easy to show, that

Proposition 2. *For $\mathfrak{a}, \mathfrak{b} \in \mathcal{I}_{\Delta_f}(f)$ and $\gamma \in \mathbb{Q}(\sqrt{\Delta})$ such that $\mathfrak{a} = \gamma\mathfrak{b}$ we have $\varphi^{-1}(\mathfrak{a}) \sim \varphi^{-1}(\mathfrak{b})$*

and that we indeed have a one to one correspondence of classes, if the norm of the reduced representatives is small:

Proposition 3. *If $\mathfrak{A} \in \mathcal{I}_{\Delta_1}(f)$ is reduced then $\varphi(\mathfrak{A}) \in \mathcal{I}_{\Delta_f}(f)$ is also reduced.*

Proposition 4. *If $\mathfrak{a} \in \mathcal{I}_{\Delta_f}(f)$ with $\mathcal{N}(\mathfrak{a}) \leq \sqrt{|\Delta_1|/4}$ then $\varphi^{-1}(\mathfrak{a}) \in \mathcal{I}_{\Delta_1}(f)$ is also reduced.*

The problem introduced by switching from the maximal order $\mathcal{O}_{\Delta_1}$ to the non-maximal order $\mathcal{O}_{\Delta_f}$ is, that there are principal $\mathcal{O}_{\Delta_1}$-ideals which image under φ is *not* principal in $\mathcal{O}_{\Delta_f}$. But the following fact is well known:

Proposition 5. *Let $\alpha \in \mathcal{O}_{\Delta_1}$ be an element of the maximal order and $\mathcal{O}_{\Delta_f}$ be the order of conductor f. Then $\varphi(\alpha\mathcal{O}_{\Delta_1}) \sim \mathcal{O}_{\Delta_q}$ if and only if*

$$\alpha \equiv a \bmod f\mathcal{O}_{\Delta_1}$$

with $a \in \mathbb{Z}$ such that $gcd(a, f) = 1$

Proof: This is an immediate consequence of the isomorphism [6, Proposition 7.22,page 145]

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

where $\mathcal{P}_{\Delta_1,\mathbb{Z}}(f)$ denotes the subgroup of $\mathcal{I}_{\Delta_1}(f)$ generated by the principal ideals of the form $\alpha\mathcal{O}_{\Delta_1}$ where $\alpha \in \mathcal{O}_{\Delta_1}$ satisfies $\alpha \equiv a \bmod f\mathcal{O}_{\Delta_1}$ for some $a \in \mathbb{Z}$ such that $gcd(a, f) = 1$. □

Finally it is well known, that the class numbers $h(\Delta_1)$ and $h(\Delta_f)$ are related by

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

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

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

Proof: See [6, Theorem 7.24, page 146] . □

3 System Setup for Rabin and RSA analogues

In this section we will discuss the system setup and the necessary procedures to implement Rabin and RSA analogues based on imaginary quadratic orders. It is clear, that the form of the public discriminant greatly affects the possible system setups and the procedures for signing/decrypting and verifying/encrypting. Therefore we will distinguish three cases $\Delta_1 = -pq$, (if $-pq \equiv 1 \bmod 4$ or $\Delta_1 = -4pq$ otherwise), $\Delta_q = -\Delta_1 q^2$ and $\Delta_{pq} = -\Delta_1 p^2 q^2$. We assume, that a message $m \in \mathbb{N}$ which is to be encrypted or signed is embedded in a reduced ideal $\mathfrak{m} \in \mathcal{I}_{\Delta_q}(q)$. This embedding, which is needed for the implementation of the ElGamal analogue proposed in [14] as well, might be accomplished by setting $a_m = \mathcal{N}(\mathfrak{m}) = 2^s m + r$, where s is fixed and r is choosen, such that a_m is prime and $\left(\frac{\Delta_q}{a_m}\right) = 1$ is the Kronecker symbol. I.e. that it is possible to compute the corresponding b_m, which is a square root of Δ_q modulo $4a_m$. That such a construction is always possible and that the resulting ideal $\mathfrak{m}$ is indeed reduced will be ensured by a suitable choice of s. Note however, that a bad embedding

might jeapordize the claimed security. Thus the embedding has to be considered with more scrutiny in a forthcoming paper. In the following we will treat the Rabin and RSA analogues seperately.

3.1 Maximal Order $\Delta_1 = -pq$ (or $\Delta_1 = -4pq$)

Rabin analogue This is the classical setup for the Rabin analogue based on *maximal* imaginary quadratic orders. Here p, q are two large primes and the public discriminant $\Delta_1 = -pq$, if $pq \equiv 3 \ mod \, 4$ or $\Delta_1 = -4pq$ otherwise. Like in the original scheme it can be shown (see [17]), that breaking this scheme (i.e. computing square roots in $Cl(\Delta_1)$) is equivalent to factoring Δ_1. An algorithm to compute square roots in $Cl(\Delta_1)$ which goes back to Gauss is outlined in Section 4. The interested reader will find the details in the appendix.

RSA analogue On the other side it is clear, that it is *not possible to set up RSA analogues*, simply because the computation of the class number $h(\Delta_1)$ is a very hard problem. Unlike the construction of the original RSA system, it does not help, that one knows the factors of Δ_1 to speed up the computation. With current algorithms it is even more difficult to compute $h(\Delta_1)$ than to factor it.

3.2 Non-maximal Order $\Delta_q = \Delta_1 q^2$

In [14] it was shown, how the utilisation of *non-maximal* imaginary quadratic orders may be used to set up ElGamal-type cryptosystems with fast decryption, incorporate key escrow functionality into classical cryptosystems and how the ElGamal signature and RSA analogue may be set up in principle. The crucial point in this system setup is the computation of the class number $h(\Delta_q)$. Let p, q be two large primes. Set $\Delta_1 = -p$ if $p \equiv 3 \ mod \, 4$, $\Delta_1 = -4p$ otherwise and $\Delta_q = \Delta_1 q^2$. If $h(\Delta_1)$ is known then computing $h(\Delta_q)$ is easy using Theorem 6. Thus it is possible to set up ElGamal-signature and RSA analogues (working exclusively in the non-maximal order).

