

Number field cryptography

Johannes Buchmann Tsuyoshi Takagi Ulrich Vollmer

Abstract

This paper gives an overview of the state of art in cryptography based on quadratic orders. It discusses the intractable problems in class groups and the infrastructure of quadratic orders, approaches to the solution to these problems, and the crypto-systems employing them as underlying problems.

1 Introduction

Public key cryptography is one of the main techniques for making the internet secure. Most public key crypto-systems are based on intractable computational problems in number theory such as factoring integers. However, no such problem is known that is provably intractable. Therefore, it is necessary to keep searching for new public key primitives whose security is unrelated to the security of the known schemes.

One source for computationally hard problems is algebraic number theory. In 1988 Buchmann and Williams [18] presented a variant of the Diffie-Hellman key exchange protocol in class groups of imaginary quadratic orders. Since then many public key crypto-systems have been suggested whose security is based on difficult problems in quadratic number fields.

In this paper, we give an overview of the state of the art of quadratic field crypto-systems. It is organized as follows: In section 2 we very briefly introduce the structures used in quadratic field cryptography: ideals and ideal classes. In section 3 we turn to imaginary quadratic cryptography. First we outline the computational problems, then we list approaches for their solution, finally we show how these problems have been used to devise cryptographic protocols. Section 4 is structured as the preceding section, but deals with real quadratic cryptography. We conclude with an overview over open problems in the area.

For other survey papers, see [20] and [13].

2 Class groups

For background on number theory see e.g. [9]. Let Δ be an integer that is not a square in \mathbb{Z} and assume that $\Delta \equiv 0, 1 \pmod{4}$. By $\mathcal{O} = \mathcal{O}(\Delta)$ denote the quadratic order of discriminant Δ .

Every fractional \mathcal{O} -ideal I has a representation

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

where q is a positive rational number, a is a positive integer, and b is an integer. The numbers q and a are uniquely determined. The integer b is unique modulo $2a$. If $q = 1$, we will write $I = (a, b)$. The norm of I is q^2a .

The fractional \mathcal{O} -ideals form a multiplicative Abelian group $\mathcal{I} = \mathcal{I}(\Delta)$. The set $\mathcal{P} = \mathcal{P}(\Delta)$ of principal \mathcal{O} -ideals is a subgroup of \mathcal{I} . The quotient group $\text{Cl} = \text{Cl}(\Delta) = \mathcal{I}/\mathcal{P}$ is finite. Its cardinality is the class number $h = h(\Delta)$ of \mathcal{O} . The ideal class of an ideal $I = (a, b)$ is written as $[I] = [a, b]$.

3 Imaginary quadratic cryptography

Let $\Delta < 0$. Then \mathcal{O} is an imaginary quadratic order.

3.1 Computational problems

Group operation The group operations in the class group Cl can be implemented efficiently. The elements of the class group are represented by their uniquely determined reduced representative (a, b) where $-a < b \leq a$ and $0 < a < \sqrt{|\Delta|}/3$. The product of two \mathcal{O} -ideal classes can be computed in time $O((\log |\Delta|)^2)$ (see [5]) or even $(\log |\Delta|)^{1+o(1)}$ (see [48]). Practical improvements are the algorithms NUCOMP and NUDUPL (see [49], and [39]). The inverse of an ideal class $[a, b]$ is $[a, -b]$. The reduced representative of $[a, -b]$ is $(a, -b)$ if $b \neq a$ and (a, b) otherwise. So inversion of \mathcal{O} -ideal classes is possible in time $O(\log |\Delta|)$.

We also explain how to choose random elements from the class group. Under the assumption of the extended Riemann hypothesis, the class group Cl is generated by the classes of all invertible prime ideals of norm smaller than $12(\log |\Delta|)^2$ (see [2]). A random element in Cl can be computed by determining a power product of the elements of that generating system where the exponents are randomly chosen from $\{1, \dots, |\Delta|\}$.

Next, we explain the intractable computational problems in imaginary quadratic class groups that can be used as the security basis of cryptographic protocols. These problems are intractable for all but possibly a very small fraction (smaller than 2^{-24}) of all discriminants $\Delta > 2^{675}$ (see [32]).

Root problem Given a positive integer $e > 2$ and a random e th power g in Cl , find an e th root of g . Solving the root problem for $e = 2$ is equivalent to factoring the discriminant Δ (see [10] with erratum in [11]).

Group order problem No efficient algorithm is known for computing the class number h of \mathcal{O} . In fact, computing the class number of an imaginary quadratic order is at least as hard as factoring the discriminant Δ .

Hence, imaginary quadratic class groups cannot be used to implement those cryptographic algorithms based on the discrete logarithm problem that require the knowledge of the group order.

