Ideally HAWKward: How *Not* to Break Module-LIP

Clémence Chevignard[1] and Guilhem Mureau[2]

[1] Univ Rennes, Inria, CNRS, Irisa, UMR 6074, France
clemence.chevignard@inria.fr
[2] Univ Bordeaux, CNRS, Inria, Bordeaux INP, IMB, UMR 5251, Talence, France
guilhem.mureau@math.u-bordeaux.fr

Abstract. The module-Lattice Isomorphism Problem (module-LIP) was introduced by Ducas et al. in [2], and used within the signature scheme and NIST candidate HAWK. In [6] it was pointed out that over certain number fields F, the problem can be reduced to enumerating solutions of $x^2 + y^2 = q$ (where $q \in \mathcal{O}_F$ is given and $x, y \in \mathcal{O}_F$ are the unknowns). Moreover one can always reduce to a similar equation which has only *few* solutions. This key insight led to a heuristic polynomial-time algorithm for solving module-LIP on those specific instances. Yet this result doesn't threaten HAWK for which the problem can be reduced to enumerating solutions of $x^2+y^2+z^2+t^2 = q$ (where $q \in \mathcal{O}_F$ is given and $x, y, z, t \in \mathcal{O}_F$ are the unknowns). We show that, in all likelihood, solving this equation requires the enumeration of a *too large* set to be feasible, thereby making irrelevant a straightforward adaptation of the approach in [6].

In [6], the authors proposed a heuristic and polynomial-time algorithm for solving certain instances of the module-Lattice Isomorphism Problem (module-LIP). Nonetheless, this algorithm does not affect the signature scheme HAWK [2], whose security is related to the hardness of module-LIP for a specific instance, not covered by the aforementionned attack. In this short note, we highlight one of the reasons why the techniques used in [6] do not apply to HAWK. Specifically, the approach in [6] relies at some point on enumerating *all ideals* of a given relative norm. In this context, a randomization argument ensures, with high probability, that only a small number of such ideals exist. Moreover, the Kummer-Dedekind theorem provides a way to compute bases for these ideals.

However, in the case of HAWK, we show that a naive adaptation of the same argument would, in most cases, require enumerating an unfeasibly large number of ideals, thereby making the attack impractical. In addition to this obstacle, the lack of a formula —like the one provided by the Kummer-Dedekind theorem in the previous setting— further complicates the situation. Ultimately, the existence of an efficient algorithm for computing generators of ideals with prescribed norm was a central result in [6], but this no longer holds for HAWK. In what follows, we focus on the first point, namely the counting argument.

Despite these complications, we highlight that [1] overcomes two out of the three issues. Indeed, they show that a single ideal is sufficient, and moreover, that

it can be entirely recovered from the input of the problem, see [1, Theorem 3.15]. However, the problem of efficiently computing a generator for the ideal remains unresolved, which prevents them from giving an efficient attack on HAWK.

1 HAWK and sums of squares

Definitions. Let K be a *cyclotomic* number field of conductor $2m$, where $m = 2^e$ for some $e \in \mathbb{Z}_{>0}$. That is, $K = \mathbb{Q}[X]/(X^m+1)$. The *ring of integers* of K is given by $\mathcal{O}_K := \mathbb{Z}[X]/(X^m+1) \subset K$. Each complex root ζ of X^m+1 defines a *complex embedding* $\sigma : K \to \mathbb{C}$, a field homomorphism defined by $\sigma(X) = \zeta$. The *absolute norm* of an element $x \in K$ is defined as the rational integer $N_{K/\mathbb{Q}}(x) := \prod_\sigma \sigma(x)$, where the product runs over all m complex embeddings of K.

In addition, K admits an automorphism $\overline{\cdot} : K \to K$ called *complex conjugation*, defined by sending X to to its inverse in K, which is equal to $-X^{m-1}$. For a matrix $B \in \mathcal{M}_n(K)$, we define its *complex-conjugate transpose* as $B^* := \overline{B}^T$.

Given these definitions, the underlying instance of the module-LIP problem in HAWK can be stated as follows. More precisely, the problem below corresponds to the problem of secret key recovery in HAWK.