In this work we will show, how the relation between the public non-maximal order and the secret maximal order may be further utilised to implement more efficient Rabin and RSA analogues.

Rabin analogue For the Rabin setup the number of square roots in the class group is essential. Therefore we introduce a slight restriction on the form of the fundamental discriminant Δ_1 in this case. We choose a large prime $p \equiv 3 \ mod \, 4$ and $\Delta_1 = -p$. Then we know by genus theory (see e.g. [30]), that there is exactly one genus in $Cl(\Delta_1)$, i.e. every class in $Cl(\Delta_1)$ is a square, the square root of a class is unique and that the class number $h(\Delta_1)$ is *odd*. We will return to this fact in the next section, where we introduce a new algorithm for the computation of square roots in $Cl(\Delta_q)$, which is more efficient than Gauss' algorithm.

We omit the presentation of the signature, verification and encryption procedure, because it is completely analogous to the original scheme [22] over $(\mathbb{Z}/n\mathbb{Z}^*)$.

Algorithm 7. *(RabinDecrypt)*
Input: $(\mathfrak{c}, \Delta_1, q)$, *where* $\mathfrak{c} \in \mathcal{I}_{\Delta_q}(q)$ *is the cyphertext,* $\Delta_1 = -p \equiv 1 \bmod 4$ *is the fundamental discriminant and* q *is the conductor*
Output: *The message* $\mathfrak{m} \in \mathcal{I}_{\Delta_q}(q)$

1. $\mathfrak{m}_1 \leftarrow \mathsf{Sqrt}_q(\mathfrak{c}, \Delta_1, q)$
2. $\mathfrak{p} \leftarrow (p, 0)$
3. $\mathfrak{m}_2 \leftarrow \rho_q(\mathfrak{m}_1\mathfrak{p})$
4. *choose message* $\mathfrak{m}$ *(out of* $\mathfrak{m}_{1,2}$*) with the appropriate form, redundancy,* $\cdots$
5. *RETURN*$(\mathfrak{m})$

Correctness: Since we choose $\Delta_q = -pq^2$ there are by genus theory exactly two square roots in $Cl(\Delta_q)$. The ideal $\mathfrak{p} = (p, 0)$ is the reduced representative of the unique (non-trivial) ambigue ideal in $Cl(\Delta_q)$. That means, that $\mathcal{O}_{\Delta_q} \neq \mathfrak{p} \in \mathcal{I}_{\Delta_q}(q)$ is the only ideal such that $\mathfrak{p}^2 = \mathcal{O}_{\Delta_q}$. Thus if we compute one square root $\mathfrak{m}_1$ of the ciphertext $\mathfrak{c}$ using the procedure Sqrt_q we immediately get the second square root $\mathfrak{m}_2 = \rho_q(\mathfrak{m}_1\mathfrak{p})$ by a simple multiplication with reduction. That it is possible to distinguish between the two possible messages one has to embed some redundancy into the message ideal, just like in the original Rabin scheme over $(\mathbb{Z}/n\mathbb{Z}^*)$. □

RSA analogue If $h(\Delta_1)$ is known and $h(\Delta_q)$ can be computed using Theorem 6, it is a natural generalization to allow public exponents e other than 2, as long as $gcd(e, h(\Delta_q) = 1$ to implement RSA type cryptosystems in this spirit.
The signature setup for the RSA analogue is completely analogous to the original scheme. I.e. the public exponent e and the secret exponent d are related by $ed \equiv 1 \bmod h(\Delta_q)$. For the encryption of small messages $\mathfrak{m}$ with $\mathcal{N}(\mathfrak{m}) \leq \sqrt{|\Delta_1|/4}$ however we are able to set up a more efficient decryption procedure in analogy to Shamir's unbalanced RSA [27]. Here the exponents are related by $ed \equiv 1 \bmod h(\Delta_1)$ and the decryption takes place in the class group of the *maximal order*. We will show in Section 5 that this scheme seems to be immune against the chosen ciphertext attack proposed in [10].

Algorithm 8. *(RSADecrypt-unbalanced)*
Input: $(\mathfrak{c}, \Delta_1, q)$, *where* $\mathfrak{c} \in \mathcal{I}_{\Delta_q}(q)$ *is the cyphertext,* Δ_1 *is the fundamental discriminant,* q *is the conductor and* d *is the secret exponent.*
Output: *The message* $\mathfrak{m} \in \mathcal{I}_{\Delta_q}(q)$

1. $\mathfrak{C} \leftarrow$ *GotoMaxOrder*$(\mathfrak{c}, q)$
2. $\mathfrak{M} \leftarrow \rho_1(\mathfrak{C}^d)$
3. $\mathfrak{m} \leftarrow$ *GotoNonMaxOrder*$(\mathfrak{M}, q)$

4. *RETURN*($\mathfrak{m}$)

Correctness: By Proposition 2 we may switch to the maximal order without problems. Since $ed \equiv 1 \ mod\, h(\Delta_1)$ and the norm $\mathcal{N}(\mathfrak{M})$ of the resulting $\mathfrak{M}$ is small by assumption we may switch back to the non-maximal order by considering Proposition 3. □

3.3 Totally Non-maximal Order $\Delta_{pq} = \Delta_1 p^2 q^2$

To set up RSA analogues one has to be able to compute $h(\Delta_1)$ using the subexponential algorithm of Hafner/McCurley [11] to derive $h(\Delta_q)$ by application of Theorem 6. If Δ_1 is choosen to be large this will become a formidable task or (for $\Delta_1 >> 10^{80}$) even impossible. In this case we suggest to use public discriminants of the form $\Delta_{pq} = \Delta_1 p^2 q^2$, where p, q are two large primes and the fundamental discriminant might be choosen to be $\Delta_1 = -8$ for example. In this case it is well known, that $h(\Delta_1) = 1$ and therefore one may easily compute $h(\Delta_{pq})$ using Theorem 6. Since one has to deal with larger numbers however this setup seems to be of theoretical interest only.

