Cryptanalysis of HAWK: a Guessing Game

Ben Nelson[1⋆], Joshua Limbrey[2], Cong Ling[2], and Andrew Mendelsohn[2]

[1] Independent Researcher
b.p.nelson2003@gmail.com
[2] Department of EEE, Imperial College London, United Kingdom
{j.limbrey24, c.ling, andrew.mendelsohn18}@imperial.ac.uk

Abstract. HAWK is a signature scheme that was introduced in 2022, and uses the lattice isomorphism problem (LIP) as a basis for post-quantum cryptography. In this work, we describe a classical algorithm that recovers the HAWK secret key in probabilistic polynomial time, assuming four number-theoretic heuristics. The reduction from the rank-2 module-LIP instances underlying HAWK to nrdPIP (Eurocrypt '25) is central to our algorithm. At a high level, we first conjugate the HAWK public Gram matrix G by a random lower-triangular unimodular matrix U with 'short' entries, forming a new Gram matrix $G' := U^*GU$, and then test whether the $\mathcal{O}$-nrdPIP instance attached to G' is unusually easy. In particular, for a non-negligible proportion of such instances G', one can use the Lenstra-Silverberg algorithm to solve the corresponding $\mathcal{O}$-nrdPIP instance using a subfield approach. By resampling U until such an instance is uncovered and solved, which can be seen as 're-randomising' the $\mathcal{O}$-nrdPIP instance whilst fixing the corresponding module-LIP instance, we are then able to recover a valid HAWK private key. At the time of writing, we do not claim that HAWK is broken, as we have not yet verified these heuristics experimentally. On the other hand, these heuristics seem to be very plausible, and we hope to be able to verify this in the future with an implementation of our algorithm.

Keywords: HAWK, cryptanalysis, lattice isomorphism problem

Update (30/06): Following discussions with Daniel Apon and Markku-Juhani Saarinen, we acknowledge that Heuristic 4 is insufficient to conclude that the main algorithm runs in polynomial time, and in fact the main algorithm appears to run in super-polynomial time. This mistake originates from the count of ideals of norm q' in $\mathcal{O}_F$: one must include fractional ideals in this count, of which there are many. We note as an aside that Heuristics 1-3 have been independently experimentally verified.

We would also like to thank the HAWK team and Alice Pellet-Mary for their responses to our work.

⋆ Corresponding and main author: comments and corrections are very welcome.

Disclaimer: This article is part of an ongoing discussion on the security of HAWK involving the authors and members of the HAWK team. We are grateful for this discussion, but the claims and conclusions presented here are solely our own. We invite the wider cryptographic community to scrutinise our arguments carefully, so as to improve our collective understanding of the matter. This preprint will further evolve in the coming months, with an emphasis on experimentally proving or disproving our heuristic assumptions.[3]

1 Introduction

Since the first description and subsequent introduction of public-key cryptography [10,38], much of practical cryptography has relied on the hardness of the discrete logarithm or prime factorisation problems. Since the publication of Shor's algorithm(s) [40], the threat of a sufficiently capable quantum adversary has driven researchers to find cryptographic assumptions believed to be hard for such an opponent. The search for practical instantiations has only been hastened by the NIST calls for standardisation of post-quantum schemes [33,34].

One class of assumptions relied upon by the majority of schemes selected by the initial NIST standardisation effort [39,28,37], as well as one third-round candidate [3] of the NIST additional signatures call is that of lattice problems. We are interested in the latter of these schemes mentioned, and its underlying hardness assumption of the lattice isomorphism problem (LIP). The LIP, in its search form, asks one to recover an isometry between two given challenge lattices, assuming that one exists, and is an attractive hardness assumption as it allows one to choose lattices with remarkable decoding properties for the construction of a scheme.

A major obstacle for the post-quantum cryptographer seeking adoption of their scheme is achieving sizes and efficiency comparable to the exceptional standards set by classical schemes. Notably, for lattices this primarily revolves around reducing the size of keys and ciphertexts, and the preferred method for this is the introduction of algebraic structure, usually that of modules. This leads nicely to the introduction of the module-LIP, and its crown jewel scheme, the aforementioned HAWK [11].

The hardness of the LIP has been studied in its vanilla flavour by Haviv and Regev in [21], where they present an algorithm to solve the rank-n LIP in $n^{O(n)}$ time, but since the explicit constructions of Ducas and van Woerden [13], the LIP and its structured variants have seen considerable cryptanalytic effort.

The cryptanalysis of HAWK by the use of automorphisms has been studied in [27,18], invalidating the one-more-SVP assumption of HAWK (though this did not lead to a break on HAWK), and demonstrating that knowledge of any non-trivial automorphism more than halves the security of the LIP instance. Turning more generally to the module-LIP (still with sights set on HAWK), existing literature has shown that instances over totally real number fields [32],

[3] An implementation of our algorithm is available at https://github.com/supinie/HAWK_guessing_game_aux.

and even number fields in which there exists at least one real embedding [1] can be solved in polynomial time.

This stems from the fact that with one real embedding, there exists a reduction to the nrdPIP in CM fields. The setting of HAWK, and more generally the module-LIP over totally complex number fields was explored in [7], demonstrating that one is left with a 'sum of four squares' problem, from which a tractable nrdPIP instance cannot be constructed. In the line of work [6,15,8][4], an explicit reduction to the nrdPIP in quaternion algebras was given. We remark that this last reduction did not affect the security of HAWK. We now briefly review the history of the principal ideal problem (PIP).

Originating in the study of a different (but also lattice-based) scheme, NTRU, Gentry and Szydlo published a polynomial-time algorithm to recover a generator of a principal ideal in $\mathbb{Z}[\zeta_p]$ given its norm [20]. The work of GCHQ with Soliloquy [4] both constructed and broke a scheme based on the so-called short-generator principal ideal problem (SG-PIP), which was then followed by [9] making many details more explicit, and [2] giving quantum polynomial-time algorithms for the PIP over general number fields. The work of Gentry and Szydlo was extended in the line of work [24,26] and [22], culminating in an algorithm to compute isomorphisms between ideal lattices in orders of CM fields.

All of these approaches to solving the PIP (and its variants) rely on the commutativity of the ambient field; once again, HAWK has evaded cryptanalytic efforts thanks to the non-commutativity of the quaternions.

At the time of writing, the best algorithm for solving the nrdPIP in quaternion orders is due to Kirschmer and Voight [23, Algorithm 6.3], in which an ideal SVP oracle is appealed to in order to recover a generator. It follows that, assuming the quaternion ideal lattice is of sufficiently large rank, recovering the principal generator remains an intractable problem.

1.1 Our Contribution

Assuming certain number-theoretic heuristics, we provide a classical probabilistic polynomial-time algorithm to solve the rank-2 module-LIP instances underpinning the security of HAWK, using the algorithm of Lenstra and Silverberg [25] as a subroutine. The primary observation that enables the use of [25] is the following:

Suppose that one is given the public Gram matrix G that represents a LIP instance. One may construct arbitrarily many equivalent instances $G' = U^*GU$ by conjugating G with a random unimodular matrix U. However, under the reduction to a quaternion nrdPIP instance, G and G' give rise to distinct nrdPIP instances. In this way, we are able to construct what is akin to a worst-to-average-case reduction and, under certain heuristics, use this re-sampling method to find an easy nrdPIP instance underlying the original module-LIP challenge.

