Identification and signatures based on **NP**-hard problems of indefinite quadratic forms

Rupert J. Hartung Claus-Peter Schnorr

Johann Wolfgang Goethe Universität Frankfurt a. M.
Postfach 11 19 32; Fach 238
60054 Frankfurt a. M.
Germany
hartung@math.uni-frankfurt.de
schnorr@mi.informatik.uni-frankfurt.de

Abstract

We prove **NP**-hardness of equivalence and representation problems of quadratic forms under probabilistic reductions, in particular for indefinite, ternary quadratic forms with integer coefficients. We present identifications and signatures based on these hard problems. The bit complexity of signature generation and verification is quadratic using integers of bit length 150.

Keywords. Identification, signature, indefinite quadratic forms, **NP**-hardness, proof of knowledge, zeroknowledge, anisotropic form, equivalence class.

AMS classification. 11E20, 94A60, 68D15, 11D09, 11R29

1 Introduction

The arithmetic theory of quadratic forms goes back to Fermat, Legendre, Lagrange, and Gauss. Algorithmic problems for lattices and quadratic forms have been promoted by the LLL-algorithm [12]. Recently definite forms or lattices gave rise to cryptographic protocols related to the **NP**-hard problems of finding a shortest or a closest lattice vector; see [13], [17] for hardness results and [1], [7], [9], [10] for applications. Cryptographic protocols based on **NP**-hard problems seem to withstand attacks by quantum computers. However, lattice cryptography requires lattices of high dimension. This yields long cryptographic keys and slow protocols.

By contrast, we present identification and signatures based on hard problems of quadratic forms in dimension three and four. Bounded solutions of equivalence and representation problems for indefinite ternary forms are shown to be **NP**-hard for probabilistic reductions. This follows from Adleman and Manders [15] who proved **NP**-completeness of deciding solvability of inhomogeneous binary quadratic equations over the integers. Signature generation and verification have quadratic bit complexity for integers of bit length 150. Note that RSA has cubic bit complexity for much longer integers.

Outline. Section 2 introduces computational problems of quadratic forms. Section 3 presents an identification scheme that proves knowledge of an equivalence transform for ternary anisotropic forms. This scheme is statistical zeroknowledge under heuristics. It performs one LLL-reduction and a few arithmetic steps per round. Section 4 extends the identification to long challenges and signatures. Section 5 gives **NP**-hardness proofs. Section 6 presents polynomial time solutions for problems of isotropic forms of odd squarefree determinant. Section 7 characterizes anisotropic forms.

2 The equivalence problem of quadratic forms

Quadratic forms. An n-ary *quadratic form* (or simply *form*) f over $\mathbb{Z}$ is a homogeneous quadratic polynomial $f = f_A = \sum_{i,j=1}^{n} a_{i,j} x_i x_j$ with coefficients $a_{i,j} = a_{j,i} \in \frac{1}{2}\mathbb{Z}$ for $i \neq j$, $a_{i,i} \in \mathbb{Z}$, $A = (a_{i,j}) \in \mathbb{Z}^{n\times n}$. Note that f takes integer values for $x_1, ..., x_n \in \mathbb{Z}$. By definition $\det f = \det A$, $\dim f = n$.

Equivalence classes. Let $f = f_A$ be an n-ary form. For $T \in \mathbb{Z}^{n\times n}$ let $f_A T$ denote the form $f_{T^t A T}$. The forms f, fT are called *equivalent* if $T \in \mathrm{GL}_n(\mathbb{Z})$, i.e., $|\det T| = 1$. Then $\det(fT) = (\det T)^2 \det f = \det f$. We call the equivalence class of f simply the *class* of f. Let $\mathcal{O}(f) = \{T : fT = f, |\det T| = 1\}$ denote the group of *automorphisms* of f. The textbook by Cassels [3] surveys the theory of classes.

Relevant properties of forms are: f is *regular* if $\det f \neq 0$; f is *indefinite* if f takes both positive and negative values. Otherwise f is either *positve* or *negative*, positive forms correspond to the Gram matrices $A = B^t B \in \mathbb{R}^{n\times n}$ of lattice bases $B \in \mathbb{R}^{n\times n}$. $f = f_A$ is *primitive* if $\gcd(a_{ij} \mid 1 \leq i, j \leq n) = 1$; f is *isotropic* if $f(\mathbf{u}) = 0$ holds for some nonzero $\mathbf{u} \in \mathbb{Z}^n$, otherwise f is *anisotropic*. Every regular isotropic form is necessarily indefinite. The form $f = \sum_{i=1}^{n} a_i x_i^2$ is called *diagonal*.

We study the equivalence of forms $f \in \mathcal{Q}$ for various sets of forms $\mathcal{Q}$.

Computational equivalence problem, CEP$(\mathcal{Q})$

GIVEN: equivalent forms $f, g \in \mathcal{Q}$.
FIND: $T \in \mathrm{GL}_n(\mathbb{Z})$ such that $g = fT$.

Representations. An n-ary form f *represents* the integer m if there exists $\mathbf{u} \in \mathbb{Z}^n \setminus \{0\}$ such that $f(\mathbf{u}) = m$. The representation $\mathbf{u}$ is *primitive* if $\gcd(u_1, \ldots, u_n) = 1$. Let $\mathbf{CR}(\mathcal{Q})$ denote the problem to compute for given $f \in \mathcal{Q}$ and $m \in \mathbb{Z}$ a primitive $\mathbf{u} \in \mathbb{Z}^n$ such that $f(\mathbf{u}) = m$ whenever such $\mathbf{u}$ exists.

We show in section 5 that bounded solutions of **CEP** and **CR** are **NP**-hard to find for indefinite forms f of $\dim f = 3$ and for definite forms f of $\dim f = 5$.

LLL-reduction [12] extends from lattice bases and definite forms to indefinite forms. LLL-forms f_A, $A = (a_{i,j})$ satisfy $a_{1,1}^2 \leq 2^{n/2}(\det A)^{2/n}$. There is a polytime algorithm that transforms f into an LLL-form fT with $T \in \mathrm{GL}_n(\mathbb{Z})$, see [11], [22], [24].

3 Identification via the equivalence problem

We present efficient proofs of knowledge of an equivalence transform for indefinite forms. We use anisotropic forms for keys because there exist poly-time (unbounded) solutions of **CEP** and **CR** for isotropic forms f given the factorization of $\det f$, see section 6. No relevant poly-time solutions are known for **CEP** and **CR** and anisotropic forms. Let $k \in \mathbb{N}$ be a security parameter.