4 Computing square roots in $Cl(\Delta)$

In Section 4.1 we will outline the Gaussian algorithm which may be used to compute square roots in the class group of maximal as well as non-maximal imaginary quadratic orders. In Section 4.2 we will introduce a new algorithm, which is more suitable for our purpose, because it allows more efficient computation.

4.1 Gauss' square root extraction algorithm

Here we will turn to the description of an algorithm due to Gauss, Shanks, and Lagarias which determines the square root of a given square in the class group of an imaginary quadratic order $\mathcal{O}_\Delta$. This algorithm runs in random polynomial time in the binary length of the input $O(log\,|\Delta|)$ if the factorization of the discriminant is given as part of input ([16]).

First, we note that there is another way of describing the class group of an imaginary quadratic order. One can describe the same object in terms of binary quadratic forms instead of ideals. The use of binary quadratic forms will simplify the presentation of the square root extraction algorithm in quadratic class groups. There is a well known isomorphism between the (ideal) class group of an imaginary quadratic order and the form class group of the corresponding discriminant (see e.g. [26]). If Q is a *positive definite binary quadratic form* then the equivalence class of Q is given by $[Q]$. For the form class group we also write $Cl(\Delta)$. We will recall the most important definitions concerning binary

and ternary quadratic forms in the appendix. The most details can be found in standard books like [1], [15]. All the details are given in [17].

Now we present the square root extraction algorithm due to Gauss, Shanks, and Lagarias. Let Δ be an arbitrary negative integer, which is not a square in $\mathbb{Z}$ with $\Delta < -4$, $\Delta \equiv 0 \ mod\ 4$. (Odd discriminants are handled in a similiar fashion, see [28].) We assume that the factorization of the disriminant Δ is given as part of the input. Without loss of generality let $Q = (\alpha, 2\beta, \gamma)$ be the uniquely determined representative in $[Q]$.

Outline of the Gaussian algorithm for computing square roots in $Cl(\Delta)$

1. **Embedding in a ternary form of determinant -1**
   Embed Q in a ternary quadratic form Q_1 with determinant -1:

   $$Q(x, y) = Q_1(x, y, 0) \qquad \text{with} \qquad det\, Q_1 = -1$$

   Solve the system of simultaneous congruences for m, n, where $\delta = \frac{\Delta}{4} = det\, Q$.

   $$m^2 \equiv \alpha \ mod\ \delta$$
   $$m \cdot n \equiv -\beta \ mod\ \delta$$
   $$n^2 \equiv \gamma \ mod\ \delta$$

   We can find a solution of this system because we know the factorization of $\delta = \frac{\Delta}{4}$:

   $$\delta = p_1^{\mu_1} \dots p_r^{\mu_r}$$

   So we have to solve the congruences $mod\ p_i^{\mu_i}$ and to bring together the solutions with the Chinese remainder theorem. For the computation of square roots $mod\ p_i^{\mu_i}$ we know an efficient algorithm which (in general) presupposes the knowledge of a quadratic non-residue $mod\ p_i$. In practice, we can determine efficiently such a non-residue (by try and error), but we do not know a deterministic polynomial time algorithm for this task. This is the only random step of the algorithm.

   Determine a symmetric matrix $A \in \mathbb{Z}^{3\times 3}$ with $det\, A = -1$ and

   $$A = \begin{pmatrix} \alpha & \beta & * \\ \beta & \gamma & * \\ * & * & * \end{pmatrix} \text{ and adjoint matrix } A^* = \begin{pmatrix} * & * & n \\ * & * & m \\ n & m & \delta \end{pmatrix}.$$

   (By the relation between A and its adjoint A^* this can be done in a unique way.) Let Q_1 be the associated ternary quadratic form, then Q_1 accomplishes the conditions given above.

2. **Reduction to $\Phi = \mathbf{y^2 - 2xz}$**
   Determine the matrix $M \in \mathbf{SL}(\mathbf{3}, \mathbb{Z})$, which reduces Q_1 to $\Phi = y^2 - 2xz$:

   $${Q_1}^M = \Phi = y^2 - 2xz$$

   This is done in the following way: Reduce Q_1 in the sense of reduction of ternary quadratic forms and carry the transformation matrix along. There is at least one reduced ternary quadratic form in every equivalence class. Especially, there are exactly 10

reduced forms with determinant -1. After transforming Q_1 to an equivalent reduced ternary form, we have to apply yet another transformation which is easily found in order to get the ternary form Φ.

3. **Construction of a square root**

   Compute $S := M^{-1}$ and write $S = \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix}$.

   Set $u := b_1,\ v := -a_1,\ d := gcd(u, v)$; replace u, v by $\frac{u}{d}$, $\frac{v}{d}$, respectively. Set $k := \left|\frac{1}{d}(a_2 b_1 - b_2 a_1)\right|$. If $gcd(k^2, 2\Delta) > 1$ then

   $\Big\{$ set $u := b_3,\ v := -a_3,\ d := gcd(u, v)$; replace u, v by $\frac{u}{d}$, $\frac{v}{d}$, respectively, and set $k := \left|\frac{1}{d}(a_2 b_3 - b_2 a_3)\right|$ $\Big\}$.

   Applying the extended Euclidean algorithm determine some integers r, s where $ur - vs = 1$. Set $W := \begin{pmatrix} u & s \\ v & r \end{pmatrix}$. Compute $Q^W = (k^2, l, m)$ $(l, m \in \mathbb{Z})$. Set $G := (k, l, km)$. Then we have $[G] \in Cl(\Delta)$ and $[G]^2 = [Q]$.