By bounding the norm of a random element $x \in \mathcal{O}_L$ used in the construction of U, we are able to construct alternative PIP instances with certain properties.

[4] The latter is a merger of the former two. Henceforth, we cite only the merger.

We then use probabilistic results to show that, with non-negligible probability, we are able to find a quaternion nrdPIP instance which is reducible to the nrdPIP over a commutative subfield, and then use the Lenstra-Silverberg algorithm to recover a generator [25].

We finally check that this is a valid solution before recovering the basis corresponding to G', following the last steps of [8], in turn permitting the recovery of a private key.

In essence, our algorithm boils down to 'rigging the game', and then 're-rolling the dice' until a favourable outcome is achieved; we show that with overwhelming probability, we require a polynomial number of 'rolls'.

1.2 Open Questions

In this work, we assume Weber's conjecture and use various heuristics. In particular, for $q', \alpha \in \mathcal{O}_K := \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$ with 'high entropy', we assert the following:

Heuristic 1 *Let α be sampled as in our main algorithm (Algorithm 2). The probability that α is square-free is lower bounded by $1/2$.*

Heuristic 2 *Let $K = \mathbb{Q}(\zeta_{2^l} + \zeta_{2^l}^{-1})$ for some $l \in \mathbb{N}$ and write $\mathfrak{d} \leq \mathcal{O}_K$ for the unique prime ideal of $\mathcal{O}_K$ lying over 2. There is a natural isomorphism $\mathcal{O}_K/\mathfrak{d}^2 \cong \mathbb{F}_2[X]/(X^2)$. The image of α in the quotient $\mathcal{O}_K/\mathfrak{d}^2$ corresponds to $X + 1 \in \mathbb{F}_2[X]/(X^2)$ with probability around $1/4$.*

Heuristic 3 (Restated) *Let $K = \mathbb{Q}(\zeta_{2^l} + \zeta_{2^l}^{-1})$ for some $l \in \mathbb{N}$, and let $S \subset \mathrm{Pl}(K)$ consist of all finite places dividing q', all places ramified in $K(\sqrt{\alpha})/K$, and all archimedean places of K. Write $U_{K,S}$ for the S-units in K. There is a map $\mathrm{Log} : U_{K,S} \to \mathbb{R}^{\#S}$, and we can construct a pair of lattices $\mathcal{L}'' \subset \mathcal{L}'$ in $\mathbb{R}^{\#S}$ such that, with overwhelming probability,*

$$|\mathcal{L}' : \mathcal{L}''| = O(n^{2+o(1)}).$$

The image of $\mathrm{Log}(q')$ in $\mathcal{L}'/\mathcal{L}''$ is 0 with probability $\Omega(n^{-2-o(1)})$.

Heuristic 4 (Restated) *Let $K = \mathbb{Q}(\zeta_{2^l} + \zeta_{2^l}^{-1})$ and suppose that F is a field isomorphic to $K(\sqrt{\alpha})$. During our main algorithm (Algorithm 2), we form an ideal $\mathfrak{a} \leq \mathcal{O}_F$ that depends on both q' and α, and $N_{F/K}(\mathfrak{a}) = q'\mathcal{O}_K$. In Section 9, we show that, with overwhelming probability, there are $O(n^{1+o(1)})$ ideals of $\mathcal{O}_F$ with norm $q'\mathcal{O}_K$. Given that one of these ideals is principal, the probability that $\mathfrak{a}$ itself is principal is $\Omega(n^{-1-o(1)})$.*

Although the number-theoretic heuristics underlying our analysis are plausible, their verification would strengthen the evidence supporting our claims.

Moreover, an implementation of our main algorithm (Algorithm 2) using the Lenstra-Silverberg algorithm would provide concrete validation of the attack, for example against the HAWK-256 challenge.

This attack, in its current state, does not break the general rank-2 module-LIP, and instead focuses on the special case relevant to HAWK. On the other hand, the extension of this attack to module lattices over $\mathcal{O}_F$, where F/K is a CM extension and K has class number one, appears to be possible.

We stress that this does not break the quaternion nrdPIP, and is instead taking advantage of specially constructed easy cases where extra information (e.g. a commutative subfield containing a principal generator) is known. Developing efficient algorithms for the quaternion nrdPIP and the associated ideal SVP instances remain important open problems.

1.3 Roadmap

We leave a technical overview for Section 4, where we provide a high-level discussion of the algorithm and describe the flavour of the attack; the technical details are then given in the following sections, where we provide further justification using various heuristics. We begin by presenting the necessary preliminaries in Sections 2 and 3.

2 Mathematical Foundations

2.1 Number Fields

An *algebraic number field* is a finite extension of the rational numbers $\mathbb{Q}$. If F is an algebraic number field of degree $d = [F : \mathbb{Q}]$, then there are exactly d embeddings $F \hookrightarrow \mathbb{C}$. An embedding $\iota\colon F \hookrightarrow \mathbb{C}$ is said to be *real* if the image of ι is contained in $\mathbb{R}$; otherwise, ι is said to be *complex*. If all of the embeddings $F \hookrightarrow \mathbb{C}$ are real, then we say that F is *totally real*, and likewise, if all of the embeddings $F \hookrightarrow \mathbb{C}$ are complex, then F is *totally complex*. Any number field F contains a *maximal totally real subfield* F^+, which is the unique totally real subfield of F that is not properly contained in any other totally real subfield.

Given a pair of number fields $E \subset F$, we define $\mathrm{Aut}(F/E)$ to be the set of bijective ring homomorphisms $F \to F$ that fix E pointwise. If

$$\#\mathrm{Aut}(F/E) = [F : E],$$

then the extension F/E is said to be *Galois*, and we write '$\mathrm{Gal}(F/E)$' in place of '$\mathrm{Aut}(F/E)$'. Suppose that F/E is a Galois extension, and abbreviate $G := \mathrm{Gal}(F/E)$. In this setting, we define the *algebraic norm* $N_{F/E} : F \to E$ by the formula

$$N_{F/E}(y) = \prod_{\sigma \in G} \sigma(y),$$

where $y \in F$. For any number field F, an element $y \in F$ is said to be *integral* if y is a root of some monic polynomial $f \in \mathbb{Z}[X]$. The *ring of integers* of F, written $\mathcal{O}_F$, consists of all the integral elements of F, which naturally forms a

ring. A finite collection of elements $\{y_r\}_{r\in S}$ forms an *integral basis* of $\mathcal{O}_F$ if every element $z \in \mathcal{O}_F$ has a unique expression of the form

$$z = \sum_{r\in S} a_r y_r,$$

where the coefficients a_r are rational integers. Every number field F has a (non-unique) integral basis.

