A One Way Function Based on Ideal Arithmetic in Number Fields

Johannes Buchmann Sachar Paulus

Department of Computer Science
TH Darmstadt
64283 Darmstadt
Germany

Abstract. We present a new one way function based on the difficulty of finding shortest vectors in lattices. This new function consists of exponentiation of an ideal in an order of a number field and multiplication by an algebraic number which can both be performed in polynomial time. The best known algorithm for inverting this function is exponential in the degree of the lattices involved.

Key words: one way function, number fields, shortest vectors in lattices.

1 Introduction

In the past 20 years several number theoretic problems have been identified on whose difficulty the security of cryptographic protocols can be based. Prominent examples are the factoring problem for integers [RSA78] and the discrete logarithm problem in the multiplicative group of a finite field [Odl85], in the class group of an order of a quadratic field [BW88], and on an elliptic curve curve over a finite field [Kob87]. There is, however, no guarantee that those problems remain difficult to solve in the future. On the contrary, as the experience with the factoring problem for integers shows unexpected breakthroughs are always possible. It is therefore important to design cryptographic schemes in such a way that the underlying mathematical problem can easily be replaced with another one. It is also important to search for mathematical problems on which secure one way functions can be based.

In this paper we show how to use ideal arithmetic in number fields to design a cryptographic one way function NF-EXP with the following properties:

- NF-EXP can be computed in polynomial time.
- Inverting NF-EXP is at least as hard as factoring integers.
- The only method currently known for inverting NF-EXP requires computing shortest vectors in lattices whose dimension is the degree of the number field. This currently requires exponential time in the degree of the number field.

This papers generalizes ideas which have been introduced in [BW90] for orders of quadratic number fields. However, for quadratic fields, or more generally for number fields of fixed degree NF-EXP can be inverted in subexponential time (see [Buc88]). The new idea in this paper is to introduce the problem of computing shortest vectors in lattices of growing dimension as the basis for cryptographic security. This is done by considering number fields of growing degree. The problem of computing shortest vectors in lattices is known to be very difficult. It does not play a role in any of the schemes based on factoring, finite fields, quadratic number fields, and curves over finite fields. We therefore believe that the new one way function has some potential in future cryptographic applications.

The paper is organized as follows: In a first section, we present the necessary concepts from algebraic number fields. Then, we explain NF-EXP and show how to compute it efficiently. In Section 3, we sketch how to invert NF-EXP and show its difficulty. Finally, we present an example.

2 Algebraic number fields

In this section we briefly introduce the reader to algebraic number fields, orders, fractional ideals, and the arithmetic in those structures. For more details see [BS96].

By an *algebraic number field* we mean an extension field of the field $\mathbb{Q}$ of rational numbers which, as a $\mathbb{Q}$-vector space, is finite dimensional. The dimension is called the *degree* of the number field. Let F be an algebraic number field of degree n. Then there is a monic irreducible polynomial $f \in \mathbb{Z}[X]$ such that F is isomorphic to the residue class field $\mathbb{Q}[x]/(f)$ where (f) denotes the ideal generated by f in $\mathbb{Q}[x]$. We call f a *generating polynomial* of F. In the sequel we will assume that the number field F is represented by a generating polynomial f and that $F = \mathbb{Q}[x]/(f)$.

The elements of F are residue classes, i.e. they are of the form $g + (f)$ with $g \in \mathbb{Q}[x]$. Any such residue class has a unique representative of degree less than n. We assume that the residue classes are represented by those representatives. They can be obtained from any representative by division with remainder by f. Addition, subtraction, and multiplication of elements of F can be effected by the addition, subtraction, and multiplication of the representing polynomials followed by a division with remainder by f. If $g + (f)$ is a non zero element of f then its inverse can be computed as follows. Using the extended Euclidean algorithm a polynomial h is computed with $gh \equiv 1 \bmod (f)$. Then $h + (f)$ is the inverse of $g + (f)$. Addition, subtraction, multiplication and inversion can obviously be performed in polynomial time.

