Cryptanalysis of Definite and Indefinite Lattice Isomorphism Problems With Applications to DEFI

Markus Kirschmer[1], Cong Ling[2], Ali Sadreddin[2]

[1] Fakultät für Mathematik, Universität Bielefeld, Germany
mkirschm@math.uni-bielefeld.de
[2] Department of EEE, Imperial College London, United Kingdom
c.ling@ic.ac.uk, sas23@ic.ac.uk

Abstract. We study the Lattice Isomorphism Problem (LIP) for both indefinite and definite quadratic forms, with applications to the DEFI signature scheme. By combining arithmetic and algorithmic techniques, we obtain efficient attacks on DEFIv2, a digital signature scheme based on isotropic quadratic forms. Our approach to the Decision/Distinguishing-LIP draws on the arithmetic theory of quadratic forms, with particular emphasis on indefinite forms of dimension at least 3. We show that such forms arise naturally in the analysis of DEFI and prove that, under suitable assumptions, the genus, spinor genus, and equivalence class coincide. This structural collapse leads to a classical polynomial-time algorithm for the Decision/Distinguishing-LIP instances obtained from DEFI. In addition, we present an efficient algorithm for recovering the secret key of DEFIv2 and demonstrate practical signature forgeries within minutes using the authors' public challenge instances. Finally, we evaluate the impact of our methods on HAWK and show that, in contrast to DEFI, they do not compromise its security.

Keywords: lattice isomorphism problem · quadratic forms · genus · spinor genus · ideal class group

1 Introduction

The security of several newly emerged lattice-based cryptographic schemes relies on the assumed hardness of finding isometries between lattices. One formalisation of this challenge is the *Lattice Isomorphism Problem* (LIP) [11]: given two lattices or their associated quadratic/Hermitian forms, determine whether they are isometric and if so recover an explicit isometry. HAWK, a digital signature scheme in the second round of the call for additional digital signatures for the NIST post-quantum cryptography (PQC) standardisation process, is based on LIP for lattices over number fields [10]. HAWK is defined over the cyclotomic ring $R = \mathbb{Z}[x]/(x^m + 1)$ where m is a positive power of 2. Most cryptographic work and cryptanalysis to date have focused on positive definite quadratic/Hermitian forms or lattices; by contrast, schemes built on indefinite or isotropic quadratic forms have appeared less frequently in cryptography.

DEFI is a signature scheme defined over the ring $R = \mathbb{Z}[x]/(f)$ for a monic irreducible polynomial $f(x)$, and its security is based on the equivalence problem of isotropic quadratic forms [13]. The private key of DEFI is a unimodular change-of-basis matrix B that acts on an indefinite diagonal form $J = \mathrm{diag}(1, 1, -1, -1)$, giving a public symmetric matrix $C = B^T JB$. The cryptographic challenge is to prevent an adversary from recovering such a secret matrix B (*i.e.*, solving the associated search problem) and forging signatures.

Attacking DEFI is reducible to solving a quadratic Diophantine equation over R, or equivalently, solving a system of quadratic Diophantine equations over the integers, $\mathbb{Z}$. DEFIv1 used the cyclotomic ring $R = \mathbb{Z}[x]/(x^m + 1)$. However, proposed challenges defined over rings $\mathbb{Z}[x]/(x^{32}+1)$ and $\mathbb{Z}[x]/(x^{64}+1)$ were broken by Bambury and Nguyen [2]. Following this attack, DEFI authors changed the irreducible polynomial to $f(x) = x^m + x + 1$ so that the underlying ring features a less symmetrical structure compared to the one in DEFIv1, such that it is more resilient against lattice attacks.

At the end of their paper [2], the authors posed an open problem of recovering a secret key from the equation $C = B^T JB$ using algorithmic methods of quadratic forms and classification of isotropic forms. In this paper, we solve that open problem and give a full exposition of the links between the class group, idèles and the integral theory of quadratic forms over global fields, namely the genus $\mathrm{gen}(\cdot)$, spinor genus $\mathrm{sgen}(\cdot)$, and equivalence class $\mathrm{cls}(\cdot)$. We investigate the problem from an explicit algorithmic perspective and show how this could be used in the cryptanalysis of DEFIv2.

It is shown in [11] that the security of LIP-based cryptographic protocols is typically reducible to the hardness of the Distinguishing-LIP, i.e. given a quadratic form, deciding which class from a list of possible classes it comes from. Next, we define the Decision, Distinguishing and Search versions of LIP for DEFI, using quadratic forms. Let K be a number field and $\mathcal{O}_K$ its ring of integers, and let n be the rank of the lattices over $\mathcal{O}_K$.

Problem 1 (Decision-LIP). *Let Q_1 be a quadratic form over $\mathcal{O}_K$. Given any quadratic form Q_2 over $\mathcal{O}_K$, determine if there exists $U \in \mathrm{GL}_n(\mathcal{O}_K)$ such that $Q_2 = U^T Q_1 U$.*

Problem 2 (Distinguishing-LIP). *For two quadratic forms Q_1 and Q_2 over $\mathcal{O}_K$, given any quadratic form Q from the class of Q_1 or Q_2, determine which class Q is from.*

Problem 3 (Search-LIP). *Suppose two quadratic forms Q_1 and Q_2 are equivalent over $\mathcal{O}_K$. Find a $U \in \mathrm{GL}_n(\mathcal{O}_K)$ such that $Q_2 = U^T Q_1 U$.*

Moving to Hermitian forms in HAWK, the above equivalence problems translate into $Q_2 = U^* Q_1 U$, where $(^*)$ denotes transpose conjugation with $U \in \mathrm{GL}_2(\mathcal{O}_K)$.

Note that Distinguishing-LIP can be reduced to Decision-LIP, which in turn can be reduced to Search-LIP.

It is well known that for indefinite forms over $\mathbb{Z}$ of rank $n \geq 3$, there is only a single integral equivalence class in each spinor genus [12]. Further, it is often the case that a genus of an indefinite form over $\mathbb{Z}$ contains a single spinor genus [9]. This hints at a potential weakness of indefinite forms for cryptographic applications, since the Decision-LIP and hence Distinguishing-LIP may be solved efficiently by local theory. In this paper, we will generalise this useful result to indefinite forms over $\mathcal{O}_K$ for certain number fields K, and thereby solve the decision variant for DEFIv1 and DEFIv2. Moreover, isotropic forms admit non-trivial isotropic vectors, which can be exploited to reduce the analogue of LIP and signature-generation tasks to arithmetic problems, for example, solving norm equations or, equivalently, finding rational points on a conic. Utilising these named properties can significantly weaken the assumed hardness of signature schemes such as DEFI that are based on indefinite quadratic forms.

1.1 Main Results

Let (V, Q) be a regular quadratic space over a number field K. Following [24], we call a quadratic form Q *positive definite* if K is totally real and $Q(z)$ is totally positive (i.e. all algebraic conjugates of $Q(z)$ are positive) for all $z \in V \setminus \{0\}$. The space (V, Q) is *definite* if (V, aQ) is positive definite for some $a \in K^*$, otherwise it is called *indefinite*. Note that by definition, definite forms only exist if K is totally real. By an *indefinite lattice* over $\mathcal{O}_K$, we mean an $\mathcal{O}_K$-module whose associated quadratic form over K is indefinite in the above sense [16, page 129].

We begin by presenting a novel criterion (see Theorem 7) on the coincidence of the genus and spinor genus. The criterion is quite general and applies to both definite and indefinite modular lattices. It is our starting point for the cryptanalysis of DEFI and HAWK.

Theorem 1. *Let $\mathcal{L}$ be a modular $\mathcal{O}_K$-lattice with rank ≥ 3 in (V, Q) and let $\mathrm{Cl}_S(K)$ be the ray class group of K with respect to S which is the set of real places v of K such that (V_v, Q) is anisotropic. If the ray class number $\#\,\mathrm{Cl}_S(K)$ is odd, then $\mathrm{gen}(\mathcal{L}) = \mathrm{sgen}(\mathcal{L})$.*

Applying this criterion to totally complex number fields, we establish the equality of the genus and the isometry class of indefinite forms under certain conditions (see Corollary 5).

Corollary 1. *Let $\mathcal{L}$ be a modular $\mathcal{O}_K$-lattice with rank ≥ 3 in a regular quadratic space (V, Q) over a totally complex number field K with odd class number. Then $\mathrm{cls}(\mathcal{L}) = \mathrm{gen}(\mathcal{L})$.*

In other words, the *local-global principle* holds for such lattices, which is a rather surprising result. Theorem 1 and Corollary 1 vastly generalise the classical result [24, 102:10], which holds for $K = \mathbb{Q}$. Corollary 1 provides a powerful method for solving the Decision-LIP for DEFI.

Applying Corollary 1 to DEFIv2, we have (see Corollary 8 for details)

Corollary 2. *Suppose $f(x) = x^m + x + 1$ is irreducible. Let $K = \mathbb{Q}[x]/(f)$ be a monogenic, totally complex number field with an odd class number. Let $\mathcal{L}$ be a modular lattice with rank ≥ 3 over $R = \mathbb{Z}[x]/(f)$. Then $\mathrm{cls}(\mathcal{L}) = \mathrm{gen}(\mathcal{L})$.*

In particular, Corollary 2 implies that the Decision/Distinguishing-LIP for DEFIv2 with $m \in \{16, 28\}$ can be solved by deciding if two lattices lie in the same genus.

Weber [29] showed the class number of a 2-power cyclotomic field is always odd. Applying Corollary 1 to DEFIv1, we obtain (see Corollary 7 for details)

Corollary 3. *Let $K := \mathbb{Q}[x]/(x^m + 1)$ be a 2-power cyclotomic field. Let $\mathcal{L}$ be a modular lattice with rank ≥ 3 over $R = \mathbb{Z}[x]/(x^m + 1)$. Then $\mathrm{cls}(\mathcal{L}) = \mathrm{gen}(\mathcal{L})$.*

In particular, Corollary 3 implies that the Decision/Distinguishing-LIP for DEFIv1 can be solved by deciding if two lattices lie in the same genus.

We then give an efficient polynomial-time algorithm (Algorithm 2) to decide if two abstract lattices over some number field lie in the same genus, which is of independent interest. It is worth mentioning that Algorithm 2 applies to both definite and indefinite lattices.

Theorem 2. *There is a polynomial-time algorithm to decide if two lattices over $\mathcal{O}_K$ lie in the same genus, assuming the factorisation of their determinant ideal is known.*

Combining Corollary 1 and Theorem 2, we obtain

Corollary 4. *Let $\mathcal{L}$ be a modular lattice with rank ≥ 3 over a totally complex number field K with an odd class number. Then there is a polynomial-time algorithm to solve the Decision-LIP, assuming the factorisation of its determinant ideal is known.*

Therefore, the Decision/Distinguishing problem of DEFIv1 and DEFIv2 can be solved by a polynomial-time algorithm (if K has an odd class number).

For the search variant, we give an explicit method to recover an isometry, provided one exists (see Theorem 3).

Theorem 3. *Let K be an algebraic number field with class number one and odd discriminant. Given a matrix $C = B^T J B$ with $B \in \mathrm{GL}_4(\mathcal{O}_K)$, there exists an efficient algorithm that constructs a matrix $S \in \mathrm{GL}_4(\mathcal{O}_K)$ such that $S^T C S = J$.*

The above condition on the number field K is satisfied by DEFIv2 with parameter $m \in \{16, 28\}$.

We present algorithms addressing Decision and Search-LIPs. Algorithm 2 solves the Decision-LIP, using Algorithm 1 to compute the Gram matrix of the Jordan decomposition of a lattice. Algorithm 5 solves the Search-LIP in DEFIv2.

We implemented our method in Magma [4]. Our codes [15] recover a suitable transformation S, i.e. an (equivalent) private key, and forge valid short signatures in practical time on a personal MacBook laptop; signature size comparisons show

that our produced signatures are smaller than the authors' DEFIv2-c signatures for the first 20 challenge instances tested.

Finally, we apply Theorem 1 to the cryptanalysis of HAWK. The authors of [18] noted that the spinor genus classification cannot be applied directly to HAWK, since it is defined as a Hermitian form. They left it as an open problem whether the spinor genus can be efficiently computed for integral binary Hermitian forms. We have answered this open problem for HAWK in the affirmative, which (un)fortunately does not lead to any attack (see Theorem 11).

Theorem 4. *The genus of the HAWK lattice $\mathbb{Z}[\zeta_{2m}]^2$, viewed as a quaternary quadratic lattice over the maximal totally real subfield $\mathbb{Q}(\zeta_{2m}+\zeta_{2m}^{-1})$ of $\mathbb{Q}(\zeta_{2m})$, coincides with its spinor genus, for $m>1$ a power of 2.*

This is the best possible scenario from a security point of view, implying that HAWK is immune to the spinor genus attack described in [18]. We therefore conclude that the spinor genus has no impact on the security of HAWK[3].