Definition 1.1 (Key recovery in HAWK). *Consider $B \in \mathbf{GL}_2(\mathcal{O}_K)$ and set $G := B^*B$. Given as input G, the problem asks to compute any $C \in \mathbf{GL}_2(\mathcal{O}_K)$ such that $C^*C = G$.*

To understand the approach taken in [6], we need first to unpack the previous definition. To that end, let us denote the input of HAWK by $G = \begin{pmatrix} q_1 & q_2 \\ \overline{q_2} & q_3 \end{pmatrix}$,[3] and a solution by $C = \begin{pmatrix} x & z \\ y & t \end{pmatrix} \in \mathbf{GL}_2(\mathcal{O}_K)$. By definition we have the identity:

$$\begin{pmatrix} q_1 & q_2 \\ \overline{q_2} & q_3 \end{pmatrix} = C^*C = \begin{pmatrix} x\bar{x} + y\bar{y} & \bar{x}z + \bar{y}t \\ x\bar{z} + y\bar{t} & z\bar{z} + t\bar{t} \end{pmatrix}. \tag{1}$$

The totally real case. We define the *totally real subfield* of K by $F := \{x \in K \,|\, \overline{x} = x\}$, and its ring of integers is denoted by $\mathcal{O}_F$. In [6], Mureau et al. focused on the case where the instance takes place in the subfield F, *i.e.*, when $G = B^*B = B^TB$ for some $B \in \mathbf{GL}_2(\mathcal{O}_F)$. Since complex conjugation acts trivially on elements of F, in that case Equation 1 can be rewritten as:

$$\begin{pmatrix} q_1 & q_2 \\ q_2 & q_3 \end{pmatrix} = C^TC = \begin{pmatrix} x^2 + y^2 & xz + yt \\ xz + yt & z^2 + t^2 \end{pmatrix}. \tag{2}$$

In particular one observes that the diagonal entries q_1 and q_3 of G are *sums of two squares* in $\mathcal{O}_F$. Recovering these squares would allow the reconstruction of C, and thereby yield a solution to the problem. The key observation is that sums of two squares in F are *relative norms* of elements of K down to F. Indeed

[3] Notice that G is Hermitian (*i.e.*, $G^* = G$), so its non diagonal entries are conjugates.

we have $K = F[X]/(X^2+1) =: F(i)$,[4] where $i \in K$ satisfies $i^2 = -1$, and the relative norm of an element $x + iy \in K$ is given by

$$N(x+iy) := (x+iy)(\overline{x+iy}) = x^2 + y^2.$$

The problem therefore reduces to finding *all* solutions $\alpha \in \mathcal{O}_K$ to norm equations of the form $N(\alpha) = q$, where $q \in \mathcal{O}_F$. Indeed certain solutions $x + iy$ to the norm equation will give the first column $\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$ of a matrix C satisfying $C^*C = G$, thus leading to a key recovery in HAWK. However, we stress that not every solution can necessarily be completed to such a matrix C, which is why an enumeration of all solutions is required.

Rather than searching directly for such elements in K, the method of Howgrave-Graham and Szydlo [4] suggests first constructing the set of *ideals* $I \subseteq \mathcal{O}_K$ satisfying $N(I) = q \cdot \mathcal{O}_F$, where the norm of an ideal is defined as $N(I) := (I \cdot \overline{I}) \cap \mathcal{O}_F$, which is an ideal of $\mathcal{O}_F$.[5] The solutions $\alpha \in \mathcal{O}_K$ to $N(\alpha) = q$ then correspond to generators of the principal ideals $I = \alpha \cdot \mathcal{O}_K$ within this set.

An important parameter when counting the number of solutions to $N(I) = q \cdot \mathcal{O}_F$ is the number r of distinct *prime ideals* dividing $q \cdot \mathcal{O}_F$.[6] Recall that any ideal of $\mathcal{O}_F$ can be uniquely factored as a product of prime ideals. Precisely, if

$$q \cdot \mathcal{O}_F = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i},$$

then [6, Theorem 2.16] shows that the number of ideals $I \subseteq \mathcal{O}_K$ satisfying $N(I) = q \cdot \mathcal{O}_F$ can be exponentially large in r. To ensure a small value of r —ideally $r = 1$— [6, Section 4.2] introduces a randomization technique. In summary, the overall approach can be outlined as follows.