Key generation. Pick an anisotropic form $f_1 = ax^2 + by^2 - cz^2$ with $a, b, c \in_R [1, 2^k[$. Verify via the factorization of $\det f$ that f is anisotropic, see section 7. Generate T and $f_1 T$ by $\mathbf{CT}(f_1)$ and set $S := T$, $f_0 := f_1 S$.

The *public key* is f_0, f_1, the *private key* is S.

$\mathbf{CT}(f)$: *Computes an LLL-form $f := fT$ for a randomized $T = (t_{i,j}) \in \mathrm{GL}_3(\mathbb{Z})$.*

1. Pick $t_{i,j} \in_R]-2^k, 2^k[$ at random for $j \neq 1$.
Compute the coefficients $t^{adj}_{i,1}$ of $(t^{adj}_{i,j}) = T^{-1} \det T$.

2. Solve $\sum_{i=1}^{3} t_{i,1}\, t^{adj}_{i,1} = \gcd(t^{adj}_{1,1}, t^{adj}_{2,1}, t^{adj}_{3,1}) =: \gcd$ for $t_{i,1} \in \mathbb{Z}$ by the extended Euclidean algorithm. If $\gcd \neq 1$ then repeat with some new $t_{i,j}$, $j \neq 1$.

3. LLL-reduce fT to fTT', replace $T := TT'$.

The $t^{adj}_{i,1}$ in Step 2 are quadratic polynomials in the $t_{k,j}, j \neq 1$. Step 3 balances the initially large $|t_{i,1}| \le \max_i |t^{adj}_{i,1}| < 2^{2k+2}$ with the smaller $t_{i,j}$, $j \neq 1$. The random initial $t_{i,j}$, $j \neq 1$ randomize the leading and the least significant k bits of the final $t_{i,j}$.

Identification $(\mathcal{P}, \mathcal{V})_1$
The prover $\mathcal{P}$ proves to the verifier $\mathcal{V}$ knowledge of S.

1. $\mathcal{P}$ computes an LLL-form $\bar{f} := f_0 T$ via $\mathbf{CT}(f_0)$, sends the commitment $\bar{f}$,

2. $\mathcal{V}$ sends a random one-bit challenge $b \in_R \{0, 1\}$,

3. $\mathcal{P}$ sends the reply $R_b := S^b T$, and $\mathcal{V}$ checks that $f_b R_b = \bar{f}$.

Obviously, the honest prover $\mathcal{P}$ withstands the test $f_b R_b = \bar{f}$.

Proof of knowledge. Consider a fraudulent $\widetilde{\mathcal{P}}$ that sends arbitrary $\bar{f}, \bar{R}_b$. The trivial $\widetilde{\mathcal{P}}$ guesses b in step 1 with probability $\frac{1}{2}$, generates an LLL-form $f_b T$ via $\mathbf{CT}(f_b)$, sends $\bar{f} := f_b T$ and replies $\bar{R}_b := T$. Then $\widetilde{\mathcal{P}}$ withstands the verification with probability $\frac{1}{2}$. The probability $\frac{1}{2}$ cannot be increased. If an arbitrary $\widetilde{P}$ withstands the verification for the same $\bar{f}$ and both challenges $b = 0, 1$ then $f_0 \bar{R}_0 = \bar{f} = f_1 \bar{R}_1$, and thus $f_1 \bar{R}_1 \bar{R}_0^{-1} = f_0$. This yields an alternative private key $\bar{S} = \bar{R}_1 \bar{R}_0^{-1} \in \mathcal{O}(f_1)\, S$ in time proportional to $|(\widetilde{\mathcal{P}}, \mathcal{V})_1|$ (which denotes the number of steps of $(\widetilde{\mathcal{P}}, \mathcal{V})_1$). This proves

Theorem 3.1 *An arbitrary fraudulent prover $\widetilde{P}$ that succeeds in $(\widetilde{\mathcal{P}}, \mathcal{V})_1$ with probability $\varepsilon > \frac{1}{2}$ finds some $\bar{S} \in \mathcal{O}(f_1)\, S$ in expected time $|(\widetilde{\mathcal{P}}, \mathcal{V})_1| / (\varepsilon - \frac{1}{2})$.*

Statistical zeroknowledge. The protocol $(\mathcal{P}, \mathcal{V})_1$ is by definition *statistical ZK* if there is a probabilistic poly-time simulator $\mathcal{S}$ which produces randomized strings, distributed statistically close to the communication $(\bar{f}, b, R_b)$ of $(\mathcal{P}, \widetilde{\mathcal{V}})_1$, where $\|\cdot\|_1$-distance $\le 2^{-100}$ suffices in practice. The simulator $\mathcal{S}$ has resettable black-box access to $\widetilde{\mathcal{V}}$ but does not know the secret key.

Let the simulator $\mathcal{S}$ mimic the trivial $\widetilde{\mathcal{P}}$ sending the LLL-form $\bar{f} = f_b T$ and replying $\bar{R}_b = T$ whereas the true prover sends the LLL-form $\bar{f} = f_0 T$ and replies $R_b = S^b T$. The distributions of the LLL-forms $f_1 T, f_0 T = f_1 ST$ generated by $\mathbf{CT}(f_1)$, $\mathbf{CT}(f_0)$ are close. We assume that, due to LLL-reducedness, the distributions of T and of ST are close too. This holds if the automorphisms of f_1 can be neglected. This proves

Theorem 3.2 *Identification* $(\mathcal{P}, \mathcal{V})_1$ *is statistical zeroknowledge under heuristics.*

Zeroknowledge extends to independent sequential executions of $(\mathcal{P}, \mathcal{V})_1$, the simulator $\mathcal{S}$ can easily be extended. Since $(\mathcal{P}, \mathcal{V})_1$ is restricted to one-bit challenges, a security level 2^{100} requires 100 independent executions of $(\mathcal{P}, \mathcal{V})_1$ consisting of 300 rounds.

4 Three round identification and signatures

Our signatures correspond to identification in three rounds with long challenges, where the verifier is simulated using a hash function. This identification releases some information about the private key which we argue to be irrelevant. This information cannot be combined over several identifications, but it reduces **CEP** to $(n-1)$-ary subforms of f_b. To make the reduced **CEP** hard we increase $\dim f_1$ to $n = 4$.
Private key $S \in \mathrm{GL}_4(\mathbb{Z})$,
Public key anisotropic forms $f_0 = f_1 S$, $f_1 = \sum_{i=1}^4 a_i x_i^2$ with $(-1)^i a_i \in [1, 2^k[$.