Previous works [20,19] presented attacks on positive-definite binary *Hermitian* forms when the underlying number field is totally real. A subsequent work [1] extended these attacks to number fields with at least one real embedding[4]. However, such fields are not used in HAWK. The case of totally complex fields has remained intractable. Indeed, [7] reduced such rank-2 module LIP instances to the principal ideal problem in orders of quaternion algebras, for which no efficient algorithms are currently known.

In summary, by employing a positive-definite *Hermitian* form over a CM field, HAWK magically avoids all types of known attacks.

1.2 Technical Overview

We view the machinery of genera and spinor genera of quadratic forms within the framework of the class group of a number field. The celebrated local-global principle states that two quadratic forms over a number field K are equivalent if and only if they are equivalent over K_v for every place v of K. However, this principle does not generally extend to the classification of quadratic forms over the ring of integers $\mathcal{O}_K$. If two forms are equivalent over $\mathcal{O}_{K_v}$ for all places v, then they lie in the same genus, but they need not be equivalent over $\mathcal{O}_K$.

The spinor genus provides a finer classification than the genus and a coarser one than the equivalence class of quadratic forms and their associated lattices. The work [18] presented a quantum polynomial-time algorithm to decide if two binary quadratic lattices over a number field with class number 1 lie in the same spinor genus. In [21], the author gave a classical polynomial-time algorithm that

[3] We remark that a genus of the Hermitian HAWK lattice $(\mathcal{H},\varphi)$ contains a large number of special genera [21]. However, since a special genus apparently contains exponentially many equivalence classes, it does not seem to offer a significant advantage in solving Decision-LIP.

[4] It is interesting to note that our attack on quadratic forms often works if there is at least one *complex* embedding.

decides if two binary Hermitian lattices of HAWK belong to the same special genus. Our work is inspired by these recent advances on cryptanalysis of the Module LIP.

To solve the Decision-LIP, we establish the hierarchy of equivalence relations for integral lattices, illustrated in the following diagram (assuming rank ≥ 3).

$$\textbf{Genus} \xrightarrow[\text{over fields } K \text{ with odd ray class number}]{\text{equal for modular lattices}} \textbf{Spinor genus} \xrightarrow[\text{indefinite forms}]{\text{equal for}} \textbf{Class}$$

On one hand, the genus and the spinor genus coincide for modular lattices over a number field K with odd ray class number. On the other hand, the spinor genus and the equivalence class coincide whenever the quadratic form is indefinite, in dimensions at least 3. The latter occurs when the number field K admits at least one complex embedding. In the case of DEFI, the hierarchy collapses completely, rendering the Decision/Distinguishing-LIP trivial.

For an integral lattice given by a pseudo basis, one obtains the Gram matrix of a Jordan Decomposition of the lattice locally at a fixed prime ideal $\mathfrak{p}$ of the ring of integers. With this in hand, one can determine if any two such lattices are isometric locally at $\mathfrak{p}$. Hence, one can determine whether two such lattices lie in the same genus. In particular, for unimodular lattices of rank ≥ 3 over $\mathbb{Z}[x]/(x^m+1)$ where m is a power of 2, or over $\mathbb{Z}[x]/(x^m + x + 1)$ with certain restrictions on m, there are efficient algorithms to solve the Decision-LIP. Moreover, for modular lattices with rank ≥ 3 over a totally complex number field with an odd class number, there is a polynomial-time algorithm that determines if they belong to the same class.

The problem of factorising a symmetric 4×4 matrix C into an invertible unimodular change of basis matrix B and an indefinite diagonal form $J = \mathrm{diag}(1, 1, -1, -1)$ appears in general to be no easier than solving relative norm equations in L/K where L is a quadratic extension of K with trivial class number. The work of Biasse and Song [3] allows a quantum polynomial-time algorithm to solve relative norm equations of the form $N_{L/K}(x) = \theta$ where L/K is a Galois extension. Since a quadratic extension is Galois, we can apply their algorithm to solve the Search-LIP.

1.3 Roadmap

Section 2 reviews the necessary mathematical background, terminology and notations for quadratic forms and lattices, the genus, spinor genus, idèles and ray and ideal class groups, which are key ingredients in our methods for solving Decision-LIP and some useful facts about DEFI signature schemes. In Section 3, we explore the local-global principle for lattices, compute local invariants that determine the genus of an abstract lattice in a quadratic space, prove three main theorems and derive their corollaries, and subsequently solve the Decision-LIP of DEFI. In Section 4, we discuss primitive isotropic vectors, splitting unimodular

lattices, and solve the Search-LIP problem of DEFI, and explain the key recovery and signature forgery attacks on DEFIv2. We give our experimental results in Section 5. In Section 6, we discuss HAWK and Module LIP. Finally, we conclude with a discussion and some open problems in Section 7.

2 Preliminaries

We begin with some background. For further reading, see [24] and [14]. Let K be a number field and V be an n-dimensional linear space over K. In addition, K^* denotes the group of units in K. Denote by $\mathcal{O}_K$ the ring of integers of K.

2.1 Quadratic Spaces

Definition 1. *A* quadratic form *is a map $Q\colon V \to K$ such that*

1. *$Q(ax) = a^2 Q(x)$ for all $a \in K$ and $x \in V$;*
2. *The associated map*

$$B\colon V \times V \to K,\ (x, y) \mapsto \tfrac{1}{2}(Q(x+y) - Q(x) - Q(y))$$

is bilinear.

Then (V, Q) is a quadratic space over K.

Definition 2. *Given a tuple $b = (b_1, \ldots, b_n) \in V^n$ we denote by*

$$G(b) = (B(b_i, b_j)) \in K^{n \times n}$$

the corresponding Gram matrix. *The* determinant $\det(V, Q)$ *is the determinant of $G(b)$ for any basis b of V. It is unique up to squares in K^*. The quadratic space (V, Q) is* regular *if its determinant is non-zero.*

In this paper, all quadratic spaces are assumed to be regular.

Definition 3. *Let $0 \neq x \in V$. We say x is isotropic if $Q(x) = 0$ and it is anisotropic if $Q(x) \neq 0$. We call (V, Q) isotropic if it contains an isotropic vector and anisotropic otherwise.*

Obviously, isotropic forms over a number field K are indefinite. The converse need not hold since there might be some (finite or infinite) place of K at which the form Q is anisotropic.

Example 1. Let (V, Q) be an isotropic regular space over some field of characteristic not 2. Let x be any isotropic vector. Since the space is regular, there exists $y \in V$ such that $B(x, y) \neq 0$. After rescaling y we may assume $B(x, y) = 1$ and after replacing y with $y - \frac{1}{2}Q(y)x$ the 2-dimensional subspace $W := Kx \oplus Ky$ has the Gram matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Such a quadratic space W is called a hyperbolic plane. They are the simplest regular quadratic spaces which are isotropic.

Example 2. The DEFI scheme uses a quadratic form with a Gram matrix $J = \mathrm{diag}(1, 1, -1, -1)$ over some number field K [13]. It gives rise to a 4-dimensional quadratic space (V, Q) which is regular and isotropic. Moreover, (V, Q) is isometric to the direct sum of two copies of the hyperbolic plane.

Definition 4. *The group of all linear isometries of (V, Q) is called the orthogonal group and is denoted by*

$$\mathrm{O}(V, Q) = \{\sigma \in \mathrm{GL}(V) : Q(x) = Q(\sigma(x)) \text{ for all } x \in V\}.$$

The special orthogonal group of (V, Q) is defined as

$$\mathrm{SO}(V, Q) = \{\sigma \in \mathrm{O}(V, Q) : \det(\sigma) = 1\}\,.$$

Embeddings and Places. An embedding of K is a ring homomorphism $\tau\colon K \to \mathbb{C}$. When $\tau(K) \subset \mathbb{R}$, we say it is a real embedding. Otherwise, it is called a complex embedding.

We recall that a place v of a number field K is an equivalence class of non-trivial absolute values on K. The places can be classified as *archimedean* or *non-archimedean*. Each place induces a metric, giving K a topology. When K is a number field, each non-archimedean place arises from the valuation associated to a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$, while archimedean places arise from the embeddings $\tau\colon K \to \mathbb{C}$. Each real embedding determines a real place, and each conjugate pair of complex embeddings determines a complex place. The archimedean places of K are also called the *infinite places* of K. We introduce the following notation.

- $\Omega(K)$ is the set of all places of K. Given $v \in \Omega(K)$, we denote by K_v the completion of K. Then $V_v = V \otimes_K K_v$ is the completion of V at v.
- $\mathcal{P}(\mathcal{O}_K)$ will be the set of prime ideals of $\mathcal{O}_K$. We can identify these prime ideals with finite places of K, hence we can write $\mathcal{P}(\mathcal{O}_K) \subset \Omega(K)$. For $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$, the $\mathfrak{p}$-adic valuation is the map $\mathrm{ord}_\mathfrak{p}\colon K_\mathfrak{p} \to \mathbb{Z} \cup \{\infty\}$.
  The prime ideal $\mathfrak{p}$ is called *dyadic* if it contains 2 and otherwise non-dyadic.
- Let $\mathcal{I}_K$ be the free abelian group of fractional ideals of $\mathcal{O}_K$ and P_K be the group of principal ideals. Then

  $$\mathrm{Cl}(K) = \mathcal{I}_K / P_K$$

  is the *ideal class group* of K.

The *ideal class group* is a key ingredient in solving the Decision-LIP for DEFI. This will be discussed in further detail in Section 3.

Definition 5. *Let $\mathfrak{p}$ be some prime ideal of $\mathcal{O}_K$.*

1. *The Hilbert symbol of $a, b \in K_\mathfrak{p}^*$ is*

$$(a, b)_\mathfrak{p} = \begin{cases} 1 & \text{if } ax^2 + by^2 = z^2 \text{ has a non-trivial solution in } K_\mathfrak{p}, \\ -1 & \text{otherwise.} \end{cases}$$

2. *Let* $(e_1, \dots, e_n)$ *be an orthogonal basis of* $(V_\mathfrak{p}, Q)$ *and set* $a_i = Q(e_i)$*. The Hasse invariant of* $(V_\mathfrak{p}, Q)$ *is* $c(V_\mathfrak{p}, Q) = \prod_{i<j} (a_i, a_j)_\mathfrak{p}$.

3. *Let* $\tau\colon K \to \mathbb{R}$ *be a real embedding. Let* $(e_1, \dots, e_n)$ *be an orthogonal basis of* (V_τ, Q) *and set* $a_i = Q(e_i)$*. Let* r *and* s *be the number of positive and negative numbers in* $\tau(a_1), \dots, \tau(a_n)$*. Then* (r, s) *is the signature of* (V_τ, Q)*. By Sylvester's law of inertia, it is independent of the chosen orthogonal basis.*

Given $a, b \in K^*$ and $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$, the Hilbert symbol $(a, b)_\mathfrak{p}$ can be computed in polynomial time. See [28, Proposition 5.8 and Theorem 6.1] for details. We also note that we can compute the signature of (V_τ, Q) at a given real place τ in polynomial time by computing several minors of any Gram matrix of (V, Q).

The local-global principle of Hasse-Minkowski [24] shows that the isometry class of (V, Q) is uniquely determined by

- The dimension $\dim(V)$.
- The square class of $\det(V, Q) \in K^*/(K^*)^2$.
- The signature of (V_τ, Q) at each real place $\tau\colon K \to \mathbb{R}$.
- The finite set $\{\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K) \mid c(V_\mathfrak{p}, Q) = -1\}$.

2.2 Lattices

Let us now turn our attention to lattices in a quadratic space (V, Q).

Definition 6. *An* $\mathcal{O}_K$-lattice *(or simply a lattice)* $\mathcal{L}$ *in* V *is a finitely generated* $\mathcal{O}_K$*-submodule of* V*. The* rank *of* $\mathcal{L}$ *is the dimension of the subspace of* V *generated by* $\mathcal{L}$*. We say that it has full rank if* $\mathcal{L}$ *generates* V *over* K *or, equivalently,* $\mathcal{L}$ *contains a* K*-basis of* V*.*

The determinant ideal *of a full-rank lattice* $\mathcal{L}$ *in* V *is the fractional ideal of* K *generated by*

$$\{\det(G(b)) : b \in \mathcal{L}^n\} \quad \text{where } n := \dim(V).$$

In this paper, we always assume that a lattice $\mathcal{L}$ has full rank.

Given a lattice $\mathcal{L}$ in V and $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$ we denote by $\mathcal{L}_\mathfrak{p} = \mathcal{L} \otimes_{\mathcal{O}_K} \mathcal{O}_{K_\mathfrak{p}}$ the completion of $\mathcal{L}$ at $\mathfrak{p}$. For an infinite place v of K we set $\mathcal{L}_v := V_v$.

If $G \in K^{n \times n}$ is symmetric, we can endow K^n with the quadratic form $Q\colon K^n \to K,\ x \mapsto x^T G x$. Then $\mathcal{O}_K^n$ is a free $\mathcal{O}_K$-lattice in (K^n, Q). Conversely, if $\mathcal{L}$ is a free $\mathcal{O}_K$-lattice with basis $x = (x_1, \dots, x_n)$, then the Gram matrix $G(x) \in K^{n \times n}$ is symmetric and unique up to a base change, i.e. up to equivalence in $\mathrm{GL}_n(\mathcal{O}_K)$. Every matrix determines a free quadratic module (not vice versa). Thus, the concept of lattices extends the concept of quadratic forms over $\mathcal{O}_K$.

