DIMENSION REDUCTION FOR SVP IN HAWK: A TRACE-ZERO APPROACH

GUILHEM MUREAU AND ALICE PELLET-MARY

Abstract. Let $E = \mathbb{Q}(\zeta_m)$ be a power-of-two cyclotomic field, with maximal totally real subfield $K = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$. In previous work, Chevignard et al. (Eurocrypt'25) gave a reduction from module-LIP for rank-two module lattices over $\mathcal{O}_E$ to the norm-reduced Principal Ideal Problem (nrdPIP) in a quaternion algebra. We derive two consequences of this reduction. First, we obtain a polynomial time reduction from rank-2 module-LIP over $\mathcal{O}_E$ to rank-3 module-LIP over $\mathcal{O}_K$. Note that rank-2 modules over $\mathcal{O}_E$ are naturally seen as rank-4 modules over $\mathcal{O}_K$, so this is indeed an improvement. Our second result is specific to the module $\mathcal{O}_E^2$, underlying the Hawk signature scheme. In this setting, we also obtain a reduction to a rank-3 module-LIP instance over $\mathcal{O}_K$, but we can additionally show that these modules have a simple geometric shape: they are isomorphic to $\mathbb{Z}^{m/2+1} \perp \sqrt{2}\,\mathbb{Z}^{m/4-1}$. We then adapt Ducas' result (ePrint'23) to this setting. Putting everything together we obtain an algorithm breaking Hawk's key recovery by making polynomially many exact-SVP calls in lattices of dimension at most $3m/8 + 1$. This improves upon the previous analysis from Ducas (ePrint'23) which required exact-SVP calls in lattices of dimension at most $m/2 + 1$.

1. Introduction

Two lattices are said to be isomorphic if there exists a linear isometry sending one lattice onto the other. The *Lattice Isomorphism Problem* (LIP) then asks, given as input two isomorphic lattices, to recover such an isometry. While this problem has been studied by mathematicians for a few decades [24, 14, 11] or as a tool for cryptanalysis [26], its introduction as a hard algorithmic problem used to build cryptographic primitives is quite recent [9, 2].

Soon after its introduction, a module variant of the problem was also introduced, relying on algebraically structured lattices. This variant allows the construction of more efficient primitives, and is in particular used in the signature scheme Hawk [8], which was submitted to the NIST's second call for post-quantum signatures.[1]

The introduction of LIP for constructive cryptography and the signature scheme Hawk motivated a large number of cryptanalytic works, focusing on the hardness of the lattice isomorphism problem at large [6, 7, 31, 28], on its module variant [23, 3, 19, 1, 4, 22, 15], or on the specific module variant used in Hawk [13, 30, 29]. So far, even though the rank-2 module-LIP problem has been proven to be solvable in polynomial time in many number fields (e.g., totally real fields [23], or even fields with at least one real embedding [1]), these attacks do not apply to the number fields underlying the Hawk signature scheme, namely the power-of-two cyclotomic fields.

Date: July 30, 2026.

[1] https://hawk-sign.info

Let $E = \mathbb{Q}(\zeta_m)$ be a power-of-two cyclotomic field of conductor m, and let $\mathcal{O}_E$ be its ring of integers. Note that with this notation, the degree of E over $\mathbb{Q}$ is $m/2$. The security of Hawk against key recovery attacks is strongly related to the hardness of solving module-LIP for $\mathcal{O}_E$-modules of rank 2 that are isomorphic to the specific module lattice $\mathcal{O}_E^2$.[2] The best known attack consists in forgetting about the module structure of the lattice, and solving the associated plain lattice isomorphism problem over $\mathbb{Z}$. Since $\mathcal{O}_E^2$ is isomorphic (as a $\mathbb{Z}$-lattice) to $\mathbb{Z}^m$, this means that the best key recovery attack against Hawk requires to solve the LIP problem for a lattice isomorphic to $\mathbb{Z}^m$. Exploiting the very special structure of $\mathbb{Z}^m$, in particular its orthogonal basis, Ducas [6] proved that there exists an algorithm solving LIP for lattices isomorphic to $\mathbb{Z}^m$ by making polynomially many calls to an exact-SVP oracle in lattices of dimension at most $m/2+1$. In practice, the best heuristic algorithm seems to require running BKZ with blocksize roughly $m/2 - 36.7$: see Table 1 of Hawk's specification document[3].

1.1. **Our results.** In this article, we prove that there exists a polynomial time reduction from solving Hawk's key recovery problem to solving the LIP problem in a lattice of rank $3m/4$ that is isomorphic to $\mathbb{Z}^{m/2+1} \perp \sqrt{2}\,\mathbb{Z}^{m/4-1}$ (see Theorem 4.1). We also adapt the algorithm from Ducas [6] to this setting, and we conclude that it is possible to break key recovery for Hawk by making polynomially many calls to an exact-SVP oracle in lattices of dimension at most $3m/8 + 1$ (see Corollary 5.5).

Our algorithm for Hawk is actually a specialization (and a simplification) of a more general algorithm solving module-LIP in arbitrary modules of rank-2 in E^2 (where E is a power-of-two cyclotomic field). Under Weber's conjecture, which states that the maximal totally real subfield K of E has class number 1, this algorithm reduces in polynomial time a module-LIP instance in a module of rank-2 over E into at most two module-LIP instances in rank-3 modules over K, where $K = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ is the maximal totally real subfield of E (see Theorem 3.1). Note that since E has dimension 2 over K, any rank-2 module over E can be seen as a rank-4 module over K. Hence our reduction reduces the K-rank of the module-LIP instance from 4 to 3. If we ignore the module structure, this means that we reduce a LIP problem in a lattice of rank m into at most two LIP instances in lattices of rank $3m/2$.

1.2. **Technical overview.** Our attack builds on the reduction from module-LIP to nrd-PIP that was proven in [4]. Let us first fix some notations and recall the main result of this article. As above, let $E = \mathbb{Q}(\zeta_m)$ be a power-of-two cyclotomic field of conductor m and let $K = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ be its maximal totally real subfield. Let $\mathcal{O}_E$ and $\mathcal{O}_K$ be their respective ring of integers. Note that E is isomorphic to $K \oplus Ki$ where $i = \zeta_m^{m/4}$ is a square root of -1 in E. We define the quaternion algebra $\mathcal{A} = K \oplus Ki \oplus Kj \oplus Kij = E \oplus Ej$ where $i^2 = j^2 = -1$ and $ij = -ji$. At a high level, the quaternion algebra behaves like some generalization of the cyclotomic field E, except that it is non-commutative. This non-commutativity is frequently the source of troubles.

Let $x = x_0 + x_1 i + x_2 j + x_3 ij \in \mathcal{A}$ with the x_i's in K. The reduced norm of x is defined as $\mathrm{Nrd}(x) = x_0^2 + x_1^2 + x_2^2 + x_3^2 \in K$. This is the analogue for $x \in \mathcal{A}$ of the relative algebraic norm $\mathrm{N}_{E/K}(x) = x_0^2 + x_1^2$ for $x = x_0 + x_1 i \in E$. The reduced norm is used to

[2] Depending on the security level required, the conductor m varies in $\{512, 1024, 2048\}$.

[3] https://hawk-sign.info/

define a geometry on $\mathcal{A}$: for $x \in \mathcal{A}$, we define $\|x\|^2 = \mathrm{Tr}_{K/\mathbb{Q}}(\mathrm{Nrd}(x))$. In particular, two elements of $\mathcal{A}$ with the same reduced norm have the same Euclidean norm.

An order $\mathcal{O}$ in $\mathcal{A}$ is a full rank sub-$\mathcal{O}_K$-module of $\mathcal{A}$ which is also a (non-commutative) ring containing 1. An important order for us will be the so-called natural order of $\mathcal{A}$, which is $\mathcal{O}_{\mathrm{nat}} = \mathcal{O}_E \oplus \mathcal{O}_E j$. Note that any order $\mathcal{O}$ in $\mathcal{A}$ contains $\mathcal{O}_K$, since it contains 1 and is stable by multiplication by $\mathcal{O}_K$.

1.2.1. *The main result of* [4]. Let $\mathcal{O}$ be an order in $\mathcal{A}$. The norm-reduced Principal Ideal Problem with parameter $\mathcal{O}$, denoted by $\mathcal{O}$-nrdPIP, is defined as follows. Let $\alpha \in \mathcal{O}$ be some secret element, let $I = \alpha\mathcal{O}$ be the (right) $\mathcal{O}$-ideal generated by α, and let $q = \mathrm{Nrd}(\alpha)$. Given I and q, the problem asks to recover α (or an equivalent solution). The analogue over cyclotomic fields (i.e., when $\mathcal{A}$ is replaced by E) is a well studied problem for which Gentry and Szydlo provided a polynomial time algorithm [12]. Over a quaternion algebra $\mathcal{A}$ however, the best known algorithm requires to solve the shortest vector problem (SVP) in a lattice of rank m, which takes exponential time.

The main result of [4] says that in order to solve module-LIP for module lattices of rank 2 over $\mathcal{O}_E$, it is sufficient to be able to solve $\mathcal{O}$-nrdPIP, for a specific order $\mathcal{O}$ that depends on the isometry class of the input modules. In the particular case of Hawk, solving module-LIP for module lattices isomorphic to $\mathcal{O}_E^2$ reduces to solving $\mathcal{O}_{\mathrm{nat}}$-nrdPIP.[4]

1.2.2. *Getting a rank-*3 *module over* $\mathcal{O}_K$. Our starting point is an instance of $\mathcal{O}$-nrdPIP produced by the reduction of [4]: given an ideal $I = \alpha\mathcal{O}$ (represented, e.g., by a $\mathbb{Z}$-basis) and $q = \mathrm{Nrd}(\alpha) \in K$, we seek to recover $\alpha \in \mathcal{O}$, up to multiplication by a unit of $\mathcal{O}^\times$ of reduced norm 1. The first step of our reduction uses the basis of I to build the set $\Lambda = \alpha\mathcal{O}\alpha^{-1}$. This is another order of $\mathcal{A}$, which can be computed efficiently from I using linear algebra. It is the so-called left-order of I.

Let c_α be the (secret) map on $\mathcal{A}$ defined by $c_\alpha(x) = \alpha x \alpha^{-1}$ for $x \in \mathcal{A}$. This map is K-linear, since K commutes with any element of $\mathcal{A}$, and it preserves the reduced norm: $\mathrm{Nrd}(c_\alpha(x)) = \mathrm{Nrd}(\alpha)\,\mathrm{Nrd}(x)\,\mathrm{Nrd}(\alpha)^{-1} = \mathrm{Nrd}(x)$. In particular, it defines a K-linear isometry of the quadratic space $(\mathcal{A}, \mathrm{Nrd})$. Moreover, it follows from the definition of Λ that c_α maps $\mathcal{O}$ onto Λ.

Summing up, $\mathcal{O}$ and Λ are efficiently computable $\mathcal{O}_K$-modules (they are orders in $\mathcal{A}$), and c_α defines an isomorphism between them, that is, c_α is a K-linear isometry mapping $\mathcal{O}$ onto Λ. Thus, this defines an instance of module-LIP between rank-4 $\mathcal{O}_K$-module lattices. Moreover, if one is able to compute the map c_α, then α can be recovered in polynomial time (up to multiplication by a unit of $\mathcal{O}$ of reduced norm 1, which is fine for solving $\mathcal{O}$-nrdPIP). The map c_α is not the unique isometry sending $\mathcal{O}$ to Λ, so in order to recover c_α (or an equivalent map), we need to work a little bit more.

To reduce to an instance of module-LIP between rank-3 $\mathcal{O}_K$-module lattices, we make the following key observation: $c_\alpha(1) = \alpha \cdot 1 \cdot \alpha^{-1} = 1$. More generally, for any $x \in K$, we have $c_\alpha(x) = \alpha x \alpha^{-1} = x\alpha\alpha^{-1} = x$ since the elements of K commute with any element of $\mathcal{A}$. Recall that since $\mathcal{O}$ and Λ are orders, and that they both contain $\mathcal{O}_K$ as a rank-1 submodule. This means that we can efficiently identify a rank-1 submodule of both $\mathcal{O}$ and Λ on which we know how c_α behaves. This allows us to reduce the rank of our

[4]The initial result of [4] actually only proved that solving nrdPIP in a maximal order $\mathcal{O}$ containing $\mathcal{O}_{\mathrm{nat}}$ was sufficient to break Hawk, but their result can be adapted to the order $\mathcal{O}_{\mathrm{nat}}$ itself, and we formally prove it in Section 4.

module-LIP instance by one: either by projecting $\mathcal{O}$ and Λ orthogonally to $\mathcal{O}_K$, or by intersecting them with the vector subspace of $\mathcal{A}$ orthogonal to $\mathcal{O}_K$. We opted for the second option, since it made the resulting rank-3 modules easier to describe.

We then define the 3-dimensional K-vector space $\mathcal{A}^0 = \{x_1 i + x_2 j + x_3 ij \,|\, x_1, x_2, x_3 \in K\}$, which contains precisely the elements of $\mathcal{A}$ that are orthogonal to K.[5] Intersecting $\mathcal{O}$ and Λ with $\mathcal{A}^0$ gives us two rank-three $\mathcal{O}_K$-modules $\mathcal{O}^0$ and Λ^0, and the secret isometry c_α maps bijectively $\mathcal{O}^0$ onto Λ^0. We then proceed to solve the module-LIP problem between these two rank-3 $\mathcal{O}_K$-modules. A naive approach would require to enumerate all the $\mathcal{O}_K$-isometries between $\mathcal{O}^0$ and Λ^0 until recovering the one corresponding to c_α. We show that this is not necessary, and that a single arbitrary $\mathcal{O}_K$-isometry sending $\mathcal{O}^0$ to Λ^0 suffices to recover α in polynomial time (using the knowledge of $q = \mathrm{Nrd}(\alpha)$).

1.2.3. *Finishing the attack.* At this point, the techniques start diverging between the general case of rank-2 $\mathcal{O}_E$-modules and the special case of module-LIP inderlying Hawk, where the modules are isomorphic to $\mathcal{O}_E^2$. In the general case, the order $\mathcal{O}$ produced by the reduction [4] is a maximal order of $\mathcal{A}$. Using the properties of maximal orders and technical results, we show that the recovered isometry is of the form c_b for some $b = \alpha x u$ where $x \in K$ and $u \in \mathcal{O}^\times$ is a unit. Moreover, we can recover b from c_b by linear algebra. Then, using the knowledge of $q = \mathrm{Nrd}(\alpha)$, we can get rid of x and transform u into a unit of reduced norm 1. This allows us to finally recover $\alpha u'$ with $u' \in \mathcal{O}^\times$ a unit of norm 1, which is a solution to the $\mathcal{O}$-nrdPIP instance.

In Hawk's case, the order we consider is $\mathcal{O}_{\mathrm{nat}}$, which is not maximal, so the results from the general case do not apply directly here. The reason why we chose to work with $\mathcal{O}_{\mathrm{nat}}$ instead of a maximal order containing $\mathcal{O}_{\mathrm{nat}}$ is that its trace-zero restriction $\mathcal{O}_{\mathrm{nat}}^0$ has nice geometric properties. Namely, it is isomorphic as a Euclidean lattice to $\mathbb{Z}^{m/2+1} \perp \sqrt{2}\,\mathbb{Z}^{m/4-1}$. This makes our rank-3 module-LIP instance over $\mathcal{O}_K$ easier to solve, using a slight variant of Ducas' algorithm for $\mathbb{Z}^n$ [6]. Since $\mathcal{O}_{\mathrm{nat}}$ is not maximal, the previous techniques do not apply anymore, and we need a different approach than before to recover α from a K-isometry between $\mathcal{O}_{\mathrm{nat}}^0$ and Λ^0. Here, we use the fact that $\mathcal{O}_{\mathrm{nat}}^0$ contains a special element i whose image by c_α can easily be identified in Λ^0 once the shortest vectors of Λ^0 are known. It is the case if we know an arbitrary isometry between $\mathcal{O}_{\mathrm{nat}}^0$ and Λ^0. We then use the knowledge of the pair $(i, c_\alpha(i))$ to derive a linear equation satisfied by α, and thus recover αx for some $x \in E$. Finally, we remove the element x by running the Gentry–Szydlo algorithm in E.