Apply a public hash function to a public / private random 100-bit seed to generate the pseudo-random coefficients $(-1)^i a_i \in [1, 2^k[$ of f_1 (make sure that $p^{2k} | d$, $p^{2k+1} \not| d$ holds for a small prime p and $d := a_1 a_2 a_3 a_4$ and that $\prod_{i<j} (a_i, a_j)_p = (-1)^{p \bmod 2}$ holds so that Theorem 7.2 guarantees that f is anisotropic.), resp., the pseudo-random bits for the construction of S via $\mathbf{CT}(f_1)$. This way the public / private keys have bit lengths $10k + 100$ (there are 10 coefficients of f_0, f_1) and 100, respectively. Note that **CT**, extended to $n = 4$ performs arithmetic steps on $3k$-bit integers.

Three round identification $(\mathcal{P}, \mathcal{V})_2$ *Prover* $\mathcal{P}$ *solves problems posed by the verifier* $\mathcal{V}$ *that are hard without knowledge of* S
1. $\mathcal{P}$ computes an LLL-form $\bar{f} := f_0 \bar{T}$ via $\mathbf{CT}(f_0)$and sends $\bar{f}$ to $\mathcal{V}$,
2. $\mathcal{V}$ computes an LLL-form $f' := \bar{f} T'$ via $\mathbf{CT}(\bar{f})$ and sends T' to $\mathcal{P}$,
3. $\mathcal{P}$ sends $\mathbf{e}'_b := S^b \bar{T} T' \mathbf{e}_b$ for $b = 0, 1$ and $\mathbf{e}_1 := (1, 0, 0, 0)^t$, $\mathbf{e}_0 := (0, 0, 0, 1)^t$,
$\mathcal{V}$ checks that $f_b \mathbf{e}'_b = \bar{f} T' \mathbf{e}_b$ for $b = 0, 1$. (we abbreviate $T := \bar{T} T'$)

Security against a fraudulent prover $\widetilde{\mathcal{P}}$. $\widetilde{\mathcal{P}}$ replies for an arbitrary commitment $\bar{f}$ to a challenge T' of $\mathcal{V}$. A successful $\widetilde{\mathcal{P}}$ must find solutions $\mathbf{e}'_b$ of $f_b(\mathbf{e}'_b) = m$ for both $b = 0, 1$, where the randomized m is chosen by the verifier as $m := \bar{f} T' \mathbf{e}_b$. The problem to find a small solution $\mathbf{e}'_b$ without the private key is **NP**-hard by Theorem 5.1.

Note that $\mathcal{P}$ reveals S if he replies to various challenges T' for the same $\bar{f}$.

By revealing $\mathbf{e}'_1 = (\sum_{i=1}^4 s_{j,i} t_{i,1} \,|\, j = 1, ..., 4)^t$ the honest $\mathcal{P}$ proves bounds on $\sum_i |s_{j,i}|$ for $j = 1, ..., 4$, $S = (s_{i,j})$. $\mathcal{P}$ comes close to prove a bound on $|s_{1,1}|$ as is required for the **NP**-hardness results of section 5.

Next we argue that the information $\mathbf{e}'_1 = ST\mathbf{e}_1$ released about ST is computationally irrelevant: Recovering ST from $\mathbf{e}'_1$ requires to solve hard problems for ternary forms.

Hardness of recovering ST. Let $f_1 = \sum_{i=1}^4 a_i x_i^2 = f_{A_1}$, $f' = f_{A'} = f_1 ST$. Given $\mathbf{e}'_1 = ST\mathbf{e}_1$ we can transform f' into $f'' = f_{A''} := f'T''$ such that $a_1 = a''_{1,1}$, and thus

$$\begin{pmatrix} 1 & \mathbf{0}^t \\ \mathbf{u} & Q^t \end{pmatrix} A_1 \begin{pmatrix} 1 & \mathbf{u}^t \\ \mathbf{0} & Q \end{pmatrix} = A'' =: \begin{pmatrix} a_1 & a_1\mathbf{u}^t \\ a_1\mathbf{u} & A''_+ \end{pmatrix} \qquad (5)$$

holds for some $\mathbf{u} \in \mathbb{Z}^3$, $Q \in \mathrm{GL}_3(\mathbb{Z})$, $A''_+ \in \mathbb{Z}^{3\times 3}$. We rewrite (5) as

$$Q^t A_+ Q = A''_{\mathbf{u}} \quad \text{for} \quad A''_{\mathbf{u}} := A''_+ - a_1\mathbf{u}\mathbf{u}^t,$$

where A_+ is the diagonal matrix with diagonal (a_2, a_3, a_4). Solving equation (5) for $Q \in \mathrm{GL}_3(\mathbb{Z})$ requires an unbounded solution of **CEP** for $f_{A_+}, f_{A''_{\mathbf{u}}}$. Thus, releasing $\mathbf{e}'_1$ reduces **CEP** to ternary anisotropic forms and the recovering of $\mathbf{u}$.

Hardness of recovering $\mathbf{u}$. Equation (5) implies that $\det A''_+ = \det A''_{\mathbf{u}}$, and this equation can be written as $\det A''_+ = f_D(\mathbf{u}) - a_2a_3a_4$ for the indefinite, diagonal matrix D with diagonal $a_1(a_3a_4, a_2a_4, a_2a_3)$. Hence the construction of $\mathbf{u}$ from $\mathbf{e}'_1$ requires to solve $f_D(\mathbf{u}) = \det A''_+ - a_2a_3a_4$. This problem can be made hard by ensuring that f_D is *anisotropic*, see sections 6, 7. Then no isotropic vector can help to recover $\mathbf{u}$.

The best known attack. In order to solve $fT = f'$ for $f = f_{A_+}, f' = f_{A''_{\mathbf{u}}}$ it is promising to exhaust the reduced forms f_A in the class of f, f' by simple transforms of $\mathrm{GL}_3(\mathbb{Z})$: permute two rows and columns of A and transform the result into a reduced form. For k-bit coefficients of f, f' we have that $d := \det f = O(2^{3k})$ and the number of reduced forms in the class of f is $O(d)$. This can solve $fT = f'$in time $O(2^{3k})$.

Conclusion. The problem to recover $Q, \mathbf{u}$ and thus ST from $\mathbf{e}'_1 = ST\mathbf{e}_1$ requires $\Omega(2^{3k})$ arithmetic steps for all known algorithms. No better method is known for solving $f_b\mathbf{e}'_b = \bar{f}T'\mathbf{e}_b$ for $\mathbf{e}'_b$. Therefore, $k = 50$ seems to provide sufficient security.

On the other hand $(\mathcal{P}, \mathcal{V})_2$ is less secure for $n = 3$ since most instances of the recovering problem can be solved in subexponential time for $n = 3$. For indefinite, binary A_+, D, the multiplicative structure of the Gaussian cycle [6, art.183ff] of reduced forms containing f_{A_+}, f_D, yields subexponential algorithms see [2, chap. 11].