1. Randomize the input matrix G until q_1 and q_3 generate prime ideals in $\mathcal{O}_F$.
2. Construct the sets of ideals

$$J_1 = \{I \subseteq \mathcal{O}_K \mid N(I) = q_1 \cdot \mathcal{O}_F\}, \quad J_2 = \{I \subseteq \mathcal{O}_K \mid N(I) = q_3 \cdot \mathcal{O}_F\}.$$

3. For each $I \in J_1$ (resp. $I \in J_2$), check whether it admits a generator $\alpha = x+iy$ (resp. $\beta = z + it$) such that $N(\alpha) = q_1$ (resp. $N(\beta) = q_3$).
4. Among all computed pairs $\alpha = x+iy$ and $\beta = z+it$, identify those for which $C = \left(\begin{smallmatrix} x & z \\ y & t \end{smallmatrix}\right)$ satisfies $C^TC = G$.

Thanks to the randomization, the sets J_1 and J_2 contain at most two ideals each, see [6, Equation 3]. We emphasize that the third step can be performed

[4] The equality $\mathcal{O}_K = \mathcal{O}_F[i]$ holds as well.

[5] Recall that an ideal $I \subseteq \mathcal{O}_K$ is a subset that is closed under addition and satisfies $\mathcal{O}_K \cdot I \subseteq I$. An ideal is said to be *principal* if there exists $\alpha \in \mathcal{O}_K$ such that $I = \alpha \cdot \mathcal{O}_K$, consisting of all integral multiples of α.

[6] A prime ideal $\mathfrak{p} \subseteq \mathcal{O}_F$ satisfies the property that $xy \in \mathfrak{p}$ implies $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$, for all $x, y \in \mathcal{O}_F$.

efficiently using the algorithm of Gentry and Szydlo [3], or its generalization by Lenstra and Silverberg [5].

Let us now consider the case where the instance does not lie in the totally real subfield F, but rather in the full field K, that is, $G = B^*B$ for some secret matrix $B \in \mathbf{GL}_2(\mathcal{O}_K)$. As previously mentioned, we have the decomposition $K = F + i \cdot F$ and $\mathcal{O}_K = \mathcal{O}_F + i \cdot \mathcal{O}_F$, where i denotes a square root of -1. Therefore, the first coefficient of B can be written as $x = x_1 + ix_2$, with $x_1, x_2 \in \mathcal{O}_F$, and similarly for the other coefficients.

Following Equation 1, we now obtain:

$$q_1 = x\overline{x} + y\overline{y} = x_1^2 + x_2^2 + y_1^2 + y_2^2, \tag{3}$$

and similarly, q_3 is expressed as a *sum of four squares* in $\mathcal{O}_F$. While this expression bears resemblance to the earlier case involving two squares, we will see that moving from sums of two squares to four significantly increases the complexity and introduces new challenges.

As in the previous case, we aim to interpret Equation 3 as a norm equation. A natural setting for this is the framework of a *quaternion algebra* over the base field F. Specifically, we define:

$$\mathcal{A} = F + i \cdot F + j \cdot F + ij \cdot F,$$

where the multiplication rules are $i^2 = j^2 = -1$ and $ij = -ji$. This construction endows $\mathcal{A}$ with the structure of a 4-dimensional F-algebra. Due to the anti-commutativity of the generators, multiplication in $\mathcal{A}$ is *non-commutative*.

Observe that $\mathcal{A}$ contains the field K, and can in fact be expressed as $\mathcal{A} = K + j \cdot K$. Moreover, $\mathcal{A}$ is equipped with an involutive automorphism, called *complex conjugation*, defined on elements $\alpha = \alpha_1 + i\alpha_2 + j\alpha_3 + ij\alpha_4 \in \mathcal{A}$ by:

$$\overline{\alpha} := \alpha_1 - i\alpha_2 - j\alpha_3 - ij\alpha_4.$$

The associated *reduced norm* of α is then given by:

$$\mathrm{nrd}(\alpha) := \alpha\overline{\alpha} = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2 \in F.$$

In particular, the conjugation on $\mathcal{A}$ naturally extends the complex conjugation on K, and the reduced norm generalizes the norm map $N : K \to F$.

