# On Real Quadratic Number Fields Suitable for Cryptography

Daniel Schielzeth and Michael E. Pohst

CONTENTS



We present empirical results that suggest that there are real quadratic fields with properties similar to imaginary quadratic fields in terms of size and structure of the class group. Therefore, these class groups can also be used for encryption schemes such as the ElGamal scheme, where up to now, only class groups of imaginary quadratic fields have been considered. Some security aspects are also addressed.

## 1. INTRODUCTION

The ElGamal Encryption (see [ElGamal 85]) is a public key encryption scheme that needs an abelian group $G$ with the following properties:

(i) In $G$, the Discrete Logarithm Problem (DLP) is not efficiently solvable, i.e., $\sharp G$ is the product of a small integer, say less than 10, and a big prime number.

(ii) Computations in $G$ are efficient.

In this paper, we show that class groups of special real quadratic number fields (fields of Degert type) satisfy both properties.

The ElGamal scheme evolved from the Diffie-Hellman key exchange protocol:

(i) Setup

(a) Let $C_q$ be the big cyclic factor of $G$.

(b) Randomly choose $\gamma \in C_q$ of order $q$.

(c) Randomly choose $a \in \mathbb{N}, a < q$ and compute $\alpha := \gamma^a$.

(d) Public Key: $(G, \gamma, \alpha, q)$.

(e) Secret Key: $(G, a)$.

2000 AMS Subject Classification: Primary 11R11, 11Y40

Keywords: Real quadratic fields, application in cryptography


1058-6458/2005$ 0.50 per page

(ii) Encryption

(a) Let $m \in G$ be the message.

(b) Randomly choose $b \in \mathbb{N}, b < q$.

(c) Compute $m_1 := \gamma^b$.

(d) Compute $m_2 := m \cdot \alpha^b = m \cdot \gamma^{ab}$.

(e) Send $(m_1, m_2)$.

(iii) Decryption

(a) Receive $(m_1, m_2)$.

(b) Compute $\tilde{m} = m_2 \cdot m_1^{-a} = m_2 \cdot \left(\gamma^{ab}\right)^{-1}$.

Usually, one uses a finite group of the form $(\mathbb{Z}_q^*, \cdot)$. It can be replaced by any other group which satisfies the properties mentioned above, for example, the group of points of an elliptic curve over a finite field. In this paper, we present numerical evidence that class groups of special real quadratic number fields also could be used.

Of course, the choice of (the structure of) that class group is crucial in order to avoid known attacks. We refer the reader to the papers [Boneh 98] and [Boneh et al. 00] in which the weaknesses of standard ElGamal encryption are analyzed. Even if the DLP is hard, breaking the weaker Decision Diffie-Hellman problem (DDH) is enough to make such a system insecure. The DDH is believed to be intractable in the group of a sufficiently general elliptic curve of prime order, and, to the best of our knowledge, the same also holds for a class group of prime order. In Section 3.2, we give heuristic reasoning for the frequency of this occurring in specially chosen Degert fields. In practice, it is always advisable to add padding to strengthen the security of the scheme.

## 2. MAPPING OF MESSAGES INTO CLASS GROUPS

In this paper, we consider quadratic number fields of discriminant $\Delta$. We use the following notation:

$$\begin{array}{lcl} \mathcal{O}_\Delta & = & \text{maximal order of the quadratic field with discriminant } \Delta, \\ (a,b) & = & a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z} \text{ ideal in } \mathcal{O}_\Delta, \\ \mathrm{Cl}\,(\Delta) & = & \text{class group of } \mathcal{O}_\Delta, \\ \mathrm{h}\,(\Delta) & = & \text{class number of } \mathcal{O}_\Delta, \\ \mathrm{Reg}\,(\Delta) & = & \text{regulator of } \mathcal{O}_\Delta. \end{array}$$

For an abbreviation we also let, as usual,

$$\begin{array}{lcl} L_x[u,v] & = & \exp\left((v+o\,(1))\,(\ln x)^u\,(\ln\ln x)^{1-u}\right), \\ \overline{X} & = & \text{average of } X. \end{array}$$

We denote the largest prime number below $\frac{\sqrt{|\Delta|}}{2}$ by $P$. Then we can map integer messages $a \le P$ onto reduced ideals $(a,b)$ if we choose $b$ as the square root of $\Delta$ modulo $4a$. Since the computation of such roots is rather tedious when $a$ is not a prime number, we will choose the so-called distance embedding which determines a closest prime number $\tilde{a}$ for $a$, compute $\tilde{b}$ accordingly, and store $(\tilde{a}, \tilde{b})$ along with the distance $d := a - \tilde{a}$. This leads to Algorithm 2.1.

**Algorithm 2.1. (NumberToIdeal.)**

*Input*: A discriminant $\Delta$ and a natural number $n \le \frac{\sqrt{|\Delta|}}{2}$.
*Output:* A reduced ideal $(a,b)$ belonging to $n$ of distance $d$.

$a := \max\{2, n-1\}$
repeat
  $a := NextPrime(a)$
until $\left(\frac{\Delta}{a}\right) = 1 \wedge a \equiv 3, 5, 7 \bmod 8$
if $a \equiv 3 \bmod 4$ then
  $b := \Delta^{\frac{a+1}{4}} \bmod a$
else
  if $\Delta^{\frac{a-1}{4}} \equiv 1 \bmod a$ then
    $b := \Delta^{\frac{a+3}{8}} \bmod a$
  else
    $b := 2\Delta(4\Delta)^{\frac{a-5}{8}} \bmod a$
  end if
end if
if $D \not\equiv b \bmod 2$ then
  $b := a - b$
end if
return $\mathfrak{a} = (\Delta, (a,b))$, $d := n - a$

For details and the complexity of the necessary computations refer to [Schielzeth 03].