The revealed information about S is irrelevant. $\mathbf{e}'_0 := T\mathbf{e}_0$ and $\mathbf{e}'_1 := ST\mathbf{e}_1$ are randomized primitive vectors that are nearly statistically independent of S due to the randomized T computed by **CT**. This shows that $(\mathcal{P}, \mathcal{V})_2$ reveals irrelevant information about S. The revealed information cannot be combined over several identifications as the corresponding T are nearly statistically independent.

Signatures. Extend the keys of $(\mathcal{P}, \mathcal{V})_2$ by random seeds $s', s^* \in_R \{0,1\}^{100}$, s' public and s^* private. To generate a signature for message m follow $(\mathcal{P}, \mathcal{V})_2$

but simulate $\mathcal{V}$ randomized by $H(m, s')$ for a public hash function H.

Signature generation. Compute $\bar{T}$, $\bar{f} := f_0\bar{T}$ by $\mathbf{CT}(f_0)$ randomized by $H(m, s^*)$, keep $\bar{T}$ secret. Compute $\bar{f}T', T'$ by $\mathbf{CT}(\bar{f})$ randomized by $H(m, s')$, set $\mathbf{e}'_b := S^b\bar{T}T'\mathbf{e}_b$. The resulting *signature* $(\bar{f}, \mathbf{e}'_0, \mathbf{e}'_1)$ consists of 18 k-bit integers, the entries of $\mathbf{e}'_0, \mathbf{e}'_1, \bar{f}$.

Verification computes T' from m, s' and checks that $f_b\mathbf{e}'_b = \bar{f}T'\mathbf{e}_b$ for $b = 0, 1$.

The bit complexity of signature generation and verification is quadratic $O(k^2)$, its main work is LLL-reduction within $\mathbf{CT}$. LLL-reduction using orthogonalisation in floating point arithmetic has quadratic bit complexity using school multiplication [18], [22].

5 NP-hardness

5.1 The results. Recall that a set $S \subset \mathbb{Z}^*$, consisting of sequences of integers, is in **NP** if S is decidable in nondeterministic poly-time. We prove probabilistic **NP**-hardness of decisional variants of $\mathbf{CEP}(\mathcal{Q})$ and $\mathbf{CR}(\mathcal{Q})$ that ask for a solution $\mathbf{x}$ with a given bound. We first present the results and thereafter the proofs.

Decisional Bounded Representation Problem, $\mathbf{DBR}(\mathcal{Q})$
GIVEN: $f \in \mathcal{Q}$, $m \in \mathbb{N}$, $c \in \mathbb{N}$, the factorization of $\det f$.
DECIDE: whether $\exists$ primitive $\mathbf{x} \in \mathbb{Z}^n$: $f(\mathbf{x}) = m$ and $|x_1| \le c$.

The given factorization of $\det f$ does not decrease the worst-case complexity. Recall that the class **RP** of *random polynomial time* consists of all sets $S \subset \mathbb{Z}^*$ for which there is a probabilistic, poly-time algorithm which accepts every $s \in S$ with probability $\ge \frac{1}{2}$ and rejects every $s \in \mathbb{Z}^* \setminus S$ with probability 1.

Let $\mathcal{Q}_{ind}$ consist of all indefinite, primitive forms f of $\dim f = 3$.

Theorem 5.1 $\mathbf{DBR}(\mathcal{Q}_{ind})$ *is probabilistic* **NP***-hard, i.e.,* $\mathbf{NP} \subseteq \mathbf{RP}^{\mathbf{DBR}(\mathcal{Q}_{ind})}$.

Therefore, if $\mathbf{DBR}(\mathcal{Q}_{ind})$ is in **RP** then so is every **NP**-set. The proof of Theorem 5.1 reduces a Boolean form Φ in 3-CNF to a form $f = 2x^2 + 2byz$, where $\frac{1}{2}\det f \in \mathbb{Z}$ is odd. Theorem 5.1 follows essentially from [15].

Dimension 3 is minimal for this hardness result. In fact, an algorithm of Gauß computes small representations for binary forms in subexponential time if the class number is small (see [6, art. 183–221], [5, sec. 5.2 and 5.6]).

For isotropic ternary forms of odd squarefree determinant unbounded solutions of **CEP** and **CR** can be found in poly-time given an isotropic vector. For anisotropic forms, by contrast, **CEP**, **CR** seem to be hard on average.

Theorem 5.2 shows that deciding whether a lattice of dimension 5 has a vector of given length is **NP**-hard.

Theorem 5.2 *Let* $\mathcal{Q}_{df}$ *consist of all positive definite forms* f *of* $\dim f = 5$. *Then* $\mathbf{DBR}(\mathcal{Q}_{df})$ *is* **NP***-complete.*

Representation problems for definite forms are by Theorem 5.2 harder than equivalence problems. In fact, equivalence transformations of definite forms can be efficiently computed in constant dimension by computing shortest lattice vectors [19], [20].

Incomplete forms. If some coefficients $a_{i,j}$ of A are undefined, $a_{i,j} = *$, and if $\det A$ does not depend on the undefined $a_{i,j}$ then we call f_A *incomplete.* For example the form $f = ax^2 + bxy + 2a_{1,3}xz + z^2$ is incomplete for $a_{1,3} = *$. A *completion* of f_A defines the undefined $a_{i,j}$ of A.

Decisional Bounded Equivalence Problem, DBE($\mathcal{Q}$)
GIVEN: $f, g \in \mathcal{Q}$, $c \in \mathbb{N}$, the factorization of $\det f$.
DECIDE: whether $\exists T \in \mathrm{GL}_n(\mathbb{Z})$: $f\,T = g$, $|t_{1,1}| \le c$.

DBE($\mathcal{Q}$) for given n-ary incomplete forms $f, g \in \mathcal{Q}$ asks for the existence of $T \in \mathrm{GL}_n(\mathbb{Z})$ and completions $\bar{f}, \bar{g}$ of f, g such that $\bar{f}T = \bar{g}$, $|t_{1,1}| \le c$.
Let $\mathcal{Q}_{inin}$ extend the set $\mathcal{Q}_{ind}$ by all incomplete, indefinite forms f of $\dim f = 3$.

Theorem 5.3 **DBE**($\mathcal{Q}_{inin}$) *is probabilistic* **NP**-*hard.*

Extensions.
1. The **NP**-hardness of Theorem 5.1 extends to all dimensions $n \ge 3$.
2. The proof of Theorem 5.1 can be extended from isotropic to anisotropic forms (that are used for identification and signatures). However, this requires a considerable amount of number theory and the Cohen-Lenstra heuristics for class numbers of real quadratic fields, see [8]. The main problem is to show that all values $x^2 + by$ are covered by the definite forms $x^2 + b(y^2 + pz^2)$ for a few primes p.
3. At the end of this section we sketch how extend Theorem 5.3 from $\mathcal{Q}_{inin}$ to $\mathcal{Q}_{ind}$.
4. The problem **DBR**($\mathcal{Q}_{df}$) is **NP**-complete in dimension ≥ 5 even if the condition that $|x_1| \le c$ is removed. This holds because the problem to decide whether $ax^2 + by = c$ has a solution $x, y \in \mathbb{N}$ is **NP**-hard [15].