Since reduced norms in $\mathcal{A}$ correspond to sums of four squares in F, we have once again reduced our problem to the task of enumerating solutions to a norm equation. Specifically, we now aim to enumerate *all* solutions to the equations $\mathrm{nrd}(\alpha) = q_1$ and $\mathrm{nrd}(\beta) = q_3$, where the unknowns α and β belong to the *order*:[7]

$$\mathcal{O}_0 := \mathcal{O}_F + i \cdot \mathcal{O}_F + j \cdot \mathcal{O}_F + ij \cdot \mathcal{O}_F \subset \mathcal{A}.$$

As in the totally real case, we may still assume —after applying a randomization process— that $q_1 \cdot \mathcal{O}_F$ and $q_3 \cdot \mathcal{O}_F$ are prime ideals of $\mathcal{O}_F$. Let us denote $\mathfrak{p} :=$

[7] Indeed the quaternion $\alpha = x + j \cdot y$, obtained by embedding the first column $\binom{x}{y} \in \mathcal{O}_K^2$ of B in $\mathcal{O}_0$, is a solution to $\mathrm{nrd}(\alpha) = q_1$.

$q_1 \cdot \mathcal{O}_F$. Following the earlier approach, the second step would then be to construct the set of ideals in $\mathcal{O}_0$ whose reduced norm is equal to $\mathfrak{p}$.

However, several complications arise due to the non-commutative nature of $\mathcal{A}$. Firstly, the notion of ideals in $\mathcal{O}_0$ becomes more subtle, and we must consider *one-sided* ideals instead. For consistency of notation, we focus on *right* ideals. Secondly, the order $\mathcal{O}_0$ may not be *maximal*, a property that is desirable for effectively working with ideals. Thus, we consider a maximal order $\mathcal{O}_0 \subseteq \mathcal{O} \subset \mathcal{A}$.[8]

Accordingly, the next step would consist of building the set

$$J := \{\text{right } \mathcal{O}\text{-ideals } I \subseteq \mathcal{O} \mid \text{nrd}(I) = \mathfrak{p}\}.$$

While in the totally real case this set contained at most two ideals, we will see that the cardinality of J is now exponential in the degree $d = m/2$ of F, making its enumeration computationally infeasible.[9] The next section is devoted to a proof of this fact.

2 Counting ideals with prime norm

Let $K = \mathbb{Q}[X]/(X^m + 1)$ with m a power-of-two integer and $F = \{x \in K \mid \overline{x} = x\}$ whose degree is denoted by d. We fix the quaternion algebra $\mathcal{A} = F + i \cdot F + j \cdot F + ij \cdot F$ and a maximal order $\mathcal{O} \subset \mathcal{A}$ containing $\mathcal{O}_0$ as before. Finally, we fix a principal prime ideal $\mathfrak{p} \subset \mathcal{O}_F$ together with a generator $q \in \mathcal{O}_F$.

The central theoritical result we will be using is a consequence of classical results about *Brandt matrices*, which arise in the study of quaternion algebras and modular forms, see [7, Section 41]. Given an ideal $\mathfrak{a} \subseteq \mathcal{O}_F$, the associated Brandt matrix $T(\mathfrak{a})$ encodes the number of right $\mathcal{O}$-ideals with norm $\mathfrak{a}$ and living in a prescribed coset for right multiplication of ideals by elements of $\mathcal{A}^\times$. Precisely, the entries $T(\mathfrak{a})_{ij}$ count the number of ideals $I \subseteq I_j$ in a fixed class $[I_i]$ and such that $\text{nrd}(I) = \mathfrak{a}\,\text{nrd}(I_j)$. An important property of Brandt matrices is that the sum $\sum_i T(\mathfrak{a})_{ij}$ is independent of the column index j and is, by definition, equal to the total number of left $\mathcal{O}$-ideals $I \subseteq \mathcal{O}$ satisfying $\text{nrd}(I) = \mathfrak{a}$. Additionally, [7, Proposition 41.3.1, (a)] shows that this sum is also equal to $\sum_{\mathfrak{a} \subseteq \mathfrak{d}} N_{F/\mathbb{Q}}(\mathfrak{d})$, where the latter is indexed over all ideals $\mathfrak{d} \subseteq \mathcal{O}_F$ containing $\mathfrak{a}$. In the special case where $\mathfrak{a} = \mathfrak{p}$ is a prime ideal, this gives the following simple expression for the number of left $\mathcal{O}$-ideals with reduced norm $\mathfrak{p}$.