1.2.4. *Implementation.* We implemented part of our attack in SageMath [27]. We only considered the special case of Hawk (i.e., modules isomorphic to $\mathcal{O}_E^2$), and focused on the last part of the attack, namely recovering the secret element α when given a $\mathbb{Z}$-basis of the order $\Lambda = \alpha \mathcal{O}_{\mathrm{nat}} \alpha^{-1}$ and the reduced norm $q = \mathrm{Nrd}(\alpha)$. Our implementation follows the strategy described above with some small changes that we introduced to improve the computation time. In particular, we manage to avoid the call to the Gentry–Szydlo algorithm, see Section 6 for more details. We were able to run our attack successfully up to conductor $m = 128$, and we also managed to recover α for some tests in conductor $m = 256$ (when we did not succeed, this is not because the algorithm was incorrect, but instead because we did not have enough computational power to run the lattice reduction

[5] These set is called the *trace zero* subspace of $\mathcal{A}$, hence the title of this article.

algorithm on the lattice Λ^0). Our code is available at https://plmlab.math.cnrs.fr/apelletm/attack_hawk-trace-zero.

1.3. **Concurrent works.** At the time of writing, two concurrent works have been announced on the NIST pqc-forum [25, 18].[6] The first work [25] reduces HAWK's key recovery to SVP in lattices of dimension $m/4+1$. The second one [18] proposes an attack on HAWK by solving SVP in lattices of dimension $3m/8+1$. This second attack performs similar to our attack, whereas the first one performs better.

These attacks seem to use different tools than our attack, but we cannot say at the moment whether they rely on similar ideas phrased differently or whether they are really different (and may possibly be combined). It is quite striking that all three attacks end up with lattices isomorphic to $\mathbb{Z}^a \perp \sqrt{2}\,\mathbb{Z}^b$ for some integers a and b (and with an additional copy of $2\mathbb{Z}$ in the case of [18]), this probably indicates hidden similarities between all these attacks. We note that the two attacks [25, 18] target specifically HAWK's module $\mathcal{O}_E^2$ whereas our attack can be extended to any rank-2 module of E (at the cost of loosing the nice orthogonal property of the underlying lattice that allows to halve the SVP dimension).

2. Preliminaries

This section contains the number theoretic material needed to prove our reductions. Regarding number fields, and since we restrict ourselves to the cyclotomic case, the book of Washington [33] is a useful reference. For quaternion algebras, a standard reference is the book of Voight [32]. In Section 2.3, we give a general definition of module-LIP and we recall the reduction from Chevignard et al [4], which is our starting point.

2.1. **Number fields.** Throughout the paper, $m = 2^r$ denotes a power of two, with $r \geq 3$, and ζ_m denotes a primitive m-th root of unity. We consider the cyclotomic field $E = \mathbb{Q}(\zeta_m) \simeq \mathbb{Q}[X]/(X^{m/2}+1)$ and its maximal totally real subfield $K = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$. We set $d = [K:\mathbb{Q}] = m/4$, so that $[E:\mathbb{Q}] = 2d$.

2.1.1. *Generalities.* The extension E/K is quadratic. More precisely, $i := \zeta_m^d$ satisfies $i^2 = -1$, and $E = K(i) \simeq K[X]/(X^2+1)$. Thus, every $z \in E$ can be written uniquely as $z = x + iy$, with $x, y \in K$. The non-trivial element of $\mathrm{Gal}(E/K)$ is defined by

$$\begin{aligned} \overline{\cdot} \;:\; E &\longrightarrow E \\ x + iy &\longmapsto x - iy \end{aligned}$$

and called *complex conjugation*. Since K is totally real and E is totally imaginary, E/K is a CM extension. In particular, it belongs to the setting considered in [4]. For $z = x + iy \in E$, the relative trace and norm on E/K are

$$\mathrm{Tr}_{E/K}(z) = z + \overline{z} = 2x \qquad \text{and} \qquad \mathrm{N}_{E/K}(z) = z\overline{z} = x^2 + y^2.$$

Note that $z \in K$ if and only if $\mathrm{Tr}_{E/K}(z) = 2z$, while $\mathrm{Tr}_{E/K}(z) = 0$ if and only if $z \in Ki$. For a fractional ideal $\mathfrak{a}$ of E, we denote by $\mathrm{N}_{E/K}(\mathfrak{a})$ its relative ideal norm, which is a fractional ideal of K.

The rings of integers of E and K are denoted by $\mathcal{O}_E$ and $\mathcal{O}_K$, respectively. In our setting, we have $\mathcal{O}_E = \mathbb{Z}[\zeta_m]$ and $\mathcal{O}_K = \mathbb{Z}[\zeta_m + \zeta_m^{-1}]$; see [33]. The ideal class group of

[6] https://groups.google.com/a/list.nist.gov/g/pqc-forum

K is denoted by $\mathrm{Cl}(K)$ and its cardinality is the class number h_K. Here and throughout, the class group means the ordinary ideal class group, rather than the narrow class group. The results proved in Section 3 are conditional on the following classical conjecture.

Conjecture 2.1 (Weber, 1886)**.** *With the notation above, one has $h_K = 1$.*

A recent preprint proves the conjecture unconditionally for $m \leq 4096$; see [20].

2.1.2. *Module lattices.* For the general theory of modules over a Dedekind domain, we refer to the first chapter of [5]. Let V be a finite-dimensional vector space over E. We call $\mathcal{O}_E$-lattice in V any set of the form $\mathcal{L} = \mathfrak{a}_1\mathbf{b}_1 + \cdots + \mathfrak{a}_\ell\mathbf{b}_\ell$, where $\mathfrak{a}_1, \ldots, \mathfrak{a}_\ell$ are fractional ideal of E, and $\mathbf{b}_1, \ldots, \mathbf{b}_\ell \in V$ are E-linearly independent vectors. The data of $\mathbf{B} = (B, \{\mathfrak{a}_i\}_{1\leq i\leq \ell})$, where $B = (\mathbf{b}_1|\ldots|\mathbf{b})$, is called a pseudo-basis of $\mathcal{L}$.

Two pseudo-bases $\mathbf{B} = (B, \{\mathfrak{a}_i\}_{1\leq i\leq \ell})$ and $\mathbf{C} = (C, \{\mathfrak{b}_i\}_{1\leq i\leq \ell})$ represent the same $\mathcal{O}_E$-lattice $\mathcal{L}$ if and only if there exists $U = (u_{i,j})_{1\leq i,j\leq \ell} \in \mathbf{GL}_\ell(E)$ such that the following conditions are satisfied:

(1) $C = BU$;
(2) $u_{i,j} \in \mathfrak{a}_i\mathfrak{b}_j^{-1}$ for all $1 \leq i, j \leq \ell$;
(3) $\prod_{i=1}^{\ell} \mathfrak{a}_i = (\det U) \prod_{i=1}^{\ell} \mathfrak{b}_i$.

Throughout this paper, a module lattice in E^ℓ will refer to an $\mathcal{O}_E$-lattice in E^ℓ, endowed with the norm $\|\mathbf{v}\|^2 := \sum_{i=1}^{\ell} \mathrm{Tr}_{K/\mathbb{Q}}(\mathrm{N}_{E/K}(v_i))$, for any $\mathbf{v} = (v_i)_i \in E^\ell$, and where $\mathrm{Tr}_{K/\mathbb{Q}}$ denotes the absolute trace on K. In particular, a module lattice in E^ℓ can always be seen as a Euclidean lattice in $\mathbb{R}^{2d\ell}$. Two module lattices $\mathcal{L}$ and $\mathcal{M}$ in E^ℓ are called *isomorphic* if there exists a E-linear map $\Theta \in \mathbf{GL}_\ell(E)$ such that

$$\mathcal{M} = \Theta \cdot \mathcal{L} := \{\Theta \cdot \mathbf{v} \,|\, \mathbf{v} \in \mathcal{L}\},$$

and $\Theta^*\Theta = \mathrm{I}_\ell$, where $\Theta^* = \overline{\Theta^T}$ is the transpose-conjugate of Θ.

The corresponding notions for $\mathcal{O}_K$-lattices and module lattices in K^ℓ are defined analogously. By restriction of scalars, an $\mathcal{O}_E$-lattice of rank ℓ is an $\mathcal{O}_K$-lattice of rank 2ℓ. Indeed, under the decomposition $E = K \oplus Ki$ we identify E^ℓ with $K^{2\ell}$ through

$$(x_1 + iy_1, \ldots, x_\ell + iy_\ell) \longmapsto (x_1, y_1, \ldots, x_\ell, y_\ell).$$

Moreover, this identification preserves the preceding norm defined previously.

2.1.3. *Completions.* Throughout this paper, prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ are understood to be non-zero. We denote by $v_\mathfrak{p}$ the normalized valuation associated with $\mathfrak{p}$, and we let $K_\mathfrak{p}$ be the completion of K with respect to $v_\mathfrak{p}$. Moreover, $\mathcal{O}_{K_\mathfrak{p}}$ denotes its valuation ring, and we also set $V_\mathfrak{p} := V \otimes_K K_\mathfrak{p}$ for every finite-dimensional K-vector space V. For an $\mathcal{O}_K$-lattice $\mathcal{L}$ in V, we also set $\mathcal{L}_\mathfrak{p} := \mathcal{L} \otimes_{\mathcal{O}_K} \mathcal{O}_{K_\mathfrak{p}}$.

We will use the local–global dictionary for lattices [32, Theorem 9.4.9]: If $\mathcal{L}$ and $\mathcal{M}$ are $\mathcal{O}_K$-lattices in the same K-vector space, then $\mathcal{M} = \mathcal{L}$ if and only if $\mathcal{M}_\mathfrak{p} = \mathcal{L}_\mathfrak{p}$ for every prime ideal $\mathfrak{p}$. Equivalently, after identifying V with its image in each $V_\mathfrak{p}$,

$$\mathcal{M} = \{x \in V \,|\, x \in \mathcal{M}_\mathfrak{p} \text{ for every prime ideal } \mathfrak{p}\}.$$

2.2. **Quaternion algebra.** Throughout this paper, we fix the quaternion algebra

$$\mathcal{A} := \left(\frac{E, -1}{K}\right),$$

it is a K-vector space of dimension four, with basis $\{1, i, j, ij\}$ satisfying

$$i^2 = j^2 = -1 \qquad \text{and} \quad ij = -ji.$$

In particular, $\mathcal{A}$ is a non-commutative algebra over its center K, and it contains E as a maximal commutative subfield. Alternatively, one has the decomposition

$$\mathcal{A} = E \oplus Ej, \tag{1}$$

with the rules $j^2 = -1$ and $jz = \overline{z}j$, for all $z \in E$.

We let $\psi : \mathcal{A} \to K^4$ be the map sending $x = x_0 + x_1 i + x_2 j + x_3 ij \in \mathcal{A}$ to the coordinate vector $(x_0, x_1, x_2, x_3) \in K^4$. The complex conjugation on $\mathcal{A}$ is the involution defined by $\overline{x_0 + x_1 i + x_2 j + x_3 ij} = x_0 - x_1 i - x_2 j - x_3 ij$. Under the decomposition (1), the complex conjugate of $z + wj \in \mathcal{A}$ is thus $\overline{z + wj} = \overline{z} - wj$. The reduced trace and reduced norm are the maps $\mathcal{A} \to K$ defined for $x = x_0 + x_1 i + x_2 j + x_3 ij \in \mathcal{A}$ by

$$\mathrm{Trd}(x) = x + \overline{x} = 2x_0 \qquad \text{and} \qquad \mathrm{Nrd}(x) = x\overline{x} = x_0^2 + x_1^2 + x_2^2 + x_3^2,$$

respectively. Note that Trd is K-linear and Nrd is multiplicative. Under the decomposition (1), we have the following alternative definition,

$$\mathrm{Trd}(z + wj) = z + \overline{z} = \mathrm{Tr}_{E/K}(z) \quad \text{and} \quad \mathrm{Nrd}(z + wj) = z\overline{z} + w\overline{w} = \mathrm{N}_{E/K}(z) + \mathrm{N}_{E/K}(w),$$

for all $z + wj \in \mathcal{A}$. In particular, the restriction of Trd (resp. Nrd) to E coincides with $\mathrm{Tr}_{E/K}$ (resp. with $\mathrm{N}_{E/K}$). Note that $\mathrm{Nrd}(\alpha) = 0$ if and only if $\alpha = 0$. Thus any nonzero quaternion $\alpha \in \mathcal{A} \setminus \{0\}$ has a (two-sided) inverse, given by $\alpha^{-1} = \overline{\alpha}/\mathrm{Nrd}(\alpha)$. The trace-zero subspace of $\mathcal{A}$ is $\mathcal{A}^0 := \ker(\mathrm{Trd} : \mathcal{A} \to K)$. It follows from the definition of Trd that one has $\mathcal{A}^0 = Ki \oplus Kj \oplus Kij$. In particular, $\mathcal{A}^0$ is a three-dimensional K-vector space.

2.2.1. *Ramification.* Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ and set $\mathcal{A}_\mathfrak{p} := \mathcal{A} \otimes_K K_\mathfrak{p}$. Then, $\mathcal{A}_p$ is a quaternion algebra over the $\mathfrak{p}$-adic field $K_\mathfrak{p}$. We then say that $\mathcal{A}$ *splits* at $\mathfrak{p}$ if there is an isomorphism of $K_\mathfrak{p}$-algebras $\mathcal{A}_\mathfrak{p} \simeq \mathcal{M}_2(K_\mathfrak{p})$. Otherwise, $\mathcal{A}_\mathfrak{p}$ is a division algebra over $K_\mathfrak{p}$ and we say that $\mathcal{A}$ is ramified at $\mathfrak{p}$. From [4, Corollary A.17], our quaternion algebra $\mathcal{A}$ has the property that it splits at all prime ideals $\mathfrak{p} \subset \mathcal{O}_K$. This property will be repeatedly use in Section 3.

Example 2.2. *Choose the fields $K = \mathbb{Q}$ and $E = \mathbb{Q}(i)$, and consider the Hamilton quaternion algebra $\mathcal{A} = (\frac{E,-1}{K})$. Then, $\mathcal{A}$ is ramified at 2 and split at every odd prime.*

2.2.2. *Orders and ideals.* An *order* in $\mathcal{A}$ is an $\mathcal{O}_K$-lattice $\mathcal{O} \subset \mathcal{A}$ that contains 1 and is closed under multiplication. Moreover, an order is said to be *maximal* if it is not properly contained in any other order of $\mathcal{A}$. Note that maximality is a local property: by [32, Lemma 10.4.3], an order $\mathcal{O}$ is maximal if and only if $\mathcal{O}_\mathfrak{p}$ is a maximal $\mathcal{O}_{K_\mathfrak{p}}$-order in $\mathcal{A}_\mathfrak{p}$ for every prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$.

Let $I \subseteq \mathcal{A}$ be an $\mathcal{O}_K$-lattice. Its left and right orders are defined by $\mathcal{O}_\ell(I) := \{x \in \mathcal{A} \,|\, xI \subseteq I\}$ and $\mathcal{O}_r(I) := \{x \in \mathcal{A} \,|\, Ix \subseteq I\}$, respectively. Both are orders in $\mathcal{A}$.

Let $\mathcal{O} \subseteq \mathcal{A}$ be an order. A *right $\mathcal{O}$-ideal* is an $\mathcal{O}_K$-lattice $I \subseteq \mathcal{A}$ whose right order is exactly $\mathcal{O}$, that is, $\mathcal{O}_r(I) = \mathcal{O}$. Similarly, a *left $\mathcal{O}$-ideal* is an $\mathcal{O}_K$-lattice $I \subseteq \mathcal{A}$ such that

$\mathcal{O}_\ell(I) = \mathcal{O}$.[7] A right $\mathcal{O}$-ideal is *principal* if it is of the form $I = \alpha\mathcal{O}$ for some $\alpha \in \mathcal{A}^\times$. Note that $\mathcal{O}_r(\alpha\mathcal{O}) = \mathcal{O}$ so every principal right ideal is indeed a right $\mathcal{O}$-ideal according to the previous definition. The same holds for left $\mathcal{O}$-ideals.

The reduced norm $\mathrm{Nrd}(I)$ of an $\mathcal{O}_K$-lattice $I \subseteq \mathcal{A}$ is the fractional ideal of $\mathcal{O}_K$ generated by the reduced norms of its elements. If $\mathcal{O}$ is an order and $I = \alpha\mathcal{O}$ is a principal right $\mathcal{O}$-ideal, then $\mathrm{Nrd}(I)$ is the principal fractional ideal $\mathrm{Nrd}(\alpha)\mathcal{O}_K$.