The details of this algorithm will be explained in the appendix. As we noted earlier this algorithm runs in random polynomial time in the binary input length $O(log\,|\Delta|)$ if the factorization of Δ is given as part of input:

Proposition 9 ([16]). *Let the complete factorization of the discriminant Δ be given. If the extended Riemann Hypothesis is true or, alternatively, if a quadratic nonresidue n_i is given for each prime p_i dividing Δ the square root extraction algorithm in $Cl(\Delta)$ terminates in $O(log\,|D|)^3 M(log\,|D|))$ elementary operations in the worst case where $M(n)$ is an upper bound on the number of elementary operations necessary to multiply two integers of at most n bits. (Due to Schoenhage and Strassen ([24]) such an upper bound is given by $M(n) = c \cdot n \log n \log\log n$ where c is a suitable constant.*

4.2 A new algorithm to compute square roots in $Cl(\Delta_q)$

In this section we will introduce a new method to compute square roots in $Cl(\Delta_q)$. First we show, how the computation of square roots in $Cl(\Delta_q)$ may be reduced to the computation of square roots in the maximal order $Cl(\Delta_1)$. It would be possible to compute this square root with the Gaussian algorithm above. Since $h(\Delta_1)$ is odd however, it is possible to compute such a square root in $Cl(\Delta_1)$ by a simple exponentiation.

Algorithm 10. *($Sqrt_q$ via $Sqrt_1$)*
Input: $(\mathfrak{m}, \Delta_1, q)$, *where* $\mathfrak{m} \in \mathcal{I}_{\Delta_q}(q)$, $\Delta_1 = -p \equiv 1\ mod\ 4$ *is the fundamental discriminant and q is the conductor.*
Output: *A square root* $\mathfrak{s}$ *of* $\mathfrak{m}$ *in* $Cl(\Delta_q)$.

1. $\mathfrak{M} \leftarrow GotoMaxOrder(\mathfrak{m}, q)$

2. *compute* $\mathfrak{R} \leftarrow \rho_1(\mathfrak{M})$ *and the relative generator* $\alpha \in \mathbb{Q}(\sqrt{\Delta})$, *such that* $\mathfrak{R} = \alpha\mathfrak{M}$
3. *compute* $\mathfrak{T} \leftarrow Sqrt_1(\mathfrak{R})$ *and the relative generator* $\beta \in \mathbb{Q}(\sqrt{\Delta})$, *such that* $\mathfrak{T}^2 = \beta\mathfrak{R}$
4. *compute* γ *such that* $\mathcal{O}_{\Delta_1} \ni \alpha\beta\gamma^2 \equiv a \bmod q\mathcal{O}_{\Delta_1}$ *for some* $a \in \mathbb{Z}$ *such that* $gcd(a, q) = 1$
5. $\mathfrak{S} \leftarrow \gamma\mathfrak{T}$
6. $\mathfrak{s} \leftarrow GotoNonMaxOrder(\mathfrak{S}, q)$
7. *RETURN*($\mathfrak{s}$)

Correctness: The strategy of this algorithm is to take care of the relative generators introduced by reduction during the computation and to "correct" this generator by multiplication with γ^2 in such a way, that the overall generator $\alpha\beta\gamma^2 \in \mathcal{O}_{\Delta_1}$ satisfies

$$\alpha\beta\gamma^2 \equiv a \bmod q\mathcal{O}_{\Delta_1},$$

for some $a \in \mathbb{Z}$ with $gcd(a, f) = 1$ such that $\varphi((\alpha\beta\gamma^2)) \sim \mathcal{O}_{\Delta_q}$. The rest of the algorithm is straight forward.

$$\begin{aligned}
\mathfrak{s}^2 &= \varphi(\mathfrak{S})^2 \\
&= \varphi(\mathfrak{S}^2) \\
&= \varphi(\gamma^2\mathfrak{T}^2) \\
&= \varphi(\beta\gamma^2\mathfrak{R}) \\
&= \varphi(\alpha\beta\gamma^2\mathfrak{M}) \\
&= \varphi(\alpha\beta\gamma^2\varphi^{-1}(\mathfrak{m}) \\
&= \mathfrak{m}\varphi((\alpha\beta\gamma^2)) \\
&\sim \mathfrak{m}
\end{aligned}$$

Note, that the last equivalence follows from Proposition 5. □

Note, that the general strategy of this algorithm, i.e. switching to the maximal order and taking care of the relative generators, can be applied to the ElGamal- and RSA analogues as well. It should be mentioned, however, that the size of relative generator β in step 3 depends on the exponent. I.e. this strategy is well suited for low exponents. This issue and a comparison of the algorithms in terms of complexity and efficiency will be adressed in the full paper.

Like pointed out above, it would be possible to use a tailormade version of Gauss' algorithm to implement Sqrt_1. If the (odd) class number $h(\Delta_1)$ however is known, we can do better:

Algorithm 11. *(*$Sqrt_1$ *via Exp)*
Input: $(\mathfrak{R}, h(\Delta_1))$, *where* $\mathfrak{R}$ *is a reduced* $\mathcal{O}_{\Delta_1}$*-ideal and* $h(\Delta_1)$ *is the class number, where* $\Delta_1 = -p \equiv 1 \bmod 4$ *is a prime discriminant.*
Output: *The square root* $\mathfrak{T}$ *of* $\mathfrak{R}$ *in* $Cl(\Delta_1)$.

1. $\mathfrak{T} = \rho_1(\mathfrak{R}^{(h(\Delta_1)+1)/2})$

Correctness: By genus theory we know, that $h(\Delta_1)$ is odd, because $\Delta_1 = -p$ is a prime discriminant. Noting, that $(h(\Delta_1)+1)/2 \cdot 2 \equiv 1 \ mod\, h(\Delta_1)$ concludes the proof. □

5 Security Considerations

In this section we will discuss the security of the proposed cryptosystems. First we consider the security of the Rabin analogue cryptosystem. Like in the original scheme over $(\mathbb{Z}/n\mathbb{Z}^*)$ we can prove, that breaking one of our Rabin schemes is as hard as factoring the corresponding discriminant.

Theorem 12. *Breaking the Rabin analogue cryptosystems based on maximal, non-maximal, or totally non-maximal orders is as hard as factoring the corresponding discriminant.*

Proof:(Sketch, see [17] for the details) If one knows, the factorization of the discriminant, then one will be able to compute square roots in the class group under consideration using the Gaussian algorithm in Section 4.1.