The inverse of Algorithm 2.1 is obvious.

We note, that in imaginary quadratic fields every ideal class contains exactly one reduced ideal. This is not true for real quadratic fields in which every ideal class contains a finite set (*cycle*) of reduced ideals. We therefore define a unique representative in each cycle. We emphasize that the special choice of our fields (to be of Degert type) enforces those cycles to be of small length so that computations are efficient.

**Definition 2.2.** A reduced ideal $\mathfrak{a} = (a,b)$ is called *minimal in its cycle* if

$$\forall\, \mathfrak{b} = (\tilde{a}, \tilde{b}) \sim \mathfrak{a} \text{ reduced} \Longrightarrow \tilde{a} < a \text{ or } (\tilde{a} = a \text{ and } \tilde{b} < b)\,.$$

Since the cycles in our fields are small, the determination of a minimum ideal in a cycle is straightforward. Going through all elements of a cycle is canonical.

The encryption and decryption in real quadratic fields is therefore not essentially more difficult than for imaginary fields. Additionally, we compute the distance of the message ideal from the minimal ideal in its cycle and send it. This is done in an efficient way via the corresponding reduced quadratic forms. We omit several auxiliary algorithms that can be found in [Schielzeth 03].

**Algorithm 2.3. (IdealPosInCycle.)**

*Input*: A reduced ideal $\mathfrak{a}$.
*Output*: The distance pos of $\mathfrak{a}$ to the minimal ideal in its cycle.

$f :=$ IdealToForm($\mathfrak{a}$)
$g := f = (a, b, c)$
$\min_a := |a|$, $\min_b := b$, pos $:= 0$, $k := 0$
repeat
  $g :=$ FormReductionStep$(g) = (a, b, c)$
  if $|a| < \min_a$ or $(|a| = \min_a \wedge b \leq \min_b)$ then
    $\min_a := |a|$, $\min_b := b$, pos $:= -k$
  fi
  $k := k + 1$
until $g = f$
if pos $< 0$ then pos $:=$ pos $+k - 1$ fi
return pos

Finally, the recovery of the message ideal from the recepted ideal and position is again straightforward. For estimates on the computation time, refer to [Schielzeth 03].

## 3. ELGAMAL IN IMAGINARY QUADRATIC FIELDS

Imaginary quadratic fields have been used for many cryptographic protocols (see [Buchmann and Hamdy 01] and [Hamdy 02]), since they are fairly easy to handle. Using a reduction algorithm developed for binary quadratic forms (see [Biehl and Buchmann 97]) we can find a unique reduced ideal in every class (see [Cohen 95]) and multiply efficiently (see [Buchmann and Hamdy 01]). Therefore, the representation of an ideal class requires a memory of $\log_2 |\Delta|$ bits.

There are essentially three different ways to attack this encryption scheme, i.e., solving the DLP in $\mathrm{Cl}(\Delta)$ (see [Hamdy and Möller 00]):

(i) It has been proved that Index-Calculus-Algorithms (see [Cohen 95, 5.5]) have an expected subexponential running time of $L_{|\Delta|}\left[\frac{1}{2}, \frac{3}{4}\sqrt{2}\right]$ (see also [Vollmer 00]), whereas it is suspected (see [Jacobson 99]), that for a Multi Polynomial Quadratic Sieve (MPQS) a running time of $L_{|\Delta|}\left[\frac{1}{2}, 1\right]$ is sufficient.

(ii) Shanks' Babystep-Giantstep-Algorithm (deterministic) and Pollard's $\rho$- and $\lambda$-method (probabilistic) have an (expected) exponential running time proportional to the order of $\gamma$, as in Section 1 (see [Menezes et al. 97]).

(iii) If $\mathrm{h}(\Delta)$ is very smooth with a largest prime factor $q$, one can compute $\mathrm{h}(\Delta)$ with a $(p-1)$-method with running time in $\mathcal{O}(q)$ (see [Hamdy and Möller 00] and [Hamdy 02, Algorithm 5.1]). Then it is possible to solve the DLP with the Pohlig-Hellman-Algorithm efficiently with running time in $\mathcal{O}\left(\sum_{i=1}^{k} e_i \left(\ln n + \sqrt{p_i}\right)\right)$ where $n = \prod_{i=1}^{k} p_i^{e_i}$ (see [Menezes et al. 97]).

One can show that, eventually, the Index-Calculus-Algorithm is the most dangerous. A large discriminant providing sufficient safety against attacks on this algorithm also protects messages from attacks when the other methods mentioned are used (see [Hamdy and Möller 00] and [Hamdy 02]).