Let $\alpha \in F$. Then the map $F \to F, \xi \mapsto \alpha\xi$ is an endomorphism of the $\mathbb{Q}$-vector space F. The *trace* of α is the trace of this endomorphism. It is denoted by $trace(\alpha)$. The *norm* of α is the the determinant of this endomorphism. It is denoted by $norm(\alpha)$.

Next we introduce orders and ideals thereof. An order $\mathcal{O}$ in F is a subring of F containing the element 1 which admits a $\mathbb{Z}$-basis $(\omega_1, \ldots, \omega_n)$. We represent $\mathcal{O}$ by such a $\mathbb{Z}$-basis, where the basis elements are represented as described above. The *discriminant* of $\mathcal{O}$ is $\Delta = \det((trace(\omega_i\omega_j)_{1\le i,j\le n})$. The generating polynomial and the $\mathbb{Z}$-basis of $\mathcal{O}$ can always be chosen in such a way that $(\log|\Delta|)^{O(1)}$ bits are necessary to store them. We will assume that this is done.

An integral $\mathcal{O}$-ideal is an additive subgroup I of $\mathcal{O}$ which is an $\mathcal{O}$-module. This means that $\mathcal{O}I = \{\omega\alpha : \omega \in \mathcal{O}, \alpha \in I\} \subset I$. The *norm* of I is the index of I in $\mathcal{O}$. It is denoted by N(I). If I is an integral $\mathcal{O}$-ideal then any subset of F of the form $(1/d)I$, where d is a non zero integer, is called a *fractional $\mathcal{O}$-ideal.* Its norm is $\mathrm{N(I)/d^n}$. If I and J are fractional $\mathcal{O}$-ideals then their *product*

$$I \cdot J = \{ \sum_{(\alpha,\beta)\in S} \alpha\beta \mid S \subset I \times J \text{ finite } \}$$

is again a fractional $\mathcal{O}$-ideal. The set $\mathcal{I}$ of all fractional ideals of $\mathcal{O}$ forms a commutative semi-group. The *quotient* of I and J

$$I : J = \{\alpha \in F \mid \alpha J \subset I\}$$

is a fractional $\mathcal{O}$-ideal. A fractional $\mathcal{O}$-ideal I is called *invertible* if $I(\mathcal{O} : I) = \mathcal{O}$. The invertible $\mathcal{O}$-ideals form an Abelian group $\mathcal{J}$. The set $\mathcal{P} = \{\alpha\mathcal{O} \mid \alpha \in \mathcal{F}^*\}$ of *principal* ideals is a subgroup of this group. Two fractional invertible $\mathcal{O}$-ideals I and J are called *equivalent* if there is an $\alpha \in F$ with $J = \alpha I$. Equivalence of ideals is an equivalence relation which is compatible with ideal multiplication. The equivalence class of I is called the *ideal class* of I and is denoted by $[I]$. The set of ideal classes $Cl(\mathcal{O}) = \mathcal{J}/\mathcal{P}$ forms a finite Abelian group and is called the *class group* of $\mathcal{O}$.

We explain ideal arithmetic. A fractional $\mathcal{O}$-ideal I is represented by a $\mathbb{Z}$-basis $(\alpha_1, \ldots, \alpha_n)$ where $\alpha_i \in F$, $1 \le i \le n$. As we have explained above, those elements are represented by polynomials of degree less than n. We will now assume that such a polynomial $g(x) = g_1x^{n-1} + \ldots + g_{n-1}x + g_n$ is represented by the coefficient vector $(g_1, \ldots, g_n)$. Then the ideal I can be viewed as a lattice in $\mathbb{Q}^n$. If I and J are fractional $\mathcal{O}$-ideals with bases $(\alpha_1, \ldots, \alpha_n)$ and $(\beta_1, \ldots, \beta_n)$, respectively, then $(\alpha_i\beta_j)_{1\le i,j\le n}$ is a generating system of the product IJ as a lattice in $\mathbb{Q}^n$. Using Hermite normal form computation [Coh95, 65ff], a basis thereof can be found in polynomial time.