Suppose that one posseses an algorithm Sqrt, which computes square roots in $Cl(\Delta)$ and thus can break our scheme. Then one will be able to construct a (non-trivial) ambigue class, which carries a factorization of Δ. This may be done by choosing a random class $[A] \in Cl(\Delta)$ and computing $[B] = \mathsf{Sqrt}([A]^2)$. We repeat this procedure until $[B] \neq [A]$. Then $[A] \cdot [B]^{-1}$ is a non-trivial ambigue class. This process may be iterated with the factors to obtain the complete factorization of Δ. □

Next, we discuss the security of the RSA analogue cryptosystems. If the public modulus $n = pq$ is factored, then the original RSA cryptosystem is broken. On the contrary, it is unknown whether breaking the RSA cryptosystem is as intractable as factoring the modulus. The relationship between the public exponent e and the secret exponent d for RSA cryptosystem is given by $ed \equiv 1 \pmod{L}, L = \mathrm{LCM}(p-1, q-1)$, and it is easily verified that the computation of L is as hard as factoring n.

In our RSA analogue based on non-maximal orders of discriminant $\Delta_q = \Delta_1 q^2$, the relationship between the public exponent e and the secret exponent d is given by

$$ed \equiv 1 \pmod{h(\Delta_q)}.$$

Because the fastest known algorithm to compute $h(\Delta_1)$ is sub-exponential in $\log(\Delta_1)$, we can not break the proposed RSA analogue in the non-maximal order in polynomial time by knowing the factorization of Δ_q. It is therefore unknown

whether the computation of $h(\Delta_q)$ is computationally equivalent to factoring Δ_q.

Next, we consider the RSA analogue in the totally non-maximal order $\Delta_{pq} = \Delta_1 p^2 q^2$. The relationship between the public exponent e and the secret exponent d is given by

$$ed \equiv 1 \pmod{h(\Delta_{pq})}.$$

Therefore, if the discriminant Δ_{pq} is factored, then the RSA analogue is broken. On the contrary, it is unknown that to break RSA cryptosystem is as intractable as factoring the discriminant. It is easily verified that the computation of $h(\Delta_{pq})$ is as hard as factoring the discriminant Δ_{pq}. This situation is completely analogous to the original scheme over $(\mathbb{Z}/n\mathbb{Z}^*)$.

Small message attack In the following, we explain that the usage of the small norm message is not secure, even though breaking the Rabin analogue cryptosystems is as intractable as factoring the discriminant. In the ring $\mathbb{Z}$, $a^2 \pmod{n}$ is equal to a^2 without reduction modulo n for small a such as $|a| < \sqrt{n}$. Similarly, it is known that if $\mathcal{N}(\mathfrak{a}) \leq \sqrt{|\Delta|/4}$ holds, then the ideal $\mathfrak{a}$ is already reduced. Thus, $\mathfrak{a}^2$ is a reduced ideal if $\mathcal{N}(\mathfrak{a}) < (|\Delta|/4)^{1/4}$, and the reduction operation for $\mathfrak{a}^2$ is never performed. Let $\mathfrak{a} = (a, b)$, then $\mathcal{N}(\mathfrak{a}^2)$ equals $(a/d)^2$ for $d = \gcd(a, b)$. If $d = 1$, we can simply calculate a by computing the integer square root. In the same manner, when we encrypt $\mathfrak{a}^e$ using a small norm ideal $\mathfrak{a}$ such that $\mathcal{N}(\mathfrak{a}) < (|\Delta|/4)^{1/2e}$, it is not secure in this case.

Low exponent attack For the RSA cryptosystem and Rabin cryptosystem, if we send the same message encrypted for different recipients, then the original message can be recovered. This attack is called the low exponent attack [12] [29]. The low exponent attack and its variations are based on the properties of the ring $(\mathbb{Z}/n\mathbb{Z})$ for a composite integer n. Consider a cryptosystem which encryption function is a polynomial $P(x) \pmod{n}$. When we encrypt the same message M by different encryption functions $P_i(M) \pmod{n_i}$ for $i = 1, 2, \ldots, k$, then the low exponent attack computes the polynomial with the same small message $P(M) \pmod{N}$, $N = \prod_1^k n_i$ using the Chinese remainder theorem. Thus, because $M < N^{1/k}$, the low exponent attack is converted to the previous small message attack. If attackers try to apply the low exponent attack, they have to apply the Chinese remainder theorem in the first step.

However, such an Chinese remainder concept is not known to exist for imaginary quadratic *class groups with different maximal orders.*

Let us discuss the minimal requirements to mount the low exponent attack slightly more abstract. We will only consider the Rabin scheme; the generalisation to the RSA analogue is immediate. Let $\mathfrak{m}_1 \in Cl(\Delta_1)$ and $\mathfrak{m}_2 \in Cl(\Delta_2)$ be ideal-embeddings for some message $m \in \mathbb{N}$. The corresponding ciphertexts are given by $\mathfrak{c}_1 = \rho(\mathfrak{m}_1^2)$ and $\mathfrak{c}_2 = \rho(\mathfrak{m}_2^2)$ respectively. One would have to choose a

group G and define homomorphisms $\varphi_1 : G \to Cl(\Delta_1)$ and $\varphi_2 : G \to Cl(\Delta_2)$. Then the low exponent attack would be to find a group element $\mathfrak{C} \in G$ such that $\varphi_1(\mathfrak{C}) = \mathfrak{c}_1$ and $\varphi_2(\mathfrak{C}) = \mathfrak{c}_2$ and one is able to compute a square root $\mathfrak{M}$ of $\mathfrak{C}$ in G with little effort to obtain the message by computing $\mathfrak{m}_1 = \varphi_1(\mathfrak{M})$ for example.

The most natural choice seems to be $G = Cl(\Delta_1\Delta_2)$, which is the direct analogue to the original attack [12]. In this case however such homomorphisms are not known to exist. Furthermore such homomorphisms could be useful to reduce the computation of the class number $h(\Delta_1\Delta_2)$ to the computation of $h(\Delta_1)$ and $h(\Delta_2)$. This indeed would be small revolution in algorithmic number theory.

It seems to be a difficult task to find a suitable group G and homomorphisms, with the above properties to apply the low exponent attack to our schemes with that little we know about the relation between *different maximal orders* in imaginary quadratic number fields. Thus our schemes can be implemented with low exponents and are therefore more efficient than traditional schemes over $(\mathbb{Z}/n\mathbb{Z}^*)$.