In Table 1, all class numbers with prime discriminant $\Delta$ with $10^{48} < |\Delta| < 10^{48} - 47523087$ and $\Delta \equiv 1 \bmod 8$ were computed and factored. In this range, there are 107,374 such discriminants. Since the class number is, on average, $\sqrt{|\Delta|}$, we compared this with the probability

| $u$ | Number of class numbers | Portion of class numbers | $\vartheta(u)$ |
|---|---|---|---|
| 1.5 | 63089 | 0.58756 | 0.59453 |
| 2.0 | 32047 | 0.29846 | 0.30685 |
| 2.5 | 13380 | 0.12461 | 0.13033 |
| 3.0 | 4879 | 0.04544 | 0.04861 |
| 3.5 | 1580 | 0.01472 | 0.01623 |
| 4.0 | 472 | 0.00440 | 0.00491 |
| 4.5 | 120 | 0.00112 | 0.00137 |
| 5.0 | 30 | 0.00028 | 0.00035 |
| 5.5 | 5 | 0.00005 | 0.00009 |
| 6.0 | 1 | 0.00001 | 0.00002 |
| 6.5 | 1 | 0.00001 | 0.00000 |

**TABLE 1**. Discriminants with $\sqrt{|\Delta|}^{\frac{1}{u}}$-smooth class number.

| $q = \frac{h(\Delta)}{ord[\mathfrak{a}]}$ | $\mathfrak{a} = (2,1)$ | | $\mathfrak{a} = (3,1)$ | |
|---|---|---|---|---|
| | Number | Portion | Number | Portion |
| $q = 1$ | 86599 | 0.7537 | 38857 | 0.7551 |
| $10^0 < q < 10^1$ | 22718 | 0.1977 | 10073 | 0.1957 |
| $10^1 \le q < 10^2$ | 5007 | 0.0436 | 2268 | 0.0441 |
| $10^2 \le q < 10^3$ | 522 | 0.0045 | 245 | 0.0048 |
| $10^3 \le q < 10^4$ | 50 | 0.0004 | 17 | 0.0003 |
| $10^4 \le q < 10^5$ | 6 | 0.0000 | 2 | 0.0000 |
| Total | 114902 | 1.0000 | 51462 | 1.0000 |

**TABLE 2**. Order of subgroups generated by $[\mathfrak{a}]$, where $|\Delta| \approx 10^{32}$.

$\vartheta(u)$ that an integer $\le \sqrt{|\Delta|}$ is $\sqrt{|\Delta|}^{\frac{1}{u}}$-smooth. Table 1 suggests that these probabilities are about the same.

We want to consider discriminants as used in Table 1, since for those, $(a, b) = (2, 1)$ is an ideal. Table 2 shows that the ideal class $[(2, 1)]$ has a large order with high probability. Further computations for other ideals (Table 3) and other discriminants (Table 4) show that, in general, a randomly chosen ideal class has a large order. Tables 1–4 are found in [Hamdy 02].

| $q = \frac{h(\Delta)}{ord[\mathfrak{a}]}$ | $\mathfrak{a} = (1009,1)$ | | $\mathfrak{a} = (1000003,1)$ | |
|---|---|---|---|---|
| | Number | Portion | Number | Portion |
| $q = 1$ | 43562 | 0.7535 | 53013 | 0.7555 |
| $10^0 < q < 10^1$ | 11481 | 0.1986 | 13784 | 0.1964 |
| $10^1 \le q < 10^2$ | 2475 | 0.0428 | 3043 | 0.0434 |
| $10^2 \le q < 10^3$ | 263 | 0.0045 | 288 | 0.0041 |
| $10^3 \le q < 10^4$ | 27 | 0.0005 | 43 | 0.0006 |
| $10^4 \le q < 10^5$ | 2 | 0.0000 | 2 | 0.0000 |
| Total | 57810 | 1.0000 | 70173 | 1.0000 |

**TABLE 3**. Order of subgroups generated by $[\mathfrak{a}]$, where $|\Delta| \approx 10^{32}$.

| $q = \frac{h(\Delta)}{ord[\mathfrak{a}]}$ | $\mathfrak{a} = (2,1)$ | | $\mathfrak{a} = (3,1)$ | |
|---|---|---|---|---|
| | Number | Portion | Number | Portion |
| $q = 1$ | 81093 | 0.7552 | 29256 | 0.7530 |
| $10^0 < q < 10^1$ | 21667 | 0.1971 | 7678 | 0.1976 |
| $10^1 \le q < 10^2$ | 4621 | 0.0430 | 1701 | 0.0438 |
| $10^2 \le q < 10^3$ | 445 | 0.0041 | 196 | 0.0050 |
| $10^3 \le q < 10^4$ | 41 | 0.0004 | 19 | 0.0005 |
| $10^4 \le q < 10^5$ | 7 | 0.0000 | 1 | 0.0000 |
| Total | 107374 | 1.0000 | 38851 | 1.0000 |

**TABLE 4**. Order of subgroups generated by $[\mathfrak{a}]$, where $|\Delta| \approx 10^{48}$.

## 4. ELGAMAL IN REAL QUADRATIC FIELDS

We studied the possibilities of employing real quadratic fields for the ElGamal scheme and encountered two problems:

(i) The class number is usually small; in more than 95 percent of the cases it is less than ten (see [Cohen and Martinet 87]).

(ii) There is a large number of reduced ideals in every class, arranged in a cycle (see [Ince 34]). If $k$ is the number of reduced ideals in an ideal class we have $\frac{2\mathrm{Reg}(\Delta)}{\ln \Delta} \le k \le \frac{2\mathrm{Reg}(\Delta)}{\ln 2}$ (see [Buchmann et al. 95]).

The Brauer-Siegel-Theorem (see [Lang 91]) states that

$$\ln \sqrt{\Delta} \sim \ln \left( \mathrm{h}\left(\Delta\right) \mathrm{Reg}\left(\Delta\right) \right)$$

and empirical data even suggest

$$\sqrt{\Delta} \sim \mathrm{h}\left(\Delta\right) \mathrm{Reg}\left(\Delta\right).$$

This means that these two problems are actually only one.

Now we introduce a family of real quadratic fields with small regulator.

**Definition 4.1.** Let $N \in \mathbb{N}$ and $D = N^2 + 1$ be square-free. Then $K = \mathbb{Q}\left(\sqrt{D}\right)$ is called a *Degert field*.