Diffie-Hellman problem The Diffie-Hellman problem is the following. Given a random $g \in \text{Cl}$ and random a, b in $\{0, \dots, 2^t\}$ where t is a positive integer, $t \geq 160$. Given g, g^a and g^b , find g^{ab} .

Discrete logarithm problem No efficient discrete logarithm algorithm for imaginary quadratic class groups is known. We give a more precise description of the discrete logarithm problem in imaginary quadratic class groups (IQ-DL). Choose a random element g in $\text{Cl}(\Delta)$. Choose a random element k in $\{0, \dots, 2^t\}$ where t is a positive integer, $t \geq 160$. Set $h = g^k$. Given g and h , find $m \in \mathbb{Z}$ with $h = g^m$.

Hidden kernel problem The *hidden kernel problem* is the basis of the NICE crypto-system (see [46]). Assume that Δ is a fundamental discriminant and let p be an odd prime. The extension map

$$e : \text{Cl}(p^2\Delta) \rightarrow \text{Cl}(\Delta), \quad [I] \mapsto [I\mathcal{O}(\Delta)]$$

is a surjective homomorphism. The kernel $\ker(e)$ of that map is a cyclic group with $p - \left(\frac{\Delta}{p}\right)$ elements.

We explain the *hidden kernel problem*. Let $[a, b]$ be an $\mathcal{O}(p^2\Delta)$ -ideal class with $a < \sqrt{|\Delta|}/2$. Let $[P]$ be a generator of $\ker(e)$. Given the generator $[P]$, a random element in the coset $[a, b]\ker(e)$, and the discriminant $p^2\Delta$, the task is to find (a, b) . The use of a generator $[P]$ as input in the hidden kernel problem is explained by the fact that random elements in $\ker(e)$ have to be generated using public information.

If the fundamental discriminant Δ is known, then the hidden kernel problem can be easily solved. This can be seen as follows. If $[A, B]$ is in $[a, b]\ker(e)$ then $(a, b) = (A, B)\mathcal{O}(\Delta) \cap \mathcal{O}(p^2\Delta)$.

3.2 Solving the computational problems

The most efficient class number algorithm is the index calculus algorithm IQ-MPQS by Jacobson [36]. IQ-MPQS also solves the discrete logarithm problem in the class group Cl . Its running time is conjectured to be $L_\Delta[1/2, \sqrt{9/8} + o(1)]$ where

$$L_\Delta[u, v] = \exp(v((\log |\Delta|)^u (\log \log |\Delta|)^{1-u})).$$

The most efficient algorithm for solving the root problem in Cl has the complexity $L_\Delta[1/2, 1]$ which is slightly smaller than the complexity of the computation of the class number since the linear algebra stage can be performed (mod e).

Jacobson [37] reports running times of less than an hour for the computation of the structure of class groups of random 40 digit discriminants, and

running (CPU) times of less than 10 days for special 80 digit discriminants on a 296 MHz SUN UltraSPARC-II platform. The running time of his algorithms can be improved using the optimized linear algebra techniques of [26].

Vollmer ([52] with corrigendum in [53]) has presented an IQ-DL algorithm that assuming the extended Riemann hypothesis has running time bounded by $L_{\Delta}[1/2, \sqrt{9/8} + o(1)]$. For a proof of this bound see [54]. An extension of this algorithm that also computes the class number and class group structure is shown to have the same complexity.

The improvement of these results in comparison to those of the first sub-exponential algorithm that computes the class group of a maximal imaginary quadratic order by Hafner and McCurley [28] lie in the generation of relations with few non-zero entries, the termination of the algorithm before a full relation lattice is computed, and faster linear algebra routines on the basis of the work of Mulders and Storjohann [44].

The difficulty of the hidden kernel problem is based on that of the factoring problem. If the discriminant $p^2\Delta$ can be factored, the hidden kernel problem for $p^2\Delta, [P]$ can be solved in polynomial time. The converse is not known. Because the generator $[P]$ is published, the knowledge of $[P]$ might be used in factoring $p^2\Delta$.

3.3 Cryptographic algorithms

The intractable problems described in the previous section can be used as the security basis for several cryptographic algorithms.

Since the Diffie-Hellman problem in Cl is intractable, the Diffie Hellman key exchange protocol ([21]) and the Diffie Hellman integrated encryption scheme DHIES ([3]), a simple extension of the ElGamal encryption scheme ([23]), can be implemented in Cl yielding variants called IQ-DH and IQ-IES, see [31]. In order to avoid the embedding of plain texts into ideal classes, encryption can be effected by xoring the plain text with the Diffie-Hellman key.