An *ideal* $\mathfrak{a}$ of the ring of integers $\mathcal{O}_F$ is an additive subgroup with the property that, for any $y \in \mathfrak{a}$ and $z \in \mathcal{O}_F$, we have $yz \in \mathfrak{a}$. A non-zero proper ideal $\mathfrak{a}$ is said to be *prime* if for all $y, z \in \mathcal{O}_F$ where $y \notin \mathfrak{a}$, we have

$$yz \in \mathfrak{a} \implies z \in \mathfrak{a}.$$

Given ideals $\mathfrak{a}, \mathfrak{b} \leq \mathcal{O}_F$, we define the *product* of $\mathfrak{a}$ and $\mathfrak{b}$ as the $\mathcal{O}_F$-ideal generated by $\{yz\colon y \in \mathfrak{a},\, z \in \mathfrak{b}\}$. A classical result due to Dedekind is that any non-zero ideal $\mathfrak{a} \leq \mathcal{O}_F$ has a unique factorisation into prime ideals, that is,

$$\mathfrak{a} = \prod_{r=1}^{\ell} \mathfrak{p}_r,$$

where $\ell \geq 0$, and each $\mathfrak{p}_r \leq \mathcal{O}_F$ is prime.

Given a number field F, a non-zero prime ideal $\mathfrak{p} \leq \mathcal{O}_F$, and an element $y \in F^\times$, we define $v_\mathfrak{p}(y)$ to be the exponent of $\mathfrak{p}$ occurring in the factorisation of the fractional ideal (y) into prime ideals. We can define a corresponding absolute value on F as

$$\|y\|_\mathfrak{p} := |\mathcal{O}_F/\mathfrak{p}|^{-v_\mathfrak{p}(y)}.$$

We also set $\|0\|_\mathfrak{p} = 0$. Similarly, given an embedding $\sigma : F \hookrightarrow \mathbb{C}$, we define an archimedean absolute value by

$$\|y\|_\sigma := |\sigma(y)|,$$

where $|\cdot|$ denotes the usual complex absolute value. A *place* of F is an absolute value on F, up to equivalence. We may identify the *finite* places with the non-zero prime ideals of $\mathcal{O}_F$, and the *archimedean* places with the real embeddings of F together with the conjugate pairs of complex embeddings of F.

2.2 *S*-Unit Attacks

Let K be a number field and let $S \subset \mathrm{Pl}(K)$ be a finite set of places including all archimedean places of K. We define

$$U_{K,S} = \{y \in K^\times\colon \|y\|_v = 1 \ \ \forall v \notin S\}.$$

The S-unit group $U_{K,S}$ is a finitely generated abelian group of rank $\#S - 1$, although we postpone the formal statement of this result until Section 8.2 (Theorem 7). The notion of S-units has been central to many breakthroughs in modern

cryptanalysis, perhaps most notably the line of work [4,9,2], in which a quantum polynomial-time algorithm solving the PIP in general number fields was developed, leading to a break on multiple schemes, for example, [4] and [41]. In essence, this is possible due to the following. Suppose that $\mathfrak{a}$ is a principal $\mathcal{O}_K$-ideal and define

$$S := \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t \leq \mathcal{O}_K \text{ prime with } \mathfrak{p}_r \mid \mathfrak{a}\} \cup \{v \in \mathrm{Pl}(K) \text{ archimedean}\}.$$

Assume that one can compute an explicit basis $\mathcal{B} = \{u_r \colon 1 \leq r \leq \#S - 1\}$ of the S-unit group $U_{K,S}$. One can record the set of valuations at the finite primes of S in a $t \times (\#S - 1)$ matrix M with entries

$$M_{rs} = v_{\mathfrak{p}_r}(u_s).$$

Using simple linear algebra, one can then find $u \in U_{K,S}$ with $v_{\mathfrak{p}_r}(u) = v_{\mathfrak{p}_r}(\mathfrak{a})$ for $1 \leq r \leq t$. It immediately follows that $(u) = \mathfrak{a}$, solving the PIP instance attached to $\mathfrak{a}$.

2.3 Local Fields

This section provides an extremely short introduction to local fields: we guide the interested reader to [5, Chapter 1] for a more complete treatment. One can endow the rational numbers $\mathbb{Q}$ with the 'usual' absolute value $|\cdot|_\infty$ defined as $|a/b|_\infty = +\sqrt{a^2/b^2}$ for any $a/b \in \mathbb{Q}$. This allows one to formally construct the real numbers $\mathbb{R}$ as the set of Cauchy sequences in $\mathbb{Q}$, not distinguishing between different sequences with the same limit. In this sense, $\mathbb{R}$ is known as the *completion* of $\mathbb{Q}$ with respect to $|\cdot|_\infty$. Analogously, given a rational prime p and $a/b \in \mathbb{Q}$, one can define an absolute value

$$\|a/b\|_p := p^{v_p(b) - v_p(a)}.$$

Following the construction of the reals, one can define the p-adic rationals $\mathbb{Q}_p$ as the completion of $\mathbb{Q}$ with respect to the above absolute value. This definition can be extended to general number fields: given a number field K and a prime ideal $\mathfrak{p} \leq \mathcal{O}_K$, we can consider the corresponding *local field* $K_\mathfrak{p}$.

3 Preliminaries

Theorem 1 (Erdős-Kac Theorem). *For an integer $m \in \mathbb{Z}$, let $\nu(m)$ denote the number of prime divisors of m, and A_n denote the number of integers from 1 to n for which*

$$\nu(m) < \log\log(n) + \omega\sqrt{2\log\log(n)},$$

where ω is an arbitrary real number. Then

$$\lim_{n\to\infty} \frac{A_n}{n} = \pi^{-\frac{1}{2}} \int_{-\infty}^{\omega} \exp(-u^2)\mathrm{du}.$$

Proof. This is the classical Erdős-Kac Theorem [14]. □

For our purposes, the following theorem can be taken as a definition of the zeta function ζ_K over a general number field:

Theorem 2. *For any number field K of degree d, ζ_K is a meromorphic function on the half-plane $\Re s > 1 - 1/d$, analytic everywhere except for a simple pole at $s = 1$. For $\Re s > 1$, we have*

$$\zeta_K(s) = \sum_{\mathfrak{a} \leq \mathcal{O}_K} \frac{1}{N\mathfrak{a}^s} = \prod_{\mathfrak{p} \leq \mathcal{O}_K \text{ prime}} \left(1 - \frac{1}{N\mathfrak{p}^s}\right)^{-1}.$$

Here, $N\mathfrak{a} = |\mathcal{O}_K/\mathfrak{a}|$ denotes the absolute norm of $\mathfrak{a}$.

Proof. For example, see [30, Chapter 7, Theorem 42]. □

3.1 A Dash of Class Field Theory

Here, we give some *very* brief statements from class field theory. We guide the interested reader to the classical text [5] for a good introduction to the subject.

Theorem 3 (Hasse Norm Theorem). *Let F/K be a separable quadratic field extension and let $b \in K^\times$. Suppose that $b \in N_{F_v/K_v}(F_v^\times)$ for every place $v \in \mathrm{Pl}(K)$. Then $b \in N_{F/K}(F^\times)$.*

Proof. For example, see [42, Theorem 26.8.23]. □

Theorem 4 (Local Artin Reciprocity). *Suppose that K is a local field and F/K a finite Galois extension. Then there is a canonical isomorphism*

$$K^\times / N_{F/K}(F^\times) \cong \mathrm{Gal}(F/K)^{ab},$$

where $\mathrm{Gal}(F/K)^{ab}$ denotes the abelianisation of $\mathrm{Gal}(F/K)$.