Definition 7. *Let* $\mathcal{L}$ *be a full-rank lattice in* V*. The* dual lattice *of* $\mathcal{L}$ *is*

$$\mathcal{L}^\# := \{x \in V : B(x, \mathcal{L}) \subseteq \mathcal{O}_K\}\,.$$

The lattice $\mathcal{L}$ *is called*

– integral *if* $\mathcal{L} \subseteq \mathcal{L}^{\#}$.
– unimodular *if* $\mathcal{L} = \mathcal{L}^{\#}$.
– $\mathfrak{a}$-modular *if* $\mathcal{L} = \mathfrak{a}\mathcal{L}^{\#}$ *for some fractional ideal* $\mathfrak{a}$ *of* K.
– modular *if* $\mathcal{L}$ *is* $\mathfrak{a}$*-modular for some* $\mathfrak{a}$.

After rescaling Q, we may assume that all lattices are integral. We also assume that $\mathcal{L}$ is given in terms of a pseudo-basis

$$\mathcal{L} = \sum_{i=1}^{n} \mathfrak{a}_i x_i$$

with fractional ideals $\mathfrak{a}_i$ of $\mathcal{O}_K$ and a basis $x := (x_1, \ldots, x_n)$ of V. The pseudo-Gram matrix associated to the pseudo-basis is $(G(x), \{\mathfrak{a}_i\}_{1 \leq i \leq n})$ and the determinant ideal of $\mathcal{L}$ is $\det(\mathcal{L}) = \prod_{i=1}^{n} \mathfrak{a}_i^2 \det(G(x))$. The dual of $\mathcal{L}$ is

$$\mathcal{L}^{\#} = \sum_{i=1}^{n} \mathfrak{a}_i^{-1} x_i^*$$

where $(x_1^*, \ldots, x_n^*)$ is the dual basis of x which is determined by $B(x_i, x_j^*) = \delta_{i,j}$ for all $1 \leq i, j \leq n$. In particular, the determinant ideal $\det(\mathcal{L})$ and the dual $\mathcal{L}^{\#}$ can be computed in polynomial time.

Example 3. The quadratic form $J = \mathrm{diag}(1, 1, -1, -1)$ of the DEFI scheme [13] is associated to a unimodular lattice over $\mathcal{O}_K$.

The orthogonal group $\mathrm{O}(V, Q)$ acts on the lattices in (V, Q). We say that two lattices $\mathcal{L}$ and $\mathcal{L}'$ are isometric and write $\mathcal{L} \cong \mathcal{L}'$ if $\mathcal{L}' = \sigma(\mathcal{L})$ for some $\sigma \in \mathrm{O}(V, Q)$. Next, we define the lattice version of the Search-LIP.

Definition 8 (Search-LIP (lattice version)). *Given two isometric lattices* $\mathcal{L} \cong \mathcal{L}'$*, find* $\sigma \in \mathrm{O}(V, Q)$ *such that* $\mathcal{L}' = \sigma(\mathcal{L})$.

Lattice versions of Decision/Distinguishing-LIP are defined analogously.

The stabiliser of $\mathcal{L}$ in $\mathrm{O}(V, Q)$

$$\mathrm{O}(\mathcal{L}) = \{\sigma \in \mathrm{O}(V, Q) : \sigma(\mathcal{L}) = \mathcal{L}\}$$

is called the *automorphism group* of $\mathcal{L}$ and we denote by

$$\mathrm{SO}(\mathcal{L}) = \{\sigma \in \mathrm{SO}(V, Q) : \sigma(\mathcal{L}) = \mathcal{L}\}$$

the stabiliser of $\mathcal{L}$ in $\mathrm{SO}(V, Q)$.

Given a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ we denote by $\mathrm{O}(\mathcal{L}_\mathfrak{p})$ and $\mathrm{SO}(\mathcal{L}_\mathfrak{p})$ the stabilisers of $\mathcal{L}_\mathfrak{p}$ in $\mathrm{O}(V_\mathfrak{p}, Q)$ and $\mathrm{SO}(V_\mathfrak{p}, Q)$ respectively.

2.3 Genus and Spinor Genus

Each anisotropic vector $x \in V$ induces the *(hyperplane) reflection* $\tau_x \in \mathrm{O}(V,Q)$ given by

$$\tau_x \colon V \to V,\ y \mapsto y - \frac{2B(y,x)}{Q(x)}x\,.$$

Every reflection has determinant -1, and they generate the orthogonal group $\mathrm{O}(V,Q)$. There is a unique homomorphism

$$\theta \colon \mathrm{O}(V,Q) \to K^*/(K^*)^2$$

defined by $\theta(\tau_x) = Q(x) \in K^*/(K^*)^2$ for all reflections τ_x. The map θ is called the spinor norm of $\mathrm{O}(V,Q)$. The same holds at the completions of K.

The spinor kernel is of special interest, namely the kernel of the restriction $\theta \colon \mathrm{SO}(V,Q) \to K^*/(K^*)^2$.

Definition 9. *The* spinor kernel *is*

$$\mathrm{S}(V,Q) = \{\sigma \in \mathrm{SO}(V,Q) : \theta(\sigma) = 1\}\,.$$

Given a prime ideal $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$ *we similarly define* $\mathrm{S}(V_\mathfrak{p},Q)$*. We denote*

$$\theta(\mathcal{L}_\mathfrak{p}) := \theta(\mathrm{SO}(\mathcal{L}_\mathfrak{p})) = \{\theta(\sigma) : \sigma \in \mathrm{SO}(\mathcal{L}_\mathfrak{p})\} \subseteq K_\mathfrak{p}^*/(K_\mathfrak{p}^*)^2$$

to be the image of $\mathrm{SO}(\mathcal{L}_\mathfrak{p})$ *under the spinor norm.*

For further readings on spinor norm and how it is constructed from Clifford algebras, see [24].

We now define two important mathematical definitions for local and global classification of lattices.

Definition 10. *Let* $\mathcal{L} \subset (V,Q)$ *be a full-rank lattice. The* genus *and* isometry class *of* $\mathcal{L}$ *are*

$$\begin{aligned}\mathrm{gen}(\mathcal{L}) &= \{\mathcal{L}' \subset V : \mathcal{L}'_\mathfrak{p} \cong \mathcal{L}_\mathfrak{p} \text{ for all } \mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)\}\,,\\ \mathrm{cls}(\mathcal{L}) &= \{\mathcal{L}' \subset V : \mathcal{L}' \cong \mathcal{L}\}\,.\end{aligned}$$

We note that lattices in the same genus must have the same determinant ideal since its $\mathfrak{p}$-adic valuations can be computed locally over $K_\mathfrak{p}$.

Being in the same genus (or isometry class) defines an equivalence relation on the set of full-rank lattices in (V,Q). To be able to describe the isometry classes in the genus of $\mathcal{L}$, Eichler introduced an additional equivalence relation which is finer than being in the same genus but coarser than being isometric.

Definition 11. *Two full-rank lattices* $\mathcal{L}$ *and* $\mathcal{L}'$ *in* V *are in the same* spinor genus *if there exists* $\varphi \in \mathrm{O}(V,Q)$ *such that* $\forall \mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$

$$\mathcal{L}'_\mathfrak{p} = \varphi(\psi_\mathfrak{p}(\mathcal{L}_\mathfrak{p})) \quad \text{for some } \psi_\mathfrak{p} \in \mathrm{S}(V_p,Q)\,.$$

If φ *can be picked from* $\mathrm{SO}(V,Q)$*, then the lattices are said to be in the same proper spinor genus. We denote by* $\mathrm{sgen}(\mathcal{L})$ *and* $\mathrm{sgen}^+(\mathcal{L})$ *the spinor genus and proper spinor genus of* $\mathcal{L}$*.*

There is a classical correspondence between ideal class groups and the equivalence of quadratic forms. To study the classification of quadratic forms globally, namely genus and spinor genus, rooted in the local-global principle, it is natural to appeal to class field theory. The theory of idèles is the right language for describing genus and spinor genus of lattices. The analogue of the multiplicative group in local class field theory is given by the idèle class group in global class field theory, while the ray class group generalises the ideal class group. A more comprehensive treatment of idèles and ray class groups may be found in [23, Chapter VI, Section 1], while the extension of idèles to orthogonal groups is discussed in [24, Section 101 D].

The number of (proper) spinor genera in a given genus is determined by local invariants, as established by Kneser [17]. We follow the exposition [24, Section 102]. To this end, we use the following notation.

- The group of idèles of K is

$$J = \{(j_v)_v \in \prod_{v \in \Omega(K)} K_v^* : j_{\mathfrak{p}} \in (\mathcal{O}_{K_{\mathfrak{p}}})^* \text{ for all but finitely many } \mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)\} .$$

  We view K^* as a subgroup of J via the diagonal embedding.
- Let $J^{\mathcal{L}} = \{j \in J; j_{\mathfrak{p}} \in \theta(\mathcal{L}_{\mathfrak{p}}),\ \text{for all } \mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)\}$. Note that $J^2 \subseteq J^{\mathcal{L}}$.
- Let S be the set of real places v of K such that (V_v, Q) is anisotropic. Further let $K_S^* = \{a \in K^*; \tau(a) > 0 \text{ for all real places } \tau \in S\}$.
- Let $\mathrm{Cl}_S(K) = \mathcal{I}(\mathcal{O}_K)/\{a\mathcal{O}_K : a \in K_S^*\}$ be the ray class group[5] of $\mathcal{O}_K$ with respect to S.

With the above notation, the number of proper spinor genera in $\mathrm{gen}(\mathcal{L})$ can be specified explicitly.

Theorem 5 ([24, 102:7]). *If* $\dim_K(V) \geq 3$ *then the number of proper spinor genera in* $\mathrm{gen}(\mathcal{L})$ *is given by the index* $[J : K_S^* J^{\mathcal{L}}]$.

The Strong Approximation Theorem [24, 104:4] implies that spinor genera and equivalence classes of indefinite lattices coincide.

Theorem 6. *Let* $\mathcal{L}$ *be a full-rank lattice in an indefinite regular quadratic space over* K *with* $\dim_K(V) \geq 3$. *Then* $\mathrm{cls}(\mathcal{L}) = \mathrm{sgen}(\mathcal{L})$.

Proof. See for example [24, 104:5].

2.4 DEFI Signature Schemes

Finally, we wish to record some useful facts about DEFIv1 and DEFIv2 for later.

[5] Here $\mathrm{Cl}_S(K)$ is a rather special case of the ray class group without considering any prime ideals.

DEFIv1: Let $m \in \mathbb{N}$ be a power of 2 and let $\zeta_{2m} = e^{i\frac{2\pi}{2m}} = e^{i\frac{\pi}{m}}$. The cyclotomic field $K = \mathbb{Q}(\zeta_{2m}) \cong \mathbb{Q}[x]/(x^m + 1)$ is totally complex for $m > 1$. Its ring of integers $\mathcal{O}_K = \mathbb{Z}[\zeta_{2m}] \cong \mathbb{Z}[x]/(x^m + 1)$. The discriminant is given by $(-1)^{m/2}m^m$ for $m > 1$, which is also a power of 2. DEFIv1 sets the parameter $m \in \{32, 64\}$, for which the class number is 17 and 359057, respectively [26].

DEFIv2: The authors of DEFIv2 set $m \in \{16, 28\}$, but did not specify generally for which values of $m \in \mathbb{N}$ the polynomial $f(x) = x^m + x + 1$ is irreducible. Selmer [25] initiated the study of trinomials $x^m \pm x \pm 1$. We collect several interesting properties in the following:

- Selmer showed that the polynomial $f(x) = x^m + x + 1$ is irreducible for $m \not\equiv 2 \pmod 3$. If m is even, all roots are complex. Its discriminant is $(-1)^{m(m-1)/2}(m^m + (-1)^{m-1}(m-1)^{m-1})$, and always odd.
- When $f(x)$ is irreducible with square-free discriminant, the field $K = \mathbb{Q}[x]/(f)$ is *monogenic*, that is $\mathcal{O}_K = \mathbb{Z}[\alpha]$ where α is a root of $f(x)$. We have found that the discriminant of $f(x) = x^m + x + 1$ is square-free for $m \leq 64$.
- The class group of the number fields $\mathbb{Q}[x]/(x^m + x + 1)$ is trivial whenever $m \leq 67$.
- The Galois group of the splitting field of irreducible $x^m + x + 1$ is the symmetric group S_m for all $m \geq 2$ [22].
- Selmer showed $g(x) = x^m - x - 1$ is always irreducible. The class group of $\mathbb{Q}[x]/(g(x))$ is trivial whenever $m \leq 64$.
- The Galois group of its splitting field is S_m for all $m \geq 2$ [22]. For this reason, it is used in NTRU Prime (with prime degree m).
- The (odd) discriminant of $g(x) = x^m - x - 1$ is $(-1)^{(m-1)(m-2)/2}(m^m + (-1)^m(m-1)^{m-1})$. It is square-free for all $m < 130$ [5].
- It is conjectured in [5] that $\mathrm{disc}(x^m - x - 1)$ is square-free with probability 99.34%. It is reasonable to conjecture that $\mathrm{disc}(x^m + x + 1)$ for $m \not\equiv 2 \pmod 3$ is square-free with similar probability.