Some DL-based signature schemes such as the ElGamal signature scheme and the DSA (see [22]) cannot be implemented in imaginary quadratic class groups since they require the knowledge of the group order. However, the DSA variant described in [32], called IQ-DSA, does not require the knowledge of the group order. Hence, it can be implemented in imaginary quadratic class groups. The disadvantage of IQ-DSA compared to DSA is that it requires larger exponents and produces larger signatures. Another DSA variant called RDSA was suggested in [6]. A version of RDSA that uses exponents that are as small as DSA exponents was broken in [25].

Since the root problem in imaginary quadratic class groups is intractable, the Guillou-Quisquater signature scheme [27] can be implemented in those groups. This variant of the Guillou-Quisquater scheme is referred to as

IQ-GQ.

In [31] Hamdy reports about experimental results concerning IQ-DSA and IQ-GQ. For example, for a 671-bit discriminant which guarantees a security comparable to 1024-Bit RSA generating a signature with IQ-GQ takes 139.06 ms and verifying a signature takes 93.74 ms on a 500MHz SunBlade 100. Hamdy offers a C-library with improved performance [30].

In the random oracle model, the security of IQ-DSA can be reduced to the difficulty of the IQ discrete logarithm problem. Also, in the random oracle model IQ-GQ can be reduced to the IQ root problem (see [32] and [31]). The security proofs of IQ-DH, and IQ-IES carry directly over from the known proofs for e.g. elliptic curve Diffie Hellman key exchange, EC-DH, and the analysis of IES in [1].

The NICE encryption scheme is based on the hidden kernel problem. It is a refinement of ElGamal-type crypto-system proposed by Hühnlein et al. [35]. We sketch the NICE crypto-system. The public key is a pair $(p^2\Delta, P)$ where Δ is a fundamental discriminant, p is a prime, and P an $\mathcal{O}(p^2\Delta)$ -ideal whose class $[P]$ is a generator of $\ker(e)$. Here, e is the extension map introduced in the previous section. The secret key is p .

To encrypt a message, that message is embedded into an $\mathcal{O}(p^2\Delta)$ -ideal class (a, b) with $a < \sqrt{|\Delta|}/2$. That ideal class is multiplied by a random power of $[P]$. The resulting ideal class is the cipher text C . The cipher text $C = [A, B]$ is decrypted by computing $(a, b) = (A, B)\mathcal{O}(\Delta) \cap \mathcal{O}(p^2\Delta)$. The decryption algorithm requires only quadratic bit complexity $O((\log(p^2\Delta))^2)$. If $p^2\Delta$ is a 1024-bit discriminant then decryption takes about 2 ms on a Celeron 500 MHz using LiDIA and under 1 second on a Siemens SLE 66CX80S at 5 MHz [33].

Jaulmues et al. presented a chosen cipher text attack against the NICE primitive [40]. A semantically secure variant of NICE in the random oracle model was then proposed in [16]. The hidden kernel problem has been used for several cryptographic applications, namely digital signatures [34], undeniable signatures [4], distributed RSA key generation [8], and ID-based cryptography [8].

Meyer [42] has shown how to transfer the Fiat-Shamir signature protocol to $\text{Cl}(\Delta)$. Since it is possible to extract quadratic roots in $\text{Cl}(\Delta)$ in polynomial time once a factorization of the discriminant is known—this was already noted by Gauss, see [10]—the discriminant has to be chosen as large as an RSA key at the same security level, rendering IQ-FS inefficient.

4 Real quadratic cryptography

Let $\Delta > 0$. Then \mathcal{O} is a real quadratic order.

The real quadratic case differs from the imaginary one by three effects: Class groups of real quadratic fields are usually small. Real quadratic fields

have non-trivial units. Ideal reduction in real quadratic orders is not unique. Indeed, there is not one reduced form in each class, but a cycle of forms which is traversed by successive reduction. Typically, the number of reduced ideals in an ideal class is approximately $\sqrt{\Delta}$.

Thus there is no efficient algorithm for deciding equality of \mathcal{O} -ideal classes. Therefore, DL-based cryptographic protocols cannot be directly implemented in real quadratic class groups. The question whether there is an analogue of the NICE crypto-system in real quadratic orders has not been discussed.

4.1 Computational problems

Group operation An element of the class group is represented by a reduced representative (a, b) . It satisfies $|a|, |b| < \sqrt{\Delta}$. As in the imaginary quadratic case, the product of two \mathcal{O} -ideal classes can be computed in time $O((\log \Delta)^2)$ or even $(\log \Delta)^{1+o(1)}$, see again [5] and [48]. Again, one can apply variants of the NUCOMP, and NUDUPL algorithms for practical improvements (see [51] and [39]). The inverse of an ideal class $[a, b]$ is $[a, -b]$. So inversion of \mathcal{O} -ideal classes is possible in time $O(\log \Delta)$.