5.2 From SAT to squares.

The following problem on binary Diophantine equations will be used as an intermediary problem for reductions.

Modular Square Problem, MS
GIVEN: $a, b, c \in \mathbb{N}$ such that $b = p^{m+1}b'$; a, p prime, b' squarefree, $p \ge 5$.
DECIDE: $\exists x \in \mathbb{Z}$: $x^2 \equiv a \bmod b$ and $|x| \le c$.

Let $\preccurlyeq_r$ denote that there is a probabilistic, poly-time Karp reduction, and let 3SAT be the problem to decide satisfiability of Boolean forms in 3-CNF. Proposition 5.4 is similar to a result of Adleman and Manders [15].

Proposition 5.4 *3SAT* $\preccurlyeq_r$ **MS**.

Proof. We transform a given Boolean form Φ in 3-CNF into an instance (a, b, c)

of **MS** that is solvable if and only if Φ is satisfiable. Let Φ contain each clause at most once, and let no clause of Φ contain a variable both complemented and uncomplemented. Let ℓ be the number of variables in Φ. Choose an enumeration $\sigma_1, \ldots, \sigma_m$ of all such clauses in the variables $x_1, \ldots, x_\ell$ with exactly three literals such that the bijection $i \mapsto \sigma_i$ and its inverse are poly-time. We write $\sigma \in \Phi$ if σ occurs in Φ, and $x_j \in \sigma$ ($\bar{x}_j \in \sigma$) if the j-th variable occurs uncomplemented (complemented) in clause σ. Let $n = 2m+\ell$. Let $r = (r_1, ..., r_\ell) \in \{0,1\}^\ell$ denote Boolean values for $x_1, ..., x_\ell$, where 1 corresponds to **true** and 0 corresponds to **false**. For a clause σ and $r \in \{0,1\}^\ell$ define

$$W(\sigma, r) = \textstyle\sum_{i:x_i \in \sigma} r_i + \sum_{i:\bar{x}_i \in \sigma} (1 - r_i).$$

Introducing new variables $y_1, \ldots, y_m$ we set for $k = 1, ..., m$

$$R_k := \begin{cases} y_k - W(\sigma_k, r) + 1 & \text{if } \sigma_k \in \Phi, \\ y_k - W(\sigma_k, r) & \text{if } \sigma_k \notin \Phi, \end{cases}$$

Since Φ is in 3-CNF, we have $W(\sigma_k, r) = 0$ if assignment r does not satisfy clause σ_k, and $1 \le W(\sigma_k, r) \le 3$ otherwise. Hence the equations $R_1 = \cdots = R_m = 0$ have a solution $r \in \{0,1\}^\ell$, $y \in \{0,1,2,3\}^m$ if and only if Φ is satisfiable.

We select a prime $p \ge 5$. As $-3 \le R_k \le 4$ for all choices of $y_k \in \{0,1,2,3\}$, $r_i \in \{0,1\}$, the equations $R_1 = \cdots = R_m = 0$ holds if and only if $\sum_{k=1}^m R_k p^k = 0$. The latter equation is equivalent to

$$\textstyle\sum_{k=1}^m (2\, R_k) p^k \equiv 0 \bmod p^{m+1}. \tag{1}$$

since $\left|\sum_{k=1}^m R_k p^k\right| \le 4 \sum_{k=1}^m p^k < p^{m+1}$ holds for $p \ge 5$ and p is odd.

We express $y_1, ..., y_m$ and $r_1, ..., r_\ell$ in (1) by new variables $\alpha_1, ..., \alpha_n$, $n = 2m + \ell$ ranging over $\{1, -1\}$, we set

$$y_k := \tfrac{1}{2}((1 - \alpha_{2k-1}) + 2(1 - \alpha_{2k})), \qquad r_i := \tfrac{1}{2}(1 - \alpha_{2m+i}). \tag{2}$$

Exactly all combinations of $y_k \in \{0,1,2,3\}$, $r_i \in \{0,1\}$ are covered by $\alpha_1, ..., \alpha_n \in \{\pm 1\}$. We can rewrite (1) via (2) into

$$\textstyle\sum_{j=1}^n c_j \alpha_j \equiv \tau' \bmod p^{m+1} \tag{3}$$

for some $c_j, \tau' \in \mathbb{Z}$, where $\tau' = 0 \bmod p$.

Using an extra variable α_0 and $c_0 := 1$, $\tau := \tau' + 1$ we rewrite equation (5.3) into

$$\textstyle\sum_{j=0}^n c_j \alpha_j \equiv \tau \bmod p^{m+1}. \tag{4}$$

We see that Φ is satisfiable if and only if (4) is solvable for $\alpha \in \{-1, 1\}^{n+1}$. Note that $p \not| \tau$ since $p | \tau'$.

We select a prime $p_0 > 4 \cdot p^{m+1}(n+1)$ and primes $p_0 < p_1 < \cdots < p_n$ that are of polynomial size in p^m. For $j = 1, ..., n$ compute θ_j via the Chinese Remainder Theorem to be the smallest positive integer satisfying

$$\theta_j \begin{cases} \equiv c_j & \bmod & p^{m+1}, \\ \equiv 0 & \bmod & \prod_{i \ne j} p_i, \\ \not\equiv 0 & \bmod & p_j. \end{cases}$$

We see that Φ is satisfiable if and only if (5.5) is solvable for $\alpha \in \{\pm 1\}^{n+1}$,

$$\textstyle\sum_{j=0}^n \theta_j \alpha_j \equiv \tau \bmod p^{m+1}. \tag{5}$$

Lemma 5.5 *Let* $K := \prod_{j=0}^{n} p_j$ *and* $c := \sum_{j=0}^{n} \theta_j$*. For* $x \in \mathbb{Z}$*,* $|x| \le c$ *the equation* $c^2 \equiv x^2 \bmod K$ *holds if and only if* $x = \sum_{j=0}^{n} \alpha_j \theta_j$ *for some* $\alpha \in \{\pm 1\}^{n+1}$*.*

Proof. Since $\theta_j \theta_{j'} \equiv 0 \bmod K$ for $j \ne j'$ each $x = \sum_{j=0}^{n} \alpha_j \theta_j$ satisfies $c^2 \equiv x^2 \bmod K$. Conversely, $c^2 \equiv x^2 \bmod K$ implies $0 \equiv (c-x)(c+x) \bmod K$, and thus either $p_j | c-x$ or $p_j | c+x$ holds for every $j = 0, \ldots, n$. This disjunction is exclusive: if $p_j | c-x$ and $p_j | c+x$ then $p_j | 2c$, and thus $p_j | c$. This contradicts the fact that $c \equiv \theta_j \not\equiv 0 \bmod p_j$.