Chosen ciphertext attack Adi Shamir proposed an interesting variant of RSA - the *unbalanced RSA* scheme [27], which allows faster decryption of comparably small messages. The key generation is performed by computing $ed \equiv 1 \ mod\, p-1$, the encryption is performed by computing $C \equiv M^e \ mod\, n$ and the decryption of messages, which have to be smaller than p, is performed by computing $M \equiv C^d \ mod\, p$.

In [10] it is shown that a chosen ciphertext attack, with a ciphertext whose corresponding plain message $M > p$ will entirely break the scheme, i.e. factor the modulus $n = pq$ by computing $gcd(M' - M, n) = p$, where $M' < p$ is the falsely decrypted message. Note that this kind of attack works, because $\mathbb{Z}/n\mathbb{Z}$ is not only a group but a ring.

In the following we will give strong evidence that our proposed unbalanced RSA scheme over non-maximal imaginary quadratic class groups does *not* have this vulnerability and thus can be used for efficiently decrypting rather small messages in a secure manner.

Consider the attack against our proposed scheme. Let $\mathfrak{m}$ be a message ideal such that $\mathcal{N}(\mathfrak{m}) > \sqrt{|\Delta_1|/3}$. Thus by getting decrypted the ciphertext $\mathfrak{c} = \rho_q(\mathfrak{m}^e)$ one obtains a reduced ideal $\mathfrak{m}' \neq \mathfrak{m}$, where $\varphi^{-1}(\mathfrak{m}) \sim \varphi^{-1}(\mathfrak{m}')$ in $Cl(\Delta_1)$. From knowing these two ideals only it seems impossible to factor the discriminant Δ_q.

Now we will consider the case where we apply the above attack several times. Let $\mathbf{AL}_D$ be an oracle which decrypts ciphertexts $\mathfrak{c}$ of previously encrypted messages $\mathfrak{m}$. I.e. $\mathbf{AL}_D(\mathfrak{m})$ returns some message ideal $\mathfrak{m}'$ with $\mathcal{N}(\mathfrak{m}') < \sqrt{|\Delta_1|/3}$ where $\mathfrak{m}'$ is the decrypted ciphertext $\mathfrak{c} = \rho_q(\mathfrak{m}^e)$. By the answer of this oracle we can obtain some information about the size of Δ_1:

$$\mathbf{AL}_D(\mathfrak{m}) \neq \mathfrak{m} \Rightarrow \mathcal{N}(\mathfrak{m}) > \sqrt{|\Delta_1|/4} \quad \mathbf{AL}_D(\mathfrak{m}) = \mathfrak{m} \Rightarrow \mathcal{N}(\mathfrak{m}) < \sqrt{|\Delta_1|/3}$$

Note that if $\sqrt{|\Delta_1|/4} < \mathcal{N}(\mathfrak{m}) < \sqrt{|\Delta_1|/3}$ then the oracle may return the right message depending on whether $\varphi^{-1}(\mathfrak{m})$ is reduced in $Cl(\Delta_1)$ or not. Because this range has size about $0.07735\sqrt{|\Delta_1|}$ it would need an exponential number (in $\log_2 |\Delta_1|$) of trials to obtain a good approximation of $\sqrt{|\Delta_1|/3}$ or $\sqrt{|\Delta_1|/4}$. Therefore the chosen ciphertext attack is not applicable in our case.

References

1. Z.I. Borevich and I.R. Shafarevich: *Number Theory* Academic Press: New York, 1966
2. W. Bosma & P. Stevenhagen, *On the computation of quadratic 2-class groups*, University of Amsterdam, Journal de Théorie des nombres, Bordeaux, 1997
3. J. Buchmann, S. Düllmann: *On the computation of discrete logarithms in class groups*, Advances in Cryptology - CRYPTO '90, Springer-Verlag, **LNCS 537**, 1991, pp. 134-139
4. J. Buchmann and H.C. Williams: *A key-exchange system based on imagninary quadratic fields.* Journal of Cryptology, **1**, 1988, pp. 107-118
5. H. Cohen: *A Course in Computational Algebraic Number Theory.* Graduate Texts in Mathematics **138**. Springer: Berlin, 1993.
6. D.A. Cox: *Primes of the form $x^2 + ny^2$*, John Wiley & Sons, New York, 1989
7. W. Diffie and M. Hellman: *New directions in cryptography*, IEEE Transactions on Information Theory **22**, 1976, pp. 472-492
8. S. Düllmann: *Ein Algorithmus zur Bestimmung der Klassenzahl positiv definiter binärer quadratischer Formen*, PHD-thesis (in german), University of Saarbrücken: 1991
9. T. ElGamal: *A public key cryptosystem and a signature schem based on discrete logarithms*, IEEE Transactions on Information Theory **31**, 1985, pp. 469-472
10. H. Gilbert, D. Gupta, A.M. Odlyzko and J.-J. Quisquater: *Attacks on Shamir's "RSA for paranoids"*, preprint, http://www.research.att.com/ amo/doc/recent.html, 1998
11. J.L. Hafner, K.S. McCurley: *A rigorous subexponential algorithm for computation of class groups*, Journal of the American Mathematical Society, **2**, 1989, 837-850
12. J. Håstad, *Solving simultaneous modular equations of low degree*, SIAM J. Computing, Vol. **17**, No.2, 1988, pp.336-341.
13. L.K. Hua: *Introduction to Number Theory.* Springer-Verlag, New York, 1982.
14. 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**, 1998, pp. 294-307
15. E. Landau, *Aus der elementaren Zahlentheorie*, (in german) , Chelsea Publishing Company 1950, 1927
16. J.C. Lagarias, *Worst-case complexity bounds for algorithms in the theory of integral quadratic forms*, Journal of Algorithms **1**, 1980, pp. 142-186.
17. A. Meyer, *Ein neues Identifikations- und Signaturverfahren über imaginär-quadratischen Zahlkörpern*, Master's Thesis, University of Saarland, Germany, 1997 (ftp://ftp.informatik.tu-darmstadt.de/pub/TI/reports/amy.diplom.ps.gz)