Theorem 2.1. *The set J of left $\mathcal{O}$-ideals contained in $\mathcal{O}$ and having reduced norm $\mathfrak{p}$ has cardinality:*

$$|J| = 1 + N_{F/\mathbb{Q}}(q).$$

Proof. This follows from [7, Proposition 41.3.1, (a)] applied with $\mathfrak{a} = \mathfrak{p}$, plus the fact that $N_{F/\mathbb{Q}}(\mathfrak{p}) = N_{F/\mathbb{Q}}(q)$. □

[8] Unlike the totally real case, where $\mathcal{O}_K$ is the unique maximal order of K, the quaternion algebra $\mathcal{A}$ does not admit a unique maximal order containing $\mathcal{O}_0$.

[9] In HAWK [2], the security parameter m is typically chosen to be 512, 1024, or 2048.

Example 2.2. Let us consider $K = \mathbb{Q}(i)$, $F = \mathbb{Q}$, and the quaternion algebra $\mathcal{A} = \mathbb{Q} + i \cdot \mathbb{Q} + j \cdot \mathbb{Q} + ij \cdot \mathbb{Q}$, where $i^2 = j^2 = -1$ and $ji = -ij$. The prime case of Jacobi's theorem on sums of four squares states that there are exactly $8(p+1)$ representations of an odd prime number p as a sum of four squares in $\mathbb{Z}$. Indeed, the maximal order $\mathcal{O} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}\frac{1+i+j+ij}{2} \subset \mathcal{A}$ has exactly $p+1$ left $\mathcal{O}$-ideals of norm p, which is a consequence of the previous theorem.[10] Moreover, these ideals are all principal, and multiplying each generator by the elements of the unit group $\mathcal{O}^1 = \{\pm 1, \pm i, \pm j, \pm ij\}$, we obtain a total of $8(p+1)$ quaternions of norm p, as claimed.

Our impossibility result will follow from the previous theorem combined with an estimate on the size of $N_{F/\mathbb{Q}}(q)$ when q is sampled according to a "four squares version" of the one considered in [6]: that is, when q is a sum of four squares of independent discrete Gaussian in $\mathcal{O}_F$ with the same standard deviation $s > 0$. This distribution is, however, difficult to analyze (see [6, Appendix B] for the case of sums of two squares), and we will rely on a heuristic. We begin by studying a "continuous" version of this distribution. Let us define $F_{\mathbb{R}} := F \otimes_{\mathbb{Q}} \mathbb{R}$,[11] and observe that every complex embedding $\sigma : F \to \mathbb{R}$ extends uniquely to a map $F_{\mathbb{R}} \to \mathbb{R}$. Therefore the algebraic norm naturally extends to $q \in F_{\mathbb{R}}$ as $\prod_\sigma \sigma(x)$.

When $\mathbf{x}_1, \mathbf{x}_2, \mathbf{y}_1, \mathbf{y}_2 \in F_{\mathbb{R}}$ are sampled independently from a continuous Gaussian distribution over $F_{\mathbb{R}}$, we establish in the next proposition an estimate on the algebraic norm of $q = \mathbf{x}_1^2 + \mathbf{x}_2^2 + \mathbf{y}_1^2 + \mathbf{y}_2^2$. This follows from the observation that each $\sigma(q)$ follows a scaled chi-squared distribution, so that its algebraic norm becomes a product of d independent such random variables. Once this estimate is obtained, we transfer the result to the discrete case, *i.e.*, when $x_1, x_2, y_1, y_2 \in \mathcal{O}_F$, under the heuristic assumption that the algebraic norm of q follows a similar distribution in both settings.