We explain module reduction. For this purpose we need yet another interpretation of a fractional $\mathcal{O}$-ideal as an n-dimensional lattice. Let $\rho^{(1)}, \ldots, \rho^{(n)}$ be the complex zeros of the generating polynomial f. For $\alpha = g + (f) \in F$ the numbers $\alpha^{(i)} = g(\rho^{(i)})$, $1 \le i \le n$ are the *conjugates* of α. There are positive integers r_1, r_2 with $r_1 + 2r_2 = n$ such that $\rho^{(i)} \in \mathbb{R}$ for $1 \le i \le r_1$, $\rho^{(i)} \notin \mathbb{R}$ for $r_1 < i \le n$ and $\rho^{(i)} = \overline{\rho^{(i+r_2)}}$ for $r_1 < i \le r_1 + r_2$. Define the map

$$\begin{aligned} \varphi : \quad & F \to \mathbb{R}^n \\ & \alpha \mapsto (\alpha^{(1)}, \ldots, a^{(r_1)}, Re\,\alpha^{(r_1+1)}, Im\,\alpha^{(r_1+1)}, \ldots, Re\,\alpha^{(r_1+r_2)}, Im\,\alpha^{(r_1+r_2)}). \end{aligned}$$

If I is a fractional $\mathcal{O}$-ideal then $\varphi(I)$ is an n-dimensional lattice of determinant $2^{-r_2}N(I)\sqrt{|\Delta|}$. Let $c \in \mathbb{R}$, $c \geq 1$. An $\mathcal{O}$-ideal I is called *c-reduced* if the fractional $\mathcal{O}$-ideal $\mathcal{O} : I$ contains the element 1 and

$$\{\alpha \in \mathcal{O} : I \mid \forall i = 1, \ldots, n \ |\alpha^{(i)}| < 1/c\} = \{0\}.$$

If I is c-reduced then I is integral and $\mathrm{N(I)} \leq \mathrm{c^n}\sqrt{|\Delta|}$. It follows that $(\log c + \log|\Delta|)^{O(1)}$ bits are sufficient to store I. A c-reduced ideal can be computed as follows. Determine $\mathcal{O} : I$. In $\mathcal{O} : I$ find a number α such that the length of the shortest non zero vector in the lattice $\varphi(\mathcal{O} : I)$ is at least as large as $||\varphi(\alpha)||/c$. Then αI is c-reduced. It follows that 1-reduced ideals can be computed using the shortest vector algorithm of [Kan87] in time $n^{O(n)}(\log|\Delta|)^{O(1)}$. Also, if we use LLL-reduction [Coh95, 83ff] then we obtain 2^n-reduced ideals in time $n^{O(1)}(\log|\Delta|)^{O(1)}$.

3 The one way function NF-EXP

Let F be an algebraic number field of degree n over $\mathbb{Q}$. Let $\mathcal{O}$ be an order in F and let I be an $\mathcal{O}$-ideal. Recall that $\mathcal{I}$ denotes the group of fractional $\mathcal{O}$-ideals. We define the following function parameterized by $\mathcal{O}$ and I:

$$\begin{aligned} \text{NF-EXP}: \quad & F^* \times \mathbf{N} \to \mathcal{I} \\ & (\alpha, k) \mapsto \alpha I^k. \end{aligned}$$

There is a problem in using NF-EXP for cryptographic purposes: If we use a $\mathbb{Z}$-basis to represent the ideal αI^k then the number of bits needed to represent αI^k is $\Omega(k)$. Hence, we cannot even write down $\text{NF-EXP}(\alpha, k)$ in polynomial time. One solution is to restrict the set of arguments of NF-EXP such that the restricted function can be computed in polynomial time. This can be done in such a way that we get a compact representation of αI^k without affecting the security of NF-EXP.