**Theorem 4.2.** *For a Degert field* $\mathbb{Q}\left(\sqrt{N^2+1}\right)$ *with* $N \neq 2$ *the number* $k$ *of reduced ideals in an ideal class satisfies* $k = \mathcal{O}\left(\ln \Delta\right)$.

*Proof:* From the fundamental unit $N + \sqrt{N^2+1}$ it is obvious that $\mathrm{Reg}\left(\Delta\right) = \mathcal{O}\left(\ln \Delta\right)$. Using $k \le \frac{2\mathrm{Reg}(\Delta)}{\ln 2}$ from [Buchmann et al. 95] gives the result. □

So, for Degert fields we can expect a large class number and a cycle of reduced ideals that is small and can be computed efficiently. In this cycle, there are different possibilities to define a unique ideal which can be found in polynomial time $\mathcal{O}(\ln(\Delta)^3)$.

In order to study the quality of Degert fields, we computed the Degert fields for $3 \le N \le 10^4$ and $N^2 + 1$ square-free. There are 8,950 such fields. In Tables 5–7, we present the results.

First, we want to find out whether Degert fields satisfy

$$\mathrm{Reg}\left(\Delta\right) \mathrm{h}\left(\Delta\right) \sim \sqrt{\Delta},$$

| Range | Number | $\min \mu(N)$ | $\max \mu(N)$ | $\overline{\mu(N)}$ |
|---|---|---|---|---|
| $2 < N \leq 1000$ | 893 | 0.121 | 2.607 | 0.815 |
| $1000 < N \leq 2000$ | 897 | 0.138 | 2.642 | 0.817 |
| $2000 < N \leq 3000$ | 895 | 0.118 | 3.246 | 0.819 |
| $3000 < N \leq 4000$ | 896 | 0.121 | 2.874 | 0.816 |
| $4000 < N \leq 5000$ | 892 | 0.121 | 3.046 | 0.815 |
| $5000 < N \leq 6000$ | 896 | 0.129 | 2.812 | 0.814 |
| $6000 < N \leq 7000$ | 890 | 0.134 | 2.858 | 0.816 |
| $7000 < N \leq 8000$ | 899 | 0.136 | 3.375 | 0.822 |
| $8000 < N \leq 9000$ | 894 | 0.116 | 2.809 | 0.814 |
| $9000 < N \leq 10000$ | 898 | 0.124 | 2.986 | 0.817 |
| Total | 8950 | 0.116 | 3.375 | 0.817 |

**TABLE 5**. Behaviour of $\mu(N)$ with increasing $N$.

| Divisors of $N$ | Number | $\min \mu(N)$ | $\max \mu(N)$ | $\overline{\mu(N)}$ |
|---|---|---|---|---|
| 1 | 8950 | 0.116 | 3.096 | 0.571 |
| 2 | 4475 | 0.116 | 3.096 | 0.652 |
| $2^2$ | 2231 | 0.344 | 3.096 | 0.980 |
| $2^3$ | 1116 | 0.376 | 2.874 | 0.979 |
| 3 | 2987 | 0.216 | 3.096 | 0.857 |
| $3^2$ | 997 | 0.247 | 3.096 | 0.858 |
| 5 | 1945 | 0.185 | 3.096 | 0.727 |
| 7 | 1280 | 0.158 | 2.741 | 0.668 |
| $2^2 \cdot 3$ | 744 | 0.712 | 3.096 | 1.469 |
| $2^2 \cdot 3 \cdot 5$ | 163 | 1.109 | 3.096 | 1.866 |
| $2^2 \cdot 3 \cdot 5 \cdot 7$ | 23 | 1.519 | 2.741 | 2.136 |

**TABLE 6**. Influence of prime divisors.

like imaginary fields do. We define

$$\mu(N) := \frac{\mathrm{Reg}(\Delta)\mathrm{h}(\Delta)}{\sqrt{\Delta}}$$

where $\Delta$ is the discriminant of $\mathbb{Q}\left(\sqrt{N^2+1}\right)$.

Table 5 shows that in fact, $\mu(N)$ is a good measure for the size of the class group with respect to the size of $\Delta$. It seems that Degert fields have properties similar to imaginary quadratic fields, in terms of the size of $\mathrm{Cl}(\Delta)$. Now, we want to study how different properties of $N$ influence $\mu(N)$.

In Table 6, we see that $\mu(N)$ is large when $N$ is divisible by 4 and many small prime numbers. This property does not depend on the size of $N$. Having seen that we can produce real quadratic fields with arbitrarily large class numbers, we will now study the cyclic part of $\mathrm{Cl}(\Delta)$.

### 4.1 The Cyclic Part of a Degert Class Group

If $\mathrm{Cl}(\Delta)$ is not cyclic, in more than 99 percent of cases, the additional factors of the class group have even order. It has been proved (see [Hasse 63]) that we can avoid these cases by choosing $N^2+1 \in \mathbb{P}$. For practical applications, this is a necessary choice, since it is hard to prove that a number is square-free unless it is a prime.

Now, we want to study the probability of choosing an ideal class with large order. From [Lang 68, IV.3], we cite the lemma below.