2.2.3. *A consequence of the Skolem-Noether theorem.* The Skolem–Noether theorem [32, Theorem 7.7.1] implies that every K-algebra automorphism of $\mathcal{A}$ is inner, that is, of the form $c_b : x \mapsto bxb^{-1}$ for a certain $b \in \mathcal{A}^\times$.

Here, we are interested more specifically in the group $\mathbf{SO}(\mathcal{A}^0, \mathrm{Nrd})$ of direct isometries of the trace-zero quadratic space $(\mathcal{A}^0, \mathrm{Nrd})$. It is defined as follows:

$$\mathbf{SO}(\mathcal{A}^0, \mathrm{Nrd}) := \{g \in \mathbf{GL}_K(\mathcal{A}^0) \mid \det(g) = 1 \text{ and for all } x \in \mathcal{A}^0,\ \mathrm{Nrd}(g(x)) = \mathrm{Nrd}(x)\}.$$

An element of $\mathbf{SO}(\mathcal{A}^0, \mathrm{Nrd})$ does not *a priori* extend to a multiplicative map on $\mathcal{A}$. The following lemma, adapted from [32, Proposition 4.5.10], shows that every such isometry is in fact the restriction to $\mathcal{A}^0$ of an inner automorphism of $\mathcal{A}$.

Lemma 2.3. *Every direct K-linear isometry g of $(\mathcal{A}^0, \mathrm{Nrd})$ is induced by an inner automorphism of $\mathcal{A}$. More precisely, there exists $b \in \mathcal{A}^\times$ such that for every $x \in \mathcal{A}^0$,*

$$g(x) = c_b(x) = bxb^{-1}.$$

Proof. Conjugation by an element in $\mathcal{A}^\times$ preserves both the reduced trace and the reduced norm and therefore induces a K-linear homomorphism

$$\begin{aligned} \mathcal{A}^\times &\longrightarrow \mathbf{SO}(\mathcal{A}^0, \mathrm{Nrd}) \\ b &\longmapsto \left(c_b : x \longmapsto bxb^{-1}\right) \end{aligned}$$

By [32, Proposition 4.5.10], there is a short exact sequence

$$1 \longrightarrow K^\times \longrightarrow \mathcal{A}^\times \longrightarrow \mathbf{SO}(\mathcal{A}^0, \mathrm{Nrd}) \longrightarrow 1.$$

In particular, the surjectivity gives the result. □

2.2.4. *Properties of maximal orders.* Recall that for $m \geq 8$, the algebra $\mathcal{A}$ is split at every finite prime ideal of $\mathcal{O}_K$, by [4, Corollary A.17(1)]. Its discriminant is therefore equal to $\mathcal{O}_K$. Thus for any maximal order $\mathcal{O}$ in $\mathcal{A}$, its reduced discriminant $\mathrm{discrd}(\mathcal{O})$ is also trivial, by [32, Theorem 15.5.5]. The following lemma shows that $\mathcal{O}$ is generated by its trace-zero part $\mathcal{O}^0 := \mathcal{O} \cap \mathcal{A}^0$.

Lemma 2.4. *If $\mathcal{O}$ is a maximal order of $\mathcal{A}$, then the $\mathcal{O}_K$-algebra generated by $\mathcal{O}^0$ is $\mathcal{O}$.*

Proof. It is enough to prove the result at every prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. After identifying $\mathcal{A}_\mathfrak{p}$ with $\mathcal{M}_2(K_\mathfrak{p})$, the maximal order $\mathcal{O}_\mathfrak{p}$ is conjugate to $\mathcal{M}_2(\mathcal{O}_{K_\mathfrak{p}})$. Notice that the reduced trace then acts as the usual trace map on $\mathcal{M}_2(K_\mathfrak{p})$. Let $\{e_{i,j}\}_{1 \leq i,j \leq 2}$ denote the standard basis, that is, $e_{i,j}$ is the matrix whose (i,j)-entry is 1 and whose other entries are zero.

The trace-zero part of $\mathcal{M}_2(\mathcal{O}_{K_\mathfrak{p}})$ then contains $e_{1,2}$ and $e_{2,1}$. Since $e_{1,2}e_{2,1} = e_{1,1}$ and $e_{2,1}e_{1,2} = e_{2,2}$, the algebra generated by the trace-zero part contains all four matrix units. The order generated by $\mathcal{O}_\mathfrak{p}^0$ is therefore equal to the maximal order $\mathcal{O}_\mathfrak{p}$. □

[7] In the terminology of [32, Definition 16.2.11 and Remark 16.2.13], these are sated fractional ideals.

Remark 2.5. The previous property need not hold for maximal orders in other quaternion algebras, where finite ramification may occur. For example let $m = 4$ and

$$\mathcal{A} = \left(\frac{\mathbb{Q}(i), -1}{\mathbb{Q}}\right)$$

be the Hurwitz quaternions, with maximal order $\mathcal{H} = \mathbb{Z}\left[1, i, j, \frac{1+i+j+ij}{2}\right]$.

Let $\mathcal{L} = \mathbb{Z}[1, i, j, ij]$ be the Lipschitz order. Writing $w = (1 + i + j + ij)/2$, one has $\mathcal{H} = \mathcal{L} \sqcup (w + \mathcal{L})$. Since every element of $w + \mathcal{L}$ has odd reduced trace, it holds that

$$\mathcal{H}^0 = \mathcal{L}^0 = \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}ij.$$

Consequently, the $\mathbb{Z}$-algebra generated by $\mathcal{H}^0$ is $\mathcal{L}$, which has index two in $\mathcal{H}$. In this example, the quaternion algebra $\mathcal{A}$ is ramified at $p = 2$.

Proposition 2.6. *Assume Weber's conjecture for K. Then, the normalizer of any maximal order $\mathcal{O}$ of $\mathcal{A}$ is*

$$\mathcal{N}_{\mathcal{A}}(\mathcal{O}) = K^\times \mathcal{O}^\times.$$

Moreover, the reduced norm of every element of $N_{\mathcal{A}}(\mathcal{O})$ is a square in $K^\times$.

Proof. The inclusion $K^\times\mathcal{O}^\times \subseteq \mathcal{N}_{\mathcal{A}}(\mathcal{O})$ is immediate. For the converse, let $x \in \mathcal{N}_{\mathcal{A}}(\mathcal{O})$. At every finite prime $\mathfrak{p}$, the algebra $\mathcal{A}_\mathfrak{p}$ is split and $\mathcal{O}_\mathfrak{p}$ is maximal. Thus by [32, (23.2.4)],

$$\mathcal{N}_{\mathcal{A}_\mathfrak{p}}(\mathcal{O}_\mathfrak{p}) = K_\mathfrak{p}^\times \mathcal{O}_\mathfrak{p}^\times. \tag{2}$$

For any $\mathfrak{p}$, we may therefore write $x = k_\mathfrak{p} u_\mathfrak{p}$, where $k_\mathfrak{p} \in K_\mathfrak{p}^\times$ and $u_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}^\times$. The set of valuations $\{v_\mathfrak{p}(k_\mathfrak{p})\}_\mathfrak{p}$ then define a unique fractional ideal $\mathfrak{a}$ of K such that

$$x\mathcal{O} = \mathfrak{a}\mathcal{O}.$$

Under Weber's conjecture, this ideal is principal, so $\mathfrak{a} = k\mathcal{O}_K$ for some $k \in K^\times$. It follows that $x\mathcal{O} = k\mathcal{O}$, and hence $u := k^{-1}x$ belongs to $\mathcal{O}^\times$. Therefore $x = ku \in K^\times\mathcal{O}^\times$, proving the equality $\mathcal{N}_{\mathcal{A}}(\mathcal{O}) = K^\times\mathcal{O}^\times$.

It remains to prove the claim on reduced norms. Let $x = ku \in K^\times\mathcal{O}^\times$. Then,

$$\mathrm{Nrd}(x) = k^2 \,\mathrm{Nrd}(u),$$

and $\mathrm{Nrd}(u)$ is a totally positive unit of K. Under Weber's conjecture, and by the equivalence between *(b1)* and *(b2)* in [10, Proposition 1], totally positive units of K are squares. Thus, $\mathrm{Nrd}(u) \in \mathcal{O}_K^{\times 2}$, and it follows that $\mathrm{Nrd}(x) \in K^{\times 2}$, as claimed. □

Remark 2.7. The local equalities (2) do *not* directly imply the global one, since the usual local–global dictionary [32, Theorem 9.4.9] does not apply: the normalizers are multiplicative groups, not $\mathcal{O}_K$-lattices. In general, the obstruction $\mathcal{N}_{\mathcal{A}}(\mathcal{O})/K^\times\mathcal{O}^\times$ can be interpreted in terms of principal two-sided ideals; see [32, Proposition 18.5.3].

2.3. **Module-LIP and reduction to nrdPIP.** Following [23], we first define module-LIP for module lattices in E^ℓ. We then introduce nrdPIP in quaternion algebras. The ideas behind the reduction from module-LIP to nrdPIP due to Chevignard et al. [4] are recalled at the beginning of Section 4.

Definition 2.8 (Pseudo-Gram matrices)**.** *Let $\mathbf{B} = (B, \{\mathfrak{a}_i\}_{1\le i\le \ell})$ be a pseudo-basis of a module-lattice $\mathcal{M}$ in E^ℓ. The pseudo-Gram matrix associated to $\mathbf{B}$ is $\mathbf{G} = (G, \{\mathfrak{a}_i\}_{1\le i\le \ell})$, where $G = B^*B$. Moreover, two pseudo-Gram matrices $\mathbf{G} = (G, \{\mathfrak{a}_i\}_{1\le i\le \ell})$ and $\mathbf{H} = (H, \{\mathfrak{b}_i\}_{1\le i\le \ell})$ are called congruent if there exists a matrix $U = (u_{i,j})_{1\le i,j\le \ell} \in \mathbf{GL}_\ell(E)$ satisfying the following conditions:*

1. *$H = U^*GU$;*
2. *$u_{i,j} \in \mathfrak{a}_i\mathfrak{b}_j^{-1}$ for all $1 \le i, j \le \ell$;*
3. *$\prod_{i=1}^{\ell} \mathfrak{a}_i = (\det U) \prod_{i=1}^{\ell} \mathfrak{b}_i$.*

Such a matrix U is called a congruence matrix between $\mathbf{G}$ and $\mathbf{H}$, and the set of all congruence matrices is denoted by $\mathrm{Cong}(\mathbf{G}, \mathbf{H})$.

Definition 2.9 (wc-smodLIP [23, Definition 3.11])**.** *Let $\mathbf{B} = \big(B, (\mathfrak{a}_i)_{1\le i\le \ell}\big)$ be a pseudo-basis of a rank-ℓ module lattice $\mathcal{M}$ in E^ℓ, and let $\mathbf{G} = \big(G, (\mathfrak{a}_i)_{1\le i\le \ell}\big)$ be its associated pseudo-Gram matrix. The worst-case search module-Lattice Isomorphism Problem with parameters E and $\mathbf{B}$ (denoted by $\text{wc-smodLIP}_K^{\mathbf{B}}$) asks, given a pseudo-Gram matrix $\mathbf{H}$ congruent to $\mathbf{G}$, to compute an element of the set $\mathrm{Cong}(\mathbf{G}, \mathbf{H})$.*

Remark 2.10. The module lattice underlying Hawk is $\mathcal{O}_E^2$, equipped with its canonical (pseudo-)basis $\mathbf{I}_2 := \big(I_2, (\mathcal{O}_E, \mathcal{O}_E)\big)$, and whose pseudo-Gram matrix is again $\mathbf{I}_2$. Therefore, $\text{wc-smodLIP}_E^{\mathbf{I}_2}$ admits the following simpler interpretation: given a public matrix H known to satisfy $H = C^*C$ for some $C \in \mathbf{GL}_2(\mathcal{O}_E)$, the problem asks to compute any matrix $\widehat{C} \in \mathbf{GL}_2(\mathcal{O}_E)$ such that $H = \widehat{C}^*\widehat{C}$.

Thus for Hawk, the underlying module-LIP instance is seen as an integral Gram-matrix factorization problem. This is the key-recovery problem underlying Hawk.

It was proven in [4] that module-LIP in rank two modules over E can be reduced to a problem called the norm-reduced Principal Ideal Problem. We recall its definition below.

Definition 2.11 ($\mathcal{O}$-nrdPIP)**.** *Let $\mathcal{O}$ be an order in the quaternion algebra $\mathcal{A}$. The norm-reduced Principal Ideal Problem with parameter $\mathcal{O}$, denoted by $\mathcal{O}$-nrdPIP, is defined as follows. It takes as input a pseudo-basis over $\mathcal{O}_K$ of a right $\mathcal{O}$-ideal I, and an element q, under the promise that there exists $\alpha \in \mathcal{A}^\times$ such that $I = \alpha\mathcal{O}$ and $\mathrm{Nrd}(\alpha) = q$. The problem then asks to compute any such element α.*

Remark 2.12. Fix a solution α to the instance (I, q). Then $\widehat{\alpha} \in \mathcal{A}^\times$ is another solution if and only if $\alpha^{-1}\widehat{\alpha} \in \mathcal{O}^1 := \{u \in \mathcal{O} : \mathrm{Nrd}(u) = 1\}$. Indeed, the equality $\widehat{\alpha}\mathcal{O} = \alpha\mathcal{O}$ is equivalent to $\alpha^{-1}\widehat{\alpha} \in \mathcal{O}^\times$, while equality of the reduced norms is equivalent to this unit having reduced norm one. Since $\mathcal{A}$ is totally definite, $\mathcal{O}^1$ is finite; see [32, Chapter 32].

The main result of Chevignard et al. [4] is the following reduction. At the beginning of Section 4, we briefly recall how the reduction proceeds, in the case of a Hawk instance.

Proposition 2.13 ([4, Corollary 3.9])**.** *There exists a non-uniform polynomial time reduction from wc-smodLIP$_E^{\mathbf{B}}$ to $\mathcal{O}$-nrdPIP, where $\mathbf{B}$ is any pseudo-basis of a rank-2 module included in E^2 and $\mathcal{O}$ is a particular maximal order of $\mathcal{A}$ depending on $\mathbf{B}$. The reduction makes two calls to the $\mathcal{O}$-nrdPIP oracle.*

2.4. **Algorithmic considerations.** This section collects several computational results in number fields and quaternions algebras, that will be used latter on.

Lemma 2.14 (Square roots in K)**.** *There is a polynomial-time algorithm for factoring univariate polynomials over K. In particular, given $r \in K^{\times 2}$, one can compute an element $\lambda \in K^\times$ such that $\lambda^2 = r$ in polynomial time.*

Proof. Apply the polynomial-time factorization algorithm of [16] to $X^2 - r \in K[X]$. □

We will use the Gentry–Szydlo [12]/Lenstra–Silverberg [17] algorithm, recalled below.