We can for example choose (α, k) such that αI^k is 2^n-reduced. More precisely: We choose $k \in \{1, \ldots, |\Delta|\}$. Using fast exponentiation techniques we can compute a 2^n-reduced ideal J in $[I]^k$ and a number $\alpha \in F$ with $J = \alpha I^k$. The reduced ideal J is not uniquely determined. In fact, there are in general many such reduced ideals. Using techniques of [Buc88] and [Thi95] it is possible to choose α in such a way that J could be any of all 2^n-reduced ideals in its ideal class. Note that all those computations can be carried out in polynomial time since 2^n-reduction can be performed in polynomial time.

Using the same idea, one can obtain a compact representation of αI^k for general α and k as follows: Compute $\beta \in F$ such that $J = \beta\alpha I^k$ is 2^n-reduced and $||\mathrm{Log}\beta||$ is minimal, where

$$\mathrm{Log}(\alpha) = (\log|\alpha^{(1)}|, \ldots, \log|\alpha^{(r_1+r_2-1)}|).$$

This is again done by fast exponentiation. Then represent αI^k by J and a suitable approximation of $\mathrm{Log}\beta$. Using the results of [Thi95] it can be shown that this representation has polynomial length and can be computed in polynomial time.

In practice, we could for example choose a series of number fields of growing degree generated by a sparse polynomials of small discriminant, since the complexity of computing NF-EXP depends on the discriminant and on the number of non-zero coefficients of the generating polynomial. A careful analysis together with experiments in practice have to be done.

Using the arguments of [BBM+92] it follows that the one way function NF-EXP can be used to implement many cryptographic protocols, e.g. a Diffie-Hellman key exchange or a ElGamal signature scheme.

4 Inverting NF-EXP

It has been shown in [BW88] that there is a polynomial time reduction of the factorization problem for integers to inverting NF-EXP for imaginary quadratic orders.

Now we sketch an algorithm for inverting NF-EXP. We use the same notation as in the previous section. The problem of inverting NF-EXP will be called the NF-DL-problem: Given two ideals I and J of an Order $\mathcal{O}$ in a number field F find $\alpha \in F$ and $k \in \mathbb{N}$ such that $J = \alpha I^k$. Solving the NF-DL-problem is closely related to computing the unit group and the class group of the order $\mathcal{O}$. An algorithm computing these groups is described in [Buc88]. We will now explain how this algorithm can be modified to solve NF-DL. We will see that the running time of this algorithm which is the fastest we can currently obtain is exponential in the degree.

Suppose that I and J are fractional $\mathcal{O}$-ideals and that we wish to solve the NF-DL-problem

$$J = \alpha I^k.$$

Without loss of generality we assume that I and J are invertible $\mathcal{O}$-ideals. If they are not, then one can compute the so-called *order of multipliers* in polynomial time, where both ideals are invertible. First we determine an exponent k which is a solution of the equation

$$[J] = [I]^k.$$

For this purpose we choose a factor base FB which contains finitely many invertible prime ideals of $\mathcal{O}$ and also the ideals I and J. Then we determine exponent vectors $v = (v_P)_{P \in FB} \in \mathbb{Z}^{|FB|}$ with

$$\prod_{P \in FB} [P]^{v_P} = [\mathcal{O}].$$

Those vectors v are called *relations* on FB. The set of all relations on FB is an $|FB|$-dimensional $\mathbb{Z}$-lattice. If a generating system of this lattice is known, then the exponent k can be determined by means of linear algebra. This has been explained in [BD90]. The relations on FB are found by the method from [Buc88]. The basic idea is as follows. A random exponent vector $e \in \{1, \ldots, |\Delta|\}^{|FB|}$ is chosen. Then a reduced ideal K in the class $[\prod_{P \in FB} P^{e(P)}]$ is computed. If K can be factored over FB, i.e. if $K = \prod_{P \in FB} P^{f(P)}$ for some $f \in \mathbb{Z}^{|FB|}$ then

$v = e - f$ is a relation on FB. To guarantee that the decomposition is successful with a sufficient probability we use 1-reduction as in [Buc88]. This means that we have to compute shortest vectors in n-dimensional lattices. Using the best known algorithm [Kan87] for this problem this requires exponential time in n.