3 Decision-LIP

In this section, we revisit the local-global principle for lattices, study the equality of the genus, spinor genus and class under certain assumptions, compute the genus of a lattice in a quadratic space, and solve the Decision-LIP for DEFI.

Theorem 7. *If* $\#\,\mathrm{Cl}_S(K)$ *is odd,* $\dim_K(V) \geq 3$ *and* $\mathcal{L}$ *is modular, then* $\mathrm{gen}(\mathcal{L}) = \mathrm{sgen}(\mathcal{L})$.

Proof. Let $g = [J : K_S^* J^{\mathcal{L}}]$ be the number of proper spinor genera in $\mathrm{gen}(\mathcal{L})$. It suffices to show that $g = 1$. From $J^2 \subseteq J^{\mathcal{L}}$ it follows that g is a power of 2.

To this end, let

$$J^{\mathcal{P}(\mathcal{O}_K)} = \{j \in J : \mathrm{ord}_{\mathfrak{p}}(j) = 0 \text{ for all } \mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)\}\,.$$

The homomorphism $J \to \mathrm{Cl}_S(K),\ j \mapsto \left[\prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(j_{\mathfrak{p}})}\right]$ has kernel $K_S^* J^{\mathcal{P}(\mathcal{O}_K)}$. Since $\mathcal{L}$ is a modular lattice, for any prime ideal $\mathfrak{p}$ we have $\mathcal{O}_{K_{\mathfrak{p}}}^* (K_{\mathfrak{p}}^*)^2 \subseteq \theta(\mathcal{L}_{\mathfrak{p}})$,

with equality if $\mathfrak{p}$ is non-dyadic, see [24, 92:5 and 93:20] for details. Hence $J^{\mathcal{P}(\mathcal{O}_K)} \subseteq J^{\mathcal{L}}$. From

$$g = [J : K_S^* J^{\mathcal{L}}] \mid [J : K_S^* J^{\mathcal{P}(\mathcal{O}_K)}] = \#\operatorname{Cl}_S(K)$$

i.e., g divides the odd integer $\#\operatorname{Cl}_S(K)$ and therefore must be odd. □

Example 4. Let $K = \mathbb{Q}(\sqrt{10})$ and consider the free $\mathcal{O}_K$-lattice $\mathcal{L}$ with Gram matrix $J = \operatorname{diag}(1, 1, -1, -1)$. Since J is isotropic, the set S is empty. Hence $\operatorname{Cl}_S(K) = \operatorname{Cl}(K)$ has order 2. Using an equivalent formulation of Theorem 5 using ray class groups [14, Theorem 5.4.6], one can check that $\operatorname{gen}(\mathcal{L})$ consists of two (proper) spinor genera. So, the assumption in Theorem 7 that $\operatorname{Cl}_S(K)$ has odd order is essential.

Combining Theorems 6 and 7 gives the following result.

Corollary 5. *Let (V, Q) be a regular quadratic space over a totally complex number field K with an odd class number and $\dim_K(V) \geq 3$. Suppose $\mathcal{L}$ is a full-rank modular lattice. Then $\operatorname{cls}(\mathcal{L}) = \operatorname{gen}(\mathcal{L})$.*

Proof. Since K is totally complex, the space (V, Q) is indefinite. By Theorem 6, it is immediate that $\operatorname{cls}(\mathcal{L}) = \operatorname{sgen}(\mathcal{L})$. Moreover, the set S is empty, and the ray class group $\operatorname{Cl}_S(K)$ is just the usual class group $\operatorname{Cl}(K)$. By Theorem 7, $\operatorname{sgen}(\mathcal{L}) = \operatorname{gen}(\mathcal{L})$, completing the proof. □

The idèle group J and its subgroup $K_S^* J^{\mathcal{L}}$ are not finitely presented. This makes the quotient $J/K_S^* J^{\mathcal{L}}$ difficult to handle algorithmically. By [14, Corollary 5.4.10] one can identify $J/K_S^* J^{\mathcal{L}}$ with some quotient of a ray class group of K.

3.1 Algorithm to Decide If a Lattice Lies in a Given Genus

We want to decide whether two given full-rank lattices $\mathcal{L}$ and $\mathcal{L}'$ in some quadratic spaces (V, Q) and (V', Q') over K are isometric locally over all places of K.

We start with the finite places. Given a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, we need to decide whether $\mathcal{L}_\mathfrak{p} \cong \mathcal{L}'_\mathfrak{p}$. To this end, we compute some Jordan decomposition of $\mathcal{L}$, that is, an orthogonal decomposition

$$\mathcal{L} = \mathcal{L}_1 \perp \mathcal{L}_2 \perp \ldots \perp \mathcal{L}_r \tag{1}$$

where $\mathcal{L}_i$ is $\mathfrak{p}^{s_i}$-modular with integers $s_1 < s_2 < \ldots < s_r$.

We do not actually need an explicit Jordan decomposition. It is enough to compute a Gram matrix of such a decomposition. Algorithm 1 computes such a matrix.

Algorithm 1 JordanDecomposition

Input: An $\mathcal{O}_K$-lattice $\mathcal{L} = \bigoplus_{i=1}^{m} \mathfrak{a}_i x_i$ and a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$.
Output: A Gram matrix of a Jordan decomposition of $\mathcal{L}_\mathfrak{p}$.

1: Let $\pi \in \mathfrak{p}$ with $\mathrm{ord}_\mathfrak{p}(\pi) = 1$.
2: For $1 \leq i \leq m$ set $e_i = \pi^{\mathrm{ord}_\mathfrak{p}(\mathfrak{a}_i)} x_i$.
3: Let G be the Gram matrix of $(e_1, \ldots, e_m)$ and set $r = 1$.
4: **while** $r < m$ **do**
5: Pick $r \leq i \leq j \leq m$ with $i = j$ if possible, such that $G_{i,j}$ has minimal valuation at $\mathfrak{p}$.
6: **if** $i \neq$j and $2 \notin \mathfrak{p}$ **then**
7: Add the j-th column and row of G to the i-th column and row respectively.
8: Set $j = i$.
9: **end if**
10: **if** $i = j$ **then**
11: Swap the r-th and i-th columns and rows of G.
12: **for** $r < k \leq m$ **do**
13: Subtract $\frac{G_{r,k}}{G_{r,r}}$ times the r-th column/row from the k-th column/row.
14: **end for**
15: Increase r by 1.
16: **else**
17: Swap the r-th and i-th columns and rows of G.
18: Swap the $(r+1)$-th and j-th columns and rows of G.
19: Let $d = G_{r,r+1}^2 - G_{r,r} G_{r+1,r+1}$.
20: **for** $r + 2 \leq k \leq m$ **do**
21: Let $(\lambda\,, \mu) = d^{-1} \cdot (G_{r,k},\ G_{r+1,k}) \cdot \begin{pmatrix} G_{r,r} & G_{r,r+1} \\ G_{r,r+1} & G_{r+1,r+1} \end{pmatrix}$.
22: Subtract λ times the r-th column/row from the k-th column/row.
23: Subtract μ times the $(r+1)$-th column/row from the k-th column/row.
24: **end for**
25: Increase r by 2.
26: **end if**
27: **end while**
28: **return** G.

Proof (of correctness). Lines 6–10 ensure that if $2 \notin \mathfrak{p}$ then the entry $G_{i,i}$ has minimal valuation. The loop in line 12 is just the usual Gram-Schmidt process. The resulting matrix G is still a Gram matrix of $\mathcal{L}_\mathfrak{p}$ and its r-th row is well known to be perpendicular to the other rows.

If $i \neq j$ and $2 \in \mathfrak{p}$, one checks that the element d in line 19 lies in $\mathcal{O}_K\mathfrak{p}$. Thus, the subtractions in Lines 22 and 23 correspond to a base change of $\mathcal{L}_\mathfrak{p}$ as well. After this base change, the r-th and $(r+1)$-th rows are perpendicular to the k-th row for $k > r + 1$. □

Remark 1. We do not claim that Algorithm 1 runs in polynomial time because there might be an explosion of the coefficients in G. For deciding whether two lattices are isometric over $\mathcal{O}_\mathfrak{p}$, we do not need an explicit Gram matrix of the Jordan decomposition (1) but rather some invariants that can be read off it.

More precisely, we need the scales $s_1, \dots, s_r$, the ranks of the lattices $\mathcal{L}_i$ and the determinants $\det(\mathcal{L}_i) \in K_\mathfrak{p}^*/(K_\mathfrak{p}^*)^2$.

Algorithm 1 can easily be adapted to compute these invariants in polynomial time as follows. We first compute the largest scale s_r. To this end, we compute the local basis $e = (e_1, \dots, e_m)$ of $\mathcal{L}_\mathfrak{p}$ as in line 2. Then $-s_r$ is the minimal $\mathfrak{p}$-adic valuation of any entry in $G(e)^{-1}$. Note that the matrix inversion and thus the computation of s_r can be done in polynomial time [31].

For computing $s_1, \dots, s_r$, the ranks of the lattices $\mathcal{L}_i$ and the determinants $\det(\mathcal{L}_i) \in K_\mathfrak{p}^*/(K_\mathfrak{p}^*)^2$, we only need the valuations and square classes of the entries in G. By Hensel's Lemma, the square classes of units are distinguished modulo $\mathfrak{p}^{1+\mathrm{ord}_\mathfrak{p}(4)}$. So once s_r is known, all other steps of the algorithm can be computed in the finite ring $\mathcal{O}_K/\mathfrak{p}^{s_r+1+\mathrm{ord}_\mathfrak{p}(4)}$, preventing an explosion of the coefficients of G.

Remark 2. Note that if $\mathfrak{p}$ is non-dyadic, Algorithm 1 yields a diagonal Gram matrix of $(V_\mathfrak{p}, Q)$. If $\mathfrak{p}$ is dyadic, the returned Gram matrix might have 2×2 diagonal blocks of the form $G = \left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right)$ where $\mathrm{ord}_\mathfrak{p}(b) < \mathrm{ord}_\mathfrak{p}(a) \le \mathrm{ord}_\mathfrak{p}(c)$. Set $a' = a$ if $\mathrm{ord}_\mathfrak{p}(a) \le \mathrm{ord}_\mathfrak{p}(2b)$ and set $a' = 2b$ otherwise. The quadratic space with Gram matrix G over $K_\mathfrak{p}$ has the diagonalised Gram matrix $\mathrm{diag}(a', a'(ac - b^2))$.

So in either case, we end up with a diagonal Gram matrix of $(V_\mathfrak{p}, Q)$. To compute $c(V_\mathfrak{p}, Q)$, we only need the square classes of a' and $a'(ac - b^2)$. In particular, we can run the algorithm using arithmetic modulo $\mathfrak{p}^{s_r+1+\mathrm{ord}_\mathfrak{p}(4)}$ as mentioned in Remark 1. This way, we can compute the Hasse invariant of $(V_\mathfrak{p}, Q)$ in polynomial time.

To distinguish the isometry classes over dyadic prime ideals, some more invariants are needed. Suppose now $e := \mathrm{ord}_\mathfrak{p}(2) > 0$.

Definition 12. *The quadratic defect of $a \in K_\mathfrak{p}^*$ is*

$$\mathfrak{d}(a) := \bigcap_{b \in K_\mathfrak{p}} (a - b^2)\mathcal{O}_{K\mathfrak{p}} \,.$$

So the quadratic defect is an ideal. By [24, 63:2], the valuation of $\mathfrak{d}(a)$ for a unit $a \in \mathcal{O}_{K\mathfrak{p}}^*$ is one of

$$1,\ 3, \dots,\ 2e-1,\ 2e \text{ or } \infty \,. \tag{2}$$

For a polynomial-time algorithm to compute the quadratic defect, see Appendix A.

Definition 13. *Let $\mathfrak{p}$ be a dyadic prime ideal and $\mathcal{L}$ a $\mathcal{O}_K$-lattice in V. A* norm generator *of $\mathcal{L}_\mathfrak{p}$ is an element in $\{Q(x) \mid x \in \mathcal{L}_\mathfrak{p}\}$ with minimal $\mathfrak{p}$-adic valuation. The* weight *of $\mathcal{L}_\mathfrak{p}$ is*

$$\mathfrak{w}(\mathcal{L}) = \mathfrak{p} \cdot \mathfrak{m}(\mathcal{L}_\mathfrak{p}) + \{2B(x, y) \mid x, y \in \mathcal{L}_\mathfrak{p}\}$$

where $\mathfrak{m}(\mathcal{L}_\mathfrak{p})$ denotes the largest ideal of $\mathcal{O}_{K_\mathfrak{p}}$ in $\{Q(x) \mid x \in \mathcal{L}_\mathfrak{p}\}$.