Since p_j divides exactly one of $c \pm x$ we define $\alpha_j \in \{\pm 1\}$ such that $p_j | c - \alpha_j x$, hence $x \equiv \alpha_j c \bmod p_j$. Setting $x' := \sum_{i=0}^{n} \alpha_i \theta_i$ yields $x \equiv x' \bmod p_j$ for all j, and thus $x \equiv x' \bmod K$.
We see from $|x'| \le \sum_{j=0}^{n} \theta_j = c$ and $|x| \le c$ that $|x - x'| \le 2c$.
The choice of p_j guarantees that $\frac{2 \cdot p^{m+1}}{p_j} \le \frac{1}{2(n+1)}$, and thus

$$\theta_j < 2 \cdot p^{m+1} \prod_{\substack{i=0 \\ i \ne j}}^{n} p_i = \frac{2 \cdot p^{m+1} K}{p_j} \le \frac{K}{2(n+1)}.$$

Hence $c = \sum_{j=0}^{n} \theta_j < K/2$. We see from $|x - x'| \le 2c$ that $|x - x'| < K$, and from $x \equiv x' \bmod K$ that x and x' coincide. This proves the lemma. □

Combining (5) with Lemma 5.5 we see that Φ is satisfiable if and only if there exists $x \in \mathbb{Z}$, $|x| \le c$ such that

$$c^2 \equiv x^2 \bmod K, \quad x \equiv \tau \bmod p^{m+1}.$$

These equations are equivalent to each of the following equations

$$c^2 \equiv x^2 \bmod K, \quad \tau^2 \equiv x^2 \bmod p^{m+1} \quad (\mathbb{Z}^*_{p^{m+1}} \text{ is cyclic}),$$

$$p^{m+1}(c^2 - x^2) + K(\tau^2 - x^2) \equiv 0 \bmod p^{m+1} K,$$
$$(p^{m+1} + K)\, x^2 \equiv K\tau^2 + p^{m+1} c^2 \bmod p^{m+1} K.$$

Since $p \not| K$ the latter equation can be written as

$$x^2 \equiv a \bmod b \tag{6}$$

$$\text{for } \; b = p^{m+1} K \text{ and } a \equiv (p^{m+1} + K)^{-1} (K\tau^2 + p^{m+1} c^2) \bmod p^{m+1} K. \tag{7}$$

Then (6) has a solution $x \in \mathbb{Z}$ with $|x| \le c$ if and only if Φ is satisfiable. We can select a prime a in the arithmetic progression (7) in random poly-time. Clearly K is odd and squarefree, and the prime a is coprime to b.

Then (a, b, c) is a solvable instance of **MS** if and only if Φ is satisfiable. □

5.1 Proofs of Theorems.

Proof of Theorem 5.1. Let Φ be a boolean formula in 3-CNF. The proof of Prop. 5.4 transforms Φ into an instance (a, b, c) of **MS**, ab odd, such that there exist $x, y \in \mathbb{Z}$ satisfying $x^2 + by = a$, $|x| \le c$ if and only if Φ is satisfiable.

We see that the form $f = 2x^2 + 2byz$ yields a solvable instance $f(x, y, z) = 2a$ of $\mathbf{DBR}(\mathcal{Q}_{ind})$ if and only if Φ is satisfiable. For a primitive solution (x, y, z) choose $z = 1$. Note that f is primitive since b is odd. Moreover, f is indefinite, isotropic and $\det f = 2b^2$. This proves the claim. $\square$

Proof of Theorem 5.2. As in the proof of Prop. 5.4 we transform Φ into an instance (a, b, c) of **MS**. Here we choose a that satisfies equation (7) such that $a > c^2$. Then all integer solutions x, y of $x^2 + by = a$, $|x| \leq c$ satisfy $y > 0$. Lagrange's Four Square Theorem shows that $y \in \mathbb{N}$ can be represented as a sum of four squares. Therefore, we have transformed Φ into $(a, b, c) \in \mathbb{N}^3$ such that $x_1^2 + b(x_2^2 + \cdots + x_5^2) = a$, $|x_1| \leq c$ is solvable for $(x_1, ..., x_5) \in \mathbb{N}^5$ if and only if Φ is satisfiable. This proves the theorem. $\square$

Proof of Theorem 5.3. We transform instances (a, b, c) of **MS** constructed in the proof of Prop. 5.4 into instances of $\mathbf{DBE}(\mathcal{Q}_{inin})$, preserving solvability. We have that

$$\begin{pmatrix} a & b/2 & x \\ b/2 & 0 & 0 \\ x & 0 & 1 \end{pmatrix} = \begin{pmatrix} x & y & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & b/2 \\ 0 & b/2 & 0 \end{pmatrix} \begin{pmatrix} x & 0 & 1 \\ y & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

for $a = x^2 + by$. Let $f = x^2 + byz$ and $f' = ax^2 + bxy + \gamma yz + z^2$ with $\gamma = *$, then $f = f'T$ is solvable with $|t_{1,1}| \leq c$ if and only if $a = x^2 + by$, $|x| \leq c$ is solvable. $\square$

NP-*hardness of* $\mathbf{DBE}(\mathcal{Q}_{ind})$. We sketch how to extend the proof of Theorem 5.3 to reduce to complete forms in $\mathcal{Q}_{ind}$. We construct for $f = x^2 + byz$ a list of forms $f_1, \cdots, f_N$ such that every solution (x, y, z) of $a = x^2 + byz, |x| \leq c$ provides a first column of some $S \in \mathrm{GL}_3(\mathbb{Z})$ satisfying $fS = f_j$ for some f_j. Hence (a, b, c) is solvable for **MS** if and only if (f, f_j, c) is for some $1 \leq j \leq N$ solvable for **DBE**. This proves the desired reduction.

We construct the f_j to represent all *orbits* of primitive representations of a by f under $\mathcal{O}(f)$. Zhuravlev [25, sec. 1.2] classifies these orbits in terms of modular matrix equations. We construct the f_j by solving these equations. First we determine the *genus* of f_j, i.e., the f_j up to simultaneous equivalence over the reals $\mathbb{R}$ and over all rings of p-adic integers. Then we construct the actual f_j by a constructive version of the classical proof of the existence of genera [3, sec. 9.5]. According to **MS**, the integer a is prime, and this ensures that $N = O(1)$. Moreover, the construction is poly-time per entry f_j, given the factorization of ab.