18. K. McCurley: *Cryptographic key distribution and computation in class groups.* In: R.A. Mollin (ed.), *Number Theory and Applications*, Kluwer Academic Publishers, 1989, pp. 459-479
19. National Institute of Standards and Technology (NIST): *Digital Signature Standard (DSS).* Federal Information Processing Standards Publication 186, **FIPS-186**, 19th May, 1994
20. K. Nyberg, R. Rueppel: *A new signature scheme based on the DSA giving message recovery.* 1st ACM Conference on Computer and Communications Security, Fairfax, Virginia. Nov. 3-5, 1993.
21. S. Paulus, T. Takagi: *A new public-key cryptosystem over the quadratic order with quadratic decryption time*, submitted to Journal of Cryptology, 1998
22. M.O. Rabin: *Digitalized signatures and public key functions as intractable as factorization*, **MIT/LCS/TR-212**, MIT Laboratory for Computer Science, 1979
23. R. Rivest, A. Shamir, L. Adleman: *A method for obtaining digital signatures and public key-cryptosystems*, Communications of the ACM,**21**, 1978, pp. 120-126
24. A. Schoenhage and V. Strassen: *Schnelle Multiplikation grosser Zahlen*, Computing **7** (1971), pp. 281-292.
25. C.P. Schnorr: *Efficient identification and signatures for smart cards*, Advances in Cryptology - CRYPTO '89, Springer-Verlag, **LNCS 435**, 1990, pp. 239-252
26. 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.
27. A. Shamir: *RSA for paranoids*, CryptoBytes, 1, Autumn, pp. 1-4, 1995
28. D. Shanks: *Gauss' ternary form reduction and the 2-Sylow subgroup*, Math. Comp. **25**, 1971, pp. 837-853.
29. T. Takagi and S. Naito, *The multi-variable modular polynomial and its applications to cryptography*, Proc. of ISAAC'96, **LNCS 1178**, 1996, pp.386-396.
30. D.B. Zagier: *Zetafuntionen und quadratische Körper*, (in german), Berlin, Springer, 1981, ISBN 3-540-10603-0

A Appendix

In the first two sections of the appendix we will recall the most important notions about binary and ternary quadratic forms. In an third section we will explain why the Gaussian square root extraction algorithm outlined in Section 4.1 works.

A.1 Preliminaries

Let $\Delta \equiv 0,1 \ mod\ 4$ be an integer which is not a square. We consider *binary quadratic forms* $F = (a,b,c) = F(X,Y) = aX^2 + bXY + cY^2$ in two variables X, Y with coefficients $a, b, c \in \mathbb{Z}$. Let $U \in SL(2,\mathbb{Z})$ (i.e. an integral 2×2-matrix of determinant 1), then we define $F^U := F\left([U \cdot (X,Y)^T]^T\right)$, and the relation $F \sim G \overset{def}{\Leftrightarrow} \exists U \in SL(2,\mathbb{Z}) : F^U = G$ is an equivalence relation. $[F]$ is the *equivalence class* of F. The binary quadratic form $F = (a,b,c)$ has the *discriminant* $\Delta = b^2 - 4ac$. F is *positive definite* (*negative definite*), if $\Delta < 0$ and $a > 0$ ($a < 0$, resp.). F is *indefinite* if $\Delta > 0$. If Δ is a square then F

is *irregular*. F is called *primitive* if $gcd(a,b,c) = 1$. If F is positive definite or negative definite then there is a unique representative in the equivalence class of F, and this representative (called *reduced* form) can easily and efficiently be computed. Such a reduced form $F = (a,b,c)$ satisfies $|a| \leq \sqrt{|\Delta|/3}$. This fact is used in the reduction algorithm for ternary quadratic forms which is applied in the square root extraction algorithm in Section 4.1. (For details see [17].)

A.2 Ternary quadratic forms

In the following, we give a short introduction to the reduction of ternary quadratic forms which is a subroutine of the Gaussian square root extraction algorithm.
A *ternary quadratic form* is a polynomial in three variables $F(x,y,z) = a_{11}x^2 + a_{22}y^2 + a_{33}z^2 + 2a_{12}xy + 2a_{13}xz + 2a_{23}yz$, where a_{ij} are some fixed integers. The *associated matrix* of F is the matrix $M_F := \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{pmatrix}$. Let F be the *associated ternary form* of M_F. The *determinant* of F is $det\, F := det\, M_F$, and we say that the adjoint of M_F is $M_F{}^* = \begin{pmatrix} A_{11} & A_{12} & A_{13} \\ A_{12} & A_{22} & A_{23} \\ A_{13} & A_{23} & A_{33} \end{pmatrix} \in \mathbb{Z}^{3\times 3}$ where $A_{ij} = (-1)^{i+j} \cdot det(A'_{ij})$, $(A'_{ij}) \in \mathbb{Z}^{2\times 2}$ is the matrix which one obtains after deleting the i*th* row and the j*th* column. The *adjoint form* F^* of F is defined as the associated ternary form of $(M_F)^*$. Let $X^T = (x,y,z)$, $S \in \mathbb{Z}^{3\times 3}$ We define $F^S(X^T) := F((SX)^T)$. The ternary quadratic forms F, G are *equivalent*, if there is a unimodular matrix $S \in SL(3,\mathbb{Z})$ such that $F^S(X^T) = G(X^T)$. It holds, that $F^S = G$ if and only if $S^T M_F S = M_G$. We say in this case that S is a *transformation matrix* which *transforms* the ternary form F to the form G. This relation is an equivalence relation. A ternary quadratic form F with associated matrix $M_F = (a_{ij})_{i,j}$ and adjoint $M_F{}^* = (A_{ij})_{i,j} \in \mathbb{Z}^{3\times 3}$ is called *reduced* if the following relations holds

(i) $|a_{11}| \leq \frac{4}{3} \cdot |det\, F|^{\frac{1}{3}}$ and (ii) $|A_{33}| \leq \frac{4}{3} \cdot |det\, F|^{\frac{2}{3}}$.