O'Meara explains in [24, page 280] how to compute a norm generator and the weight of $\mathcal{L}_\mathfrak{p}$ from any Gram matrix G of $\mathcal{L}_\mathfrak{p}$. The discussion actually shows that it suffices to know the $\mathfrak{p}$-adic valuations of the entries of G and the square-classes of the diagonal entries.

Theorem 8. *Let $\mathcal{L}$ and $\mathcal{L}'$ be integral lattices in quadratic spaces (V, Q) and (V', Q'). Given a prime ideal $\mathfrak{p}$, one can decide if $\mathcal{L}_\mathfrak{p}$ and $\mathcal{L}'_\mathfrak{p}$ are isometric in polynomial time.*

Proof. Using Remark 1 we compute the invariants s_i, $\operatorname{rank}(\mathcal{L}_i)$ and $\det(\mathcal{L}_i) \in K_\mathfrak{p}^*/(K_\mathfrak{p}^*)^2$ of some Jordan decomposition $\mathcal{L}_1 \perp \ldots \perp \mathcal{L}_r$ of $\mathcal{L}_\mathfrak{p}$. If $\mathfrak{p}$ is not dyadic, these invariants separate the isometry classes, and we are done. So suppose $\mathfrak{p}$ is dyadic. We first check if the necessary condition $c(V_\mathfrak{p}, Q) = c(V'_\mathfrak{p}, Q')$ holds using Remark 2. If it does, some more information is needed. More precisely, let a_i and $\mathfrak{w}_i$ be a norm generator and the weight of $\mathcal{L}^{s_i} := \sum_{k \le i} \mathfrak{p}^{s_i - s_k} \mathcal{L}_k + \sum_{k > i} \mathcal{L}_k$. As mentioned before, this can be done in polynomial time as well. Then the isometry type of $\mathcal{L}_\mathfrak{p}$ is determined by r, s_i, $\det(L_i)$, a_i, $\mathfrak{w}_i$. Note that the norm generators a_i and the weights $\mathfrak{w}_i$ are not invariants of $\mathcal{L}_\mathfrak{p}$, but [24, Theorem 93:28 and Example 93:26] gives a method to decide if two sets of parameters represent isometric lattices. O'Meara's method only needs to check if some $(n-1)$-dimensional local quadratic space embeds into an n-dimensional one. By [24, Theorem 63:21], this amounts to checking if two local quadratic spaces are isometric. The latter can be decided by comparing the square classes of the determinants and computing several Hilbert symbols in polynomial time. □

The above result immediately yields the method shown in Algorithm 2 to decide whether two lattices are in the same genus.

Algorithm 2 DecidingGenus

Input: Integral full-rank lattices $\mathcal{L}$ and $\mathcal{L}'$ in quadratic spaces (V, Q) and (V', Q').
Output: true if and only if $\mathcal{L}_v \cong \mathcal{L}'_v$ at all places v of K.

1: **if** $\operatorname{rank}(\mathcal{L}) \neq \operatorname{rank}(\mathcal{L}')$ or $\det(\mathcal{L}) \neq \det(\mathcal{L}')$ **then return** false.
2: **if** $\det(V, Q) \cdot \det(V', Q') \notin (K^*)^2$ **then return** false.
3: **if** the signatures of (V, Q) and (V', Q') disagree at some real place of K **then return** false.
4: **for** $\mathfrak{p} \mid 2\det(\mathcal{L})$ **do**
5: **if** $\mathcal{L}_\mathfrak{p} \ncong \mathcal{L}'_\mathfrak{p}$ by Theorem 8 **then return** false
6: **end if**
7: **end for**
8: **return** true.

Proof. Clearly, if the algorithm returns false, the lattices cannot be isometric locally everywhere. Suppose the algorithm returns true. The first 3 lines ensure that the lattices (or spaces) are isometric at the infinite places of K. Let $\mathfrak{p}$ be

a prime ideal of $\mathcal{O}_K$. If $\mathfrak{p} \mid 2\det(\mathcal{L})$ then the lattices are isometric by line 5. If $\mathfrak{p} \nmid 2\det(\mathcal{L})$ then $\mathcal{L}_\mathfrak{p}$ and $\mathcal{L}'_\mathfrak{p}$ are both unimodular by line 1. As $\mathfrak{p}$ is not dyadic, the isometry type of $\mathcal{L}_\mathfrak{p}$ only depends on $\det(V, Q)$ and the rank. Lines 1 and 2 thus ensure that $\mathcal{L}_\mathfrak{p} \cong \mathcal{L}'_\mathfrak{p}$. □

Line 2 of the previous algorithm can be done in polynomial time by factoring a quadratic polynomial over K. The signature of (V, Q) at a real place can be read off from the leading principal minors of a Gram matrix of (V, Q). Computing these determinants can be done in polynomial time. Hence, the overall algorithm runs in polynomial time provided that we know the prime divisors of the ideal $2\det(\mathcal{L})$. This proves the following result.

Theorem 9. *Let $\mathcal{L}$ and $\mathcal{L}'$ be integral lattices in quadratic spaces (V, Q) and (V', Q'). Given the factorisation of the determinant ideal $2\det(\mathcal{L})$, one can decide whether $\mathcal{L}$ and $\mathcal{L}'$ are isometric locally everywhere in polynomial time.*

The following is an immediate corollary.

Corollary 6. *Suppose $K \cong \mathbb{Q}[x]/(f)$ for some monic irreducible polynomial $f \in \mathbb{Z}[x]$ with odd discriminant. If $\mathcal{L}$ is unimodular, then Algorithm 2 runs in expected polynomial time.*

Proof. $\mathcal{L}$ is unimodular, thus factorization of $2\det(\mathcal{L}) = 2\mathcal{O}_K$ only requires to factor f over the finite field $\mathbb{F}_2$ [8, Theorem 4.8.13]. The latter can be done in expected polynomial time using the method of Cantor and Zassenhaus [8, Section 3.4]. Hence, Algorithm 2 runs in expected polynomial time. □

Note that the above corollary can be applied to all irreducible polynomials of the form $f(x) = x^m + x + 1$.

3.2 Solving Decision-LIP of DEFI

We now solve the Decision-LIP for DEFIv1 and DEFIv2 using Algorithm 2.

In DEFIv1, the only ramified prime is $(2) = (1 - \zeta_{2m})^m$, so the factorisation of $2\mathcal{O}_K$ is free. Moreover, its class number is always odd [29]. Therefore, we derive from Corollary 5 and Theorem 9

Corollary 7. *Let $\mathcal{L}$ be a modular lattice with rank ≥ 3 over $R = \mathbb{Z}[x]/(x^m + 1)$ where $m \in \mathbb{N}$ is a positive power of 2. Then there is an efficient algorithm to solve the Decision-LIP for $\mathcal{L}$.*

For DEFIv2, we have the following result.

Corollary 8. *Let $\mathcal{L}$ be a modular lattice with rank ≥ 3 over $R = \mathbb{Z}[x]/(x^m + x + 1)$ for m even, $m \leq 67$ and $m \not\equiv 2 \pmod 3$. Then there is an efficient algorithm to solve the Decision-LIP for $\mathcal{L}$.*

Proof. By [25, Theorem 1], $f(x) = x^m + x + 1$ is irreducible when $m \not\equiv 2 \pmod 3$. Since m is even, all roots of f are complex. Thus, its fractional field $K = \mathbb{Q}[x]/(f)$ is totally complex. In all cases, the class number of K is one. It is immediate from Corollary 5 that $\mathrm{cls}(\mathcal{L}) = \mathrm{gen}(\mathcal{L})$. Further, since the discriminant is odd, the Decision-LIP can be solved efficiently by Corollary 6. □

The condition of a totally complex field in Corollary 5 is sufficient, but not necessary. Next, we show that even if the fractional field $K = \mathbb{Q}[x]/(x^m - x - 1)$ is not totally complex[6], we have a similar result if the Gram matrix of $\mathcal{L}$ is restricted to be $J = \mathrm{diag}(1, 1, -1, -1)$.

Corollary 9. *Let $\mathcal{L}$ be the free lattice associated with the quadratic form J over $R = \mathbb{Z}[x]/(x^m - x - 1)$ for $2 \leq m \leq 64$. Then there is an efficient algorithm to solve the Decision-LIP for $\mathcal{L}$.*

Proof. Note also that the set S as in Section 2.3 is vacuous, because $J = \mathrm{diag}(1, 1, -1, -1)$ is isotropic, implying the ray class group $\mathrm{Cl}_S(K) = \mathrm{Cl}(K)$. For the given values of m, the field K has a trivial class group. Theorem 7 shows that $\mathrm{gen}(\mathcal{L}) = \mathrm{cls}(\mathcal{L})$. Finally, since the discriminant of $x^m - x - 1$ is odd, we can apply Corollary 6 to check if any other lattice $\mathcal{L}'$ lies in the genus of $\mathcal{L}$. □

Selmer [25] showed that $f(x) = x^m + x + 1$ has one real root if m is odd, but all other roots are complex. For the same reason, the assumption of even m in Corollary 8 can be dropped.

Corollary 10. *Let $\mathcal{L}$ be the free lattice associated with quadratic form J over $R = \mathbb{Z}[x]/(x^m + x + 1)$ for $m \leq 67$ and $m \not\equiv 2 \pmod 3$. Then there is an efficient algorithm to solve the Decision-LIP for $\mathcal{L}$.*

4 Search-LIP of DEFI

The definition of DEFIv2 can be found in the Appendix B. We begin this section by solving Problem 3.

The security of DEFIv2 is based on the hardness of finding isotropic vectors for quadratic forms over $\mathcal{O}_K$. The cryptanalysis was reduced to solving quadratic Diophantine equations over $\mathcal{O}_K$ or to solving systems of quadratic Diophantine equations over $\mathbb{Z}$ in [13]. We run both key recovery and signature forgery attacks on DEFIv2.

Private Key Recovery: Given public matrix C, the adversary is tasked to recover a matrix $S \in \mathcal{O}_K^{n \times n}$ such that $C = S^T J S$.

Forgery Attack: Given public matrix C and oracle access to the signing algorithm, the adversary is asked to output a new message along with a valid signature. Since our attack is based on key recovery, it gives a total break of the signature scheme.

[6] Selmer [25] showed that $x^m - x - 1$ has one or two real roots, depending on whether m is odd or even.

4.1 Primitive Isotropic Vector

Let K be an algebraic number field of class number one and (V, Q) an isotropic non-degenerate quadratic space over K. Let $\mathcal{L}$ be a full lattice in V. As $\mathcal{O}_K$ is a principal ideal domain, $\mathcal{L}$ is free with a basis $(e_1, \ldots, e_n)$.

Our starting point is to find a primitive isotropic vector $x = \sum_{i=1}^{n} x_i e_i \in \mathcal{L}$. Primitive means that x can be extended to a basis of $\mathcal{L}$ or equivalently, the ideal of $\mathcal{O}_K$ generated by $(x_1, \ldots, x_n)$ is trivial, see for example [6, Page 108].

We restrict the discussion to the cases $n \in \{2, 3\}$ as we will only need these two cases.

Algorithm 3 Primitive isotropic vector

Input: An isotropic quadratic space V, of rank 2 or 3 over an algebraic number field K with class number 1 and a full lattice $\mathcal{L}$ in V.
Output: A primitive isotropic vector $x \in \mathcal{L}$.

1: Let $(f_1, \ldots, f_n)$ be any orthogonal basis of (V, Q) and set $a_i = Q(f_i)$.
2: **if** $a_1 = 0$ **then**
3: Set $x' = f_1$.
4: **else if** $-a_2/a_1 = s^2$ is a square **then**
5: Set $x' = sf_1 + f_2$.
6: **else**
7: Solve the norm equation $-a_3/a_1 = x_1^2 + a_2/a_1 x_2^2$ in $K(\sqrt{a_2/a_1})/K$.
8: Set $x' = x_1 f_1 + x_2 f_2 + f_3$.
9: **end if**
10: Compute a generator g of the fractional ideal $\{a \in K : ax' \in \mathcal{L}\}$.
11: **return** $x := x'/g$.

Proof. We first note that if $n = 2$, then $-\det(V, Q) = -a_1 a_2$ is a square, see Example 1. So in this case, line 7 cannot be reached. Whether $n = 2$ or $n = 3$, it is readily verified case-by-case that the chosen vector x' is isotropic. Hence $x \in \mathcal{L}$ is also isotropic and primitive by construction. □

Remark 3. The above algorithm needs to solve a norm equation over a quadratic field extension of K and construct a generator of a principal ideal. For both tasks, there are quantum polynomial-time algorithms available, see [3].

4.2 Split an Isotropic Unimodular Lattice

Next, we wish to find a basis of a unimodular lattice. If one applies Algorithm 3 to an indefinite unimodular ternary lattice, one can split it into a hyperbolic lattice of rank 2 and a unimodular lattice of rank 1 as follows.

Algorithm 4 Split an isotropic unimodular lattice

Input: An isotropic quadratic space V of rank 3 over an algebraic number field K with class number 1 and a full unimodular lattice in $\mathcal{L} \subset V$.