Proof. For example, see [35, Theorem 7.2.3]. □

3.2 Quaternion Algebras

Let K be a totally real number field, and suppose that $a, b \in K^\times$. The *quaternion algebra* $\mathcal{A} = (a, b \,|\, K)$ is the algebra over K generated by elements $1, i, j, k$ that satisfy the following relations: $i^2 = a$, $j^2 = b$, and $ij = -ji = k$. Any element $q \in \mathcal{A}$ has a unique expression of the form

$$q = q_1 + q_2 i + q_3 j + q_4 k,$$

where $q_1, q_2, q_3, q_4 \in K$. We define the *conjugate* of q as

$$\overline{q} := q_1 - q_2 i - q_3 j - q_4 k.$$

We may further define the *reduced norm* of q as $\mathrm{nrd}(q) = q\overline{q}$, and the *reduced trace* of q as $\mathrm{trd}(q) = q + \overline{q}$.

We now make a sequence of definitions that allow us to describe the theory of ideals in the quaternion setting. First, we can capture the discrete nature of the ring of integers with the notion of an R-lattice:

Definition 1 (R-lattice). *Let R be a domain with field of fractions K. An R-lattice in a K-vector space V is a finitely generated R-submodule of V that spans V over K.*

Of course, the ring of integers has more structure than an arbitrary lattice. We next define a *maximal order*, which generalises the notion of the ring of integers to the quaternion setting, at least in some sense.

Definition 2 (Order, Maximal Order). *Let R be a domain with field of fractions K, and suppose that $\mathcal{A}$ is a quaternion algebra over K. An R-order $\mathcal{O} \subset \mathcal{A}$ is an R-lattice that is also a subring of $\mathcal{A}$. We say that an order is a maximal order if it is not properly contained in any other order of $\mathcal{A}$.*

We note that, in contrast to the 'standard' number field case, a quaternion algebra over a number field contains infinitely many distinct maximal orders.

Definition 3. *Suppose that $\mathcal{A}$ is a quaternion algebra and let $\mathcal{L} \subset \mathcal{A}$ be an R-lattice. The right order of $\mathcal{L}$ is defined as*

$$\mathcal{O}_R(\mathcal{L}) := \{\alpha \in \mathcal{A} \colon \mathcal{L}\alpha \subset \mathcal{L}\}.$$

Note that $\mathcal{O}_R(\mathcal{L})$ is the largest order $\mathcal{O}$ for which $\mathcal{L}$ is a right $\mathcal{O}$-module.

Next, we define the parallel notions of integral and fractional ideals in the quaternion setting:

Definition 4 (Integral/Fractional Right Ideal). *Suppose that $\mathcal{A}$ is a quaternion algebra over $K = \mathrm{Frac}(R)$, and let $\mathcal{O} \subset \mathcal{A}$ be an R-order. A right fractional $\mathcal{O}$-ideal is an R-lattice $\mathcal{I} \subset \mathcal{A}$ such that $\mathcal{O} \subset \mathcal{O}_R(\mathcal{I})$. We say that $\mathcal{I}$ is principal if $\mathcal{I} = \alpha\mathcal{O}$ for some $\alpha \in \mathcal{A}$. If $\mathcal{I} \subset \mathcal{O}$, then we say that $\mathcal{I}$ is an integral right $\mathcal{O}$-ideal. When clear, we will simply refer to an integral right $\mathcal{O}$-ideal as a right $\mathcal{O}$-ideal.*

We define the *reduced norm* of an ideal as follows:

Definition 5. *Suppose that $\mathcal{A}$ is a quaternion algebra over $K = \mathrm{Frac}(R)$, and let $\mathcal{O} \subset \mathcal{A}$ be an R-order. Let $\mathcal{I} \subset \mathcal{A}$ be a right fractional $\mathcal{O}$-ideal. The reduced norm $\mathrm{nrd}(\mathcal{I})$ of $\mathcal{I}$ is the R-submodule of K generated by $\{\mathrm{nrd}(\alpha) \colon \alpha \in \mathcal{I}\}$.*

3.3 Module-LIP

Definition 6. *Let L be a number field of degree d with ring of integers $\mathcal{O}_L$ and suppose we are given an order $R \subset \mathcal{O}_L$. A full-rank R-module $\mathcal{M} \subset L^m$ is a set of the form*

$$\mathcal{M} = \sum_{r=1}^{m} \mathfrak{a}_r \mathbf{b}_r,$$

where $\mathbf{b}_1, \ldots, \mathbf{b}_m \in L^m$ are linearly independent vectors, and $\mathfrak{a}_1, \ldots, \mathfrak{a}_m$ are non-zero fractional ideals of R. Define B as the $m \times m$ matrix with columns

$\mathbf{b}_r$ *for* $1 \leq r \leq m$. *We will often refer to such a module* $\mathcal{M}$ *by its pseudo-basis* $\mathbf{B} := (B, (\mathfrak{a}_r)_{r=1}^m)$. *The pseudo-Gram matrix associated to* $\mathbf{B}$ *is defined as*

$$\mathbf{G} := (B^*B, (\mathfrak{a}_r)_{r=1}^m).$$

Definition 7. *Given a number field* L *of degree* d, *let* $\sigma \colon L \hookrightarrow \mathbb{R}^d$ *denote the 'usual' canonical embedding of* L. *Let* $\mathcal{M} \subset L^m$ *be a full-rank* R*-module for some order* $R \subset \mathcal{O}_L$. *We can extend the definition of* σ *to* L^m *by defining* $\boldsymbol{\sigma}(\mathbf{v})$ *as the concatenation of each* $\sigma(v_r)$ *for* $1 \leq r \leq m$, *where* $\mathbf{v} = (v_1, \ldots, v_m)^\intercal$. *A full-rank module lattice in* $\mathbb{R}^{dm}$ *is a lattice of the form* $\boldsymbol{\sigma}(\mathcal{M})$ *where* $\mathcal{M} \subset L^m$ *is a full-rank* R*-module.*

Definition 8. *Let* $O_m(\mathbb{R})$ *denote the set of* $m \times m$ *orthogonal matrices over* $\mathbb{R}$. *The (search) lattice isomorphism problem (LIP) asks, given bases* (B, B') *representing two lattices in* $\mathbb{R}^m$, *recover an orthogonal transform* $O \in O_m(\mathbb{R})$ *and* $U \in \mathrm{GL}_m(\mathbb{Z})$ *such that* $B' = OBU$, *assuming that one exists.*

Definition 9 (Congruent Pseudo-Gram Matrices). *We continue with the notation given in Definitions 6 and 7. Two pseudo-Gram matrices* $\mathbf{G} := (G, (\mathfrak{a}_r)_{r=1}^m)$ *and* $\mathbf{G}' := (G', (\mathfrak{b}_r)_{r=1}^m)$ *are said to be congruent if there exists*

$$U = (u_{r,s})_{1 \leq r,s \leq m} \in \mathrm{GL}_m(L)$$

such that

1. $G' = U^*GU$.
2. $u_{r,s} \in \mathfrak{a}_r \mathfrak{b}_s^{-1}$ *for all* $1 \leq r, s \leq m$.
3. $\prod_r \mathfrak{a}_r = \det(U) \prod_r \mathfrak{b}_r$.