6 Solving quadratic equations using an isotropic vector

Isotropic forms f_A are *universal* over any field $\mathbb{F}$, i.e., for $A \in \mathbb{F}^{n \times n}$ the equation $f_A(\mathbf{x}) = m$ is solvable for all $m \in \mathbb{F}$ if it is solvable for $m = 0, \mathbf{x} \neq 0$, [3, chap. 2.2]. We show that $f_A(\mathbf{x}) = m$ can easily be solved for all $m \in \mathbb{Z}$ over the integers if an *isotropic* vector is given and $\det A$ is odd and squarefree. Theorem 6.1 transforms an isotropic form f_A with odd, squarefree determinant $d = \det A$

into the form $2xy - dz^2$ and Theorem 6.2 solves the equation $2xy - dz^2 = m$. Importantly, Simon [23], [24] has shown that an isotropic vector can be found in poly-time for any isotropic form f given the factorization of $\det f$.

Theorem 6.1 *Let f_A be an isotropic, ternary form and let $d := \det A$ be odd and squarefree. Given an isotropic vector (x', y', z') the form f_A can be transformed in poly-time into the equivalent form $2xy - dz^2$.*

Proof. Make (x', y', z') primitive by dividing it by $\gcd(x', y', z')$. Extend (x', y', z') to some $S \in \mathrm{GL}_3(\mathbb{Z})$ with first column vector $(x', y', z')^t$. Set $A' = (a'_{i,j})_{1\le i,j\le 3} := S^t AS$. Then $a'_{1,1} = 0$ as (x', y', z') is isotropic.

Compute via the extended *gcd*-algorithm some $V \in \mathrm{GL}_2(\mathbb{Z})$ such that $(a'_{1,2}, a'_{1,3})V = (r, 0)$ holds for $r := \gcd(a'_{1,2}, a'_{1,3})$. This yields integers g, t, h such that

$$\begin{pmatrix} 1 & \\ & V^t \end{pmatrix} A' \begin{pmatrix} 1 & \\ & V \end{pmatrix} = \begin{pmatrix} 0 & r & 0 \\ r & g & t \\ 0 & t & h \end{pmatrix}.$$

As $d = -r^2 h$ and d is squarefree we have $r = \pm 1$. So let $r = 1$, $h = -d$, and thus

$$\begin{pmatrix} 1 & & \\ -\lfloor g/2 \rfloor & 1 & \\ -t & & 1 \end{pmatrix} \begin{pmatrix} & 1 & \\ 1 & g & t \\ & t & h \end{pmatrix} \begin{pmatrix} 1 & -\lfloor g/2 \rfloor & -t \\ & 1 & \\ & & 1 \end{pmatrix} = \begin{pmatrix} & 1 & \\ 1 & e & 0 \\ & 0 & -d \end{pmatrix},$$

where $e = g - 2\lfloor g/2 \rfloor \in \{0, 1\}$. So far we have transformed f_A into $2xy + ey^2 - dz^2$. We are finished if $e = 0$.

Case $e = 1$. We transform $2xy + y^2 - dz^2$ into $2\bar{x}y - d\bar{z}^2$. As d is odd let $-d = 1 + 2k$. Transforming $2xy + y^2 - dz^2$ via $x := \bar{x} + ky - dz$ yields

$$2\bar{x}y + 2ky^2 + y^2 - 2dyz - dz^2 = 2\bar{x}y - dy^2 - 2dyz - dz^2 = 2\bar{x}y - d(y + z)^2.$$

Setting $\bar{z} := y + z$ yields $2\bar{x}y - d\bar{z}^2$. □

Theorem 6.2 *Let $d \in \mathbb{Z}$ be odd. Then the equation $2xy - dz^2 = m$ is solved by any z satisfying $z = m \bmod 2$ and $x := (m + dz^2)/(2y)$ where y is an arbitrary integer divisor of $(m + dz^2)/2$.*

Proof. For odd d we have that $m + dz^2$ is even if and only if $z = m \bmod 2$. Hence $(m + dz^2)/2$ is integer and the claimed (x, y, z) is a solution. □

Extensions. Ternary isotropic forms f_A of odd, squarefree $\det A$ are equivalent if and only if they coincide in $\det A$. Moreover, **CEP** for such f_A can be solved in poly-time by Theorem 6.1. In particular, such f_A is equivalent to $2xy - \det A\, z^2$ by Theorem 6.1. However, f_A can be inequivalent to $2xy - \det A\, z^2$ for even $\det A$. For example, the forms $ax^2 + by^2 - cz^2$ and $2xy + abcz^2$ can be inequivalent for even abc because only the second form is a multiple of 2 unless a, b, c are all even.

The equation $2xy - dz^2 = m$ is unsolvable for even d and odd m. However, all solvable instances of $f_A(\mathbf{x}) = m$ for even, squarefree $d = \det A$ can easily be solved given an isotropic vector.

Even when $d = \det A$ is not squarefree the equation $f_A(\mathbf{x}) = m$ can in practice be solved by the method of Theorems 6.1, 6.2. It is unlikely that a large squarefactor $r^2 \neq 1$ shows up in the algorithm of Theorem 6.1.

The set of all solutions. We get all solutions $(x, y, z) \in \mathbb{Z}^3$ of $2xy - dz^2 = m$ by extending the solutions of Theorem 6.2 in that we allow to permute x and y and to change the signs of x, y, z. In fact, we easily get all solutions of $2xy - dz^2 = 0$ given the factorization of d.

Moreover, when we replace $\mathbb{Z}$ by a finite field, a finite ring or the field of real numbers then solving the equation $f_A(\mathbf{x}) = m$ is relatively easy for $m \neq 0$. Solutions over the ring $\mathbb{Z}_N$, N composite, can be found using Pollard's algorithm [21].

7 Characterization of isotropic and anisotropic indefinite forms

For fixed n, every n-ary form f over $\mathbb{Z}$ can be transformed in poly-time into a diagonal form $fT = \frac{1}{a_0} f' = \frac{1}{a_0} \sum_{i=1}^n a_i x_i^2$, where $a_0, ..., a_n \in \mathbb{Z}$ and $T \in \mathbb{Q}^{n\times n}, \det T = 1$. Then f is isotropic if and only if f' is isotropic. Next we characterize isotropic diagonal forms. The form $ax^2 + by^2 - cz^2$ is anisotropic if and only if the Legendre equation

$$ax^2 + by^2 = cz^2 \tag{8}$$

is solvable. The equation (8) is in *normal form* if $a, b, c \in \mathbb{N}$ are positive, squarefree and pairwise coprime. Let QR_a denote the set of quadratic residues modulo a.