The problem of deciding equality of real quadratic ideal classes is very similar to a discrete logarithm problem. We explain this similarity and we show how to implement cryptographic protocols based on that problem.

Let $[I]$ and $[J]$ be two \mathcal{O} -ideal classes with reduced representatives I and J . Those ideal classes are equal if there exists α in the field F of fractions of \mathcal{O} such that

$$J = \alpha I.$$

If such an α exists, then the coset $\alpha\mathcal{O}^*$ is uniquely determined where \mathcal{O}^* is the unit group of \mathcal{O} . This implies that $\ln |\alpha|$ is uniquely determined modulo the regulator $R = R(\mathcal{O})$ of \mathcal{O} . Now consider the set P of all reduced principal \mathcal{O} -ideals. For each $I \in P$ we can write

$$I = \alpha\mathcal{O}$$

with $\alpha \in F$. Then $\ln |\alpha|$ is called a distance of I (from \mathcal{O}). It can be considered as a kind of discrete logarithm of I . To explain the analogy, we let G be a cyclic group of order n with generator g written additively. Then for $u, v \in \mathbb{Z}$ we have $u \cdot g = v \cdot g$ if and only if $u \equiv v \pmod{n}$. Likewise, for $\alpha, \beta \in F^*$ we have $\alpha\mathcal{O} = \beta\mathcal{O}$ if and only if $\ln |\alpha| \equiv \ln |\beta| \pmod{R}$. Hence, R plays the role of the group order and P plays the role of the group. Next, consider the set of distances $D = \{\ln |\alpha| \in \mathbb{R} : \alpha \in F^*, \text{ and } \alpha\mathcal{O} \text{ is reduced}\}$. We have already seen that this set has additive period R . Also, this set is discrete on the real line. To be more precise, any interval of length $\ln 2$ contains at most two elements of D and any interval of length $(\ln \Delta)/2$ contains at least one element of D .

So it is justified to view the elements in D as discrete logarithms. We describe the algorithmic situation.

In the group G , raising elements to powers is efficiently possible if the group operations can be efficiently implemented. This means that if $a \in \mathbb{Z}$, it is possible to compute $h = a \cdot g$ in polynomial time. Note that a is a discrete logarithm of h . So we can determine elements of prescribed discrete logarithm in polynomial time. Also, given h and an integer k but not a it is possible to compute in polynomial time a group element with discrete logarithm ka . That group element is $k \cdot h$.

In P the following are possible. Let $a \in \mathbb{Z}$. It is possible to determine in polynomial time an $I \in P$ with distance close to a . More precisely, an I can be found such that there is a generator α of I for which $\ln |\alpha|$ is an element of D which is the closest or the second closest element of D to a . Also, given I with distance close to a , an approximation to $\delta(a) = \ln |\alpha| - a$ and an integer k but not α , an ideal $J \in P$ with distance close to ka can be found in polynomial time. We call J a k th power of I in P .

If $I \in P$ and an approximation of error < 1 to a distance of I is given, then it is possible in polynomial time to find $\alpha \in F^*$ in compact representation (see [17]) with $I = \alpha\mathcal{O}$. This process is also very efficient in practice: Maurer [41] has computed the compact representation of the fundamental unit of an order with 63-digit discriminant given a regulator approximation in less than 0.35 seconds on a 296MHz SUN UltraSparc-II. Given the compact representation of a generator, the distance of I can be computed efficiently to arbitrary precision.

Next, we explain the intractable computational problems in the infrastructure of real quadratic orders that can be used as the security basis of cryptographic protocols.

Root problem We can consider the following generalized root problem. Let I be a random element in P , let e be a positive integer, $e \geq 2$. Find all $J \in P$ such that the e -th power of J in the sense explained previously is I .

Regulator problem We have seen that the regulator R plays the role of a group order. The regulator problem is the following. Given Δ . Find an integer R' with $|R' - R| < 1$. From R' an approximation of R with any given precision can be computed in polynomial time.

Diffie-Hellman problem The real quadratic Diffie-Hellman problem is the following. Given random a, b in $\{0, \dots, 2^t\}$ where t is a positive integer, $t \geq 160$. Let $I \in P$ have distance close to a and let $J \in P$ have distance close to b . Given I and J find $K \in P$ with distance close to ab .

Principal ideal problem We describe the analogue of the discrete logarithm problem in P . Given a random element I in P , find an approximation $d \in \mathbb{Q}$ to a distance δ of I such that $|d - \delta| < 1$.