Such a matrix U *is called a congruence matrix between* $\mathbf{G}$ *and* $\mathbf{G}'$. *The set of congruence matrices between* $\mathbf{G}$ *and* $\mathbf{G}'$ *is denoted by* $\mathrm{Cong}(\mathbf{G}, \mathbf{G}')$. *The (search) module-LIP asks us to find such a matrix* U *given two isometric module lattices corresponding to the aforementioned pseudo-Gram matrices.*

Remark 1. Consider two Gram matrices $G = B^*B$, $G' = B'^*B'$ and suppose that $B' = OBU$. Then

$$G' = (OBU)^*(OBU) = U^*B^*O^*OBU = U^*GU.$$

Therefore, finding a congruence matrix between two Gram matrices is an equivalent problem to that of the LIP.

3.4 Cryptography and Algorithmic Tools

Here we present the key results in cryptography used in our algorithm. First, we recall Babai's celebrated *rounding off* algorithm:

Algorithm 1 $\mathsf{Round}_{\mathcal{B}}(y)$

Require: – A basis $\mathcal{B} = \{\mathbf{b}_r : 1 \leq r \leq d\}$ of a vector space V.
– A vector $y = \sum_{r=1}^{d} y_r \mathbf{b}_r$ expressed in terms of $\mathcal{B}$.
Ensure: $w = \sum_{r=1}^{d} w_r \mathbf{b}_r$ expressed in terms of $\mathcal{B}$.
1: $w_r \leftarrow \lfloor y_r \rceil$ for $1 \leq r \leq d$ ▷ $\lfloor \cdot \rceil$ denotes rounding
2: **return** $w = \sum_{r=1}^{d} w_r \mathbf{b}_r$

Suppose that $\mathcal{B} = \{\mathbf{b}_r \colon 1 \leq r \leq d\}$ is a basis of V and we are given $y = \sum_{r=1}^{d} y_r \mathbf{b}_r$. If for some constant $C > 0$, we have $\|\mathbf{b}_r\|_2 \leq C$ for all $1 \leq r \leq d$, then by the Cauchy-Schwarz inequality,

$$\|y - \mathsf{Round}_{\mathcal{B}}(y)\|_2 \leq Cd.$$

We now define several versions of the principal ideal problem, covering the setting of both number fields and quaternion algebras:

Definition 10 (PIP). *Suppose that F is a number field with ring of integers $\mathcal{O}_F$. Given a principal ideal $\mathfrak{a} \leq \mathcal{O}_F$, compute $g \in \mathfrak{a}$ such that $\mathfrak{a} = (g)$.*

Definition 11 ($\mathcal{O}$-PIP). *Suppose that $\mathcal{A}$ is a quaternion algebra, $\mathcal{O} \subset \mathcal{A}$ an order, and let $\mathcal{I}$ be a principal right $\mathcal{O}$-ideal. Find $g \in \mathcal{I}$ such that $\mathcal{I} = g\mathcal{O}$.*

Definition 12 ($\mathcal{O}$-nrdPIP). *Suppose that $\mathcal{A}$ is a quaternion algebra, $\mathcal{O} \subset \mathcal{A}$ an order, and let $\mathcal{I}$ be a principal right $\mathcal{O}$-ideal. Given $q \in K$ such that $\mathrm{nrd}(\mathcal{I}) = q\mathcal{O}_K$, compute an element $g \in \mathcal{I}$ such that $\mathrm{nrd}(g) = q$, assuming that one exists.*

Definition 13. *Suppose that A is an order. We denote the $\mathbb{Q}$-algebra $A \otimes_{\mathbb{Z}} \mathbb{Q}$ by $A_{\mathbb{Q}}$. We write $(A_{\mathbb{Q}}^{+})_{\gg 0}$ for the set of all $w \in A_{\mathbb{Q}}$ with the property that $\psi(w) \in \mathbb{R}_{>0}$ for each ring homomorphism $\psi \colon A_{\mathbb{Q}} \to \mathbb{C}$.*

Remark 2. Suppose that K is a totally real number field with ring of integers $A := \mathcal{O}_K$. Note that $A_{\mathbb{Q}} := \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Q} \cong K$ and the kernel of any ring homomorphism $\psi \colon A_{\mathbb{Q}} \cong K \to \mathbb{C}$ can be identified with an ideal of K. Of course, K is a field, so the kernel must either be $A_{\mathbb{Q}}$ or 0. In other words, any non-zero ring homomorphism $\psi \colon A_{\mathbb{Q}} \to \mathbb{C}$ is automatically injective. Therefore, $\mathrm{Hom}(A_{\mathbb{Q}}, \mathbb{C})$ is the set of embeddings $A_{\mathbb{Q}} \cong K \hookrightarrow \mathbb{C}$. We conclude that $(A_{\mathbb{Q}}^{+})_{\gg 0}$ can be identified with the set of totally positive elements of K.[5]

Definition 14. *A CM-order A is an order such that:*

- *A has no non-zero nilpotent elements;*
- *A is equipped with an automorphism $x \mapsto \overline{x}$ of A such that $\psi(\overline{x}) = \overline{\psi(x)}$ for all $x \in A$ and all ring homomorphisms $\psi : A \to \mathbb{C}$.*

[5] One can generalise this remark to an arbitrary number field F by taking K to be the maximal totally real subfield of F.

Theorem 5 (Lenstra-Silverberg). *There is a deterministic polynomial-time algorithm that given a CM-order A, a fractional A-ideal I, and an element $w \in (A_{\mathbb{Q}}^{+})_{\gg 0}$ satisfying $I\overline{I} = Aw$, decides whether there exists $v \in A_{\mathbb{Q}}$ such that $I = Av$ and $v\overline{v} = w$, and if so computes such an element v.*

Proof. This is precisely [25, Theorem 1.3]. □

A reduction from the rank-2 module-LIP instances underlying HAWK to nrdPIP is given in [8]: this result lies at the very core of our algorithm. Before we present the main result of this work, we must provide some technical definitions.

Definition 15. *Let L be a number field of degree d, and suppose that $\mathcal{B}$ is a fixed LLL-reduced $\mathbb{Z}$-basis of $\mathcal{O}_L$. Given an element $x \in L$, we can represent x as a vector in $\mathbb{Q}^d$ by recording the coordinates of x with respect to $\mathcal{B}$. For a rational number a/b with a, b coprime, we define*

$$\mathrm{size}(a/b) = \lceil \log_2 |a| \rceil + \lceil \log_2 |b| \rceil.$$

If x is represented by $(x_r)_{r=1}^{d}$ with respect to $\mathcal{B}$, then we set

$$\mathrm{size}(x) = \sum_{r=1}^{d} \mathrm{size}(x_r).$$

Suppose that $\mathbf{G} = (G, (\mathfrak{a}_r)_{r=1}^{m})$ is a pseudo-Gram matrix over L. Set

$$\mathrm{size}(G) = \sum_{1 \le r,s \le m} \mathrm{size}(G_{rs}).$$

Any fractional ideal $\mathfrak{a}$ of $\mathcal{O}_L$ has an LLL-reduced $\mathbb{Z}$-basis $(y_1, \ldots, y_d)$. We define

$$\mathrm{size}(\mathfrak{a}) = \sum_{r=1}^{d} \mathrm{size}(y_r).$$

Finally, we define the size of $\mathbf{G}$ as

$$\mathrm{size}(\mathbf{G}) := \mathrm{size}(G) + \sum_{r=1}^{m} \mathrm{size}(\mathfrak{a}_r).$$

We now give a brief description of the construction of a principal ideal with desired reduced norm as given in [8, Section 3.1]. In what follows, we take $L = \mathbb{Q}(\zeta_n)$. We begin by recalling the map

$$\begin{aligned} \varphi : L^2 &\to \mathcal{A}, \\ (x, y) &\mapsto x + yj. \end{aligned}$$

Consider a module lattice $\mathcal{M} \subset L^2$ defined by the pseudo-basis $\mathbf{B} = (B, \mathfrak{a}_1, \mathfrak{a}_2)$, where $\mathfrak{a}_1, \mathfrak{a}_2$ are fractional ideals of $\mathcal{O}_L$ and $B = (\mathbf{b}_1 \mid \mathbf{b}_2)$.