Output: A basis (x, y, z) of $\mathcal{L}$ with Gram matrix

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & a & 0 \\ 0 & 0 & u \end{pmatrix} \quad \text{where } a \in \mathcal{O}_K \text{ and } u \in \mathcal{O}_K^*.$$

1: Let x be a primitive isotropic vector in $\mathcal{L}$, see Algorithm 3.
2: Using linear algebra over $\mathbb{Z}$, find some $y \in \mathcal{L}$ with $B(x, y) = 1$.
3: Using linear algebra over K, compute $z' \in V \setminus \{0\}$ perpendicular to x and y.
4: Compute a square root $t \in K$ of $-\det(\mathcal{L})/Q(z')$ and set $z = tz'$.
5: **return** (x, y, z).

Proof. As $\mathcal{L}$ is unimodular, the ideal $\{B(x, v) : v \in V\}$ equals $\mathcal{O}_K$. Hence y exists. The submodule $S := \mathcal{O}_K x \oplus \mathcal{O}_K y$ has the Gram matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_K)\,. \tag{3}$$

Thus S is a direct summand of $\mathcal{L}$, say $\mathcal{L} = S \perp \mathcal{O}_K z$. Then $z = tz'$ for some $t \in K^*$. Comparing determinants shows that $\det(\mathcal{L}) = -Q(z) = -t^2 Q(z')$ or equivalently $t^2 = -\det(\mathcal{L})/Q(z')$. □

Remark 4. Lines 1–2 of Algorithm 4 when applied to an isotropic unimodular lattice $\mathcal{L}$ of rank 2 yield a basis (x, y) with Gram matrix as in eq. (3).

4.3 Solution to Search-LIP/Key Recovery Attack for DEFIv2

Let us consider the DEFIv2 key recovery problem. The DEFIv2 challenge [13] asks for key recovery and signature forgery in the case that $n = 4, r = 1, s = 3$, $J = \mathrm{diag}(1, 1, -1, -1)$ and $B_{11} = 1$. To this end, we solve the search problem for this setup over any algebraic number field K with class number 1. This includes the cases $K = \mathbb{Q}[x]/(x^m + x + 1)$ with $m \in \{16, 28\}$ proposed in [13].

The authors of the DEFI signature scheme picked a secret random unimodular matrix

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 \\ b_{21} & b_{22} & b_{23} & b_{24} \\ b_{31} & b_{32} & b_{33} & b_{34} \\ b_{41} & b_{42} & b_{43} & b_{44} \end{pmatrix} \in \mathrm{GL}_4(\mathcal{O}_K). \tag{4}$$

The public key is the symmetric matrix

$$C = B^T J B\,.$$

To recover a similar private key, we need to find an invertible matrix T as in Eq. (4) such that $T^T C T = J$.[7]

Let t be the first column of T and let $(e_1, \dots, e_4)$ be the standard basis of $\mathcal{O}_K^4$. Let $\mathcal{L}$ be the $\mathcal{O}_K$-lattice generated by the last three columns of T. Since the lower right 3×3 submatrix of T is invertible, the lattice $\mathcal{L}$ is simply $\bigoplus_{i=2}^4 \mathcal{O}_K e_i$. We set $V = \bigoplus_{i=1}^4 K e_i$ and equip V with the quadratic form $Q \colon V \to K,\ x \mapsto x^T C x$.

The column t must be perpendicular to the last three columns of T (with respect to Q). If we apply Algorithm 4 to $\mathcal{L}$ we get a basis (x, y, z). Comparing determinants shows that (after rescaling z by some unit in $\mathcal{O}_K^*$) the Gram matrix of Q with respect to the basis (t, x, y, z) is

$$J' := \begin{pmatrix} 1 & & & \\ & 0 & 1 & \\ & 1 & a & \\ & & & -1 \end{pmatrix}. \tag{5}$$

Then

$$A := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix} \in \mathrm{GL}_4(\mathcal{O}_K), \tag{6}$$

satisfies $A^T J' A = J$. This leads to the following algorithm.

Algorithm 5 SearchProblem

Input: Public key C over an algebraic number field K with class number 1.
Output: $S \in \mathrm{GL}_4(\mathcal{O}_K)$ as in (4) with $S^T C S = J$.

1: Let $\{e_1, e_2, e_3, e_4\}$ be the standard basis of $\mathcal{O}_K^4$ and set $\mathcal{L} = \bigoplus_{i=2}^4 \mathcal{O}_K e_i$.
2: Compute $t \in K^4$ with $t_1 = 1$ such that $e_i^T C t = 0$ for $2 \le i \le 4$ using linear algebra over K.
3: Let (x, y, z') be the basis from Algorithm 4 when applied to $\mathcal{L}$.
4: Compute a square root $s \in K$ of $-(z')^T C z'$ and set $z = z'/s$.
5: Let T be the matrix with columns (t, x, y, z).
6: **return** $S := TA$ where A is given by eq. (6).

Algorithm for general B: With some extra work, we can even recover $S \in \mathrm{GL}_4(\mathcal{O}_K)$ such that $S^T C S = J$ without assuming that C was derived from J with a change-of-basis matrix B as in (4). This solves Search-LIP and hence Decision/Distinguishing-LIP for lattices in the genus of J.

[7] The automorphism group of C is well known to be infinite, see for example [27]. Hence, there is no way to recover the matrix B from C.

Algorithm 6 SearchProblemGeneral

Input: An algebraic number field K with class number one and odd discriminant. A symmetric matrix C in the genus of J.

Output: A matrix $S \in \mathrm{GL}_4(\mathcal{O}_K)$ such that $S^T C S = J$.

1: Equip K^4 with the quadratic form $Q(x) = x^T C x$.
2: Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_\ell$ be the prime ideals over $2\mathcal{O}_K$.
3: Let $(e_1, \ldots, e_4)$ be a basis of $\mathcal{O}_K^4$.
4: Let x_1 be a primitive isotropic vector in $\bigoplus_{i=1}^3 e_i \mathcal{O}_K$.
5: Using linear algebra over $\mathbb{Z}$ compute $x_2 \in \mathcal{O}_K^4$ such that $B(x_1, x_2) = 1$.
6: Let $\mathcal{L} = \{v \in \mathcal{O}_K^4 \mid B(x_1, v) = B(x_2, v) = 0\}$.
7: Let x_3 be a primitive isotropic vector in $\mathcal{L}$ and let $x_4 \in \mathcal{L}$ such that $B(x_3, x_4) = 1$.
8: **if** $Q(x_2) \in \mathfrak{p}_j$ for some j **then**
9: For $1 \leq i \leq \ell$ set $\lambda_i = 0$ if $Q(x_2) \notin \mathfrak{p}_i$ and set $\lambda_i = 1$ otherwise.
10: Compute $\lambda \in \mathcal{O}_K$ such that $\lambda \equiv \lambda_i \pmod{\mathfrak{p}_i}$ for all $1 \leq i \leq \ell$.
11: Replace x_2 by $x_2 + \lambda x_4$ and go to step 6.
12: **end if**
13: For $1 \leq i \leq \ell$ let $\mu_i \in \mathcal{O}_K$ such that $Q(x_4) + \mu_i^2 Q(x_2) \equiv 0 \pmod{\mathfrak{p}_i}$.
14: Compute $\mu \in \mathcal{O}_K$ such that $\mu \equiv \mu_i \pmod{\mathfrak{p}_i}$ for all $1 \leq i \leq \ell$.
15: Replace x_4 by $x_4 + \mu x_2$. Then replace x_4 by $x_4 - Q(x_4)/2 x_3$.
16: Let $\mathcal{L} = \{v \in \mathcal{O}_K^4 \mid B(x_3, v) = B(x_4, v) = 0\}$.
17: Let x_1 be a primitive isotropic vector in $\mathcal{L}$ and let $x_2 \in \mathcal{L}$ with $B(x_1, x_2) = 1$.
18: For $1 \leq i \leq \ell$ let $\alpha_i \in \mathcal{O}_K$ such that $Q(x_2)\alpha_i^2 \equiv 1 \pmod{\mathfrak{p}_i}$.
19: Pick $\alpha \in \mathcal{O}_K$ such that $\alpha \equiv \alpha_i \pmod{\mathfrak{p}_i}$ for all $1 \leq i \leq \ell$.
20: Set $t = \alpha x_2 - (Q(x_2)\alpha^2 - 1)/2 \cdot (x_3 + x_4)$ and $\mathcal{L} := \{v \in \mathcal{O}_K^4 \mid B(t, v) = 0\}$.
21: Let (x, y, z') be the basis from Algorithm 4 when applied to $\mathcal{L}$.
22: Compute a square root $s \in K$ of $-Q(z')$ and set $z = z'/s$.
23: Let T be the matrix with columns (t, x, y, z).
24: **return** $S := TA$ where A is given by eq. (6).

Theorem 10. *Let K be an algebraic number field with class number one and odd discriminant. Given a matrix $C \in \mathrm{GL}_4(\mathcal{O}_K)$ in the genus of J, Algorithm 6 constructs a matrix $S \in \mathrm{GL}_4(\mathcal{O}_K)$ such that $S^T C S = J$.*

Proof. We first note that $2\mathcal{O}_K = \prod_{i=1}^{\ell} \mathfrak{p}_i$ since the discriminant of K is odd. By assumption, (K^4, Q) has a basis such that the corresponding Gram matrix is J. It is thus the orthogonal sum of two hyperbolic planes. Hence it contains a 2-dimensional subspace W such that $Q(W) = \{0\}$. Thus $\bigoplus_{i=1}^3 e_i \mathcal{O}_K$ intersects W non-trivially and is therefore isotropic. This shows that x_1 and x_2 from steps 4 and 5 exist. The lattice $\mathcal{L}_1 := \mathcal{O}_K x_1 \oplus \mathcal{O}_K x_2$ is unimodular and thus $\mathcal{O}_K^4 = \mathcal{L}_1 \perp \mathcal{L}$ with $\mathcal{L}$ as in line 6. Since (K^4, Q) is the sum of two hyperbolic planes, the unimodular lattice $\mathcal{L}$ is isotropic. By Remark 4 it has the basis (x_3, x_4) from line 7. Hence (x_1, x_2, x_3, x_4) is a basis of $\mathcal{O}_K^4$ with Gram matrix

$$\begin{pmatrix} 0 & 1 & & \\ 1 & a & & \\ & & 0 & 1 \\ & & 1 & b \end{pmatrix} \tag{7}$$

where $a = Q(x_2)$ and $b = Q(x_4)$. By assumption, there exists $e = \sum_{i=1}^{4} e_i x_i \in \mathcal{O}_K^4$ such that $Q(e) = 1$. Hence

$$1 = Q(e) = 2e_1e_2 + ae_2^2 + 2e_3e_4 + be_4 \equiv ae_2^2 + be_4^2 \pmod{2\mathcal{O}_K}\,. \tag{8}$$

In particular, a and b cannot both lie in $\mathfrak{p}_i$. Steps 9–11 ensure that $a \notin \mathfrak{p}_i$ for all i. In particular, step 11 can only be reached once, thus the algorithm terminates. In step 13, $a = Q(x_2)$ is a unit modulo $\mathfrak{p}_i$ and thus the quadratic equation $b = \mu_i^2 a \pmod{\mathfrak{p}_i}$ has a solution. The element μ in line 14 satisfies $b+\mu^2 a \in 2\mathcal{O}_K$. Hence, line 15 is just a base change of $\mathcal{O}_K$. As before, the lattice $\mathcal{L}$ from line 16 is hyperbolic, so after line 17 we end up with a basis $(x_1, \ldots, x_4)$ of $\mathcal{O}_K^4$ with Gram matrix as in eq. (7) but this time with $b = 0$. Then eq. (8) shows that α_i from line 18 exists. The element α then satisfies $Q(x_2)\alpha^2 \in 2\mathcal{O}_K$. Hence the vector $t \in \mathcal{O}_K^4$ from step 20 satisfies $Q(t) = 1$. The last 4 steps then compute a basis (x, y, z) of $\mathcal{L}$ such that (t, x, y, z) has Gram matrix J as in Algorithm 5. □

Remark 5. As Algorithm 6 is based on Algorithm 3, it needs to solve norm equations over a quadratic field extension of K and construct generators of principal ideals. For both tasks, there are quantum polynomial-time algorithms available, see [3].

4.4 Signature Forgery

For forging signatures, it is easier to work with the matrix T with columns (t, x, y, z) of Algorithm 5 than with the output matrix S. Given a message with hash $h \in \mathcal{O}_K$, any vector $v = (h, b, 0, h)^T \in \mathcal{O}_K^4$ satisfies

$$w = Tv = ht + bx + hz = h(t + z) + bx\,. \tag{9}$$

Then

$$w^T C w = v^T J' v = 0$$

and the first coefficient of w is the hash h. Hence, the last three entries of w form a valid signature for h.

4.4.1 Small signatures

Let $(b_1, \ldots, b_m)$ be any $\mathbb{Z}$-basis of $\mathcal{O}_K$. Then

$$e' := (e_i b_j : 1 \le i \le 4,\ 1 \le j \le m)$$

is a $\mathbb{Z}$-basis of $\mathcal{O}_K^4$. Using this basis, we identify $\mathcal{O}_K^4$ with the standard $\mathbb{Z}$-lattice $\mathbb{Z}^{4m}$ equipped with the usual inner product.