Discrete logarithm problem A generalization of the principal ideal problem is the general discrete logarithm problem. This problem is the

following. Let I be a reduced \mathcal{O} -ideal. Let k be a random element in $\{1, \dots, 2^t\}$ with $t \geq 160$. Let J be a reduced \mathcal{O} -ideal in $[I]^k$. Given I, J . Find $m \in \mathbb{Z}$, and $a \in \mathbb{Q}$ such that there is $\alpha \in F$ with $J = \alpha I^m$, and $|a - \ln |\alpha|| < 1$.

4.2 Solving the computational problems

The most efficient algorithm for solving the root problem in P requires the computation of the regulator. The most efficient regulator algorithm is the index calculus algorithm MPQS by Jacobson [37]. MPQS also solves the discrete logarithm problem in the class group Cl.

It is reported in [38] that using Jacobson's MPQS, the regulator of an order with 101-digit discriminant was computed in 3.8 years of CPU time on 550 MHz Pentium III machines.

Vollmer ([52],[53]) has presented probabilistic algorithms for all but the first of the listed problems which—assuming an extended Riemann hypothesis—have running time $L_\Delta[1/2, \sqrt{9/8}]$. For a proof of this bound for a Monte Carlo regulator algorithm, see [53], otherwise see [54]. A solution of the root problem can be obtained by a simple extension of his results.

4.3 Cryptographic algorithms

Since the intractable problems described in the previous section are very similar to the problems in the imaginary quadratic case, the cryptographic algorithms that can be implemented in real quadratic orders are very similar to the imaginary quadratic cryptography schemes. However, since approximations to logarithms of real numbers are used in the real quadratic case, real quadratic cryptography schemes are less efficient than imaginary quadratic cryptography algorithms. Nevertheless, it is very interesting that cryptography in the set P is possible despite the fact that P is not a group.

The first cryptographic algorithm in real quadratic fields was the real quadratic Diffie-Hellman scheme [19] (see also [12] and [47]). It is slightly more complicated than the Diffie-Hellman key exchange algorithm in a group. The parties select secret integers a and b . They calculate ideals A and B in P with distance close to a and b , respectively. The common key is an ideal K with distance close to ab . However, there is a possible ambiguity in the computation of K . So an extra communication step may be necessary to remove that ambiguity. A DH key exchange in an order with 768-bit discriminant can be performed in 2 seconds CPU time on an 800 MHz Pentium III machine [39].

Real-quadratic ElGamal encryption can also be implemented based on real quadratic Diffie-Hellman key exchange. Moreover, there is a variant of the Fiat-Shamir signature protocol [24], called PIP-FS, which relies on the

intractability of the Principal Ideal Problem (see above), and was proposed and analyzed in [14].

Choosing the discriminant of the underlying order for PIP-FS at the same order of magnitude as is secure for crypto-systems in imaginary quadratic class groups at a security level corresponding to 1024-bit RSA, PIP-FS can be executed in about 3 seconds CPU time on a 300 MHz Pentium II. Key generation takes less than a minute.

5 Open Problems

This overview shows that much has been done in quadratic field cryptography. However, there are still many open problems.

Imaginary quadratic field cryptography is ready for practical use. Offered are a Java implementation [45], and a C-library for IQ-cryptography [30]. It would be nice to see IQ-cryptography being used in real applications.

Real quadratic field cryptography is still too inefficient to be used in practice. Security of RQ schemes hinges on the right choice of the underlying order. To increase security, the authors of [38] suggest the use of orders with discriminants of a particular form, since in these orders the application of the currently fastest algorithm for the computation of the regulator is considerably slower than in the average case. The record computations also given in the paper give valuable data points for estimates of lower bounds on the size of cryptographically secure discriminants. In general, however, a comprehensive analysis and, on its basis, a recommendation for the right choice of parameters in RQ cryptography is still outstanding.

There are generalizations of quadratic field cryptography to arbitrary number fields. First ideas are described in [15], [43] and [7]. A very interesting aspect of general number field cryptography is the fact that no attack is known that is sub-exponential in the field degree. This is due to the fact that breaking crypto-systems in number fields of degree n requires the computation of short vectors in n -dimensional lattices.

One possible set-up of number field cryptography is to use number fields with small regulators and large discriminants. They have large class groups and deciding equality in such class groups is easy. Therefore, the IQ-crypto-algorithms can be implemented in such fields. However, when the field degree is large, arithmetic in the class group is very inefficient. There is a big need for optimization.

Also, the right choice of parameters is an open problem. In particular, it is an interesting question how to generate infinite families of number fields of very large degree with small regulators. It is in principle also possible to use number fields with small class numbers and large regulators. Very little is known about such applications.

Finally, it is an open question to what extent general number field cryp-

tography is resistant to quantum computer attacks. Discrete logarithms in the imaginary quadratic class group can be computed in polynomial time using standard techniques since there is a unique representation for each group element, see [50]. Hallgren has sketched in [29] a polynomial time quantum algorithm for the computation of the regulator of a real quadratic order and the solution of the principal ideal problem (PIP) in it. Extensions to higher degree fields and their behavior at increasing degree remain to be studied.