**Lemma 4.3.** *Let $D = N^2+1 \equiv 1 \bmod 4$, i.e. $N = 2 \cdot N_0$. Then $\mathfrak{a} = \mathfrak{h}(N,p) := (p,1)$ is an ideal $\forall\, p \mid N_0$ with $\mathrm{ord}_{\mathrm{Cl}(\Delta)}([\mathfrak{a}]) > 1$.*

Similar to what we did in Tables 2–4, we now want to study the probability of randomly choosing an ideal class with large order. We will consider ideals of the form $\mathfrak{h}(N,p)$ with $p$ minimal ($p_{\min}$), with $p_{\mathrm{best}}$ where $\mathrm{ord}(\mathfrak{h}(N,p))$ is largest, and finally $p = 2$ when $N \equiv 0 \bmod 4$. We did this for all $N$ (Table 8), $N^2+1 \in \mathbb{P}$ (Table 9), and $N^2+1 \in \mathbb{P}, 12 \mid N$ (Table 10).

As we can see, these ratios improve significantly if we chose $N^2+1 \in \mathbb{P}$ since, in this case, we cannot have any even factors of $\mathrm{Cl}(\Delta)$. It also decreases the possibility of an ideal class having an order other than $\mathrm{h}(\Delta)$. It

| $q := \frac{h(\Delta)}{h_{cycl}(\Delta)}$ | | | | $N^2+1 \in \mathbb{P}$ | | $12 \mid N, N^2+1 \in \mathbb{P}$ | |
|---|---|---|---|---|---|---|---|
| | Number | Portion | Even | Number | Portion | Number | Portion |
| $q = 1$ | 3618 | 0.4042 | 0 | 831 | 0.9905 | 142 | 0.9793 |
| $q \leq 2$ | 6560 | 0.7330 | 2942 | 831 | 0.9905 | 142 | 0.9793 |
| $q \leq 3$ | 6598 | 0.7372 | 2942 | 837 | 0.9976 | 144 | 0.9931 |
| $q \leq 4$ | 8410 | 0.9397 | 4754 | 837 | 0.9976 | 144 | 0.9931 |
| $q \leq 10$ | 8857 | 0.9896 | 5193 | 838 | 0.9988 | 144 | 0.9931 |
| $q \leq 28$ | 8946 | 0.9996 | 5281 | 839 | 1.0000 | 145 | 1.0000 |
| $q \leq 64$ | 8950 | 1.0000 | 5285 | 839 | 1.0000 | 145 | 1.0000 |
| Total | 8950 | 1.0000 | 5285 | 839 | 1.0000 | 145 | 1.0000 |

**TABLE 7**. Behaviour of $h(\Delta)/h_{cycl}(\Delta)$.

| $q := \frac{ord[\mathfrak{a}]}{h(\Delta)}$ | $\mathfrak{a} := \mathfrak{h}(N, p_{min})$ | | $\mathfrak{a} := \mathfrak{h}(N, p_{best})$ | | $\mathfrak{a} := \mathfrak{h}(N, 2)$ | |
|---|---|---|---|---|---|---|
| | Number | Portion | Number | Portion | Number | Portion |
| $q = 1$ | 839 | 0.1875 | 1723 | 0.3851 | 835 | 0.3744 |
| $q \leq 5$ | 1832 | 0.4095 | 2372 | 0.5302 | 1813 | 0.8130 |
| $q \leq 10$ | 2105 | 0.4705 | 2497 | 0.5581 | 2061 | 0.9242 |
| $q \leq 20$ | 2294 | 0.5127 | 2577 | 0.5760 | 2185 | 0.9798 |
| $q \leq 50$ | 2549 | 0.5697 | 2778 | 0.6209 | 2225 | 0.9978 |
| $q \leq 100$ | 2959 | 0.6614 | 3041 | 0.6797 | 2230 | 1.0000 |
| Total | 4474 | 1.0000 | 4474 | 1.0000 | 2230 | 1.0000 |

**TABLE 8**. Order of $[\mathfrak{a}] \in Cl(\Delta)$ where $N$ is even.

| $q := \frac{ord[\mathfrak{a}]}{h(\Delta)}$ | $\mathfrak{a} := \mathfrak{h}(N, p_{min})$ | | $\mathfrak{a} := \mathfrak{h}(N, p_{best})$ | | $\mathfrak{a} := \mathfrak{h}(N, 2)$ | |
|---|---|---|---|---|---|---|
| | Number | Portion | Number | Portion | Number | Portion |
| $q = 1$ | 325 | 0.3874 | 653 | 0.7783 | 321 | 0.7589 |
| $q \leq 5$ | 387 | 0.4613 | 707 | 0.8427 | 380 | 0.8983 |
| $q \leq 10$ | 428 | 0.5101 | 738 | 0.8796 | 412 | 0.9740 |
| $q \leq 20$ | 451 | 0.5375 | 752 | 0.8963 | 420 | 0.9929 |
| $q \leq 50$ | 498 | 0.5936 | 771 | 0.9190 | 422 | 0.9976 |
| $q \leq 100$ | 588 | 0.7008 | 805 | 0.9595 | 423 | 1.0000 |
| Total | 839 | 1.0000 | 839 | 1.0000 | 423 | 1.0000 |

**TABLE 9**. Order of $[\mathfrak{a}] \in Cl(\Delta)$ where $N$ is even and $N^2+1$ prime.

| $q := \frac{ord[\mathfrak{a}]}{h(\Delta)}$ | $\mathfrak{a} := \mathfrak{h}(N, p_{min})$ | | $\mathfrak{a} := \mathfrak{h}(N, p_{best})$ | | $\mathfrak{a} := \mathfrak{h}(N, 2)$ | |
|---|---|---|---|---|---|---|
| | Number | Portion | Number | Portion | Number | Portion |
| $q = 1$ | 107 | 0.7379 | 136 | 0.9379 | 107 | 0.7379 |
| $q \leq 5$ | 128 | 0.8828 | 144 | 0.9931 | 128 | 0.8828 |
| $q \leq 10$ | 139 | 0.9586 | 144 | 0.9931 | 139 | 0.9586 |
| $q \leq 20$ | 144 | 0.9931 | 145 | 1.0000 | 144 | 0.9931 |
| $q \leq 50$ | 144 | 0.9931 | 145 | 1.0000 | 144 | 0.9931 |
| $q \leq 100$ | 145 | 1.0000 | 145 | 1.0000 | 145 | 1.0000 |
| Total | 145 | 1.0000 | 145 | 1.0000 | 145 | 1.0000 |