Lemma 1. *The left ideal $\mathcal{J} := \mathcal{O}\varphi(\mathcal{M})$ may be explicitly written as*

$$\mathcal{J} = \mathcal{O}\mathfrak{a}_1\varphi(\mathbf{b}_1) + \mathcal{O}\mathfrak{a}_2\varphi(\mathbf{b}_2).$$

Proof. See [8, Definition 3.1, Lemma 3.2]. □

Proposition 1. *Take $\mathcal{J}$ as in Lemma 1 and define $\mathcal{O}' = \mathcal{O}_R(\mathcal{J})$. Then $\mathcal{O}' = \mathcal{J}^{-1}\mathcal{J}$ is a maximal order, and moreover*

$$\varphi(\mathbf{b}_1)\mathcal{O}' = \mathfrak{a}_1^{-1}\mathcal{J} \cap \varphi(\mathbf{b}_1)\varphi(\mathbf{b}_2)^{-1}\mathfrak{a}_2^{-1}\mathcal{J}.$$

Proof. See [8, Proposition 3.6]. □

Lemma 2. *Consider a module $\mathcal{M}$ defined by the pseudo-Gram matrix*

$$\mathbf{G} = (G = \begin{pmatrix} q_{11} & q_{12} \\ \overline{q_{12}} & q_{22} \end{pmatrix}, \mathfrak{a}_1, \mathfrak{a}_2),$$

where $q_{rs} \in \mathcal{O}_L$ for $r, s \in \{1, 2\}$ and $\mathfrak{a}_1, \mathfrak{a}_2 \leq \mathcal{O}_L$. Then for $B \in M_2(\mathcal{O}_L)$ with columns $\mathbf{b}_1$ and $\mathbf{b}_2$, we have

$$B^*B = G \iff \begin{cases} \mathrm{nrd}(\varphi(\mathbf{b}_1)) = q_{11}, \\ \mathrm{nrd}(\varphi(\mathbf{b}_2)) = q_{22}, \\ \varphi(\mathbf{b}_1)\varphi(\mathbf{b}_2)^{-1} = q_{22}^{-1}(\overline{q_{12}} - \det(B)j). \end{cases}$$

Proof. See [8, Lemma 3.5]. □

Combining all the above results, it follows that the principal right ideal $\mathcal{I} = \varphi(\mathbf{b}_1)\mathcal{O}'$ is constructible using values from the pseudo-Gram matrix as

$$\mathcal{I} = \mathfrak{a}_1^{-1}\mathcal{J} \cap q_{22}^{-1}(\overline{q_{12}} - \det(B)j)\mathfrak{a}_2^{-1}\mathcal{J},$$

and has reduced norm $\mathrm{nrd}(\varphi(\mathbf{b}_1)) = q_{11}$. We will write $\Phi(\mathbf{G}) = \mathcal{I}$.

Now we consider the special case of HAWK, where $\mathfrak{a}_1 = \mathfrak{a}_2 = \mathcal{O}_L$, $\mathcal{M} = \mathcal{O}_L^2$, and therefore $\mathcal{J} = \mathcal{O}' = \mathcal{O}$. Combining the above results, we find that, given a HAWK pseudo-Gram matrix $\mathbf{G}$ with private pseudo-basis $\mathbf{B}$, we may construct the principal right ideal

$$\mathcal{I} = \mathcal{O} \cap q_{22}^{-1}(\overline{q_{12}} - j)\mathcal{O},$$

where $\mathrm{nrd}(\mathcal{I}) = q_{11}\mathcal{O}_K$, from public values only. This right ideal is principally generated by $\varphi(\mathbf{b}_1)$.

We are now able to introduce the rank-2 module-LIP to nrdPIP reduction:

Theorem 6. *Let $m \geq 31$ and L be the m-th cyclotomic field, of degree $d = \phi(m)$. Let $M = \mathcal{O}_L^2$, with a pseudo-basis $\mathbf{B} = (B, \mathfrak{a}_1, \mathfrak{a}_2)$ and pseudo-Gram matrix $\mathbf{G}$. Let $\mathbf{G}' = (G', \mathfrak{b}_1, \mathfrak{b}_2)$ be a pseudo-Gram matrix congruent to $\mathbf{G}$. Assume*

that we are given an oracle $\mathfrak{O}$ that solves $\mathcal{O}$-nrdPIP. There exists an algorithm that returns the set $\mathrm{Cong}(\mathbf{G}, \mathbf{G}')$ *of all congruence matrices between* $\mathbf{G}$ *and* $\mathbf{G}'$*. Moreover, this algorithm makes exactly one call to the oracle $\mathfrak{O}$ and except for this call it runs in time*

$$\mathrm{poly}(d, \mathrm{size}(\mathbf{G}), \mathrm{size}(\mathbf{G}')).$$

Proof. This is a slightly restated version of [8, Theorem 4.3]. □

3.5 Notation and Assumptions

Throughout the rest of the paper, we adopt the following non-standard notation. Let $L = \mathbb{Q}(\zeta_n)$ where $n = 2^l$ and define K as the maximal totally real subfield of L. We define $\mathcal{A} := (-1, -1 \,|\, K)$ to be the totally definite quaternion algebra over K with the 'usual' relations $i^2 = j^2 = k^2 = -1$ and $ij = -ji = k$. Choose a maximal order $\mathcal{O} \subset \mathcal{A}$ containing $\Lambda := \mathcal{O}_L + j\mathcal{O}_L$. Given a matrix $M \in M_2(\mathbb{C})$, we denote the Hermitian conjugate of M by M^*. As in Section 3.4, given a pseudo-Gram matrix $\mathbf{G}$, we can construct a corresponding right $\mathcal{O}$-ideal $\Phi(\mathbf{G})$, which we take as global notation.

Throughout this work, we will assume Weber's conjecture, a long-standing open problem in number theory:

Conjecture 1 (Weber's Class Number Problem) *Consider the following family of number fields:*

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

Let $h_{K_{2^l}}$ denote the class number of K_{2^l}. Weber's class number problem, also known as Weber's conjecture, postulates that $h_{K_{2^l}} = 1$ for all $l \geq 3$.

Remark 3. This is presented as a reasonable conjecture in the literature. For example, it has been shown that $h_{K_{2^l}}$ is not divisible by any prime number less than 1.2×10^8 for $l \geq 3$ [17].

Following Remark 3, we will assume Weber's conjecture throughout the paper. This is standard throughout the surrounding cryptographic literature, for example, see [9].