Once k is known we must find α. Note that $JI^{-k} = \alpha\mathcal{O}$. Since we know k this means that we have to find a generator of the principal ideal JI^{-k}. More generally let L be a principal ideal and suppose that we want to find a generator of L. This generator can again be found by means of linear algebra. With each relation v on FB that we have computed we have also obtained a number $\alpha = \alpha(v) \in F$ such that $\prod_{P \in FB} P^{v_P} = \alpha\mathcal{O}$. Now we choose again random vectors $e \in \{1, \ldots, |\Delta|\}^{|FB|}$. Then we compute $\gamma \in F$ and a reduced $\mathcal{O}$-ideal K such that $\gamma K = L \prod_{P \in FB} P^{e_P}$. If K can be factored over FB, i.e. if $K = \prod_{P \in FB} P^{f_P}$ for some $f \in \mathbb{Z}^{|FB|}$ then $L = \gamma \prod_{P \in FB} P^{e_P - f_P}$. Then $w = e - f$ is a relation on FB. Use linear algebra to write w as an integer linear combination on the generators of the relation lattice, i.e. $w = \sum_v w_v v$. Then $L = \gamma \prod_v \alpha(v)^{w_v}$. So we have found a generator for L.

A careful analysis of this algorithm together with experiments has to be done to evaluate the practical security of NF-EXP.

5 Two small examples

We present computations for the one way function NF-EXP in the order $\mathcal{O}$ of the equation $f(x) = x^4 + 989$. Elements of the number field $F = \mathbb{Q}[x]/(f(x))$ are multiplied as described above; this is realized using a multiplication table of size $4 \times 4 \times 4$, where there are 16 non-zero entries of which 10 equal to 1 and 6 equal to -989. A polynomial yielding such a *sparse* multiplication table is of special interest for practical purposes, since multiplication of number field elements is a basic operation in the evaluation of NF-EXP.

We start with the (prime) ideal I given by the matrix

$$\begin{pmatrix} 5 & 1 & 4 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

where the columns are the coefficient vectors representing the ideal basis elements. Now we choose $k = 200$; exponentiation of I by k yields a representation of I^k as a matrix with entries in the first row having more than 160 digits. Reducing this matrix using LLL with a large parameter (see [Coh95, 83ff]) induces an ideal J having a matrix representation

$$\begin{pmatrix} 1474 & 0 & 737 & 595 \\ 0 & 1474 & 0 & 1277 \\ 0 & 0 & 737 & 199 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

and a number α given by the coefficient vector

$$\begin{aligned}&(900815506274542631714225629195137 27,\\ &-503841134277550505015598483795925 42,\\ &135374570150008211758174790992165 37,\\ &-354818413579696566144053600893027 4)/1474\end{aligned}$$

(we use a common denominator for all vector components) such that we have

$$\text{NF-EXP}_I(\alpha, k) = J.$$

The computation of J and α took 61 ms.

As claimed in Section 3, we cannot compute α and J from I and k in this way in general, since the size of the intermediate results and of α is exponential. We explain a fast exponentiation technique which computes only with numbers of polynomial length. It is called *square, multiply and reduce.* It proceeds as follows:

Let $(b_{l_k}, \ldots, b_0)_2$ be the binary expansion of k and denote $(J, \alpha) \leftarrow \mathit{reduce}(I)$ the computation of an equivalent, reduced ideal together with a number $\alpha \in F$ such that $I = \alpha J$.