**TABLE 10**. Order of $[\mathfrak{a}] \in Cl(\Delta)$ for $12 \mid N$ and $N^2+1$ prime.

is interesting that these ratios improve even more when considering only smooth $N$ (Table 10). Table 10 shows that $p = 2$ is not always the best choice, but is still amazingly good. In Tables 8 and 9, the results for $p = 2$ are the best because there we consider slightly smoother $N$, since 4 divides $N$. It is not possible to determine $p_{best}$ efficiently. Comparing the results with Tables 2 and 4 we see that the order of the ideal class chosen of $[\mathfrak{h}(N, 2)]$ for $N^2+1 \in \mathbb{P}$ shows a similar behaviour as the order in imaginary quadratic fields.

| | | | $N^2+1 \in \mathbb{P}$ | | $12 \mid N, N^2+1 \in \mathbb{P}$ | | |
|---|---|---|---|---|---|---|---|
| $u$ | Number | Portion | Number | Portion | Number | Portion | $\vartheta(u)$ |
| 1.0 | 8945 | 1.0000 | 834 | 1.0000 | 145 | 1.0000 | 1.00000 |
| 1.5 | 7675 | 0.8580 | 479 | 0.5743 | 58 | 0.4000 | 0.59453 |
| 2.0 | 5686 | 0.6357 | 261 | 0.3129 | 28 | 0.1931 | 0.30685 |
| 2.5 | 4163 | 0.4654 | 128 | 0.1535 | 16 | 0.1103 | 0.13033 |
| 3.0 | 2933 | 0.3279 | 63 | 0.0755 | 7 | 0.0483 | 0.04861 |
| 3.5 | 2195 | 0.2454 | 31 | 0.0372 | 3 | 0.0207 | 0.01623 |
| 4.0 | 1584 | 0.1771 | 15 | 0.0180 | 3 | 0.0207 | 0.00491 |
| 4.5 | 1135 | 0.1269 | 7 | 0.0084 | 2 | 0.0138 | 0.00137 |
| 5.0 | 889 | 0.0994 | 5 | 0.0060 | 2 | 0.0138 | 0.00035 |
| 5.5 | 743 | 0.0831 | 2 | 0.0024 | 1 | 0.0069 | 0.00009 |
| 6.0 | 549 | 0.0614 | 0 | 0.0000 | 0 | 0.0000 | 0.00002 |
| 6.5 | 350 | 0.0391 | 0 | 0.0000 | 0 | 0.0000 | 0.00000 |
| 7.0 | 207 | 0.0231 | 0 | 0.0000 | 0 | 0.0000 | 0.00000 |
| 10.0 | 34 | 0.0038 | 0 | 0.0000 | 0 | 0.0000 | 0.00000 |
| 15.0 | 0 | 0.0000 | 0 | 0.0000 | 0 | 0.0000 | 0.00000 |

**TABLE 11**. Discriminants with $(\sqrt{\Delta}/\mathrm{Reg}(\Delta))^{\frac{1}{u}}$-smooth class number.

### 4.2 The Smoothness of a Degert Class Number

To prevent attacks on the Pohlig-Hellman-Algorithm, $\mathrm{h}(\Delta)$ must not be very smooth, since the running time of this algorithm essentially depends on the size of the largest prime factor of $\mathrm{h}(\Delta)$. A class number that is not smooth also increases the probability that a randomly chosen class in $\mathrm{Cl}(\Delta)$ has a large order, which prevents attacks by other methods.

For arbitrary $N$ the number of (not necessarily different) prime factors of $\mathrm{h}(\Delta)$ is, on average, 4.36. We can push this number down to 2.03 by also choosing $N^2+1 \in \mathbb{P}$, because this prevents even factors of $\mathrm{Cl}(\Delta)$. Further, choosing $12 \mid N$ we get down to 2.28 prime factors on average. This is slightly larger, but with increasing $N$ this value gets closer to the case $N^2+1 \in \mathbb{P}$.

Now, we want to compare the smoothness of Degert class numbers with the smoothness of class numbers of imaginary quadratic fields. From Table 1, we conclude that the smoothness is about the same as the smoothness of a randomly picked integer. Table 11 shows that for arbitrary $N$ there are many more smooth class numbers than for imaginary quadratic fields, unless we chose $N^2+1 \in \mathbb{P}$ (compare with Table 1). If $N$ is smooth we get even fewer smooth class numbers.

### 4.3 Summary

Assuming that our results are representative of the behaviour of Degert fields, we conclude:

(i) $\mathrm{h}(\Delta)$ is large if $\Delta$ is large. For a sufficiently smooth $N$ we get

$$\mathrm{h}(\Delta) \geq \frac{\sqrt{\Delta}}{\mathrm{Reg}(\Delta)} \approx \frac{2\sqrt{\Delta}}{\ln \Delta}.$$

(ii) With high probability, $\mathrm{Cl}(\Delta)$ contains a big cyclic factor. The probability that the order of a randomly chosen ideal class is close to $\mathrm{h}(\Delta)$ is also high. For $\Delta \in \mathbb{P}$, the results are similar to those of imaginary quadratic fields.