Lemma 2.15 (Specialization of [17, Theorem 1.3])**.** *There exists a deterministic polynomial-time algorithm* `GentrySzydlo` *that given a $\mathbb{Z}$-basis of $\mathcal{O}_E$, a fractional ideal $\mathfrak{a}$ of E and an element $q \in K$ satisfying $\mathrm{N}_{E/K}(\mathfrak{a}) = q\mathcal{O}_K$, decides whether there exists $h \in E$ such that $\mathfrak{a} = h\mathcal{O}_E$ and $\mathrm{Nrd}(h) = q$, and if so computes such an element h.*

Lemma 2.16 (Inner representative)**.** *Let $g : \mathcal{A}^0 \longrightarrow \mathcal{A}^0$ be a K-linear map known to be the restriction of an inner automorphism of $\mathcal{A}$. Given the image by g of a K-basis of $\mathcal{A}^0$, one can compute in polynomial time an element $b \in \mathcal{A}^\times$ such that*

$$g(x) = bxb^{-1}, \qquad \text{for every } x \in \mathcal{A}^0.$$

Proof. Let (x_1, x_2, x_3) be a K-basis of $\mathcal{A}^0$. We compute the solutions $b \in \mathcal{A}$ of the K-linear system $g(x_i)b = bx_i$, for $1 \le i \le 3$. By assumption, this system has a non-zero solution. Moreover, the set of solutions to this system forms a K-vector space of dimension 1: indeed, for any two solutions b_0 and b_1, the element $b_0^{-1}b_1$ commutes with every element of $\mathcal{A}^0$, and hence with all of $\mathcal{A} = K \oplus \mathcal{A}^0$. It therefore belongs to the center K, i.e., $b_1 = b_0 x$ for some $x \in K$. In particular, every non-zero solution induces g. The result follows by polynomial-time linear algebra over K. □

Lemma 2.17 (Left and right orders of a lattice)**.** *Let I be a full $\mathcal{O}_K$-lattice in $\mathcal{A}$, given by a pseudo-basis. Then, pseudo-bases of its left and right orders can be computed in polynomial time.*

Proof. Write the given pseudo-basis as $I = \mathfrak{a}_1\mathbf{b}_1 \oplus \cdots \oplus \mathfrak{a}_4\mathbf{b}_4$. For $x \in \mathcal{A}$ and $1 \le j \le 4$, write $x\mathbf{b}_j = \sum_{i=1}^4 \ell_{ij}(x)\mathbf{b}_i$, where each $\ell_{ij} : \mathcal{A} \to K$ is a K-linear form that can be computed from the multiplication table of $\mathcal{A}$. Since the fractional ideals $\mathfrak{a}_j$ are invertible, the condition $x\mathfrak{a}_j\mathbf{b}_j \subseteq I$ is equivalent to

$$\ell_{ij}(x) \in \mathfrak{a}_i{\mathfrak{a}_j}^{-1},$$

for every $1 \le i \le 4$. Consequently, $\mathcal{O}_\ell(I) = \{x \in \mathcal{A} \,|\, \ell_{ij}(x) \in \mathfrak{a}_i\mathfrak{a}_j^{-1} \text{ for all } 1 \le i, j \le 4\}$. For each choice of the pair (i, j), the set $\{x \in \mathcal{A} \,|\, \ell_{ij}(x) \in \mathfrak{a}_i\mathfrak{a}_j^{-1}\}$ is an $\mathcal{O}_K$-module of rank 4 and we can efficiently compute a pseudo-basis of it by knowing the linear form ℓ_{ij} and the ideal $\mathfrak{a}_i\mathfrak{a}_j^{-1}$. The set $\mathcal{O}_\ell(I)$ is then the intersection of at most 16 such $\mathcal{O}_K$-modules, and a pseudo-basis of this intersection can be computed in polynomial time, by adapting the algorithm for $\mathbb{Z}$-lattices and $\mathbb{Q}$-vector spaces (see [21, Section 2.2]) and using a pseudo-Hermite normal form algorithm (see [5, Algorithm 1.4.7]).

The computation of the right order is identical: writing $\mathbf{b}_j x = \sum_i r_{ij}(x)\mathbf{b}_i$, one obtains $\mathcal{O}_r(I) = \{x \in \mathcal{A} \,|\, r_{ij}(x) \in \mathfrak{a}_i\mathfrak{a}_j^{-1} \text{ for all } 1 \le i, j \le 4\}$, from which a pseudo-basis is computed by the same procedure. □

Lemma 2.18 (Trace-zero sublattice)**.** *Let $\mathcal{O}$ be any order of $\mathcal{A}$. Given a pseudo-basis of $\mathcal{O}$ as an $\mathcal{O}_K$-module, one can compute in polynomial time a pseudo-basis $\mathcal{O}^0 = \mathcal{O} \cap \ker(\mathrm{Trd})$. Moreover, $\mathcal{O}^0$ has rank three over $\mathcal{O}_K$.*

Proof. Let $\mathcal{A}^0 = \{x \in \mathcal{A} \mid \mathrm{Trd}(x) = 0\}$ be the set of elements of reduced trace 0 in $\mathcal{A}$. We have seen that this is a K-vectors space of dimension 3 in $\mathcal{A}$. The set $\mathcal{O}^0 = \mathcal{O} \cap \mathcal{A}^0$ is simply the intersection of a rank-4 $\mathcal{O}_K$-module with a dimension 3 K-vector space (both included in the same K-vector space $\mathcal{A}$). Computing a pseudo-basis of this intersection can be done in polynomial time (by adapting the algorithm for $\mathbb{Z}$-lattices and $\mathbb{Q}$-vector spaces, see [21, Section 2.2]) using pseudo-Hermite normal form algorithms (see [5, Algorithm 1.4.7]).

It remains to see that the intersection $\mathcal{O}^0 = \mathcal{O} \cap \mathcal{A}^0$ has rank 3 as an $\mathcal{O}_K$-module. This can be proven by extending the scalars to K, which gives $\mathcal{O}^0 \otimes_{\mathcal{O}_K} K = \mathcal{A}^0$. Since the latter has dimension three over K, the module $\mathcal{O}^0$ has rank three over $\mathcal{O}_K$. □

3. The general reduction

In this section, we provide a polynomial time reduction from $\mathcal{O}$-nrdPIP in a maximal order $\mathcal{O}$ of $\mathcal{A}$ to the module-LIP problem for rank-three module lattices over $\mathcal{O}_K$ (see Corollary 3.7). This reduction relies on Weber's conjecture for the totally real subfield K. Combined with the reduction from Chevignard et al. [4], this gives us a reduction from module-LIP for rank-two module lattices over $\mathcal{O}_E$ to module-LIP for rank-three module lattices over $\mathcal{O}_K$. More precisely, we prove the following result.

Theorem 3.1 (rank-two module-LIP in $\mathcal{O}_E$ to rank-three module-LIP in $\mathcal{O}_K$)**.** *Assume that Weber's conjecture holds for K. There exists a non-uniform polynomial time reduction from wc-smodLIP$^{\mathbf{B}}_E$ to wc-smodLIP$^{\mathbf{C}}_K$, where $\mathbf{B}$ is any pseudo-basis of an $\mathcal{O}_E$-module of rank 2 included in E^2 and $\mathbf{C}$ is a particular pseudo-basis of an $\mathcal{O}_K$-module of rank 3 included in K^4 depending on $\mathbf{B}$. The reduction makes two calls to the wc-smodLIP$^{\mathbf{C}}_K$.*

In the rest of this section, we assume that a maximal order $\mathcal{O}$ if $\mathcal{A}$ has been fixed, and we are given as input an instance (I, q) of $\mathcal{O}$-nrdPIP. We let α denote a (secret) solution of the nrdPIP instance, that is $I = \alpha\mathcal{O}$ and $q = \mathrm{Nrd}(\alpha)$.

3.1. The public ternary instance.

Let us start with a few observations regarding the left order of I and its relations with the order $\mathcal{O}$.

Lemma 3.2. *Let $\mathcal{O}$ be a maximal order of $\mathcal{A}$ and $\alpha \in \mathcal{O}$. Define $I = \alpha\mathcal{O}$. Then the left order of I is $\Lambda = \mathcal{O}_\ell(I) = \alpha\mathcal{O}\alpha^{-1}$.*

Proof. For any $x \in \mathcal{A}$, the condition $xI \subseteq I$ is equivalent to $\alpha^{-1}x\alpha\mathcal{O} \subseteq \mathcal{O}$. Since $1 \in \mathcal{O}$, the latter holds exactly when $\alpha^{-1}x\alpha \in \mathcal{O}$. This proves the formula. □

Definition 3.3. *Let $\Lambda = \mathcal{O}_\ell(I) = \alpha\mathcal{O}\alpha^{-1}$. We set $\mathcal{O}^0 := \mathcal{O} \cap \mathcal{A}^0$ and $\Lambda^0 := \Lambda \cap \mathcal{A}^0$.*

Proposition 3.4. *Conjugation by α restricts to an $\mathcal{O}_K$-linear isometry*

$$c_\alpha : (\mathcal{O}^0, \mathrm{Nrd}) \longrightarrow (\Lambda^0, \mathrm{Nrd}).$$

In particular, $\mathcal{O}^0$ and Λ^0 are isomorphic rank-three $\mathcal{O}_K$-lattices.

Proof. By Lemma 3.2, conjugation by α sends $\mathcal{O}$ onto Λ. Moreover, this map is invertible with inverse $c_{\alpha^{-1}}$ so it induces a bijection from $\mathcal{O}$ onto Λ. Note that the map c_α preserves the reduced norm, and so it induces an isometry between $(\mathcal{O}, \mathrm{Nrd})$ and (Λ, Nrd). Finally, c_α also preserves the reduced trace so it must map the kernel of Trd in $\mathcal{O}$ bijectively (and isometrically) onto the kernel of Trd in Λ. □

3.2. **Recovery from an arbitrary isometry.** We have seen that the map c_α (where α is the secret element we seek to recover) induces an $\mathcal{O}_K$-isometry between $\mathcal{O}^0$ and Λ^0 (which are both public $\mathcal{O}_K$-modules of rank 3). In this section, we show that the knowledge of any $\mathcal{O}_K$-isometry between $\mathcal{O}^0$ and Λ^0 can be used to recover an element α up to multiplication by an element of $K^\times\mathcal{O}^\times$. Combining this with the knowledge of $q = \mathrm{Nrd}(\alpha)$ allows us to recover α up to an element of $\mathcal{O}^1$ and hence solve the nrdPIP instance.

Proposition 3.5. *Let $\mathcal{O}$ be maximal and let $f : (\mathcal{O}^0, \mathrm{Nrd}) \longrightarrow (\Lambda^0, \mathrm{Nrd})$ be any $\mathcal{O}_K$-linear direct isometry.*[8] *Then there exists $b \in \mathcal{A}^\times$ such that $f = c_{b\,|\mathcal{O}^0}$ is inner. Moreover, one has $\Lambda = b\mathcal{O}b^{-1}$.*

Proof. Since $\mathcal{O}^0$ and Λ^0 both span $\mathcal{A}^0$ over K, the map f extends uniquely to a K-linear direct isometry $g : (\mathcal{A}^0, \mathrm{Nrd}) \longrightarrow (\mathcal{A}^0, \mathrm{Nrd})$. By Lemma 2.3, there exists $b \in \mathcal{A}^\times$ such that $g = c_b$ on $\mathcal{A}^0$. In particular, restricting this equality to $\mathcal{O}^0$ gives $f = c_{b\,|\mathcal{O}^0}$ and $b\mathcal{O}^0b^{-1} = \Lambda^0$. This proves the first claim.

By Lemma 2.4, a maximal order in $\mathcal{A}$ is generated as an $\mathcal{O}_K$-algebra by its trace-zero submodule. Note that since $\mathcal{O}$ is maximal, so is Λ, so both $\mathcal{O}^0$ and Λ^0 generate $\mathcal{O}$ and Λ respectively as $\mathcal{O}_K$-algebra. We thus obtain $b\mathcal{O}b^{-1} = \Lambda$ as claimed. □

We now describe our main reduction algorithm. This algorithm takes as input an arbitrary $\mathcal{O}_K$-isometry f between the two rank-3 modules $\mathcal{O}^0$ and Λ^0 as well as the reduced norm $q = \mathrm{Nrd}(\alpha)$ and it outputs a solution $\widehat{\alpha}$ to the nrdPIP problem with input (I, q).

Algorithm 1 From nrdPIP to rank-3 module-LIP over $\mathcal{O}_K$

Input: Pseudo-bases of $\mathcal{O}^0$ and Λ^0 over $\mathcal{O}_K$; the reduced norm element $q \in K^\times$; an arbitrary $\mathcal{O}_K$-linear isometry $f : (\mathcal{O}^0, \mathrm{Nrd}) \to (\Lambda^0, \mathrm{Nrd})$.
Output: An element $\widehat{\alpha} \in \mathcal{A}^\times$ such that $I = \widehat{\alpha}\mathcal{O}$ and $\mathrm{Nrd}(\widehat{\alpha}) = q$.

1: Compute $\varepsilon \leftarrow \det(f) \in \{-1, 1\}$ and set $g \leftarrow \varepsilon f$ *// Then g is a direct isometry.*
2: Compute $b \in \mathcal{A}^\times$ such that $g = c_{b\,|\mathcal{O}^0}$ *//c.f., Proposition 3.5 and Lemma 2.16.*
3: Compute $r \leftarrow \mathrm{Nrd}(b)/q$ and $\lambda \in K^\times$ such that $\lambda^2 = r$ *//c.f., Proposition 2.6.*
4: Set $\widehat{\alpha} \leftarrow \lambda^{-1}b$
5: **return** $\widehat{\alpha}$

Theorem 3.6. *Assume Weber's conjecture for K. Let $f : (\mathcal{O}^0, \mathrm{Nrd}) \longrightarrow (\Lambda^0, \mathrm{Nrd})$ be any $\mathcal{O}_K$-linear isometry. On input pseudo-bases of $\mathcal{O}^0$ and Λ^0, the map f, and the element $q \in K$, Algorithm 1 computes an element $\widehat{\alpha} \in \mathcal{A}^\times$ which is a solution to the $\mathcal{O}$-nrdPIP instance (I, q), that is, $I = \widehat{\alpha}\mathcal{O}$ and $\mathrm{Nrd}(\widehat{\alpha}) = q$. Moreover, it runs in polynomial time in the input size.*

Proof. Correctness. Since f is an isometry, then $\det(f) \in K^\times$ is a root of unity. Because K is totally real, its only roots of unity are ± 1, and so one necessarily has $\det(f) \in \{-1, 1\}$. Moreover, $\dim_K(\mathcal{A}^0) = 3$, so the map $g = \det(f)f$ built at Step 1 has determinant $\det(g) = \det(f)^3 \cdot \det(f) = 1$. By Proposition 3.5, g extends to a

[8] We require the isometry to be direct here, that is, to have determinant 1.

K-linear direct isometry of $(\mathcal{A}^0, \mathrm{Nrd})$ which still sends $\mathcal{O}^0$ onto Λ^0 and is the restriction of an inner automorphism c_b for some $b \in \mathcal{A}^\times$. Lemma 2.16 ensures that such an element $b \in \mathcal{A}^\times$ can be computed at Step 2.

Another consequence of Proposition 3.5 is the equality

$$b\mathcal{O}b^{-1} = \Lambda = \alpha\mathcal{O}\alpha^{-1}.$$

Thus, both b and α conjugate $\mathcal{O}$ to Λ, so $n := \alpha^{-1}b$ is an element of the normalizer $\mathcal{N}_{\mathcal{A}}(\mathcal{O})$. Under Weber's conjecture, Proposition 2.6 shows that $r = \mathrm{Nrd}(b)/q = \mathrm{Nrd}(n)$ is a square in $K^\times$. This proves that Step 3 will succeed in computing a square root of r. Choosing a square root $\lambda \in K^\times$, Step 4 then builds the element $\widehat{\alpha} := \lambda^{-1}b$. By construction, $\mathrm{Nrd}(\widehat{\alpha}) = \lambda^{-2}\,\mathrm{Nrd}(b) = q$ and $u = \alpha^{-1}\widehat{\alpha}$ is a norm-one element of $\mathcal{N}_{\mathcal{A}}(\mathcal{O}) = K^\times\mathcal{O}^\times$.[9] It remains to prove that $\widehat{\alpha}$ generates I. Write $u = kv$ with $k \in K^\times$ and $v \in \mathcal{O}^\times$. From $1 = \mathrm{Nrd}(u) = k^2\,\mathrm{Nrd}(v)$, and since $\mathrm{Nrd}(v) \in \mathcal{O}_K^\times$, we obtain that $k^2 \in \mathcal{O}_K^\times$ is a unit and so is k. Since $\mathcal{O}_K^\times \subset \mathcal{O}^\times$, we have $u = kv \in \mathcal{O}^\times$ and thus

$$\widehat{\alpha}\mathcal{O} = \alpha u\mathcal{O} = \alpha\mathcal{O} = I.$$

This concludes the proof of correctness.

Complexity. Only Steps 2 and 3 require justifications. The result then follows from Lemma 2.16 and Lemma 2.14, respectively. □

Corollary 3.7 ($\mathcal{O}$-nrdPIP to rank-three module-LIP)**.** *Assume Weber's conjecture for K. Let $\mathcal{O}$ be a maximal order of $\mathcal{A}$, given by a pseudo-basis over $\mathcal{O}_K$. From Lemma 2.18, one can (pre-)compute in polynomial time a pseudo-basis $\mathbf{B}$ of $\mathcal{O}^0$. Then, there is a uniform deterministic polynomial-time reduction from* $\mathcal{O}$-nrdPIP *to* wc-smodLIP$_K^{\mathbf{B}}$. *Moreover, the resulting algorithm makes a single oracle call.*

Proof. From the pseudo-basis of $\mathcal{O}$, we first compute a pseudo-basis $\mathbf{B} = (B, (\mathfrak{b}_i)_{1\le i\le 3})$ of $\mathcal{O}^0$ using Lemma 2.18. Note that $\mathbf{B}$ depends only on $\mathcal{O}$, and not on the particular $\mathcal{O}$-nrdPIP instance. In particular, we can assume that $\mathbf{B}$ has been precomputed. Here, elements of $\mathcal{A}$ are mapped to vectors of K^4 by the map $\psi(x) = (x_0, x_1, x_2, x_3)$ where $x = x_0 + x_1 i + x_2 j + x_3 ij$ with the x_i's in K (see preliminaries). This map ensures that $\mathrm{Trd}(x)$ corresponds to the usual quadratic form $\sum_i x_i^2$ on K, for which wc-smodLIP is defined.