Procedure Square, Multiply and Reduce:

1. IF $b_0 = 1$ THEN $E \leftarrow I$ ELSE $E \leftarrow \mathcal{O}$
2. $S \leftarrow I$
3. FOR $i \leftarrow 1$ TO l_k

3.1 $S^* \leftarrow S^2$, $(S, \beta_i) \leftarrow \mathit{reduce}(S^*)$

3.2 IF $b_i = 1$ THEN $E^* \leftarrow E \cdot S$, $(E, \alpha_i) \leftarrow \mathit{reduce}(E^*)$

This procedure yields a reduced ideal $J = E$ equivalent to I^k and a number α coded by the $\alpha_1, \ldots, \alpha_{l_k}, \beta_1, \ldots, \beta_{l_k}$. In our example, J is then represented by the matrix

$$\begin{pmatrix} 350 & 0 & 275 & 147 \\ 0 & 350 & 150 & 319 \\ 0 & 0 & 25 & 13 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

and the α_i and β_i are given by the following table. We mention only those β_i for which $b_i = 1$.

$$\begin{array}{ll}
\alpha_1: & (-9,1,0,0)/302 \\
\alpha_2: & (-32398,3816,122,-20)/1665 \\
\alpha_3: & (-8452,71353,-2467,163)/1185 \\
\beta_3: & (1,0,0,0) \\
\alpha_4: & (-94051,-51202,-8704,1592)/19489 \\
\alpha_5: & (3078261,-726226,-349243,171480)/7458 \\
\alpha_6: & (-131260,-476600,-52456,8698)/3205 \\
\beta_6: & (946075,11920,-14675,1180)/10954 \\
\alpha_7: & (-46517,868,-661,30)/10 \\
\beta_7; & (127134,12057,-1464,-197)/175
\end{array}$$

This computation took 51 ms.

A measure for the practical hardness of inverting NF-EXP is given by the time used to compute the class group of $\mathcal{O}$. The algorithm used can be modified to invert NF-EXP, as explained in the last section. Assuming some mathematical reasonable conjecture, the class group of $\mathcal{O}$ is generated by two ideals and is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$. The computation took 16 seconds.

Here another example: let $f(x) = x^6 - 11$. Let I be given by

$$\begin{pmatrix}
19 & 0 & 0 & 0 & 0 & 3 \\
0 & 19 & 0 & 0 & 0 & 6 \\
0 & 0 & 19 & 0 & 0 & 12 \\
0 & 0 & 0 & 19 & 0 & 5 \\
0 & 0 & 0 & 0 & 19 & 10 \\
0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}.$$

Choose $k = 1000$; the matrix representing I^k requires more than 14,000 decimal digits, the reduction of this matrix took 97321 ms. Applying the *square, multiply and reduce* procedure, we get the following representation for I^k: an ideal J given by

$$\begin{pmatrix}
4 & 0 & 2 & 2 & 0 & 1 \\
0 & 4 & 2 & 0 & 2 & 3 \\
0 & 0 & 2 & 0 & 0 & 1 \\
0 & 0 & 0 & 2 & 0 & 1 \\
0 & 0 & 0 & 0 & 2 & 1 \\
0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}$$

and an number $\alpha \in \mathbb{Q}[x]/(f)$ given in the short representation explained above:

$$\begin{aligned}
\alpha_1 &: (-17, 99, 103, 16, 13, -12)/38 \\
\alpha_2 &: (-83, 73, -99, -113, -5, -13)/5 \\
\alpha_3 &: (2, 0, 0, 0, 0, 0) \\
\beta_3 &: (1, 0, 0, 0, 0, 0) \\
\alpha_4 &: (887, -183, 197, 27, -193, 37)/38 \\
\alpha_5 &: (-34, 524, 206, -32, 26, 24)/43 \\
\beta_5 &: (59, 469, -171, -11, -51, -41)/2 \\
\alpha_6 &: (-312, -137, 88, -151, 70, 90)/2 \\
\beta_6 &: (1, 0, 0, 0, 0, 0) \\
\alpha_7 &: (1, 0, 0, 0, 0, 0) \\
\beta_7 &: (1, 0, 0, 0, 0, 0) \\
\alpha_8 &: (-7, 0, 3, 0, 1, 0)/3 \\
\beta_8 &: (1, 0, -1, 0, 1, 0) \\
\alpha_9 &: (-6, 0, 3, 0, 0, 0) \\
\beta_9 &: (1, 0, 0, 0, 0, 0)
\end{aligned}$$

This computation took 124 ms. The class group was computed in 27,150 ms.