Number field cryptography continues to be an interesting research subject.

References

- [1] Michel Abdalla, Mihir Bellare, and Philip Rogaway, *An encryption scheme based on the Diffie-Hellman problem*, Progress in Cryptology — CT-RSA 2001 (David Naccache, ed.), Lecture Notes in Computer Science, vol. 2020, Springer-Verlag, 2001, pp. 143–158.
- [2] Eric Bach, *Explicit bounds for primality testing and related problems*, Mathematics of Computation **55** (1990), no. 191, 355–380.
- [3] Mihir Bellare and Philip Rogaway, *Minimizing the use of random oracles in authenticated encryption schemes*, Information and Communications Security, ICIS '97 (Y. Han, T. Okamoto, and S. Quing, eds.), Lecture Notes in Computer Science, vol. 1334, Springer-Verlag, 1997, pp. 1–16.
- [4] Ingrid Biehl, Sachar Paulus, and Tsuyoshi Takagi, *Efficient undeniable signature schemes based on ideal arithmetic in quadratic orders*, Designs, Codes and Cryptography (to appear).
- [5] Ingrid Biehl and Johannes Buchmann, *An analysis of the reduction algorithms for binary quadratic forms*, Voronoi's Impact on Modern Science, Kyiv, Ukraine 1998 (Peter Engel and Halyna M. Syta, eds.), National Academy of Sciences of Ukraine, 1999, pp. 71–98.
- [6] Ingrid Biehl, Johannes Buchmann, Safuat Hamdy, and Andreas Meyer, *A signature scheme based on the intractability of extracting roots*, Tech. Report TI-1/00, Technische Universität Darmstadt, Fachbereich Informatik, 2000, <http://www.informatik.tu-darmstadt.de/TI/Veroeffentlichung/TR/>.
- [7] ———, *A signature scheme based on the intractability of computing roots*, Designs, Codes and Cryptography **25** (2002), no. 3, 223–236.

- [8] Ingrid Biehl and Tsuyoshi Takagi, *A new distributed primality test for shared RSA keys using quadratic fields*, Information Security and Privacy, ACISP 2002 (Lynn Batten and Jennifer Seberry, eds.), Lecture Notes in Computer Science, vol. 2384, Springer-Verlag, 2002, pp. 1–16.
- [9] Zenon I. Borevich and Igor R. Shafarevich, *Number theory*, Pure and Applied Mathematics, Vol. 20, Academic Press, New York, 1966.
- [10] Wieb Bosma and Peter Stevenhagen, *On the computation of quadratic 2-class groups*, Journal de Théorie des Nombres de Bordeaux **8** (1996), no. 2, 283–313.
- [11] ———, *Erratum: “On the computation of quadratic 2-class groups” by W. Bosma and P. Stevenhagen*, Journal de Théorie des Nombres de Bordeaux **9** (1997), no. 1, 249.
- [12] J. Buchmann, R. Scheidler, and H.C. Williams, *A key-exchange protocol using real quadratic fields*, Journal of Cryptology **7** (1994), 171–199.
- [13] Johannes Buchmann and Safuat Hamdy, *A survey on IQ-cryptography*, Tech. Report TI-4/01, Technische Universität Darmstadt, Fachbereich Informatik, 2000, <http://www.informatik.tu-darmstadt.de/TI/Veroeffentlichung/TR/>.
- [14] Johannes Buchmann, Markus Maurer, and Bodo Möller, *Cryptography based on number fields with large regulator*, Tech. Report TI-5/00, Technische Universität Darmstadt, Fachbereich Informatik, 2000, <http://www.informatik.tu-darmstadt.de/TI/Veroeffentlichung/TR/>.
- [15] Johannes Buchmann and Sachar Paulus, *A one way function based on ideal arithmetic in number fields*, Advances in Cryptology – CRYPTO ’97 (Burton S. Kaliski, ed.), Lecture Notes in Computer Science, vol. 1294, Springer-Verlag, 1997, pp. 385–394.
- [16] Johannes Buchmann, Kouichi Sakurai, and Tsuyoshi Takagi, *An IND-CCA2 public-key cryptosystem with fast decryption*, Information Security and Cryptology - ICISC 2001 (Kwangjo Kim, ed.), Lecture Notes in Computer Science, vol. 2288, Springer-Verlag, 2002, pp. 51–71.
- [17] Johannes Buchmann, Christoph Thiel, and Hugh C. Williams, *Short representation of quadratic integers*, Computational Algebra and Number Theory, Sydney 1992 (Wieb Bosma and Alf J. van der Poorten, eds.), Mathematics and its Applications, vol. 325, Kluwer Academic Publishers, 1995, pp. 159–185.
- [18] Johannes Buchmann and Hugh C. Williams, *A key-exchange system based on imaginary quadratic fields*, Journal of Cryptology **1** (1988), no. 2, 107–118.