Now let (I, q) be an instance of $\mathcal{O}$-nrdPIP, and write $I = \alpha\mathcal{O}$ with $\mathrm{Nrd}(\alpha) = q$. From the pseudo-basis of I, we compute its left order $\Lambda = \mathcal{O}_\ell(I) = \alpha\mathcal{O}\alpha^{-1}$, as well as a pseudo-basis $\mathbf{C} = (C, (\mathfrak{c}_i)_{1\le i\le 3})$ of Λ^0. All these computations take polynomial time, thanks to Lemma 2.17 and Lemma 2.18, respectively.

Let $\mathbf{G}$ and $\mathbf{H}$ be the pseudo-Gram matrices associated with $\mathbf{B}$ and $\mathbf{C}$, respectively. We saw in Proposition 3.4 that conjugation by α induces an $\mathcal{O}_K$-linear isometry from $(\mathcal{O}^0, \mathrm{Nrd})$ to $(\Lambda^0, \mathrm{Nrd})$. Therefore, $\mathbf{H}$ is congruent to $\mathbf{G}$ and it forms a valid input to wc-smodLIP$_K^{\mathbf{B}}$, in the sense of Definition 2.9.

The oracle call returns a matrix $U \in \mathrm{Cong}(\mathbf{G}, \mathbf{H})$. This determines a K-linear isometry $f : (\mathcal{O}^0, \mathrm{Nrd}) \longrightarrow (\Lambda^0, \mathrm{Nrd})$. More precisely, the matrix of f is $C(BU)^{-1}$. Running Algorithm 1 on input $\mathbf{B}, \mathbf{C}$, the isometry f, and the norm q then produces in polynomial time a solution to the $\mathcal{O}$-nrdPIP instance (I, q), according to Theorem 3.6. □

[9] The latter equality is due to Proposition 2.6 and it assumes Weber's conjecture.

Finally, we can combine this reduction with the reduction from module-LIP in rank-2 modules over $\mathcal{O}_E$ to the nrdPIP problem that was proven in [4], and conclude the proof of our main theorem.

Proof of Theorem 3.1. The reduction is obtained by combining Proposition 2.13 and Corollary 3.7. Note that the reduction in Proposition 2.13 makes two calls to $\mathcal{O}$-nrdPIP for some maximal order $\mathcal{O}$ of $\mathcal{A}$, but the two calls are with the same order $\mathcal{O}$. Hence, both calls can be reduced to wc-smodLIP$^{\mathbf{C}}_K$ for the same pseudo-basis $\mathbf{C}$. We also note that this pseudo-basis $\mathbf{C}$ is the pseudo-basis of the rank-3 module $\mathcal{O}^0$ which is included in $\mathcal{A}$, i.e., in K^4 via the map ψ defined in Section 2.2. □

4. The special case of Hawk

We now focus on the special case of Hawk, that is, when the initial $\mathcal{O}_E$-module of rank 2 is isometric to $\mathcal{O}_E^2$. In this case, we would like to reduce the problem to module-LIP in a rank-three $\mathcal{O}_K$-module with nice geometric properties (ideally close to $\mathbb{Z}^n$ when seen as a lattice). To do so, we would like to replace the maximal order $\mathcal{O}$ by the natural order $\mathcal{O}_{\text{nat}} = \mathcal{O}_E \oplus \mathcal{O}_E j$. We will prove in Proposition 4.8 that, when seen as a lattice, the trace-zero restriction $\mathcal{O}^0_{\text{nat}}$ of $\mathcal{O}_{\text{nat}}$ is isomorphic (up to scaling) to $\mathbb{Z}^{2d+1} \perp \sqrt{2}\,\mathbb{Z}^{d-1}$, where $d = m/4$ is the degree of the field K, hence it qualifies as a lattice with nice geometric properties.

Unfortunately, the order $\mathcal{O}_{\text{nat}}$ is not a maximal order (see, e.g., [4, Corollary A.17]), and both the reduction from rank-two module-LIP in E to nrdPIP from [4] and the reduction from nrdPIP to rank-three module-LIP in K from Section 3 require the order $\mathcal{O}$ to be maximal. Hence, we need to adapt both reductions to the natural order $\mathcal{O}_{\text{nat}}$.

Overall, in this section, we prove the following result.

Theorem 4.1. *Let $E = \mathbb{Q}(\zeta_m)$ be a cyclotomic field of conductor m, with m a power-of-two. Let K be the maximal totally real subfield of E. There is a Karp uniform deterministic polynomial-time reduction from solving Hawk's key-recovery problem over the field E to computing the set of all $m+2$ minimal vectors of some rank-three $\mathcal{O}_K$-module isomorphic to $\mathcal{O}^0_{\text{nat}}$.*

Moreover, seen as a Euclidean lattice, $\mathcal{O}^0_{\text{nat}}$ is isomorphic (up to scaling) to

$$\mathbb{Z}^{\frac{m}{2}+1} \perp \sqrt{2}\,\mathbb{Z}^{\frac{m}{4}-1}.$$

4.1. Descent to the natural order.

We first explain how the reduction of Chevignard et al. [4] can be carried out over the natural order $\mathcal{O}_{\text{nat}} = \mathcal{O}_E \oplus \mathcal{O}_E j$.

Let $\mathcal{O}$ be a maximal order containing $\mathcal{O}_{\text{nat}}$. A first natural idea would be to reduce $\mathcal{O}$-nrdPIP to $\mathcal{O}_{\text{nat}}$-nrdPIP, and then apply the reduction from [4] with the maximal order $\mathcal{O}$. Unfortunately, if $I = \alpha\mathcal{O}$ is a public ideal with a secret generator α, and even if $\alpha \in \mathcal{O}_{\text{nat}}$, one cannot in general recover $\alpha\mathcal{O}_{\text{nat}}$ by intersecting $\alpha\mathcal{O}$ with $\mathcal{O}_{\text{nat}}$: the equality $\alpha\mathcal{O} \cap \mathcal{O}_{\text{nat}} = \alpha\mathcal{O}_{\text{nat}}$ need not hold.[10] We therefore proceed to adapt the reduction of [4] at the level of the natural order.

[10] For a counterexample, consider $\mathcal{A} = (\frac{\mathbb{Q}(i),-1}{\mathbb{Q}})$ and let $\mathcal{O}_{\text{nat}} = \mathbb{Z}[1,i,j,ij]$ be the natural order. It is contained in the maximal order $\mathcal{H} = \mathbb{Z}[1,i,j,(1+i+j+ij)/2]$. Set $\alpha = 1+i \in \mathcal{O}_{\text{nat}}$ and $w = (1+i+j+ij)/2 \in \mathcal{H}$. Then $\alpha w = i+ij \in \mathcal{O}_{\text{nat}}$, so $i+ij \in \alpha\mathcal{H} \cap \mathcal{O}_{\text{nat}}$. On the other hand, $i+ij \notin \alpha\mathcal{O}_{\text{nat}}$, since $\alpha^{-1}(i+ij) = w \notin \mathcal{O}_{\text{nat}}$.

Let us first recall the main ideas behind [4]. Consider the E-linear isomorphism

$$\begin{aligned}\varphi : E^2 &\longrightarrow \mathcal{A},\\ (a,b) &\longmapsto a + bj.\end{aligned}$$

Let $H \in \mathbf{GL}_2(\mathcal{O}_E)$ be a Gram matrix corresponding to a public key of Hawk, and let $C = (\mathbf{c}_1 \mid \mathbf{c}_2) \in \mathbf{GL}_2(\mathcal{O}_E)$ be a secret Gram factorization, so that $C^*C = H$. We then set $\alpha = \varphi(\mathbf{c}_1)$ and $\beta = \varphi(\mathbf{c}_2)$. In particular, both α and β belong to $\mathcal{O}_{\mathrm{nat}}$. The key steps of the reduction of [4] can be summarized as follows:

(1) From the public key H, one computes $\alpha\beta^{-1} \in \mathcal{A}$ (*c.f.,* [4, Lemma 3.5]);[11]
(2) From $\alpha\beta^{-1}$, one computes the right $\mathcal{O}$-ideal $I = \alpha\mathcal{O}$, where $\mathcal{O}$ is a maximal order of $\mathcal{A}$ containing $\mathcal{O}_{\mathrm{nat}}$ (*c.f.,* [4, Proposition 3.6]).

The first step above does not depend on the choice of an order, hence we only need to adapt the second step to the case where $\mathcal{O}$ is replaced by the natural order $\mathcal{O}_{\mathrm{nat}}$.

Proposition 4.2. *With the notation above, one has the equalities:*

$$\mathcal{O}_{\mathrm{nat}}\alpha + \mathcal{O}_{\mathrm{nat}}\beta = \mathcal{O}_{\mathrm{nat}} = \alpha^{-1}\mathcal{O}_{\mathrm{nat}} \cap \beta^{-1}\mathcal{O}_{\mathrm{nat}}.$$

Moreover, the following right $\mathcal{O}_{\mathrm{nat}}$-ideals are equal:

$$\alpha\mathcal{O}_{\mathrm{nat}} = \mathcal{O}_{\mathrm{nat}} \cap \alpha\beta^{-1}\mathcal{O}_{\mathrm{nat}}.$$

Consequently, the public element $\gamma = \alpha\beta^{-1}$ determines a pseudo-basis of $I_{\mathrm{nat}} = \alpha\mathcal{O}_{\mathrm{nat}}$.

Proof. Since the columns of C form an $\mathcal{O}_E$-basis of $\mathcal{O}_E^2$ and φ is E-linear, one has $\mathcal{O}_{\mathrm{nat}} = \varphi(\mathcal{O}_E^2) = \mathcal{O}_E\alpha + \mathcal{O}_E\beta$. The inclusion $\mathcal{O}_E \subset \mathcal{O}_{\mathrm{nat}}$ then gives $\mathcal{O}_{\mathrm{nat}} \subseteq \mathcal{O}_{\mathrm{nat}}\alpha + \mathcal{O}_{\mathrm{nat}}\beta$. The converse follows from $\alpha, \beta \in \mathcal{O}_{\mathrm{nat}}$, and the fact that $\mathcal{O}_{\mathrm{nat}}$ is an order.

Since $\alpha, \beta \in \mathcal{O}_{\mathrm{nat}}$, one has $\mathcal{O}_{\mathrm{nat}} \subseteq \alpha^{-1}\mathcal{O}_{\mathrm{nat}}$ and $\mathcal{O}_{\mathrm{nat}} \subseteq \beta^{-1}\mathcal{O}_{\mathrm{nat}}$. Thus, the inclusion $\mathcal{O}_{\mathrm{nat}} \subseteq \alpha^{-1}\mathcal{O}_{\mathrm{nat}} \cap \beta^{-1}\mathcal{O}_{\mathrm{nat}}$ holds. Conversely, let $x \in \alpha^{-1}\mathcal{O}_{\mathrm{nat}} \cap \beta^{-1}\mathcal{O}_{\mathrm{nat}}$. Then, αx and βx belong to $\mathcal{O}_{\mathrm{nat}}$. From the first equality $\mathcal{O}_{\mathrm{nat}} = \mathcal{O}_{\mathrm{nat}}\alpha + \mathcal{O}_{\mathrm{nat}}\beta$, it follows that $\mathcal{O}_{\mathrm{nat}}x \subseteq \mathcal{O}_{\mathrm{nat}}$. Since $1 \in \mathcal{O}_{\mathrm{nat}}$, we conclude that $x = 1 \cdot x \in \mathcal{O}_{\mathrm{nat}}$, proving the first part.

Multiplying the equality $\mathcal{O}_{\mathrm{nat}} = \alpha^{-1}\mathcal{O}_{\mathrm{nat}} \cap \beta^{-1}\mathcal{O}_{\mathrm{nat}}$ on the left by α gives $I_{\mathrm{nat}} = \mathcal{O}_{\mathrm{nat}} \cap \alpha\beta^{-1}\mathcal{O}_{\mathrm{nat}}$. This concludes the proof. □

Corollary 4.3 (Hawk key recovery to $\mathcal{O}_{\mathrm{nat}}$-nrdPIP)**.** *There is a uniform deterministic polynomial-time reduction from Hawk's key-recovery problem to $\mathcal{O}_{\mathrm{nat}}$-nrdPIP. Moreover, the resulting algorithm makes a single oracle call.*

Proof. Let (H, C) be a pair of keys generated by Hawk's key generation algorithm (cf, [8, Algorithm 1]). In particular, the matrix $C \in \mathbf{GL}_2(\mathcal{O}_E)$ satisfies $H = C^*C$ and $\det(C) = 1$. Write $C = (\mathbf{c}_1 \mid \mathbf{c}_2)$, and let $\alpha = \varphi(\mathbf{c}_1)$ and $\beta = \varphi(\mathbf{c}_2)$. Then, using [4, Lemma 3.5], we can compute in polynomial time the quaternion $\gamma = \alpha\beta^{-1} \in A$. Moreover, the reduced norm $q = \mathrm{Nrd}(\alpha)$ equals the top-left coefficient of H, and is therefore public.

By Proposition 4.2, using the element γ, we can compute in polynomial time a pseudo-basis of the right $\mathcal{O}_{\mathrm{nat}}$-ideal $I_{\mathrm{nat}} = \alpha\mathcal{O}_{\mathrm{nat}}$ (seen as an $\mathcal{O}_K$-module of rank 4). Thus, (I_{nat}, q) defines an instance of $\mathcal{O}_{\mathrm{nat}}$-nrdPIP. Let $\widehat{\alpha}$ be a solution returned by the oracle, and set $\widehat{\beta} = \gamma^{-1}\widehat{\alpha}$. As in the final reconstruction step of [4], applying φ^{-1} to $\widehat{\alpha}$ and $\widehat{\beta}$ yields

[11] Note that in full generality, [4, Lemma 3.5] requires a guess on $\det(C)$. However, in our situation, the key generation algorithm in Hawk [8, Algorithm 1] ensures that the secret key C satisfies $\det(C) = 1$.

a valid Gram factorization $\widehat{C}$ of the public Gram matrix. By [23, Lemma 3.12], knowledge of such a factorization is sufficient to forge valid signatures for the corresponding HAWK public key.

If one nevertheless wishes to recover the original factorization C, then C and $\widehat{C}$ differ by an automorphism of $\mathcal{O}_E^2$. By [4, Proposition 3.13], this automorphism group can be enumerated in polynomial time. Consequently, all possible integral factorizations of H, including the secret key C, can be enumerated in polynomial time. □

4.2. **The public ternary instance.** Let us now adapt the reduction from Section 3 to the case of the natural order $\mathcal{O}_{\text{nat}}$. Even though this order is non maximal and so the results of Section 3 do not directly apply, we will be able to use the special properties of this order to obtain a (simpler) reduction for $\mathcal{O}_{\text{nat}}$.

Lemma 4.4. *Let I_{nat} be the ideal constructed in Proposition 4.2. Its left order is*

$$\Lambda_{\text{nat}} := \mathcal{O}_\ell(I_{\text{nat}}) = \alpha \mathcal{O}_{\text{nat}} \alpha^{-1}.$$

Proof. For $x \in \mathcal{A}$, the condition $xI_{\text{nat}} \subseteq I_{\text{nat}}$ is equivalent to $\alpha^{-1} x \alpha \mathcal{O}_{\text{nat}} \subseteq \mathcal{O}_{\text{nat}}$. Since $1 \in \mathcal{O}_{\text{nat}}$, the latter condition holds if and only if $\alpha^{-1} x \alpha \in \mathcal{O}_{\text{nat}}$. Therefore, $\mathcal{O}_\ell(I_{\text{nat}}) = \alpha \mathcal{O}_{\text{nat}} \alpha^{-1}$. □

Definition 4.5. *We now define the trace-zero submodules:*

$$\mathcal{O}_{\text{nat}}^0 := \mathcal{O}_{\text{nat}} \cap \mathcal{A}^0 \qquad \text{and} \qquad \Lambda_{\text{nat}}^0 := \Lambda_{\text{nat}} \cap \mathcal{A}^0.$$

Proposition 4.6. *Conjugation by α restricts to an $\mathcal{O}_K$-linear isometry*

$$c_\alpha : (\mathcal{O}_{\text{nat}}^0, \text{Nrd}) \longrightarrow (\Lambda_{\text{nat}}^0, \text{Nrd}).$$

In particular, $\mathcal{O}_{\text{nat}}^0$ and Λ_{nat}^0 are isomorphic rank-three module lattices over $\mathcal{O}_K$.