Our signatures, when written as a linear combination in e' could have larger coefficients than those created using the private key B. So the DEFI-scheme might reject our signatures since there is an upper bound on the size of signatures (please refer to Section (5.2) for more details). Finding smaller signatures can be done by solving the closest vector problem (CVP) in $\mathbb{Z}^m$.

4.4.2 Optimising for all signatures We first consider elements $b \in h\mathcal{O}_K$, say $b = hb'$. Then eq. (9) reads $w = h \cdot (t+z+b'x)$, and thus we want $t+z+b'x$ to have small coefficients with respect to e'. Hence, we look for an element $v = -b'x$ in the rank m integer lattice $\mathcal{O}_K x \subseteq \mathcal{O}_K^4 \cong \mathbb{Z}^{4m}$ such that $t+z-v$ is small with respect to the standard inner product of $\mathbb{Z}^{4m}$ or equivalently v is close to $t+z$. Then the last three entries of

$$w_1 = h(t+z-v) \tag{10}$$

form a valid signature for h with very small coefficients. This approach has the advantage that we only have to do this step once for all hashes h.

4.4.3 Optimising for individual signatures To obtain even smaller signatures, we adjust the parameter b in (9) for each hash h individually. So we want $v = -bx \in \mathcal{O}_K x \subseteq \mathcal{O}_K^4$ to be close to $h(t+z)$. Then the last three entries of

$$w_2 = h(t+z) - v \tag{11}$$

form a valid signature for h with very small coefficients.

5 Experiments

All Magma computations use the environment on a personal MacBook laptop. Our codes are available online at [15]. Timings reported below were measured on that machine.

5.1 Decision-LIP

For the Decision-LIP, we take the degree of the irreducible polynomial $f(x) = x^m + x + 1$ to be $m \in \{16, 28\}$ corresponding to DEFIv2-c and DEFIv2-1. Let $\mathcal{L}_J$ be the lattice associated with $\mathrm{diag}(1, 1, -1, -1)$.

Table 1 lists the class group and the genus computations done in Magma. The class group computation returns an abelian group of order 1. This shows that the ring of integers of $\mathbb{Z}[x]/(f) = \mathbb{Z}[\alpha]$ is a PID. Genus computation returns a single genus representative, implying that the genus is equal to the equivalence class. This is the computational proof for the statement that the genus of $\mathcal{L}_J$ contains only one isometry class in $\mathbb{Z}[x]/(f)$. Consequently, we solve the Decision/Distinguishing-LIP for DEFIv2.

DEFIv2	Class Group	# Isometry Classes
$m = 16$	1.060	0.430
$m = 28$	11.680	3.220

Table 1. CPU time in seconds for DEFIv2 Decision-LIP

5.2 Search-LIP/Signature Forgery

The authors of [13] claimed 128-bit security for DEFIv2-1 where $m = 28$ (NIST security level 1). They also published a 90-bit challenge DEFIv2-c where $m = 16$. We give a full key recovery attack and signature forgery on the proposed parameters of DEFIv2-c. Forging a signature is equivalent to finding a relatively small solution to a non-homogeneous quadratic Diophantine equation in 4 variables over $\mathbb{Z}[x]/(f)$. The smallness of a signature y is controlled by a bound γ_y on the absolute value of the coefficients of the polynomial y. The bound $\gamma_y = 2^{42}$ was set for DEFIv2-c in [13]; signatures exceeding this bound will be rejected.

We run our Magma code for the first twenty entries of the challenge data DEFIv2-0a and DEFIv2-0b. For each hash h we computed three forged signatures w_0, w_1, w_2. For w_0, we simply took $b = 0$ in eq. (9), while we optimised w_1 and w_2 using the ideas of Sections 4.4.2 and 4.4.3 respectively. Tables 2 and 3 list the bit sizes of the given hash, the authors' signatures, and our three forged signatures[8]. Table 4 shows CPU time to run our Magma codes. Solving the norm equation dominates the runtime.

Hash/Signature	Number of bits																			
Hash h	12	13	13	12	13	12	12	13	12	13	12	13	13	13	13	13	12	13	13	13
DEFIv2-0a signature	41	34	41	37	34	41	39	34	36	41	35	36	42	41	41	39	36	39	38	36
Forged signature w_0	70	70	72	71	72	71	70	71	71	72	69	72	73	73	72	72	70	72	72	70
Forged signature w_1	49	49	49	50	49	48	49	49	49	50	48	49	50	49	50	50	48	49	49	49
Forged signature w_2	36	36	35	36	36	35	36	36	36	36	36	35	36	35	36	35	35	36	35	36

Table 2. Comparison of signature bit sizes for DEFIv2-0a ($m = 16$).

Hash/Signature	Number of bits																			
Hash h	13	11	12	13	12	12	12	12	13	12	13	13	11	13	13	12	12	12	12	11
DEFIv2-0b signature	36	39	42	36	36	39	43	33	39	33	38	36	36	42	38	37	39	43	35	34
Forged signature w_0	61	59	61	62	61	62	62	61	63	62	62	61	60	61	61	63	60	61	62	60
Forged signature w_1	41	39	40	40	41	40	40	40	40	40	40	41	39	41	41	40	40	40	40	39
Forged signature w_2	27	28	28	28	28	27	28	28	27	28	28	28	28	28	28	28	28	28	28	28

Table 3. Comparison of signature bit sizes for DEFIv2-0b ($m = 16$).

[8] The resulting signature sizes vary between different runs. In some cases, it may be necessary to execute the codes 2–3 times to obtain shorter signatures.

Scheme	Total CPU time	Norm equation time
DEFIv2-0a	210.840	200.380
DEFIv2-0b	780.420	455.740

Table 4. CPU time in seconds for DEFIv2-c (m=16).

It is worth noting that we successfully solved the Search-LIP for $m = 28$. The computation required approximately 15 days on a standard PC to find a secret key and produce forged signatures. The corresponding C and T matrices, along with Magma codes, are publicly available at [15].

6 HAWK and Module LIP

One may wonder whether our attack has any impact on the security of HAWK. HAWK is based on a binary *Hermitian* form over the cyclotomic field $\mathbb{Q}(\zeta_{2m}) \cong \mathbb{Q}[x]/(x^m + 1)$ where $m \geq 2$ is a power of 2 [10]. Equivalently, this construction can be viewed as a quaternary quadratic form over the maximal totally real subfield

$$K = \mathbb{Q}(\zeta_{2m} + \zeta_{2m}^{-1}).$$

Let $\bar{}: \mathbb{Q}(\zeta_{2m}) \to \mathbb{Q}(\zeta_{2m})$ denote complex conjugation, i.e. the non-trivial automorphism of $\mathbb{Q}(\zeta_{2m})/K$.

The HAWK lattice $\mathcal{H} = \mathbb{Z}[\zeta_{2m}]^2$ is equipped with the standard Hermitian form

$$\varphi\colon \mathcal{H} \times \mathcal{H} \to \mathbb{Z}[\zeta_{2m}],\ (x, y) \mapsto x^T \overline{y}$$

associated to the Gram matrix $\mathrm{diag}(1, 1)$. We can view $\mathcal{H}$ as a free lattice over $\mathcal{O}_K$ with basis $b = (e_1, \zeta_{2m}e_1, e_2, \zeta_{2m}e_2)$. Its trace form

$$Q\colon \mathcal{H} \to \mathcal{O}_K,\ x \mapsto \varphi(x, x) + \overline{\varphi(x, x)}$$

is a totally positive definite quadratic form over K. The associated Gram matrix of the basis b is given by

$$\begin{pmatrix} 2 & \zeta_{2m} + \zeta_{2m}^{-1} & 0 & 0 \\ \zeta_{2m} + \zeta_{2m}^{-1} & 2 & 0 & 0 \\ 0 & 0 & 2 & \zeta_{2m} + \zeta_{2m}^{-1} \\ 0 & 0 & \zeta_{2m} + \zeta_{2m}^{-1} & 2 \end{pmatrix}.$$

This shows that $(\mathcal{H}, Q)$ is $\mathcal{D}$-modular where $\mathcal{D} = (2 - (\zeta_{2m} + \zeta_{2m}^{-1}))\mathcal{O}_K$ is the prime ideal of $\mathcal{O}_K$ over 2.

A sufficient condition for the spinor genus of a quadratic form (or a lattice) to consist of a single class is that it is indefinite. This is not the case for the HAWK lattice $(\mathcal{H}, Q)$ as the field K is totally real and the above Gram matrix is positive definite at all real places of K.

Let $K^+ = \{a \in K^* \mid \tau(a) > 0 \text{ for all real places } \tau\colon K \to \mathbb{R}\}$ be the set of totally positive elements in K. Then

$$\mathrm{Cl}_+(K) = \mathcal{I}(K)/\{a\mathcal{O}_K : a \in K^+\}$$

is called the *narrow class group* of K.

The class group and its narrow version are connected by the exact sequence

$$\{1\} \to \mathcal{O}_K^*/(\mathcal{O}_K^* \cap K^+) \to K^*/K^+ \to \mathrm{Cl}_+(K) \to \mathrm{Cl}(K) \to \{1\}\,,$$

see for example [23, Proposition VI.1.11] for details.

Let $n = m/2$ be the degree of K. Then $K^*/K^+ \cong (\mathbb{Z}/2\mathbb{Z})^n$ by weak approximation [24, Theorem 11:8]. Weber [30, Theorem B, page 744] shows that for $\mathbb{Q}(\zeta_m)$ where m is a power of 2, the algebraic conjugates of the units in $\mathcal{O}_K^*$ already exhibit all possible signs. Thus $\mathcal{O}_K^*/(\mathcal{O}_K^* \cap K^+) \cong (\mathbb{Z}/2\mathbb{Z})^n$ as well. This shows that $\mathrm{Cl}(K) \cong \mathrm{Cl}_+(K)$.

By the work of Weber [29], the class number of K and thus the order of $\mathrm{Cl}_+(K)$ is known to be odd. Hence, Theorem 7 yields the following (noting that the ray class group becomes the narrow class group):

Lemma 1. *Let $\mathcal{L}$ be a full-rank lattice in a regular quadratic space (V, Q) over K with $\dim_K(V) \geq 3$. If $\mathcal{L}$ is modular, then $\mathrm{gen}(\mathcal{L}) = \mathrm{sgen}(\mathcal{L})$.*

Using the fact that $(\mathcal{H}, Q)$ is modular, we immediately get the following result.

Theorem 11. *The genus of the quadratic HAWK lattice $(\mathcal{H}, Q)$ coincides with its spinor genus.*

Consequently, HAWK exhibits the following diagram

$$\textbf{Genus} = \textbf{Spinor genus} \xrightarrow[\text{HAWK}]{\text{unequal for}} \textbf{Class}$$

which should be interpreted as a strength, namely, one cannot exploit the spinor genus to attack HAWK.

To get an idea of the enormity of the task to attack HAWK, we may want to know the number of isometry classes, denoted by $\eta(\mathcal{H})$, in the genus of a rank-2 Hermitian lattice. It is computationally infeasible to find $\eta(\mathcal{H})$ directly. Instead, we use the mass of a lattice to find a lower bound on $\eta(\mathcal{H})$. We let $E = \mathbb{Q}(\zeta_{2m}) = \mathbb{Q}(\zeta_{2\cdot 2^{k-1}})$, and denote the absolute value of the discriminant of K by d_K. For the Hermitian HAWK lattice [14, Proposition 6.3.6] yields the following bound for the class number

$$\eta(\mathcal{H}, \varphi) \geq \ (4\pi^2)^{-2^{(k-2)}} \cdot (d_K)^{\frac{3}{2}} = (4\pi^2)^{-2^{(k-2)}} \cdot (2^{(2^{k-2}\cdot(k-1)-1)})^{\frac{3}{2}}\,. \tag{12}$$

Viewing $\mathcal{H}$ as a quadratic lattice, one obtains the following inequality by [14, Corollary 6.3.2]

$$\begin{aligned}\eta(\mathcal{H}, Q) &\geq 2 \cdot ((2\pi)^4)^{-2^{k-2}} \cdot (d_K)^3 \cdot (\tfrac{8}{9})^{2^{k-2}} \\ &= 2 \cdot ((2\pi)^4)^{-2^{k-2}} \cdot (2^{(2^{k-2}\cdot(k-1)-1)})^3 \cdot (\tfrac{8}{9})^{2^{k-2}}.\end{aligned} \tag{13}$$

Table 5 shows approximate lower bounds for $\eta(\mathcal{H})$ in powers of 2 for both Hermitian and quadratic cases.

m	k	Hermitian	Quadratic
64	7	$2^{117} \leq \eta(\mathcal{H}, \varphi)$	$2^{229} \leq \eta(\mathcal{H}, Q)$
128	8	$2^{331} \leq \eta(\mathcal{H}, \varphi)$	$2^{652} \leq \eta(\mathcal{H}, Q)$
256	9	$2^{856} \leq \eta(\mathcal{H}, \varphi)$	$2^{1690} \leq \eta(\mathcal{H}, Q)$
512	10	$2^{2097} \leq \eta(\mathcal{H}, \varphi)$	$2^{4151} \leq \eta(\mathcal{H}, Q)$
1024	11	$2^{4963} \leq \eta(\mathcal{H}, \varphi)$	$2^{9840} \leq \eta(\mathcal{H}, Q)$

Table 5. Lower bounds on the isometry class number for the HAWK lattice $\mathcal{H}$ over 2-power cyclotomic fields.