- [19] ———, *A key-exchange system based on real quadratic fields*, Advances in Cryptology – CRYPTO '89 (Gilles Brassard, ed.), Lecture Notes in Computer Science, vol. 435, Springer-Verlag, 1990, pp. 335–343.
- [20] ———, *Quadratic fields and cryptography*, Number Theory and Cryptography (John H. Loxton, ed.), London Mathematical Society Lecture Note Series, vol. 154, Cambridge University Press, 1990, pp. 9–25.
- [21] Whitfield Diffie and Martin E. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory **IT-22** (1976), no. 6, 644–654.
- [22] *Digital signature standard*, Federal Information Processing Standards Publication FIPS 186-2, NIST, 2000.
- [23] Taher ElGamal, *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Trans. Inform. Theory **31** (1985), no. 4, 469–472.
- [24] Amos Fiat and Adi Shamir, *How to prove yourself: Practical solutions to identification and signature problems*, Advances in Cryptology – CRYPTO '86 (Andrew M. Odlyzko, ed.), Lecture Notes in Computer Science, vol. 263, Springer-Verlag, 1987, pp. 186–194.
- [25] Pierre-Alain Fouque and Guillaume Poupard, *On the security of RDSA*, Advances in Cryptology – EURCRYPT 2003 (Eli Biham, ed.), Lecture Notes in Computer Science, vol. 2656, Springer-Verlag, 2003, to appear.
- [26] Mark Giesbrecht, Michael Jacobson, Jr., and Arne Storjohann, *Algorithms for large integer matrix problems*, Applied algebra, algebraic algorithms and error-correcting codes (Melbourne, 2001), Lecture Notes in Computer Science, vol. 2227, Springer, Berlin, 2001, pp. 297–307.
- [27] Louis C. Guillou and Jean-Jacques Quisqater, *A practical zero-knowledge protocol fitted to security microprocessors minimizing both transmission and memory*, Advances in Cryptology – EUROCRYPT '88 (Christoph G. Günther, ed.), Lecture Notes in Computer Science, vol. 330, Springer-Verlag, 1988, pp. 123–128.
- [28] James L. Hafner and Kevin S. McCurley, *A rigorous subexponential algorithm for computation of class groups*, Journal of the American Mathematical Society **2** (1989), no. 4, 837–850.
- [29] Sean Hallgren, *Polynomial-time quantum algorithms for pell's equation and the principal ideal problem*, Proceedings of the thirty-fourth annual ACM symposium on the theory of computing, ACM Press, 2002, pp. 653–658.

- [30] Safuat Hamdy, `libiq` — *a library for arithmetic in class groups of imaginary quadratic orders*, <http://www.math.ucalgary.ca/~hamdy/libiq.html>.
- [31] ———, *Über die Sicherheit und Effizienz kryptografischer Verfahren mit Klassengruppen imaginär-quadratischer Zahlkörper*, Ph.D. thesis, Technische Universität Darmstadt, Fachbereich Informatik, Darmstadt, Germany, 2002, <http://www.informatik.tu-darmstadt.de/ftp/pub/TI/reports/hamdy.diss.pdf>.
- [32] Safuat Hamdy and Bodo Möller, *Security of cryptosystems based on class groups of imaginary quadratic orders*, Advances in Cryptology – ASIACRYPT 2000 (Tatsuaki Okamoto, ed.), Lecture Notes in Computer Science, vol. 1976, Springer-Verlag, 2000, pp. 234–247.
- [33] Michael Hartmann, Sachar Paulus, and Tsuyoshi Takagi, *NICE – new ideal coset encryption*, Cryptographic Hardware and Embedded Systems, CHES '99 (Çetin K. Koç and Christof Paar, eds.), Lecture Notes in Computer Science, vol. 1717, Springer-Verlag, 1999, pp. 328–339.
- [34] Detlef Hühnlein, *Faster generation of NICE-schnorr-type signatures*, Topics in Cryptology - CT-RSA 2001 (Berlin) (D. Naccache, ed.), Lecture Notes in Computer Science, vol. 2020, Springer-Verlag, 2001, pp. 1–12.
- [35] Detlef Hühnlein, Michael J. Jacobson, Jr., Sachar Paulus, and Tsuyoshi Takagi, *A cryptosystem based on non-maximal imaginary quadratic orders with fast decryption*, Advances in Cryptology – EUROCRYPT '98 (Kaisa Nyberg, ed.), Lecture Notes in Computer Science, vol. 1403, Springer-Verlag, 1998, pp. 294–307.
- [36] Michael J. Jacobson, Jr., *Applying sieving to the computation of quadratic class groups*, Mathematics of Computation **68** (1999), no. 226, 859–867.
- [37] ———, *Subexponential class group computation in quadratic orders*, Ph.D. thesis, Technische Universität Darmstadt, Fachbereich Informatik, Darmstadt, Germany, 1999.
- [38] Michael J. Jacobson, Jr., Renate Scheidler, and Hugh C. Williams, *The efficiency and security of a real quadratic field based-key exchange protocol*, Public-Key Cryptography and Computational Number Theory (Warsaw, Poland), de Gruyter, 2001, pp. 89–112.
- [39] Michael J. Jacobson, Jr. and Alfred J. van der Poorten, *Computational aspects of NUCOMP*, Algorithmic Number Theory, ANTS-V (Claus Fieker and David R. Kohel, eds.), Lecture Notes in Computer Science, vol. 2369, Springer-Verlag, 2002, pp. 120–133.