Proof. Conjugation by α maps $\mathcal{O}_{\text{nat}}$ onto Λ_{nat} and preserves both reduced trace and reduced norm. It therefore maps $\mathcal{O}_{\text{nat}}^0$ bijectively and isometrically onto Λ_{nat}^0. □

The trace-zero restriction $\mathcal{O}_{\text{nat}}^0$ enjoys the following simple description.

Lemma 4.7. *One has the following decomposition: $\mathcal{O}_{\text{nat}}^0 = \mathcal{O}_K i \oplus \mathcal{O}_E j$.*

Proof. Since $\text{Trd}(a + bj) = a + \overline{a}$, an element $a + bj \in \mathcal{O}_{\text{nat}}$ has reduced trace zero if and only if $a \in Ki$. Moreover, since $i \in \mathcal{O}_E^\times$, one has $\mathcal{O}_E \cap Ki = \mathcal{O}_K i$. Indeed, if $ai \in \mathcal{O}_E \cap Ki$ with $a \in K$, then $a = -i(ai) \in \mathcal{O}_E \cap K = \mathcal{O}_K$. Consequently, $\mathcal{O}_{\text{nat}}^0 = \mathcal{O}_K i \oplus \mathcal{O}_E j$ as was to be proved. □

We now investigate the geometry of $\mathcal{O}_{\text{nat}}^0$ when seen as a Euclidean lattice. To do so, we endow $\mathcal{A}$ with the rational quadratic form $T_{\mathcal{A}/\mathbb{Q}} := \text{Tr}_{K/\mathbb{Q}} \circ \text{Nrd}$ (which corresponds to the standard canonical embedding when $\mathcal{A}$ is mapped to K^4 via ψ). The following proposition gives a fully explicit orthogonal $\mathbb{Z}$-basis of the trace-zero lattice $(\mathcal{O}_{\text{nat}}^0, T_{\mathcal{A}/\mathbb{Q}})$.

Proposition 4.8. *Let $d = m/4$ be the degree of the totally real field K. For $1 \leq s < d$, set $u_s = \zeta_m^s + \zeta_m^{2d-s}$. Then the two families*

$$\mathcal{B}_{\text{short}} := \{i\} \cup \{\zeta_m^a j \,|\, 0 \leq a < 2d\} \qquad \text{and} \qquad \mathcal{B}_{\text{long}} := \{u_s \,|\, 1 \leq s < d\},$$

together form an orthogonal $\mathbb{Z}$-basis of $\mathcal{O}_{\text{nat}}^0$. With respect to $T_{\mathcal{A}/\mathbb{Q}}$, the vectors in $\mathcal{B}_{\text{short}}$ have squared norm d, whereas those in $\mathcal{B}_{\text{long}}$ have squared norm $2d$. Consequently, there is an isometry of quadratic $\mathbb{Z}$-lattices

$$(\mathcal{O}_{\text{nat}}^0, T_{\mathcal{A}/\mathbb{Q}}) \simeq \sqrt{d}\,\mathbb{Z}^{2d+1} \perp \sqrt{2d}\,\mathbb{Z}^{d-1}. \tag{3}$$

The same assertions hold for $(\Lambda_{\text{nat}}^0, T_{\mathcal{A}/\mathbb{Q}})$, with the families $c_\alpha(\mathcal{B}_{\text{short}})$ and $c_\alpha(\mathcal{B}_{\text{long}})$.

Proof. Recall that $m = 4d$, so that $\zeta_m^{2d} = -1$ and $i = \zeta_m^d$. We start by computing a $\mathbb{Z}$-basis for the first summand $\mathcal{O}_K i$ of $\mathcal{O}_{\text{nat}}$ (see Lemma 4.7). The ring $\mathcal{O}_K$ has the standard $\mathbb{Z}$-basis $\{1\} \cup \{\zeta_m^t + \zeta_m^{-t} : 1 \le t < d\}$; see [33, Proposition 2.16]. Multiplication by i therefore gives a $\mathbb{Z}$-basis of $\mathcal{O}_K i$. For $1 \le t < d$, one has:

$$i(\zeta_m^t + \zeta_m^{-t}) = \zeta_m^{d+t} + \zeta_m^{d-t} = u_{d-t}.$$

Thus, $\{i, u_1, \dots, u_{d-1}\}$ is a $\mathbb{Z}$-basis of $\mathcal{O}_K i$.

On the component $\mathcal{O}_E j$, the polar form associated with $T_{\mathcal{A}/\mathbb{Q}}$ is $\langle x, y\rangle = \frac{1}{2}\text{Tr}_{E/\mathbb{Q}}(x\overline{y})$. In particular, for any $0 \le a, b < 2d$, one has $\langle \zeta_m^a j, \zeta_m^b j\rangle = \frac{1}{2}\text{Tr}_{E/\mathbb{Q}}(\zeta_m^{a-b})$. Since m is a power of two, this quantity vanishes when $a \ne b$ and is equal to d when $a = b$. Hence the basis $\{j, \zeta_m j, \dots, \zeta_m^{2d-1} j\}$ is orthogonal, and each of its elements has squared norm d.

It also follows that each $u_s = \zeta_m^s + \zeta_m^{2d-s}$ is the sum of two distinct orthogonal basis elements and therefore has squared norm $2d$. Moreover, the vectors $\{i, u_1, \dots, u_{d-1}\}$ are pairwise orthogonal. Since the decomposition $\mathcal{O}_{\text{nat}}^0 = \mathcal{O}_K i \oplus \mathcal{O}_E j$ is orthogonal for $T_{\mathcal{A}/\mathbb{Q}}$, this proves the claimed basis and orthogonal decomposition for $\mathcal{O}_{\text{nat}}$.

Conjugation by α preserves $T_{\mathcal{A}/\mathbb{Q}}$ and maps $\mathcal{O}_{\text{nat}}^0$ onto Λ_{nat}^0. Therefore, conjugating the two families of vectors by α gives the corresponding orthogonal basis of Λ_{nat}^0. □

4.3. **Recovery from shortest vectors.** Unlike the approach of Section 3.2, the following method does not require computing any isometry between $\mathcal{O}_{\text{nat}}^0$ and Λ_{nat}^0. Instead, it relies only on computing the shortest vectors of Λ_{nat}^0. By Lemma 4.10, these are precisely the conjugates by α of the explicitly known shortest vectors of $\mathcal{O}_{\text{nat}}^0$. Although this description does not provide an algorithm for computing them, since α is secret, the pair $\{\pm\alpha i\alpha^{-1}\}$ can be fully characterized; see Lemma 4.11.

Consequently, once all the shortest vectors of Λ_{nat}^0 have been computed (those of Euclidean norm $\sqrt{d}$), the element $\alpha i\alpha^{-1}$ can be identified up to sign. Lemma 4.12 then allows us to compute either αE or $\alpha j E$. Finally, a solution $\widehat{\alpha}$ to the original $\mathcal{O}_{\text{nat}}$-nrdPIP instance (I_{nat}, q) is obtained using a call to the Gentry–Szydlo algorithm in E (see Lemma 2.15). The full reduction algorithm is proven in Theorem 4.13.

Remark 4.9. The argument using the normalizer of $\mathcal{O}$ that we used in the previous section does not apply here. Indeed, for the non-maximal order $\mathcal{O}_{\text{nat}}$, the corresponding description its normalizer does not hold anymore. To see this, consider the element $1+\zeta_m$: it normalizes $\mathcal{O}_{\text{nat}}$ but it does not belong to $K^\times \mathcal{O}_{\text{nat}}^\times$.

Lemma 4.10. *The minimal vectors of $(\Lambda_{\text{nat}}^0, T_{\mathcal{A}/\mathbb{Q}})$ are precisely $c_\alpha(\mathcal{B}_{\text{short}}) \cup -c_\alpha(\mathcal{B}_{\text{short}})$.*

Proof. By Proposition 4.8, the minimal vectors of $(\mathcal{O}_{\text{nat}}^0, T_{\mathcal{A}/\mathbb{Q}})$ are exactly the elements of $\mathcal{B}_{\text{short}} \cup (-\mathcal{B}_{\text{short}})$. Since conjugation by α induces an isometry from $(\mathcal{O}_{\text{nat}}^0, \text{Nrd})$ onto $(\Lambda_{\text{nat}}^0, \text{Nrd})$, this concludes the proof. □

Lemma 4.11. *The only minimal vectors v of $(\Lambda^0_{\mathrm{nat}}, T_{\mathcal{A}/\mathbb{Q}})$ that anticommute with every minimal vector outside $\{v, -v\}$ are $v = \alpha i \alpha^{-1}$ and $v = -\alpha i \alpha^{-1}$.*

Proof. By Lemma 4.10, it is enough to prove the corresponding characterization before conjugation by α, that is, among the minimal vectors of $\mathcal{O}^0_{\mathrm{nat}}$. For every $0 \le a < 2d$, one has $i(\zeta_m^a j) = -(\zeta_m^a j)i$. Hence both i and $-i$ anticommute with every minimal vector outside $\{i, -i\}$. Now let $v = \pm\zeta_m^a j$ for some $0 \le a < 2d$. For $0 \le b < 2d$, one has

$$(\zeta_m^a j)(\zeta_m^b j) = -\zeta_m^{a-b} \qquad \text{and} \qquad (\zeta_m^b j)(\zeta_m^a j) = -\zeta_m^{b-a}.$$

It follows that $\zeta_m^a j$ and $\zeta_m^b j$ anticommute if and only if $b \equiv a + d \pmod{2d}$. Since $d \ge 2$, there exists $b \not\equiv a, a+d \pmod{2d}$. The minimal vector $\zeta_m^b j$ then lies outside $\{v, -v\}$ and does not anticommute with v. Thus, none of the vectors $\pm\zeta_m^a j$ has the required property. The only such minimal vectors of $\mathcal{O}^0_{\mathrm{nat}}$ are therefore i and $-i$. □

Lemma 4.12. *Let $i' = \alpha i \alpha^{-1}$. The solution spaces in $\mathcal{A}$ of the K-linear equations*

$$i'X = Xi \qquad \text{and} \qquad -i'X = Xi$$

are the right E-lines αE and $\alpha j E$, respectively.

Proof. Let $x \in \mathcal{A}$. Then x is a solution of the first equation if and only if

$$\begin{aligned} i'x = xi &\iff \alpha i \alpha^{-1} x = xi \\ &\iff i(\alpha^{-1}x) = (\alpha^{-1}x)i \\ &\iff \alpha^{-1}x \in \mathcal{C}_{\mathcal{A}}(i). \end{aligned}$$

The set $\mathcal{C}_{\mathcal{A}}(i) = \{y \in \mathcal{A} \,|\, yi = iy\}$ is called the centralizer of i in $\mathcal{A}$ and is equal to $K(i) = E$. Indeed, if $z = a + bj \in \mathcal{A}$, with $a, b \in E$, then using $ji = -ij$ gives $zi = iz \iff ai - bij = ai + bij \iff b = 0$. Thus $\mathcal{C}_{\mathcal{A}}(i) = E$ and $x \in \alpha E$, so the solution space of the first equation is αE.

The computation is similar for the second equation. Using $ij = -ji$, one obtains that $-i'x = xi$ if and only if $j^{-1}\alpha^{-1}x \in \mathcal{C}_{\mathcal{A}}(i) = E$. Hence the solution space is $\alpha j E$. □

We now describe our reduction from solving nrdPIP in the natural order $\mathcal{O}_{\mathrm{nat}}$ to computing (all) the shortest vectors of the rank-three $\mathcal{O}_K$-module Λ^0_{nat}.

Algorithm 2 From nrdPIP in $\mathcal{O}_{\mathrm{nat}}$ to computing the shortest vectors of Λ^0_{nat}

Input: A pseudo-basis of I_{nat} over $\mathcal{O}_K$; the reduced norm element q; the set $\mathrm{Min}(\Lambda^0_{\mathrm{nat}})$ of minimal vectors of $(\Lambda^0_{\mathrm{nat}}, T_{\mathcal{A}/\mathbb{Q}})$.
Output: An element $\widehat{\alpha}$ such that $I_{\mathrm{nat}} = \widehat{\alpha}\mathcal{O}_{\mathrm{nat}}$ and $\mathrm{Nrd}(\widehat{\alpha}) = q$.

1: Find $v \in \mathrm{Min}(\Lambda^0_{\mathrm{nat}})$ such that $vw = -wv$ for every $w \in \mathrm{Min}(\Lambda^0_{\mathrm{nat}}) \setminus \{v, -v\}$.
2: Solve the K-linear equation $vX = Xi$. *//c.f., Lemma 4.12.*
3: Fix a non-zero solution δ and compute the fractional $\mathcal{O}_E$-ideal $\mathfrak{a} = (\delta^{-1} I_{\mathrm{nat}}) \cap E$.
4: Set $r \leftarrow q/\mathrm{Nrd}(\delta)$.
5: Run `GentrySzydlo` on $(\mathfrak{a}, r)$ and let h be the output.*//c.f., Lemma 2.15.*
6: **return** $\widehat{\alpha} \leftarrow \delta h$

Theorem 4.13. *On input a pseudo-basis of $I_{\mathrm{nat}} = \alpha\mathcal{O}_{\mathrm{nat}}$, the reduced norm q, and the set $\mathrm{Min}(\Lambda^0_{\mathrm{nat}})$ of all minimal vectors of Λ^0_{nat}, Algorithm 2 computes an element $\widehat{\alpha} \in \mathcal{A}^\times$ which is a solution to the $\mathcal{O}_{\mathrm{nat}}$-nrdPIP instance (I_{nat}, q), that is, $I_{\mathrm{nat}} = \widehat{\alpha}\mathcal{O}_{\mathrm{nat}}$ and $\mathrm{Nrd}(\widehat{\alpha}) = q$. Moreover, it runs in time polynomial in the input size.*

Proof. Correctness. By Lemma 4.11, Step 1 returns one of the two vectors $v = \alpha i\alpha^{-1}$ or $v = -\alpha i\alpha^{-1}$. The equation $vX = Xi$ is a K-linear equation in the four K-coordinates of $X \in \mathcal{A}$. By Lemma 4.12, its solution space is αE when $v = \alpha i\alpha^{-1}$ and αjE when $v = -\alpha i\alpha^{-1}$. Consequently, any non-zero solution may be written

$$\delta = \alpha s e,$$

with $s \in \{1, j\}$ and $e \in E^\times$. Since $s \in \mathcal{O}^\times_{\mathrm{nat}}$, one has $s^{-1}\mathcal{O}_{\mathrm{nat}} = \mathcal{O}_{\mathrm{nat}}$. Thus in both cases, the fractional ideal $\mathfrak{a}$ built at Step 3 is:

$$\delta^{-1}I_{\mathrm{nat}} \cap E = (\alpha s e)^{-1}\alpha\mathcal{O}_{\mathrm{nat}} \cap E = e^{-1}\mathcal{O}_{\mathrm{nat}} \cap E = e^{-1}(\mathcal{O}_E \oplus \mathcal{O}_E j) \cap E = e^{-1}\mathcal{O}_E.$$

Furthermore, the reduced norm of e can be computed as follows:

$$\frac{q}{\mathrm{Nrd}(\delta)} = \frac{\mathrm{Nrd}(\alpha)}{\mathrm{Nrd}(\alpha)\,\mathrm{Nrd}(s)\,\mathrm{Nrd}(e)} = \mathrm{Nrd}(e^{-1}),$$

since $\mathrm{Nrd}(s) = 1$. Thus, $(\mathfrak{a}, q/\mathrm{Nrd}(\delta))$ forms a valid input to the Gentry–Szydlo algorithm. Let h be the returned generator at Step 5. Then, there exists some unit $\varepsilon \in \mathcal{O}_E^\times$ satisfying $\varepsilon\overline{\varepsilon} = 1$ and such that $h = e^{-1}\varepsilon$. Therefore, the algorithm outputs

$$\widehat{\alpha} = \delta h = \alpha s \varepsilon.$$

Moreover, the element $s\varepsilon$ is a norm-one unit of $\mathcal{O}_{\mathrm{nat}}$, thus $\widehat{\alpha}$ satisfies both

$$\widehat{\alpha}\mathcal{O}_{\mathrm{nat}} = \alpha\mathcal{O}_{\mathrm{nat}} = I_{\mathrm{nat}} \qquad \text{and} \qquad \mathrm{Nrd}(\widehat{\alpha}) = \mathrm{Nrd}(\alpha) = q.$$

This concludes the proof of correctness.