(iii) The probability that $\mathrm{h}(\Delta)$ is $B$-smooth, becomes arbitrarily small when $\Delta$ becomes large. If $N$ is smooth and $N^2+1 \in \mathbb{P}$, the class numbers are less smooth than the class numbers of imaginary quadratic fields. The even part of $\mathrm{h}(\Delta)$ can be controlled.

These results suggest that solving the DLP in Degert class groups with $N^2+1 \in \mathbb{P}$ and $N$ divisible by 4 and other small prime numbers is about as hard as solving the DLP in a class group of an imaginary quadratic field with a discriminant of the same magnitude. This means, that Degert fields provide safety similar to imaginary quadratic fields, if used for the ElGamal encryption scheme.

## 5. PERFORMANCE

In this section, we will focus on the practical side, i.e., the running times of some examples. The algorithms were implemented in KASH and run on a AMD Athlon 1800+ Processor. The sizes of the modules and the discriminants were chosen to provide approximately the same

| | RSA | $\mathbb{Z}_q$ | $\Delta < 0$ | $\Delta > 0$ |
|---|---|---|---|---|
| Setup in ms | 21 000 | 800 000 | 52 710 | 6 840 |
| Encryption in ms | 1 | 91 | 2 640 | 2 890 |
| Decryption in ms | 38 | 43 | 3 320 | 4 280 |
| Encryptable bitlength | 1024 | 1024 | 340 | 340 |
| Effectively encryptable bitlength | 1023 | 1024 | 331 | 331 |
| Memory for encryption party in bit | 1 050 | 2 080 | 459 000 | 464 000 |
| Size of sent message in bit | 1 023 | 2 060 | 1 360 | 1 380 |
| Memory for decryption party in bit | 2 050 | 2 060 | 1 020 | 1 020 |

**TABLE 12**. Comparison of performance.

| | RSA | $\mathbb{Z}_q$ | $\Delta < 0$ | $\Delta > 0$ |
|---|---|---|---|---|
| Setup in ms | 21 000 | 800 000 | 52 710 | 6 840 |
| Encryption in ms | 1 | 91 | 7 940 | 8 710 |
| Decryption in ms | 38 | 43 | 10 000 | 12 900 |
| Size of sent message in Bit | 1 023 | 2 060 | 4 100 | 4 160 |

**TABLE 13**. Running times needed for processing one 1024-bit-message.

| | RSA | $\mathbb{Z}_q$ | $\Delta < 0$ | $\Delta > 0$ |
|---|---|---|---|---|
| Setup | $\mathcal{O}\left(\ln(n)^{7+\varepsilon}\right)$ | $\mathcal{O}\left(\ln(q)^{7+\varepsilon}\right)$ | $\mathcal{O}\left(\ln(\Delta)^{7+\varepsilon}\right)$ | $\mathcal{O}\left(\ln(\Delta)^{7+\varepsilon}\right)$ |
| Encryption | $\mathcal{O}\left(\ln(n)^3\right)$ | $\mathcal{O}\left(\ln(q)^3\right)$ | $\mathcal{O}\left(\ln(\Delta)^{7+\varepsilon}\right)$ | $\mathcal{O}\left(\ln(\Delta)^{7+\varepsilon}\right)$ |
| Decryption | $\mathcal{O}\left(\ln(n)^3\right)$ | $\mathcal{O}\left(\ln(q)^3\right)$ | $\mathcal{O}\left(\ln(\Delta)^3\right)$ | $\mathcal{O}\left(\ln(\Delta)^3\right)$ |

**TABLE 14**. Comparison of the magnitude of running times.

amount of safety according to [Hühnlein 00]:

$$\begin{array}{lcll} n & \approx & 2^{1024} & \text{for RSA} \\ q & \approx & 2^{823} & \text{for ElGamal in } \mathbb{Z}_q \\ \Delta & \approx & -2^{686} & \text{for ElGamal in } \mathrm{Cl}(\Delta), \Delta < 0 \\ \Delta & \approx & 2^{686} & \text{for ElGamal in } \mathrm{Cl}(\Delta), \Delta > 0. \end{array}$$

In each case, we chose 10 different modules and discriminants, for each of these structures 10 different keys, and again for each key 10 different messages. Altogether we encrypted 1,000 messages in each case.

In order to choose a good $\Delta > 0$ we multiplied

$$n = \pi(10)^5 \cdot \pi(30) \cdot \pi(60) \cdot \pi(150)$$

where

$$\pi(n) := \prod_{p \in \mathbb{P}, p \leq n} p$$

by random 12-bit-numbers $f$ until $\Delta = (f \cdot n)^2 + 1 \in \mathbb{P}$. Surprisingly, this was much faster than finding arbitrary prime numbers of the same size for imaginary quadratic discriminants.

**Remark 5.1.** Refer to Table 12. We cannot encrypt every number, since we cannot map every number efficiently to an ideal. If $n$ is the number of encryptable numbers then we call $\log_2(n)$ the *effectively encryptable bitlength*. The memory for the encryption and for the decryption party, is the number of bits this party has to memorize. Memory needed for computations is not included. To save time, we worked with precomputed lists of powers of ideals, explaining the large memory needed for encrypting in class groups.

The algorithms for using the ElGamal scheme with class groups are much more complicated than those used for modules (RSA and ElGamal in $\mathbb{Z}_q$). Therefore, a more efficient and direct implementation of these algorithms will significantly improve their performance with respect to the module algorithms.