(iii) If $a_{11} = 0$, then $a_{12} = A_{33} = 0$, $|a_{23}| \leq \frac{1}{2} gcd(a_{13}, a_{22})$ and $|a_{33}| \leq |a_{13}|$.

(iv) If $a_{11} \neq 0$, then $A_{33} \neq 0$, $|a_{12}| \leq \frac{1}{2}|a_{11}|$, $|A_{13}| \leq \frac{1}{2}|A_{33}|$ and $|A_{23}| \leq \frac{1}{2}|A_{33}|$.

In each equivalence class of ternary quadratic forms there is at least one reduced form, and there is a deterministic polynomial time algorithm which computes a reduced ternary form which is equivalent to the given ternary form, and the corresponding transformation matrix. The reduction of a ternary quadratic form F can be done by a combination of reduction of binary quadratic forms which are deduced from the ternary form F. The binary quadratic forms which occur here as intermediate results are not always positive definite. They can be negative definite (the discriminant and the first coefficient are both negative), indefinite (the discriminant is positive and not a square), or irregular (the discriminant is a square). "Reduction" then means finding an equivalent binary quadratic

form such that the first coefficient of the resulting form becomes less or equal to $\sqrt{|\Delta|/3}$. The details can be found in [17].

A.3 The idea of the algorithm

Let the primitive positive definite binary quadratic form Q be an arbitrary representative of the given form class $[Q] \in Cl(\Delta)$. We search for a form class $[G] \in Cl(\Delta)$ with $[G]^2 = [Q]$. We now explain the crucial idea of the Gaussian algorithm. The following lemma is for our task of central interest.

Lemma 13. *Let (a,b,c) be a binary quadratic form of discriminant Δ with $gcd(a,b) = 1$. Supposed the representation $\lambda a + \nu b = 1$ with integers λ, ν is given it holds:*

$$[(a,b,c)]^2 = \left[(a^2, b - 2\nu ac, c')\right] \in Cl(\Delta)$$

where c' is an integer which is uniquely determined by the discriminant Δ.
If, furthermore, c is a multiple of a, then the following equation holds:

$$[(a,b,c)]^2 = \left[(a^2, b, c/a)\right] \in Cl(\Delta)\,.$$

This lemma can be used in the following way for computing a square root $[G]$ of $[Q]$:

(1) *Construction of $[G]$:*
Supposed we know some integers u, v with

$$\boxed{Q(u,v) = k^2\,,}$$

where k^2 is an arbitrary square in $\mathbb{Z}$ which is relatively prime to 2Δ and where k is positive. Without loss of generality let $d := gcd(u,v) = 1$. (Otherwise we replace u, v by $\frac{u}{d}$, $\frac{v}{d}$, respectively.) Using the extended Euclidean algorithm we find $r, s \in \mathbb{Z}$ with $ur - vs = 1$. Then we have $W := \left(\begin{smallmatrix} u & s \\ v & r \end{smallmatrix}\right) \in SL(2,\mathbb{Z})$ and $Q \sim Q^W = (Q(u,v), l, m) = \left(k^2, l, m\right)$ with some integers l, m. The binary quadratic form $G := (k, l, km)$ has the discriminant $l^2 - 4k^2m = D$ and is primitive because of $gcd(k,l,km) = gcd(k,l) \stackrel{!}{=} gcd(k, 2\Delta) = 1$ ($t := gcd(k,l) \;\Rightarrow\; t \,|\, D = l^2 - 4k^2m \;\Rightarrow\; t \,|\, gcd(k, 2\Delta) = 1 \;\Rightarrow\; t = 1$). Due to Lemma 13 it holds that $[G]^2 = [Q^W] = [Q]$.

(2) *Computation of suitable integers u, v:*
We still have to explain how to find integers u, v with the properties of (1). The task of determining a representation of a square in $\mathbb{Z}$ by a quadratic form is easily solved for reduced ternary forms of determinant -1. For example, $\Phi(x,y,z) = y^2 - 2xz$ is a reduced ternary quadratic form with determinant -1. Assumed we know a matrix $S \in SL(3,\mathbb{Z})$ with

$$\boxed{Q(x,y) = \Phi^S(x,y,0)\,.}$$

If we write $S = \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix}$, then it follows:

$$\begin{aligned} Q(x,y) &= \Phi\left(\left[S \cdot \begin{pmatrix} x \\ y \\ 0 \end{pmatrix}\right]^T\right) \\ &= \Phi(a_1x + b_1y,\ a_2x + b_2y,\ a_3x + b_3y) \\ &= (a_2x + b_2y)^2 - 2(a_1x + b_1y)(a_3x + b_3y)\,. \end{aligned}$$

By a suitable choice of $x = u$ and $y = v$ the second term becomes zero and we have found a representation of a square in $\mathbb{Z}$ by Q: E.g. with $u := b_1$ and $v := -a_1$ it holds $Q(u,v) = (a_2 \cdot b_1 + b_2 \cdot (-a_1))^2 = k^2$.

(3) *Computation of a suitable matrix S:*
Finally we show how to determine a matrix $S \in SL(3,\mathbb{Z})$ with $Q(x,y) = \Phi^S(x,y,0)$. At first, we embed the binary quadratic form Q in a ternary quadratic form Q_1 of determinant -1, i.e. we compute a ternary form Q_1 with $det\,Q_1 = -1$ and $Q(x,y) = Q_1(x,y,0)$. We can find such a ternary form Q_1 if and only if $[Q]$ is a square in $Cl(\Delta)$ (see [2, ?]). This involves the computation of square roots *mod* Δ, hence the factorization of Δ (see above). Now we determine the matrix $M \in SL(3,\mathbb{Z})$ wich transforms the ternary form Q_1 to the reduced ternary form Φ:

$$Q_1{}^M(x,y,z) = \Phi(x,y,z) = y^2 - 2xz$$

By applying the unimodular transformation $S := M^{-1}$ on every side of the equation we get $Q_1(x,y,z) = \Phi^S(x,y,z)$. Setting $z = 0$ this matrix S fulfills the desired relation:

$$Q(x,y) = Q_1(x,y,0) = \Phi^S(x,y,0)\,.$$