Proposition 2.3. *Suppose that $\mathbf{x}_1, \mathbf{x}_2, \mathbf{y}_1, \mathbf{y}_2 \in F_{\mathbb{R}}$ are sampled independently and according to the same (continuous) Gaussian distribution with standard deviation $s > 0$. Further, we define $q = \mathbf{x}_1^2 + \mathbf{x}_1^2 + \mathbf{y}_1^2 + \mathbf{y}_2^2$. Assuming $s = \exp(\Omega(d))$ (as in [6, Algorithm 4.2]), then the absolute norm of q, defined by $\prod_\sigma \sigma(q)$ is, with overwhelming probability in d,[12] greater than 2^d.*

Proof. For each complex embedding $\sigma : F \to \mathbb{R}$, the element $\sigma(q) \in \mathbb{R}$ behaves like a scaled chi-squared distribution $s^2\chi_4^2$. By assumption we also have that $\sigma(q)$ and $\tau(q)$ are independent for any complex embeddings $\sigma \neq \tau$ of F. Let us fix a complex embedding σ and $Y \sim \chi_4^2$. We prove that $\sigma(q) \geq 2$ happens with overwhelming probability. Indeed, we have:

$$\mathbb{P}(\sigma(q) \leq 2) = \mathbb{P}(Y \leq 2/s^2) = \int_0^{1/s^2} te^{-t}dt = 1 - (1 + 1/s^2)e^{-1/s^2}.$$

[10] In fact, $\mathcal{O}$ is the unique maximal order of $\mathcal{A}$ containing $\mathbb{Z} + i \cdot \mathbb{Z} + j \cdot \mathbb{Z} + ij \cdot \mathbb{Z}$.

[11] Notice that if $F = \mathbb{Q}[X]/P(X)$, then $F_{\mathbb{R}} = \mathbb{R}[X]/P(X)$

[12] An event is said to occur with overwhelming probability in d if its complement has negligible probability in d, that is, if it is smaller than $1/P(d)$ for any polynomial P.

Since s is chosen of size $\exp(\Omega(d))$, we conclude that $\sigma(q) \leq 2$ happens only with negligible probability in d. Consequently, $\prod_\sigma \sigma(q) \geq 2^d$ holds with overwhelming probability in d. □

Heuristic 2.4. Let $x_1, x_2, y_1, y_2 \in \mathcal{O}_F$ be independently sampled from the same discrete Gaussian distribution with standard deviation $s > 0$. Then, the absolute norm of $x_1^2+x_2^2+y_1^2+y_2^2$ is close to (a discretization of) the one for $\mathbf{x}_1^2+\mathbf{x}_1^2+\mathbf{y}_1^2+\mathbf{y}_2^2$, where $\mathbf{x}_1, \mathbf{x}_2, \mathbf{y}_1, \mathbf{y}_2 \in F_{\mathbb{R}}$ are sampled independently and from a continuous Gaussian distribution with the same standard deviation s.

Putting together the previous results and heuristic, we obtain that if $s = \exp(\Omega(d))$ and q is the sum of four squares of independent Gaussian element in $\mathcal{O}_F$, then the set of left $\mathcal{O}$-ideals contained in $\mathcal{O}$ has, with overwhelming probability in d, cardinality $\geq 2^d$. This concludes our proof and this note.

References

1. 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.
2. Léo Ducas, Eamonn W. Postlethwaite, Ludo N. Pulles, and Wessel P. J. van Woerden. Hawk: Module LIP makes lattice signatures fast, compact and simple. In Shweta Agrawal and Dongdai Lin, editors, *Advances in Cryptology - ASIACRYPT 2022 - 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5-9, 2022, Proceedings, Part IV*, volume 13794 of *Lecture Notes in Computer Science*, pages 65–94. Springer, 2022.
3. 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.
4. Nick Howgrave-Graham and Michael Szydlo. A method to solve cyclotomic norm equations. In Duncan A. Buell, editor, *Algorithmic Number Theory, 6th International Symposium, ANTS-VI, Burlington, VT, USA, June 13-18, 2004, Proceedings*, volume 3076 of *Lecture Notes in Computer Science*, pages 272–279. Springer, 2004.
5. Hendrik W. Lenstra Jr. and Alice Silverberg. Testing isomorphism of lattices over CM-orders. *SIAM J. Comput.*, 48(4):1300–1334, 2019.
6. Guilhem Mureau, Alice Pellet-Mary, Georgii Pliatsok, and Alexandre Wallet. Cryptanalysis of rank-2 module-lip in totally real number fields. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 226–255. Springer, 2024.
7. John Voight. *Quaternion Algebras*. Springer Nature, 01 2021.