- [40] Éliane Jaulmes and Antoine Joux, *A NICE cryptanalysis*, Advances in Cryptology – EUROCRYPT 2000 (Bart Preneel, ed.), Lecture Notes in Computer Science, vol. 1807, Springer-Verlag, 2000, pp. 382–391.
- [41] Markus Maurer, *Regulator approximation and fundamental unit computation for real quadratic orders*, Ph.D. thesis, Technische Universität Darmstadt, Fachbereich Informatik, Darmstadt, Germany, 2000.
- [42] Andreas Meyer, *Ein neues Identifikations- und Signaturverfahren über imaginärquadratischen Zahlkörpern*, Master’s thesis, Technische Universität Darmstadt, Fachbereich Informatik, 1997, German. <http://www.informatik.tu-darmstadt.de/pub/TI/reports/amy.diplom.ps.gz>.
- [43] Andreas Meyer, Stefan Neis, and Thomas Pfahler, *First implementation of cryptographic protocols based on algebraic number fields*, Information Security and Privacy, ACISP 2001, Sydney (Vijay Varadharajan and Yi Mu, eds.), Lecture Notes in Computer Science, vol. 2119, Springer, 2001, pp. 84–103.
- [44] Thom Mulders and Arne Storjohann, *Diophantine linear system solving*, International Symposium on Symbolic and Algebraic Computation, ISSAC ’99 (Sam Dooley, ed.), ACM Press, 1999.
- [45] *NFProvider — a toolkit for the Java Cryptography Architecture (JCA/JCE) for Number Field Cryptography*, <http://www.informatik.tu-darmstadt.de/TI/Forschung/FlexiProvider/overview.html#NFProvider>, Part of the FlexiProvider toolkit.
- [46] Sachar Paulus and Tsuyoshi Takagi, *A new public-key cryptosystem over a quadratic order with quadratic decryption time*, Journal of Cryptology **13** (2000), no. 2, 263–272.
- [47] Renate Scheidler, *Applications of algebraic number theory to cryptography*, Ph.D. thesis, University of Manitoba, Winnipeg, Manitoba, 1993.
- [48] Arnold Schönhage, *Fast reduction and composition of binary quadratic forms*, International Symposium on Symbolic and Algebraic Computation, ISSAC ’91 (Stephen M. Watt, ed.), ACM Press, 1991, pp. 128–133.
- [49] Daniel Shanks, *On Gauss and composition I, II*, Number Theory and Applications, Calgary 1988 (Richard A. Mollin, ed.), NATO ASI Series, Series C, vol. 265, Kluwer Academic Publishers, 1989, pp. 163–178, 179–204.
- [50] Peter W. Shor, *Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM Journal on Computing **26** (1997), no. 5, 1484–1509.

- [51] Alfred van der Poorten, *A note on NUCOMP*, Mathematics of Computation, to appear.
- [52] Ulrich Vollmer, *Asymptotically fast discrete logarithms in quadratic number fields*, Algorithmic Number Theory, ANTS-IV (Wieb Bosma, ed.), Lecture Notes in Computer Science, vol. 1838, Springer-Verlag, 2000, pp. 581–594.
- [53] ———, *An accelerated Buchmann algorithm for regulator computation in real quadratic fields*, Algorithmic Number Theory, ANTS-V (Claus Fieker and David R. Kohel, eds.), Lecture Notes in Computer Science, vol. 2369, Springer-Verlag, 2002, pp. 148–162.
- [54] ———, *Invariant and discrete logarithm computation in quadratic orders*, Ph.D. thesis, Technische Universität Darmstadt, Fachbereich Informatik, 2003, to appear.