Complexity. By Proposition 4.8, the lattice Λ^0_{nat} has $4d + 2 = O(d)$ minimal vectors. Hence Step 1 runs in polynomial time by testing anticommutation between every pair of minimal vectors. Step 2 amounts to solving a linear system over K, while Step 3 consists of standard arithmetic and intersection computations with pseudo-bases. Both are performed in polynomial time. Finally, Step 5 runs in polynomial time by Lemma 2.15. □

Corollary 4.14 ($\mathcal{O}_{\mathrm{nat}}$-nrdPIP to shortest-vector enumeration)**.** *There is a uniform deterministic polynomial-time reduction from $\mathcal{O}_{\mathrm{nat}}$-nrdPIP to the enumeration of all shortest vectors of a public rank-three module lattice over $\mathcal{O}_K$ that is isometric to $(\mathcal{O}^0_{\mathrm{nat}}, \mathrm{Nrd})$. Moreover, the reduction makes a single oracle call.*

Proof. Let (I_{nat}, q) be an instance of $\mathcal{O}_{\mathrm{nat}}$-nrdPIP, with $I_{\mathrm{nat}} = \alpha\mathcal{O}_{\mathrm{nat}}$ and $q = \mathrm{Nrd}(\alpha)$. Lemmas 4.4 and 2.17 compute in polynomial time the left order

$$\Lambda_{\mathrm{nat}} = \mathcal{O}_\ell(I_{\mathrm{nat}}) = \alpha\mathcal{O}_{\mathrm{nat}}\alpha^{-1}.$$

A pseudo-basis of its trace-zero submodule Λ^0_{nat} can then be computed in polynomial time; see Lemma 2.18. By Proposition 4.6, $(\Lambda^0_{\mathrm{nat}}, \mathrm{Nrd})$ is a public rank-three module lattice over $\mathcal{O}_K$ isometric to $(\mathcal{O}^0_{\mathrm{nat}}, \mathrm{Nrd})$. The oracle call returns all $4d + 2$ shortest vectors of the associated $\mathbb{Z}$-lattice $(\Lambda^0_{\mathrm{nat}}, T_{\mathcal{A}/\mathbb{Q}})$. Theorem 4.13 then computes in polynomial time an element $\widehat{\alpha}$ satisfying $I_{\mathrm{nat}} = \widehat{\alpha}\mathcal{O}_{\mathrm{nat}}$ and $\mathrm{Nrd}(\widehat{\alpha}) = q$. All computations outside the oracle call run in deterministic polynomial time. □

We can now prove Theorem 4.1.

Proof of Theorem 4.1. By combining Corollaries 4.3 and 4.14, we obtain a Karp uniform deterministic reduction from Hawk's key recovery to computing the set of minimal vectors of the rank-3 module Λ^0_{nat}. Then Proposition 4.8 gives us the geometric shape of $\mathcal{O}_{\mathrm{nat}}$ (and Λ^0_{nat}) when seen as a lattice. □

5. A rectangular version of Ducas's reduction

After dividing the quadratic form $T_{\mathcal{A}/\mathbb{Q}}$ by d, Proposition 4.8 shows that $(\Lambda^0_{\mathrm{nat}}, T_{\mathcal{A}/\mathbb{Q}}/d)$ is isomorphic to $\mathbb{Z}^{2d+1} \perp \sqrt{2}\,\mathbb{Z}^{d-1}$. This simple geometry structure is the key ingredient in Corollary 5.5, which reduces Hawk's key recovery problem to exact-SVP in dimension at most $3m/8 + 1$. To prove this result, we need to extend Ducas's reduction [6], which says that an orthogonal basis of a rotation of $\mathbb{Z}^n$ can be computed using polynomially many exact-SVP calls in dimension at most $n/2 + 1$. Precisely, we show that this result can be adapt to the rectangular lattices

$$L_{a,b} := \mathbb{Z}^a \perp \sqrt{2}\,\mathbb{Z}^b,$$

where a and b are non-negative integers. We first recall the definition of primitive sublattices and fix standard notation used for lattice reduction.

Definition 5.1. *Let $L \subset \mathbb{R}^n$ be a Euclidean lattice. A sublattice $L' \subseteq L$ is called* primitive *if there exists a sublattice $L'' \subseteq L$ such that $L = L' \oplus L''$.*

For a real subspace V, let $\pi_V^\perp$ denote the orthogonal projection onto $V^\perp$. If $L' \subseteq L$ is a sublattice, we write $\pi_{L'}^\perp := \pi^\perp_{\mathrm{Span}_{\mathbb{R}}(L')}$ and denote by $\pi_{L'}^\perp(L)$ the corresponding projected lattice. We also write $(L')^* := \{x \in \mathrm{Span}_{\mathbb{R}}(L') : \langle x, L'\rangle \subseteq \mathbb{Z}\}$ for the dual lattice of L', and $\mathrm{vol}(L')$ for its covolume in its real span.

Let $B = (\mathbf{b}_0|\cdots|\mathbf{b}_{n-1})$ be a basis of L, and let $(\mathbf{b}_0^*|\cdots|\mathbf{b}_{n-1}^*)$ be its Gram–Schmidt orthogonalization. For $0 \le i \le j < n$, we set

$$\pi_i := \pi^\perp_{\mathrm{Span}_{\mathbb{R}}(\mathbf{b}_0,\ldots,\mathbf{b}_{i-1})} \qquad \text{and} \qquad B_{[i:j]} := \big(\pi_i(\mathbf{b}_i)|\cdots|\pi_i(\mathbf{b}_j)\big).$$

Thus, $B_{[i:j]}$ is a basis of the corresponding projected block. To primal-SVP reduce this block means to make its first vector a shortest non-zero vector of the projected lattice. To dual-SVP reduce it means to SVP reduce its dual basis in reverse order.

Lemma 5.2. *Let L' be a rank-k sublattice of $L_{a,b}$, with $k \le a$. If $\mathrm{vol}(L') = 1$, then L' is generated by k distinct norm-one vectors of the $\mathbb{Z}^a$ summand.*

Proof. Let C be the matrix whose columns form a basis of L', expressed in the canonical orthogonal basis of $L_{a,b}$. Since $L' \subseteq L_{a,b}$ is a sublattice, the coefficients of C are integers. Let C_1 and C_2 denote the submatrices formed by the first a and last b rows of C, respectively. The Gram matrix of C is then $C_1^\mathsf{T} C_1 + 2C_2^\mathsf{T} C_2$. By the Cauchy–Binet formula, we compute the volume of L' as

$$\mathrm{vol}(L')^2 = \sum_{\substack{I \subseteq \{1,\ldots,a+b\} \\ |I| = k}} \det(C_I)^2 \prod_{i \in I} \varepsilon_i,$$

where $\varepsilon_i = 1$ if $i \le a$ and $\varepsilon_i = 2$ otherwise, and C_I denotes the square submatrix of C formed by the rows indexed by I.

Since the expression above is a sum of non-negative integers, the assumption $\mathrm{vol}(L') = 1$ implies that exactly one term is non-zero. Let $C_I \in \mathbf{GL}_k(\mathbb{Z})$ be the unique block such that the minor $\det(C_I)$ is equal to ± 1. In particular, we have $\prod_{i \in I} \varepsilon_i = 1$, so $I \subseteq \{1, \dots, a\}$ and C_I is formed only by rows coming from the $\mathbb{Z}^a$ summand.

We claim that every row of C whose index does not belong to I is zero. Indeed, let $\mathbf{r}$ be such a row and suppose that $\mathbf{r} \neq 0$. Since C_I forms a basis of $\mathbb{Q}^k$, one can express $\mathbf{r}$ as a linear combination of the rows of C_I. Then, at least one coefficient is non-zero, and replacing the corresponding row of C_I by $\mathbf{r}$ then produces another non-zero $k \times k$ minor of C, contradicting the uniqueness of C_I. □

Lemma 5.3. *Let $a \in \mathbb{Z}_{\geq 2}$, and $L' \subset L_{a,b}$ be a primitive sublattice of rank $k < a$, and suppose that $\mathrm{vol}(L') > 1$. Choose $\mathbf{y} \in L_{a,b}$ such that $\pi_{L'}^{\perp}(\mathbf{y})$ is a shortest non-zero vector of $\pi_{L'}^{\perp}(L_{a,b})$, whose norm is denoted by $\mu := \|\pi_{L'}^{\perp}(\mathbf{y})\|$. We define*

$$\widetilde{L} := L' + \mathbb{Z}\mathbf{y} \qquad \text{and} \qquad \lambda := \lambda_1(\widetilde{L}^*).$$

Then, $\widetilde{L} \subseteq L_{a,b}$ is a primitive sublattice and $\mu\lambda \leq \sqrt{1 - 1/a}$.

Proof. By definition, there exists a sublattice $L'' \subset L_{a,b}$ such that $L_{a,b} = L' \oplus L''$. Hence, $\pi_{L'}^{\perp}(L_{a,b}) = \pi_{L'}^{\perp}(L'')$. Moreover, the restriction of $\pi_{L'}^{\perp}$ to L'' is injective. Indeed, an element of $\mathrm{Span}_{\mathbb{R}}(L'')$ whose projection vanishes belongs to $\mathrm{Span}_{\mathbb{R}}(L')$, and these two subspaces have trivial intersection. Therefore, the image under $\pi_{L'}^{\perp}$ of a basis of L'' is a basis of the real space $\mathrm{Span}_{\mathbb{R}}(L')^{\perp}$, and $\pi_{L'}^{\perp}(L_{a,b})$ is a lattice in this space. Its shortest non-zero vectors are primitive, and it follows that $\widetilde{L} \subseteq L$ is a primitive sublattice too.

Since $k < a$ by assumption, the span of L' cannot contain all the norm-one vectors of the summand $\mathbb{Z}^a$. Projecting one which is not in this span then gives a non-zero vector of $\pi_{L'}^{\perp}(L_{a,b})$ of norm at most one. Thus, we proved the inequality $\mu \leq 1$.

Suppose first that $\mathrm{Span}_{\mathbb{R}}(\widetilde{L})$ is not contained in the subspace $\mathbb{R}^a$. Then some vector $\mathbf{e}$ of the canonical orthogonal basis of $\sqrt{2}\,\mathbb{Z}^b$ has a non-zero orthogonal projection onto $\mathrm{Span}_{\mathbb{R}}(\widetilde{L})$. Observe that the vector $\mathbf{e}/2$ belongs to $L_{a,b}^*$ and has norm $1/\sqrt{2}$. Let $\mathbf{z}$ denote its orthogonal projection onto $\mathrm{Span}_{\mathbb{R}}(\widetilde{L})$. Then $\mathbf{z}$ belongs to $\widetilde{L}^*$, since for every $\mathbf{x} \in \widetilde{L}$, one has $\langle \mathbf{z}, \mathbf{x} \rangle = \langle \mathbf{e}/2, \mathbf{x} \rangle \in \mathbb{Z}$. Consequently, $\lambda \leq 1/\sqrt{2}$ and we obtain

$$\mu\lambda \leq 1/\sqrt{2} \leq \sqrt{1 - 1/a}.$$

Suppose now that $\mathrm{Span}_{\mathbb{R}}(\widetilde{L})$ is contained in $\mathbb{R}^a$. Then $\widetilde{L} \subseteq \mathbb{Z}^a$ and L' is primitive in $\mathbb{Z}^a$. By assumption, $\mathrm{vol}(L') > 1$ so [6, Lemma 4] ensures the existence of a non-zero vector of $\pi_{L'}^{\perp}(\mathbb{Z}^a)$ of norm at most $\sqrt{1 - 1/a}$. Since $\mathbf{y}$ was chosen by minimizing over the larger projected lattice $\pi_{L'}^{\perp}(L_{a,b})$, it follows that $\mu \leq \sqrt{1 - 1/a}$. Fix a norm-one vector of $\mathbb{Z}^a$ whose orthogonal projection onto $\mathrm{Span}_{\mathbb{R}}(\widetilde{L})$ is non-zero. As above in the first case, this projection is a non-zero vector of $\widetilde{L}^*$ and has norm at most one. Thus $\lambda \leq 1$, which proves the claim in this case and concludes the proof. □

Theorem 5.4 (Rectangular version of Ducas's reduction)**.** *Let $a \in \mathbb{Z}_{\geq 2}$ and $b \in \mathbb{Z}_{\geq 0}$, set $n = a + b$, and let $k \in \{1, \dots, a - 1\}$. There is an algorithm that, given a basis of a Euclidean lattice isomorphic to $L_{a,b}$, outputs an orthogonal basis of this lattice. The algorithm makes polynomially many exact-SVP calls on lattices of dimension at most $\max\{k+1, n-k\}$, and all remaining operations run in polynomial time in the input size.*

Proof. Since all properties used in the analysis are invariant under orthogonal transformations, we may assume without loss of generality that the input lattice is $L_{a,b}$. After applying LLL, we may also assume that the input basis $B = (\mathbf{b}_0|\cdots|\mathbf{b}_{n-1})$ is LLL-reduced. We let L' be the primitive sublattice generated by the k first vectors. While $\mathrm{vol}(L') > 1$, the algorithm performs the following operations:

(1) primal-SVP reduce the block $B_{[k:n-1]}$;
(2) dual-SVP reduce the block $B_{[0:k]}$;
(3) size-reduce the resulting basis.

After the primal operation, $\pi_{L'}^{\perp}(\mathbf{b}_k)$ is a shortest non-zero vector of $\pi_{L'}^{\perp}(L_{a,b})$. Let $\mu = \|\pi_{L'}^{\perp}(\mathbf{b}_k)\|$ be its norm, and set $\widetilde{L} = L' + \mathbb{Z}\mathbf{b}_k$ and $\lambda = \lambda_1(\widetilde{L}^*)$. By Lemma 5.3, $\widetilde{L}$ is a primitive sublattice of $L_{a,b}$. Moreover, one has

$$\mathrm{vol}(\widetilde{L}) = \mathrm{vol}(L')\mu.$$

Indeed, if $(\mathbf{c}_1, \ldots, \mathbf{c}_k)$ is a basis of L', then $(\mathbf{c}_1, \ldots, \mathbf{c}_k, \mathbf{b}_k)$ is a basis of $\widetilde{L}$, and its last Gram–Schmidt vector is $\pi_{L'}^{\perp}(\mathbf{b}_k)$.

The dual-SVP operation outputs a basis of $\widetilde{L}$ for which the last vector of the corresponding dual basis is a shortest vector of $\widetilde{L}^*$, and therefore has norm λ. Equivalently, the last Gram–Schmidt vector of the primal basis has norm $1/\lambda$. If L'' denotes the sublattice generated by the new first k vectors, the same argument as above shows

$$\mathrm{vol}(L'') = \mathrm{vol}(\widetilde{L})\lambda = \mathrm{vol}(L')\mu\lambda.$$

Since L'' is generated by a subset of a basis of the primitive sublattice $\widetilde{L}$, it is itself primitive in $\widetilde{L}$ and thus in $L_{a,b}$. In particular, Lemma 5.3 gives

$$\mathrm{vol}(L'') \le \rho\,\mathrm{vol}(L'),$$

where $\rho = \sqrt{1 - 1/a}$. At the end of the iteration, the algorithm replaces L' by L''.

By the Cauchy–Binet formula used in the proof of Lemma 5.2, the squared volume of every sublattice of $L_{a,b}$ is a positive integer. In particular, the volume of L' is always at least one. Let V denote the volume of L' at the first iteration. Since the volume of L' decreases at each iteration by the multiplicative factor ρ, it is enough to prove that the number of iterations $\lceil -\log V/\log\rho \rceil$ is polynomially bounded.