## ACKNOWLEDGEMENTS

This article is based on the *Diplom* thesis [Schielzeth 03]. We thank the referee for various insightful comments.

## REFERENCES

[Biehl and Buchmann 97] Ingrid Biehl and Johannes Buchmann. "An Analysis of the Reduction Algorithms for Binary Quadratic Forms." Technical Report TI-26/97, Technische Universität Darmstadt, Fachbereich Informatik. Available from World Wide Web (http://www.informatik.tu-darmstadt.de/TI/Veroeffentlichung/TR/), 1997.

[Boneh 98] Dan Boneh. "The Decision Diffie Hellman Problem." In *Algorithmic Number Theory, Portland, 1998*, Lecture Notes in Computer Science, 1423, edited by J. P. Buhler, pp. 48–63. Berlin: Springer-Verlag, 1998.

[Boneh et al. 00] Dan Boneh, Antoine Joux, and Phong Q. Nguyen. "Why Textbook ElGamal and RSA Encryption Are Insecure." In *Proc. Asiacrypt '00*, Lecture Notes in Computer Science, 1976, pp. 30–44. Berlin: Springer-Verlag, 2000.

[Buchmann and Hamdy 01] Johannes Buchmann and Safuat Hamdy. "A Survey on IQ Cryptography." Technical Report TI-4/01, Technische Universität Darmstadt, Fachbereich Informatik. Available from World Wide Web (http://www.informatik.tu-darmstadt.de/TI/Veroeffentlichung/TR/), 2001.

[Buchmann et al. 95] Johannes Buchmann, Christoph Thiel, and Hugh C. Williams. "Short Representation of Quadratic Integers." In *Computational Algebra and Number Theory, Sydney 1992*, Mathematics and its Applications, 325, edited by Wieb Bosma and Alf J. van der Poorten, pp. 159–185. Norwood, MA: Kluwer Academic Publishers, 1995.

[Cohen 95] Henri Cohen. *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, 138. New York: Springer-Verlag, 1995.

[Cohen and Martinet 87] Henri Cohen and J. Martinet. "Class Groups of Number Fields: Numerical Heuristics." *Mathematics of Computation* 48:177 (1987), 123–137.

[ElGamal 85] Taher ElGamal. "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms." *IEEE Transactions on Information Theory* 31:4 (1985), 469–472.

[Hamdy 02] Safuat Hamdy. "Über die Sicherheit und Effizienz kryptographischer Verfahren mit Klassengruppen imaginär-quadratischer Zahlkörper." PhD diss., Technische Universität Darmstadt, Fachbereich Informatik, Darmstadt. Available from World Wide Web (http://www.informatik.tu-darmstadt.de/TI/Veroeffentlichung/TR/), 2002.

[Hamdy and Möller 00] Safuat Hamdy and Bodo Möller. "Security of Cryptosystems Based on Class Groups of Imaginary Quadratic Orders." Technical Report TI-4/00, Technische Universität Darmstadt, Fachbereich Informatik. Available from World Wide Web (http://www.informatik.tu-darmstadt.deTI/Veroeffentlichung/TR/), 2000.

[Hasse 63] H. Hasse. *Zahlentheorie*, Second edition. Berlin: Akademie–Verlag, 1963.

[Hühnlein 00] Detlef Hühnlein. "Quadratic Orders for NESSIE – Overview and Parameter Sizes of Three Public Key Families." Technical Report TI-3/00, Technische Universität Darmstadt, Fachbereich Informatik. Available from World Wide Web (http://www.informatik.tu-darmstadt.de/TI/Veroeffentlichung/TR/), 2000.

[Ince 34] E. L. Ince. "Cycles of Reduced Ideals in Quadratic Fields." *British Assoc. Advanc. Sci. Math. Tables 4* (1934), pp. XVI + 80 p.

[Jacobson 99] Michael J. Jacobson, Jr. "Subexponential Class Group Computation in Quadratic Orders." PhD diss., Technische Universität Darmstadt, Fachbereich Informatik, Darmstadt, 1999.

[Lang 68] H. Lang. "Über eine Gattung elementar-arithmetischer Klasseninvarianten reell-quadratischer Zahlkörper." *Journal für die reine und angewandte Mathematik* 233 (1968), 123–175.

[Lang 91] Serge Lang. *Algebraic Number Theory*, Graduate Texts in Mathematics, 110, Second edition. New York: Springer-Verlag, 1991.

[Menezes et al. 97] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. Boca Raton, FL: CRC Press, 1997.

[Schielzeth 03] Daniel Schielzeth. "Realisierung der ElGamal-Verschlüsselung in quadratischen Zahlkörpern." Master's thesis, Technische Universität Berlin. Available from World Wide Web (http://www.math.tu-berlin.de/~kant/publications.html), 2003.

[Vollmer 00] Ulrich Vollmer. "Asymptotically Fast Discrete Logarithms in Quadratic Number Fields." Technical Report TI-6/00, Technische Universität Darmstadt, Fachbereich Informatik. Available from World Wide Web (http://www.informatik.tu-darmstadt.de/TI/Veroeffentlichung/TR/), 2000.

Daniel Schielzeth, Technische Universität Berlin, Institut für Mathematik, Straße des 17. Juni 136, 10623 Berlin, Germany (schielzeth@web.de)

Michael Pohst, Technische Universität Berlin, Institut für Mathematik, Straße des 17. Juni 136, 10623 Berlin, Germany (pohst@math.TU-Berlin.de)

Received January 16, 2004; accepted in revised form December 27, 2004.