4 The Algorithm

We next give an outline of our algorithm, highlighting the key steps in the procedure. Suppose that we are given a valid HAWK public key $G \in M_2(\mathcal{O}_L)$, and denote the corresponding private key as $B \in M_2(\mathcal{O}_L)$. Of course, G is

the Gram matrix associated to B, so $G = B^*B$. We begin by sampling a lower-triangular unimodular matrix $U \in M_2(\mathcal{O}_L)$ with short entries, a so-called 'guess'. Concretely,

$$U := \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix},$$

where each coefficient of $x \in \mathcal{O}_L$ is sampled from a discrete Gaussian.[6] We then define $G' := U^*GU$, set $q' := (G')_{11}$, and check that q' is 'short enough'. By Section 6, this occurs with overwhelming probability. Following the rank-2 $\mathcal{O}_L$-module LIP to $\mathcal{O}$-nrdPIP reduction of [8], we form the nrdPIP instance corresponding to G'. This produces a principal right $\mathcal{O}$-ideal $\mathcal{I} = \Phi(G', \mathcal{O}_L, \mathcal{O}_L)$ with reduced norm $q'\mathcal{O}_K$. By Theorem 6, computing an element $g \in \mathcal{I}$ of reduced norm q' is sufficient to find $C' := CU$, where $C'^*C' = G'$ and therefore recover a HAWK private key C. We then find a two-element representation $\mathcal{I} = (\beta_0, q')\mathcal{O}$, which, as in Section 5, can be done in probabilistic polynomial time. Using Babai's rounding algorithm (Algorithm 1) we can find $\beta \in \mathcal{O}$ 'short' with $\mathcal{I} = (\beta, q')\mathcal{O}$. We then define

$$\alpha = -\mathrm{nrd}(\beta) + \frac{\mathrm{trd}(\beta)^2}{4},$$

and set $F = K(\sqrt{\alpha})$, a number field (explicitly) isomorphic to $K(\beta)$. For technical purposes, we check that $\mathcal{O}_F = \mathcal{O}_K[\sqrt{\alpha}]$, which (heuristically) occurs with high probability, as shown in Section 7. If this is not the case, then we 'guess again'. In Section 8, we (heuristically) show that q' is a norm from F with non-negligible probability. If this is not the case, we take another guess. Otherwise, using the Lenstra-Silverberg algorithm (Theorem 5), we can recover $h \in F$ with $N_{F/K}(h) = q'$ in deterministic polynomial time. Let $\chi : K(\beta) \to K(\sqrt{\alpha})$ be an explicit morphism of fields. We observe that $\chi^{-1}(h)\mathcal{O}_{K(\beta)}$ and $(\beta, q')\mathcal{O}_{K(\beta)}$ are both fractional $\mathcal{O}_{K(\beta)}$-ideals of reduced norm $q'\mathcal{O}_K$. In Section 9, we show that there are only $O(n^{1+o(1)})$ such ideals. Therefore, granting Heuristic 4, $\chi^{-1}(h)\mathcal{O}_{K(\beta)} = (\beta, q')\mathcal{O}_{K(\beta)}$ with non-negligible probability. If this is not the case, we guess again. Otherwise, we find that $\mathcal{I} = \chi^{-1}(h)\mathcal{O}$, which solves the $\mathcal{O}$-nrdPIP instance associated to G'. Following [8], we can compute $C' := CU$, where $C'^*C' = G'$, and can therefore recover a HAWK private key C as $C := C'U^{-1}$. The pseudocode for our algorithm is presented below as Algorithm 2.

5 Two-Element Representations

5.1 The First Heuristic: The Probability that $\alpha\mathcal{O}_K$ is Square-Free

Definition 16. *We will refer to an element $y \in \mathcal{O}_K$ as square-free if (y) is square-free as an ideal of $\mathcal{O}_K$. We note that, under Weber's conjecture, $\mathcal{O}_K$ is a UFD, so this coincides with the 'usual' notion of square-freeness.*

[6] With respect to the power basis of $\mathcal{O}_L$.

Algorithm 2 GuessingGame

Require: – A valid HAWK public key $G \in M_2(\mathcal{O}_L)$ with corresponding pseudo-Gram matrix $\mathbf{G} := (G, \mathcal{O}_L, \mathcal{O}_L)$ and some $\sigma \approx 2$.
Ensure: $C \in M_2(\mathcal{O}_L)$ with $C^*C = G$.

win $\leftarrow 0$
while win $= 0$ **do**
  $x_r \leftarrow \mathcal{D}_{\mathbb{Z},\sigma}$ for $1 \le r \le n/2$
  $x \leftarrow \sum_{r=1}^{n/2} x_r \zeta_n^r$
  $U \leftarrow \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}$
  $G' \leftarrow U^* G U$ ▷ 'Close' rank-2 module-LIP instance
  $q' \leftarrow G'_{11}$
  if $\|q'\|_2 > \Omega(n^{11/2})$ **then** ▷ Sec. 6
    continue
  end if
  $\mathbf{G}' \leftarrow (G', \mathcal{O}_L, \mathcal{O}_L)$
  $\mathcal{I} \leftarrow \Phi(\mathbf{G}')$ ▷ Form the $\mathcal{O}$-nrdPIP Instance
  if $q'\mathcal{O}_K$ is not a prime ideal **then**
    continue
  end if
  Compute $\beta_0 \in \mathcal{O}$ with $\mathcal{I} = (\beta_0, q')\mathcal{O}$ ▷ Sec. 5
  $\mathcal{B} \leftarrow \{q'\zeta_n^r,\ q'j\zeta_n^r : 1 \le r \le n/2\}$
  Reduce β_0 using $\mathcal{B}$ to obtain β with $\mathcal{I} = (\beta, q')\mathcal{O}$, $\|\beta\|_2 < O(n^{13/2})$ ▷ Sec. 6
  $\alpha \leftarrow -\mathrm{nrd}(\beta) + \frac{\mathrm{trd}(\beta)^2}{4}$
  $F \leftarrow K(\sqrt{\alpha})$ ▷ Enter the number field setting
  if $\mathcal{O}_F \neq \mathcal{O}_K[\sqrt{\alpha}]$ **then** ▷ Sec. 7
    continue
  end if
  Let $\chi\colon K(\beta) \to K(\sqrt{\alpha})$ be an explicit morphism of fields.
  Apply the Lenstra-Silverberg algorithm (Theorem 5) to $A = \mathcal{O}_F$,
    $\mathfrak{a} = (\mathrm{trd}(\beta)/2 + \sqrt{\alpha}, q')\mathcal{O}_F$, and $w = q'$, returning $h \in F$ with $\chi^{-1}(h) \in \mathcal{I}$
    and $N_{F/K}(h) = q'$, assuming that such an element exists. In particular, since
    $\mathrm{nrd}(\chi^{-1}(h)) = N_{F/K}(h) = q'$, we have $\mathcal{I} = \chi^{-1}(h)\mathcal{O}$. ▷ Sec. 8
  if $h = \perp$ **then** ▷ Check nrdPIP instance valid
    continue
  end if
  $g \leftarrow \chi^{-1}(h)$
  Use the knowledge of a principal generator $\mathcal{I} = g\mathcal{O}$ to recover $C' := CU$
    with $C'^* C' = G'$ ▷ Sec. 10
  win $\leftarrow 1$
end while
return $C'U^{-1}$ ▷ Recover the HAWK private key