Lemma 1 can be applied to other Hermitian lattices of interest to LIP.

7 Discussion and Open Problems

Our results demonstrate that DEFI-like signature schemes based on indefinite quadratic forms are vulnerable to attacks that exploit genus and spinor genus notions. Security based on the Decision-LIP of indefinite quadratic forms is questionable under certain assumptions described in this paper. Increasing the dimension $\dim_K(V)$ alone may not be sufficient; one must carefully rule out global to local collapses, namely, single class genera, and one should avoid base rings and parameter choices that permit efficient reductions to solvable norm equations. Consequently, to avoid security weaknesses in cryptographic schemes based on LIP, one should use totally positive-definite quadratic forms over totally real number fields (such as HAWK).

Our work leaves a few open questions. First, we have only studied quadratic forms of rank ≥ 3, leaving the rank-2 case largely open (except limited results in [18]). One would consider extending our cryptanalysis to definite and indefinite quadratic forms of rank 2, in particular for number fields where the spinor genus splits to many classes.

Secondly, increasing m may thwart our attacks, which require odd class numbers. We observed that when $m \geq 64$, finding the class group for $K = \mathbb{Q}[x]/(x^m \pm x \pm 1)$ becomes computationally intensive. One could also ask for what values of m their class groups are not trivial.

Lastly, Lemma 1 requires m to be a power of 2 such that the class number of K is odd. We note that this is still the case for the totally real subfield K of many other cyclotomic fields $\mathbb{Q}(\zeta_m)$, especially when m is a prime. An extension of Lemma 1 to such fields would be an interesting problem.

Acknowledgements

The authors would like to thank Greg Martin and Andrew Mendelsohn for helpful discussions. This work was supported in part by the Engineering and Physical Sciences Research Council (EPSRC) [grant number UKRI2768].

References

1. Allombert, B., Pellet-Mary, A., van Woerden, W.: Cryptanalysis of rank-2 module-LIP: A single real embedding is all it takes. In: Fehr, S., Fouque, P.A. (eds.) Advances in Cryptology – EUROCRYPT 2025. LNCS, vol. 15602, pp. 184–212. Springer Nature Switzerland, Cham (2025). https://doi.org/10.1007/978-3-031-91124-8_7
2. Bambury, H., Nguyen, P.Q.: Cryptanalysis of an efficient signature based on isotropic quadratic forms. In: International Conference on Post-Quantum Cryptography. pp. 153–175. Springer (2025)
3. Biasse, J.F., Song, F.: Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. In: Proceedings of the twenty-seventh annual ACM-SIAM symposium on Discrete algorithms. pp. 893–902. SIAM (2016)
4. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symbolic Comput. **24**(3-4), 235–265 (1997), computational algebra and number theory (London, 1993)
5. Boyd, D.W., Martin, G., Thom, M.: Squarefree values of trinomial discriminants. LMS Journal of Computation and Mathematics **18**(1), 148–169 (2015)
6. Cassels, J.W.S.: Rational quadratic forms. Courier Dover Publications (2008)
7. Chevignard, C., Mureau, G., Espitau, T., Pellet-Mary, A., Pliatsok, H., Wallet, A.: A reduction from HAWK to the principal ideal problem in a quaternion algebra. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 154–183. Springer (2025)
8. Cohen, H.: A course in computational algebraic number theory, vol. 138. Springer Science & Business Media (2013)
9. Conway, J.H., Sloane, N.J.A.: Sphere packings, lattices and groups, vol. 290. Springer Science & Business Media (2013)
10. Ducas, L., Postlethwaite, E.W., Pulles, L.N., van Woerden, W.: HAWK: Module LIP makes lattice signatures fast, compact and simple. In: Agrawal, S., Lin, D. (eds.) Advances in Cryptology – ASIACRYPT 2022. LNCS, vol. 13794, pp. 65–94. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-22972-5_3
11. Ducas, L., van Woerden, W.P.J.: On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography. In: Advances in Cryptology – EUROCRYPT 2022. LNCS, vol. 13277, pp. 643–673. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-07082-2_23, full version: Cryptology ePrint Archive, Paper 2021/1332
12. Eichler, M.: Quadratische Formen und orthogonale Gruppen, vol. 63. Springer-Verlag (2013)
13. Feussner, M., Semaev, I.: Isotropic quadratic forms, diophantine equations and digital signatures, defiv2. In: International Workshop on Lightweight Cryptography for Security and Privacy. pp. 23–38. Springer (2025)

14. Kirschmer, M.: Definite quadratic and hermitian forms with small class number. Habilitation thesis, RWTH Aachen University (2016)
15. Kirschmer, M., Ling, C., Sadreddin, A.: Magma code for "cryptanalysis of DEFIv2". https://github.com/defiv2magmacodes/defiv2codes (2026)
16. Kitaoka, Y.: Arithmetic of quadratic forms, vol. 106. Cambridge University Press (1999)
17. Kneser, M.: Klassenzahlen indefiniter quadratischer formen in drei oder mehr veränderlichen. Archiv der Mathematik **7**(5), 323–332 (1956)
18. Ling, C., Liu, J., Mendelsohn, A.: On the spinor genus and the distinguishing lattice isomorphism problem. In: Chung, K.M., Sasaki, Y. (eds.) Advances in Cryptology – ASIACRYPT 2024. LNCS, vol. 15487, pp. 329–358. Springer, Singapore (2025). https://doi.org/10.1007/978-981-96-0894-2_11
19. Luo, H., Jiang, K., Pan, Y., Wang, A.: Cryptanalysis of rank-2 module-LIP with symplectic automorphisms. In: Chung, K.M., Sasaki, Y. (eds.) Advances in Cryptology – ASIACRYPT 2024. LNCS, vol. 15487, pp. 359–385. Springer, Singapore (2025). https://doi.org/10.1007/978-981-96-0894-2_12, full version: Cryptology ePrint Archive, Paper 2024/1173
20. Mureau, G., Pellet-Mary, A., Pliatsok, G., Wallet, A.: Cryptanalysis of rank-2 module-LIP in totally real number fields. In: Joye, M., Leander, G. (eds.) EUROCRYPT 2024. LNCS, vol. 14657, pp. 226–255. Springer Nature Switzerland (2024). https://doi.org/10.1007/978-3-031-58754-2_9
21. Mureau, G.: Special genera of hermitian lattices and applications to HAWK. In: Theory of Cryptography Conference. pp. 289–317. Springer (2025)
22. Nart, E., Vila, N.: Equations of the type $x^n + ax + b$ with absolute Galois group S_n. Revista de la universidad **2**, 821–825 (1979)
23. Neukirch, J.: Algebraic number theory. Springer (1999)
24. O'Meara, O.T.: Introduction to quadratic forms. Springer Science & Business Media (1999)
25. Selmer, E.S.: On the irreducibility of certain trinomials. Mathematica Scandinavica pp. 287–302 (1956)
26. The OEIS Foundation Inc.: A061653. https://oeis.org/A061653 (2026), the On-Line Encyclopedia of Integer Sequences, accessed 2026-05-14
27. Vinberg, È.B.: On groups of unit elements of certain quadratic forms. Sbornik: Mathematics **16**(1), 17–35 (1972)
28. Voight, J.: Identifying the matrix ring: Algorithms for quaternion algebras and quadratic forms. In: Alladi, K., Bhargava, M., Savitt, D., Tiep, P.H. (eds.) Quadratic and Higher Degree Forms, pp. 255–298. Springer New York (2013)
29. Weber, H.: Theorie der Abel'schen Zahlkörper. Acta Mathematica **8**(1), 193–263 (1886)
30. Weber, H.: Lehrbuch der Algebra, vol. 2. Vieweg (1896)
31. Zhou, W., Labahn, G., Storjohann, A.: A deterministic algorithm for inverting a polynomial matrix. Journal of Complexity **31**, 162–173 (2015)

Appendix A: Quadratic Defect Algorithm

Algorithm 7 QuadraticDefect(a)

Input: Some element $a \in K_{\mathfrak{p}}$.
Output: The valuation of the quadratic defect of a.

1: **if** $a = 0$ or $\mathrm{ord}_{\mathfrak{p}}(a)$ is odd **then return** $\mathrm{ord}_{\mathfrak{p}}(a)$.
2: **if** $\mathrm{ord}_{\mathfrak{p}}(a) \neq 0$ **then return** $\mathrm{ord}_{\mathfrak{p}}(a) + \text{QuadraticDefect}(a/\pi^{\mathrm{ord}_{\mathfrak{p}}(a)})$.
3: Compute $s \in \mathcal{O}_K^*$ such that $s^2 a \equiv 1 \pmod{\mathfrak{p}}$. Replace a by as^2.
4: Set $v = \mathrm{ord}(a-1) \geq 1$.
5: **while** $v < \mathrm{ord}(4)$ and v is even **do**
6: Compute $s \in \mathcal{O}_K^*$ such that $s^2 \equiv (a-1)/p^v \pmod{\mathfrak{p}}$.
7: Replace a by $a/(1+sp^{v/2})^2$ and set $v = \mathrm{ord}(a-1)$.
8: **end while**
9: **if** $v < 2e$ is odd **then**
10: **return** v.
11: **else if** $v = \mathrm{ord}(4)$ and $x^2 + x + (a-1)/4 \in (\mathcal{O}_{K\mathfrak{p}}/\mathfrak{p})[x]$ is irreducible **then**
12: **return** $2e$.
13: **else**
14: **return** ∞.
15: **end if**

Remark 6. For a proof of the correctness of Algorithm 7 see [14, Algorithm 3.1.3]. We also note in line 11 we have to check if a quadratic polynomial $f := x^2+x+c \in \mathbb{F}_\ell[x]$ is reducible. If $f(a) = 0$, then $(x-a)$ divides both f and $(x^\ell - x)$ and thus $\gcd(f, x^\ell - x) \neq 1$. This can be tested in polynomial time. By Eq. (2), it suffices to check if $\mathfrak{d}(a) \leq 2e$. Hence, all computation in Algorithm 7 after the first two lines can be done modulo $4\mathfrak{p}$. This way, we prevent the coefficients of a from growing excessively. In particular, the quadratic defect $\mathfrak{d}(a)$ can be computed in polynomial time.

Appendix B: DEFIv2 Signature Scheme

Let $K = \mathbb{Q}[x]/(x^m + x + 1)$ with $m \in \{16, 28\}$.

Private Key: Let $n = r + s$. The private key of DEFI is a matrix $B \in \mathcal{O}_K^{n \times n}$ with blocks

$$\begin{pmatrix} B_{11} & 0 \\ B_{21} & B_{22} \end{pmatrix}$$

where $B_{11} \in \mathrm{GL}_r(\mathcal{O}_K)$, $B_{21} \in \mathcal{O}_K^{s \times r}$ and $B_{22} \in \mathrm{GL}_s(\mathcal{O}_K)$,

Public Key: Let $J = \mathrm{diag}(\pm 1, \pm 1, \cdots, \pm 1, \pm 1) \in \mathcal{O}_K^{n \times n}$. The public Key is the matrix $C = B^T J B$, that determines quadratic form

$$Q(x) = Q(x_1, ..., x_n) = (Bx)^T J (Bx) = x^T C x. \tag{14}$$

Signature Generation:

1. Given a message M, compute its hash $h \in \mathcal{O}_K^{r\times 1}$.
2. Set $Z' = B_{11}h \in \mathcal{O}_K^{r\times 1}$. Generate a random $Z'' \in \mathcal{O}_K^{s\times 1}$ such that $Z^T JZ = 0$ with $Z = \binom{Z'}{Z''}$.
3. Find the signature $y \in \mathcal{O}_K^{s\times 1}$ through $y = B_{22}^{-1}(Z'' - B_{21}h)$.

Signature Verification: Let (M, y) be a signed message.

1. If $y \notin \mathcal{O}_K^{s\times 1}$, then reject. Otherwise, compute $h \in \mathcal{O}_K^{r\times 1}$.
2. Let $z = \binom{h}{y} \in \mathcal{O}_K^{n\times 1}$. If $Q(z) = z^T Cz = 0$, accept the signature, otherwise reject.

Verification Proof: Let (M, y) be a correct signature. For $z = \binom{h}{y}$, one has

$$B_{21}h + B_{22}y = Z''.$$

Then

$$Bz = \begin{pmatrix} B_{11} & 0 \\ B_{21} & B_{22} \end{pmatrix} \begin{pmatrix} h \\ y \end{pmatrix} = \begin{pmatrix} Z' \\ Z'' \end{pmatrix} = Z$$

$$Q(z) = z^T Cz = z^T (B^T JB)z = (Bz)^T J(Bz) = Z^T JZ = 0.$$