Theorem 7.1 (see [14], [4]) *In normal form the equation (8) has a non-zero solution if and only if $bc \in QR_a$, $ac \in QR_b$ and $-ab \in QR_c$, and solving (7.1) for given a, b, c is poly-time equivalent to each of the following problems :*
1. solve $\alpha^2 = bc \bmod a$, $\beta^2 = ac \bmod b$ and $\gamma^2 = -ab \bmod c$,
2. solve equation (8) for a non-zero $(x, y, z) \in \mathbb{Z}^3$ such that $x^2+y^2+z^2 \leq 2abc$.

Theorem 7.2 [3, chap. 4.1, 4.2, lem. 2.6] *An indefinite form $f = \sum_{i=1}^4 a_i x_i^2$ with $a_i \in \mathbb{Z}$ is anisotropic if and only if there exist a prime p and $k \in \mathbb{N}$ such that $p^{2k}|d$, $p^{2k+1} \not| d$ for $d := a_1a_2a_3a_4$ and $\prod_{i<j}(a_i, a_j)_p = (-1)^{p \bmod 2}$.*

The *Hilbert Norm Residue Symbol* $(a_i, a_j)_p \in \{\pm 1\}$ equals 1 if and only if $a_i x^2 + a_j y^2 - z^2$ is isotropic over $\mathbb{Q}_p$, the field of p-adic numbers. In particular $(a_i, a_j)_p$ is poly-time, and anisotropy of f is poly-time given the factorization of $\det f$ [3, chap. 3.2]. For $n \geq 5$ every indefinite n-ary form f is isotropic [16]. Anisotropic quaternary forms f have a square-factor dividing $\det f$.

References

[1] M. Ajtai and Cynthia Dwork, *A public-key cryptosystem with worst-case/average-case equivalence*, Proceedings STOC 1997 (New York), Association for Computing Machinery, 1997, pp. 284–293.

[2] J. Buchmann and U. Vollmer, *Binary quadratic forms. An algorithmic approach*, Algorithms and Computation in Mathematics, no. 20, Springer-Verlag, Berlin, 2007.

[3] J. W. S. Cassels, *Rational quadratic forms*, L.M.S. Monographs, no. 13, Academic Press, New York, 1978.

[4] T. Cochrane and P. Mitchell, *Small solutions of the Legendre equation*, Journal of Number Theory **70** (1998), no. 1, 62–66.

[5] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993.

[6] C. F. Gauß, *Untersuchungen über höhere Arithmetik (Disquisitiones Arithmeticae)*, Springer-Verlag, Berlin, 1889, second edition: Chelsea Publ. New York, 1965, reprinted 1981.

[7] O. Goldreich, Shafi Goldwasser, and S. Halevi, *Public-key cryptosystems from lattice reduction problems*, Proceedings Advances in Cryptology - CRYPTO '97 (Berlin), Lecture Notes in Computer Science, vol. 1294, Springer-Verlag, 1997, pp. 112–131.

[8] R. J. Hartung and C.-P. Schnorr, *Public key identification based on the equivalence of quadratic forms*, Proceedings MFCS 2007 (Berlin), Lecture Notes in Computer Science, no. 4708, Springer-Verlag, 2007, http://www.mi.informatik.uni-frankfurt.de, pp. 333–345.

[9] J. Hoffstein, N. Howgrave-Graham, J. Pipher, J. H. Silverman, and W. Whyte, *NTRUSign: Digital signatures using the NTRU lattice*, Proceedings Topics in cryptology – CT-RSA 2003 (Berlin), Lecture Notes in Computer Science, vol. 2612, Springer-Verlag, 2003, pp. 122–140.

[10] J. Hoffstein, J. Pipher, and J. H. Silverman, *NTRU: A ring-based public key cryptosystem*, Proceedings 3rd international symposium ANTS-III, 1998 (Berlin), Lecture Notes in Computer Science, vol. 1423, Springer-Verlag, 1998, pp. 267–288.

[11] G. Ivanyos and Á. Szánto, *Lattice basis reduction for indefinite forms and an application*, Journal on Discrete Mathematics **153** (1996), no. 1–3, 177–188.

[12] H. W. Lenstra jun., A. K. Lenstra, and L. Lovász, *Factoring polynomials with rational coefficients*, Mathematische Annalen **261** (1982), 515–534.

[13] S. Khot, *Hardness of approximating the shortest vector problem in lattices*, Journal of the ACM **52** (2005), no. 5, 789–808.

[14] A. M. Legendre, *Recherche d'analyse indéterminée*, Histoire de l'Académie Royale des Sciences **1788** (1785), 465–559.

[15] K. L. Manders and L. M. Adleman, *NP-complete decision problems for binary quadratics*, Journal of Computer and System Sciences **16** (1978), 168–184.

[16] A. Meyer, *Zur Theorie der indefiniten ternären quadratischen Formen*, Journal für Mathematik **108** (1891), 125–139.

[17] D. Micciancio and Shafi Goldwasser, *Complexity of lattice problems: A cryptographic perspective*, The Kluwer International Series in Engineering and Computer Science, vol. 671, Kluwer, Boston, 2002.

[18] P. Q. Nguyen and D. Stehlé, *Floating-point LLL revisited*, Proceedings Advances in Cryptology - EUROCRYPT 2005 (Berlin), Lecture Notes in Computer Science, vol. 3494, Springer-Verlag, 2005, pp. 215–233.

[19] W. Plesken and M. Pohst, *Constructing integral lattices with prescribed minimum. I*, Mathematics of Computation **45** (1985), 209–221.

[20] W. Plesken and B. Souvignier, *Computing isometries of lattices*, Mathematics of Computation **45** (1985), 209–221.

[21] J. M. Pollard and C.-P. Schnorr, *An efficient solution of the congruence* $x^2+ky^2 = m (mod\, n)$, IEEE Transactions on Information Theory **33** (1987), 702–709.

[22] C.-P. Schnorr, *Progress on LLL and lattice reduction*, Proceedings LLL+25, Caen, France, June 29–July 1, 2007, Final version to appear; http://www.mi.informatik.uni-frankfurt.de.

[23] D. Simon, *Quadratic equations in dimensions 4, 5 and more*, 2005, preprint Uni. Caen: http://www.math.unicaen.fr/s̃imon/.

[24] ———, *Solving quadratic equations using reduced unimodular quadratic forms*, Mathematics of Computation **74** (2005), no. 251, 1531–1543.

[25] V. G. Zhuravlev, *Representation of a form by the genus of quadratic forms*, St. Petersburg Mathematical Journal **8** (1997), no. 1, 15–84.