6 Conclusions

We have shown that the one way function NF-EXP can in principle be used to implement cryptographic primitives such as key exchange and digital signatures. We have also argued that the only known method for inverting NF-EXP requires computing shortest vectors in lattices whose dimension is the degree of the number field in which NF-EXP is implemented. This requires exponential time in the degree of the number field.

There are two important open problems:

- Can the algorithm for inverting NF-EXP be improved?
- Can NF-EXP be efficiently implemented?

As to the first question it is conceivable that an algorithm for solving NF-DL can be designed which uses c-reduction with $c > 1$. Certainly, $c = 2^n$, for which the reduction algorithm is polynomial, is not sufficient. But it may be possible to use some c which is subexponential in n. To implement such a c-reduction one can use the short vector algorithm described in [Sch87]. This algorithm is a candidate for a subexponential time reduction procedure.

To answer the second question much more research has to be done. We suspect that for example very efficient implementations are possible for families of number fields which are given by very sparse generating polynomials.

7 Acknowlegdement

We thank Stefan Neis for providing us with the computations in section 4. The algorithms have been implemented using the computer algebra C++ library LiDIA.

References

[BBM+92] I. Biehl, J. Buchmann, Bernd Meyer, Christian Thiel, and Christoph Thiel. Tools for proving zero knowledge. In *Proc. of EUROCRYPT'92*, Lecture Notes in Computer Science, pages 356–365. Springer, 1992.

[BD90] J. Buchmann and S. Düllmann. On the computation of discrete logarithms in class groups. In *Proc. of CRYPTO'90*, volume 537 of *Lecture Notes in Computer Science*, pages 134–139. Springer, 1990.

[BS96] E. Bach and J. Shallit. *Algorithmic number theory.* MIT Press, Cambridge, Massachusetts and London, England, 1996.

[Buc88] J. Buchmann. A subexponential algorithm for the determination of class groups and regulators of algebraic number fields. *Séminaire de théorie des nombres*, pages 28–41, 1988.

[BW88] J. Buchmann and H.C. Williams. A key-exchange system based on imaginary quadratic fields. *Journal of Cryptology*, 1:107–118, 1988.

[BW90] J. Buchmann and H.C. Williams. Quadratic fields and cryptography. *Number Theory and Cryptography, London Math. Soc. Lecture Note Series*, 154:9–26, 1990.

[Coh95] H. Cohen. *A course in computational algebraic number theory.* Springer, Heidelberg, 2nd edition edition, 1995.

[LiD97] The LiDIA Group. *LiDIA - A library for computational number theory.* Technische Hochschule Darmstadt, Germany. http://www.informatik.th-darmstadt.de/TI/LiDIA.

[Kan87] R. Kannan. Minkowski's konvex body theorem and integer programming. *Mathematics of operations research*, 12, no. 5, 1987.

[Kob87] N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48:203–209, 1987.

[Odl85] A.M. Odlyzko. Discrete logarithms in finite fields and their cryptographic significance. In *Proc. of EUROCRYPT'84*, volume 209 of *Lecture Notes in Computer Science*, pages 224–314. Springer, 1985.

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM*, 21:120–126, 1978.

[Sch87] C.P. Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. *Theoretical Computer Science*, 53:201–224, 1987.

[Thi95] C. Thiel. *On some computational problems in algebraic number theory.* PhD thesis, Universität des Saarlandes, Saarbrücken, Germany, 1995.