First, the standard inequality $-\log(1-x) \ge x$ gives

$$-\log\rho = -\frac{1}{2}\log\left(1 - \frac{1}{a}\right) \ge \frac{1}{2a}.$$

For $\log V$, recall that at the first iteration L' is generated by the first k vectors $\mathbf{b}_0, \ldots, \mathbf{b}_{k-1}$ of the LLL-reduced basis B. By Hadamard's inequality, $V \le \prod_{i=0}^{k-1} \|\mathbf{b}_i\|$, and hence

$$\log V \le \sum_{i=0}^{k-1} \log\|\mathbf{b}_i\|$$

is polynomially bounded. This proves the claim on the number of iterations. Moreover, size reduction is used after each iteration to control the lengths of the intermediate bases, exactly as in the original argument of [6].

After the last iteration, $\mathrm{vol}(L') = 1$ and Lemma 5.2 ensures that L' is generated by k norm-one vectors of the canonical basis of $\mathbb{Z}^a$. In particular, L' is isomorphic to $\mathbb{Z}^k$.

This orthogonal basis is computed by HKZ reduction; the orthogonal projection along any such vector yields a lattice isomorphic to $\mathbb{Z}^{k-1}$, so this step is recursive.

Since the final L' is generated by k vectors of the canonical basis of $\mathbb{Z}^a$, the orthogonal projection $\pi_{L'}^{\perp}(L_{a,b})$ is isomorphic to

$$L_{a-k,b} = \mathbb{Z}^{a-k} \perp \sqrt{2}\,\mathbb{Z}^b.$$

Moreover, $k < a$ so this lattice contains norm-one vectors, which are precisely the vectors of the canonical basis belonging to the $\mathbb{Z}^{a-k}$ summand. Successive HKZ reduction therefore computes all these $a-k$ vectors. After projecting them out, the remaining lattice is isomorphic to $\sqrt{2}\,\mathbb{Z}^b$, and an HKZ reduction recovers an orthogonal basis of vectors of norm $\sqrt{2}$. This gives the desired orthogonal basis of the input lattice.

Each primal-SVP call is made in dimension $n-k$, while each dual-SVP call is made in dimension $k+1$. Moreover, the final HKZ reductions use exact-SVP calls in dimensions at most k and $n-k$, respectively. We proved that the main loop has polynomially many iterations, and the two final HKZ reductions make at most n exact-SVP calls in total. Hence the total number of exact-SVP calls is polynomial, and their dimension is at most $\max\{k+1, n-k\}$. All remaining operations, including LLL reduction, size reduction, orthogonal projection, dualization, and basis transformations, run in polynomial time in the input size. □

We now apply the preceding result to the public trace-zero lattice arising from Hawk. Theorem 4.1 provides exactly the rectangular structure required for composing with Theorem 5.4. Combining both results yields the reduction from Hawk's key recovery problem to SVP in dimension at most $3m/8+1$.

Corollary 5.5 (Hawk key recovery to SVP in dimension $3m/8+1$)**.** *There is a deterministic polynomial-time reduction from Hawk's key-recovery problem to polynomially many exact-SVP in dimension at most* $3m/8+1$.

Proof. Starting from the public Hawk key, Theorem 4.1 reduces the key recovery problem to the problem of computing the set of all minimal vectors of a lattice Λ^0_{nat} isomorphic to

$$L_{2d+1,d-1} = \mathbb{Z}^{2d+1} \perp \sqrt{2}\,\mathbb{Z}^{d-1},$$

which has rank $3d$ over $\mathbb{Z}$. Since d is even, we may apply Theorem 5.4 with $a = 2d+1$, $b = d-1$, and $k = 3d/2$. The largest dimension of an exact-SVP call is then

$$\max\left\{\frac{3d}{2}+1, \frac{3d}{2}\right\} = \frac{3d}{2}+1 = \frac{3m}{8}+1.$$

The algorithm then returns an orthogonal basis of Λ^0_{nat}. Its $2d+1$ norm-one vectors, together with their opposites, form the set $\mathrm{Min}(\Lambda^0_{\mathrm{nat}})$ of minimal vectors of (the scaled lattice) Λ^0_{nat}. From these minimal vectors, the reduction then recovers the secret Hawk's key in polynomial time. Apart from the exact-SVP calls, the algorithm run in polynomial time in the input size. □

6. Implementation of the attack

We made a toy implementation of the second stage of the attack in SageMath [27]. More precisely, our implementation starts with a $\mathbb{Z}$-basis of the order $\Lambda_{\mathrm{nat}} = \alpha\mathcal{O}_{\mathrm{nat}}\alpha^{-1}$,

where $\mathcal{O}_{\text{nat}}$ is the natural order $\mathcal{O}_{\text{nat}} = \mathcal{O}_E \oplus \mathcal{O}_E j$ and $\alpha \in \mathcal{O}_{\text{nat}}$ is a secret element that we want to recover (see Section 4). Our code is available at https://plmlab.math.cnrs.fr/apelletm/attack_hawk-trace-zero.

6.1. **Description of the implementation.** Our implementation differs slightly from the algorithm described in Section 4. First, in order to avoid working with pseudo-bases, all our objects (orders, modules, ideals, ...) are represented by $\mathbb{Z}$-bases. Our implementation starts by computing a $\mathbb{Z}$-basis of the rank-3 module Λ^0_{nat} by intersecting $\mathcal{O}_{\text{nat}}$ with the subspace $\mathcal{A}^0 = \{x \in \mathcal{A} \mid \text{Trd}(x) = 0\}$. We then run lattice reduction on Λ^0_{nat} until we recover an orthogonal basis of it with $2d+1$ vectors of norm 1 and $d-1$ vectors of norm $\sqrt{2}$.

We then proceed to identify the element $\pm\alpha i\alpha^{-1}$. Here, our approach differs slightly from Lemma 4.11. Instead of using the fact that $\pm\alpha i\alpha^{-1}$ are the only norm 1 vectors that anti-commute with all the other norm 1 vectors, we use the fact that $\pm\alpha i\alpha^{-1}$ commutes with any vector of norm $\sqrt{2}$, and that is the unique norme 1 vector with this property. This is slightly more efficient to test in practice, even though it means that we need to compute not only the minimal vectors of Λ^0_{nat} but also at least one vector of norm $\sqrt{2}$.

From there, our algorithm differs more significantly from the one described in Section 4. Recall from Section 4 that once $i' = \alpha i\alpha^{-1}$ has been identified (up to sign), we solve the K-linear equation $i'X = Xi$. This equation has 4 unknowns over K, but the rank of the associated matrix over K is only 2. This means that the space of solutions is a K-vector space of dimension 2 (and indeed, we proved in Lemma 4.12 that using this equation, we are able to recover α only up to an element of E, which has rank 2 over K). This forces us to run the `GentrySzydlo` algorithm in E to conclude the attack. While this is theoretically polynomial time, this is quite costly in practice. In order to avoid the call to the `GentrySzydlo` algorithm, we decided in our implementation to collect a second relation $j' = \alpha j\alpha^{-1}$. We then solve the system formed by the two equations $i'X = Xi$ and $j'X = Xj$ and we can now prove that this system has rank 3 over K. This means that any non-zero solution to this system is of the form αx for some x in $K^\times$ (note the difference, when using only one equation we recovered αx for some $x \in E^\times$). In order to obtain the element $j' = \alpha j\alpha^{-1}$ needed in our second equation, we simply enumerate all the element of norm 1 that we have computed in Λ^0_{nat}: we know that j' will be among these elements of norm 1.

Finally, once we recover $\beta := \alpha x$ for some x in $K^\times$, we use the knowledge of $q = \text{Nrd}(\alpha)$ to get rid of the factor x. More precisely, we compute $r := \text{Nrd}(\beta)/q = x^2$, and then computes a square root λ of r in K. We then return the element $\beta \cdot \lambda^{-1}$. If our guess for j' is incorrect, the element r will not be a square in K and we will be able to detect it here. Otherwise, we recover an element $\alpha' = \alpha \cdot \mu$ where $\mu \in \mathcal{O}^\times$ is a unit of reduced norm 1. I.e., we recover a solution to the nrdPIP instance.

6.2. **Tests and results.** We tested our implementation on a personal laptop using SageMath 10.5., and as follows. For each test, we generated a random secret α in $\mathcal{O}_E \oplus \mathcal{O}_E j$ by choosing its coefficients (in the $\mathbb{Z}$-basis $\{\zeta_m^i\}_{0 \le i \le m/2}$ of $\mathcal{O}_E$) uniformly random in the set $\{-2, -1, 0, 1\}$. We then computed the HNF basis of the order $\Lambda_{\text{nat}} = \alpha\mathcal{O}_{\text{nat}}\alpha^{-1}$ which we provided to the attacker.

Up to $m = 64$, our implementation succeeds on all inputs in a bit less than 2 seconds, by running the LLL algorithm on Λ^0_{nat}. For $m = 128$, our implementation succeeds on

all inputs in roughly 20 seconds, by running the BKZ algorithm with block-size 5 on Λ^0_{nat}. For $m = 256$, our implementation succeeded on some inputs within approximately 2 hours, by running the BKZ algorithm with block-size 30 on Λ^0_{nat} (which has rank 192 over $\mathbb{Z}$). In this last case ($m = 256$), the sage implementation of the BKZ algorithm sometimes failed with a `RuntimeError`. When the error did not occur, block-size 30 seemed sufficient to recover the secret α.[12] In order to minimize the failure probability, we also tried to sample α with smaller coefficients (in $\{-1, 0\}$) and/or we generated multiple α's and kept only the one minimizing $\mathrm{N}_{K/\mathbb{Q}}(\mathrm{Nrd}(\alpha))$. This seemed to help for the BKZ algorithm.

Summing up, our toy implementation gives a complementary validation that our reduction is correct (this is is a sanity check that the proofs from the above sections should be correct). When the implementation failed in conductor $m = 256$, this was not because the reduction computed an incorrect solution, but because we did not have enough computational power to compute an HKZ reduced basis of the lattice Λ^0_{nat}.

[12] Out of 10 tests, 3 succeeded with blocksize 30, and 7 failed with a `RuntimeError` during the BKZ phase.

References

[1] Bill Allombert, Alice Pellet-Mary, and Wessel van Woerden. Cryptanalysis of rank-2 module-lip: a single real embedding is all it takes. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 184–212. Springer, 2025.

[2] Huck Bennett, Atul Ganju, Pura Peetathawatchai, and Noah Stephens-Davidowitz. Just how hard are rotations of $\mathbb{Z}^n$? algorithms and cryptography with the simplest lattice. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 252–281. Springer, 2023.

[3] Clémence Chevignard and Guilhem Mureau. Ideally hawkward: How not to break module-lip. *Cryptology ePrint Archive*, 2025.

[4] Clémence Chevignard, Guilhem Mureau, Thomas Espitau, Alice Pellet-Mary, Heorhii Pliatsok, and Alexandre Wallet. 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*, pages 154–183. Springer, 2025.

[5] Henri Cohen. *Advanced topics in computational number theory*, volume 193. Springer Science & Business Media, 2012.

[6] Léo Ducas. Provable lattice reduction of $\mathcal{F}^n$ with blocksize $n/2$. Cryptology ePrint Archive, Paper 2023/447, 2023.

[7] Léo Ducas and Shane Gibbons. Hull attacks on the lattice isomorphism problem. In Alexandra Boldyreva and Vladimir Kolesnikov, editors, *Public-Key Cryptography - PKC 2023 - 26th IACR International Conference on Practice and Theory of Public-Key Cryptography, Atlanta, GA, USA, May 7-10, 2023, Proceedings, Part I*, volume 13940 of *Lecture Notes in Computer Science*, pages 177–204. Springer, 2023.

[8] Léo Ducas, Eamonn W Postlethwaite, Ludo N Pulles, and Wessel van Woerden. Hawk: Module lip makes lattice signatures fast, compact and simple. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 65–94. Springer, 2022.

[9] Léo Ducas and Wessel van Woerden. On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 643–673. Springer, 2022.

[10] David S Dummit. A note on the equivalence of the parity of class numbers and the signature ranks of units in cyclotomic fields. *Nagoya Mathematical Journal*, 238:206–214, 2020.

[11] Mathieu Dutour Sikirić, Anna Haensch, John Voight, and Wessel P. J. van Woerden. A canonical form for positive definite matrices. In *Fourteenth Algorithmic Number Theory Symposium*, volume 4 of *The Open Book Series*, pages 179–195. Mathematical Sciences Publishers, 2020.

[12] Craig Gentry and Michael Szydlo. Cryptanalysis of the revised NTRU signature scheme. In Lars R. Knudsen, editor, *Advances in Cryptology - EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, April 28 - May 2, 2002, Proceedings*, volume 2332 of *Lecture Notes in Computer Science*, pages 299–320. Springer, 2002.

[13] Morgane Guerreau and Mélissa Rossi. A not so discrete sampler: power analysis attacks on hawk signature scheme. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2024(4):156–178, 2024.

[14] Ishay Haviv and Oded Regev. On the lattice isomorphism problem. In *Proceedings of the twenty-fifth annual ACM-SIAM symposium on Discrete algorithms*, pages 391–404. SIAM, 2014.

[15] Markus Kirschmer, Cong Ling, and Ali Sadreddin. Cryptanalysis of definite and indefinite lattice isomorphism problems with applications to hawk and defi. *Cryptology ePrint Archive*, 2026.

[16] Arjen K Lenstra. Factoring polynomials over algebraic number fields. *Computer Algebra. EUROCAL'83*, pages 245–254, 1983.

[17] Hendrik W Lenstra Jr and Alice Silverberg. Testing isomorphism of lattices over cm-orders. *SIAM Journal on Computing*, 48(4):1300–1334, 2019.

[18] Hengyi Luo. Adjoint-lattice reduction for the hawk gram-factor problem, 2026.

[19] Hengyi Luo, Kaijie Jiang, Yanbin Pan, and Anyu Wang. Cryptanalysis of rank-2 module-lip with symplectic automorphisms. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 359–385. Springer, 2024.

[20] Ming-Xing Luo. Module lattice security (part i): Unconditional verification of weber's conjecture for $k \leq 12$. *arXiv preprint arXiv:2604.15858*, 2026.
[21] Daniele Micciancio and Shafi Goldwasser. *Complexity of lattice problems: a cryptographic perspective*, volume 671. Springer Science & Business Media, 2002.
[22] Guilhem Mureau. Special genera of hermitian lattices and applications to hawk. In *Theory of Cryptography Conference*, pages 289–317. Springer, 2025.
[23] Guilhem Mureau, Alice Pellet-Mary, Georgii Pliatsok, and Alexandre Wallet. Cryptanalysis of rank-2 module-lip in totally real number fields. In Marc Joye and Gregor Leander, editors, *Advances in Cryptology - EUROCRYPT 2024 - 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26-30, 2024, Proceedings, Part VI*, volume 14656 of *Lecture Notes in Computer Science*, pages 226–255. Springer, 2024.
[24] Wilhelm Plesken and Bernd Souvignier. Computing isometries of lattices. *Journal of Symbolic Computation*, 24(3-4):327–334, 1997.
[25] Zygimantas Straznickas and Stephen A. Weis. Hawk-n key recovery reduces to svp in dimension n/2 + 1, 2026.
[26] Michael Szydlo. Hypercubic lattice reduction and analysis of GGH and NTRU signatures. In Eli Biham, editor, *Advances in Cryptology - EUROCRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4-8, 2003, Proceedings*, volume 2656 of *Lecture Notes in Computer Science*, pages 433–448. Springer, 2003.
[27] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version x.y.z)*, YYYY. `https://www.sagemath.org`.
[28] Daniël van Gent and Wessel van Woerden. A search to distinguish reduction for the isomorphism problem on direct sum lattices. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 3–33. Springer, 2025.
[29] Daniël MH van Gent. A note on the genus of the hawk lattice. *Cryptology ePrint Archive*, 2025.
[30] Daniël MH van Gent and Ludo N Pulles. Hawk: Having automorphisms weakens key. *IACR Cryptol. ePrint Arch.*, 2025:928, 2025.
[31] Wessel van Woerden. Dense and smooth lattices in any genus. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 386–417. Springer, 2024.
[32] John Voight. *Quaternion algebras*. Springer, 2021.
[33] Lawrence C Washington. *Introduction to cyclotomic fields*, volume 83. Springer Science & Business Media, 2012.

Univ Bordeaux, CNRS, Inria, Bordeaux INP, IMB, UMR 5251, Talence, France
Email address: `guilhem.mureau@math.u-bordeaux.fr`

Univ Bordeaux, CNRS, Inria, Bordeaux INP, IMB, UMR 5251, Talence, France
Email address: `alice.pellet-mary@math.u-bordeaux.fr`