When ordered by absolute norm, the density of the square-free ideals of $\mathcal{O}_K$ is precisely

$$\prod_{\mathfrak{p} \leq \mathcal{O}_K \text{ prime}} \left(1 - \frac{1}{N\mathfrak{p}^2}\right).$$

By Theorem 2, this is equal to $1/\zeta_K(2)$. We now show that, at least heuristically, $1/\zeta_K(2) > 1/2$. Let $\mathfrak{d}$ denote the unique prime ideal of $\mathcal{O}_K$ lying over 2, and split the above product into the following three factors:

$$\frac{1}{\zeta_K(2)} = \underbrace{\left(1 - \frac{1}{N\mathfrak{d}^2}\right)}_{(*)} \underbrace{\left(\prod_{\substack{\mathfrak{d} \neq \mathfrak{p} \leq \mathcal{O}_K \text{ prime}, \\ \mathfrak{p} \cap \mathbb{Z} = (p),\ f_{\mathfrak{p}|p} = 1}} 1 - \frac{1}{N\mathfrak{p}^2}\right)}_{(**)} \underbrace{\left(\prod_{\substack{\mathfrak{p} \leq \mathcal{O}_K \text{ prime}, \\ \mathfrak{p} \cap \mathbb{Z} = (p),\ f_{\mathfrak{p}|p} \geq 2}} 1 - \frac{1}{N\mathfrak{p}^2}\right)}_{(***)}.$$

First note that the first factor $(*)$ is simply $1 - \frac{1}{4} = \frac{3}{4}$. Recall that, for $\mathfrak{p} \leq \mathcal{O}_K$ lying over a rational prime $p \in \mathbb{Z}$ unramified in K,

$$f_{\mathfrak{p}|p} = \mathrm{ord}_{(\mathbb{Z}/n\mathbb{Z})^\times/\pm 1}(p).$$

Therefore, any rational prime $p \in \mathbb{Z}$ associated with the second product $(**)$ must be congruent to ± 1 modulo n. In particular, any such prime p is greater than $n - 1$. Denote $d := [K : \mathbb{Q}] = n/4$ and observe that

$$\begin{aligned}\log(**) \approx -\sum_{\substack{\mathfrak{d} \neq \mathfrak{p} \leq \mathcal{O}_K \text{ prime}, \\ \mathfrak{p} \cap \mathbb{Z} = (p),\ f_{\mathfrak{p}|p} = 1}} \frac{1}{N\mathfrak{p}^2} &\geq -d \sum_{\substack{\mathfrak{d} \neq \mathfrak{p} \leq \mathcal{O}_K \text{ prime}, \\ \mathfrak{p} \cap \mathbb{Z} = (p),\ f_{\mathfrak{p}|p} = 1}} \frac{1}{p^2} \\ &\geq -d \sum_{\ell \geq 1} \left((\ell n - 1)^{-2} + (\ell n + 1)^{-2}\right) > -O(n^{-1}).\end{aligned}$$

On the other hand,

$$\log(***) \approx -\sum_{\substack{\mathfrak{p} \leq \mathcal{O}_K \text{ prime}, \\ \mathfrak{p} \cap \mathbb{Z} = (p),\ f_{\mathfrak{p}|p} \geq 2}} \frac{1}{N\mathfrak{p}^2} = -\sum_{\substack{\mathfrak{p} \leq \mathcal{O}_K \text{ prime}, \\ \mathfrak{p} \cap \mathbb{Z} = (p),\ f_{\mathfrak{p}|p} \geq 2}} \frac{d}{f_{\mathfrak{p}|p}} p^{-2f_{\mathfrak{p}|p}}.$$

Therefore, $\log(***)$ is approximately

$$\underbrace{-\left(\sum_{\substack{\mathfrak{p} \leq \mathcal{O}_K \text{ prime}, \\ \mathfrak{p} \cap \mathbb{Z} = (p),\ f_{\mathfrak{p}|p} \geq 2,\ p \leq \sqrt{n}}} \frac{d}{f_{\mathfrak{p}|p}} p^{-2f_{\mathfrak{p}|p}}\right)}_{(a)} \underbrace{-\left(\sum_{\substack{\mathfrak{p} \leq \mathcal{O}_K \text{ prime}, \\ \mathfrak{p} \cap \mathbb{Z} = (p),\ f_{\mathfrak{p}|p} \geq 2,\ p > \sqrt{n}}} \frac{d}{f_{\mathfrak{p}|p}} p^{-2f_{\mathfrak{p}|p}}\right)}_{(b)}.$$

If $p \leq \sqrt{n}$ and $f_{\mathfrak{p}|p} \geq 2$ then

$$\frac{d}{f_{\mathfrak{p}|p}} p^{-2f_{\mathfrak{p}|p}} < n^{-1}.$$

It follows that $(a) \leq n^{-1/2}$. On the other hand,

$$(b) \leq \frac{d}{2} \sum_{p > \sqrt{n} \text{ prime}} \frac{1}{p^4} < n \sum_{\ell > \sqrt{n}} \frac{1}{\ell^4} = O(n^{-1/2}).$$

We deduce that

$$\log(***) \gtrsim -O(n^{-1/2}).$$

Putting this all together, we conclude that

$$\log\left(\frac{1}{\zeta_K(2)}\right) \approx \log(3/4) + O(n^{-1/2}),$$

and therefore

$$\frac{1}{\zeta_K(2)} \approx \frac{3}{4}.$$

After weakening this approximation to $1/\zeta_K(2) \gtrsim 1/2$, we obtain the following heuristic:

Heuristic 1 *Let $\alpha \in \mathcal{O}_K$ be sampled as in our main algorithm (Algorithm 2). The probability that α is square-free is lower bounded by $1/2$.*

5.2 Computing Two-Element Representations

Throughout this section, we assume that one can compute a factorisation of $q' \in \mathcal{O}_K$ into primes in classical polynomial time.[7] For example, for a classical polynomial-time algorithm, we can re-sample U until q' is prime, and then test q' for primality in classical deterministic polynomial time. Here, we deal with the more general case of q' square-free, with the hope that one could perhaps use a larger class of 'easy-to-factor' integers than (just) the primes, in order to obtain a more efficient variant of GuessingGame (Algorithm 2). We briefly explain why q' is prime with non-negligible probability: in Section 6.2, we show that

$$|N_{K/\mathbb{Q}}(q')|^{1/[K:\mathbb{Q}]} < O(n^{11/2}),$$

so $|N_{K/\mathbb{Q}}(q')| < C^{n/4} n^{11n/8}$ for some constant $C > 0$. If $|N_{K/\mathbb{Q}}(q')|$ is a rational prime, then $q'\mathcal{O}_K$ is automatically a prime ideal. Heuristically, the 'density' of rational primes of size around y is approximately

$$\frac{\mathrm{d}}{\mathrm{d}y}\left(\frac{y}{\log y}\right) \approx \frac{1}{\log y}.$$

[7] Again, we use the term 'primes' as opposed to 'prime ideals' since $\mathcal{O}_K$ is a UFD under Weber's conjecture.

Therefore, the probability that $q'\mathcal{O}_K$ is a prime ideal is (heuristically) at least

$$\frac{1}{\log(N_{K/\mathbb{Q}}(q'))} > \Omega\left(\frac{1}{n\log(n)}\right).$$

Therefore, on average, we expect to re-sample x polynomially many times before $q'\mathcal{O}_K$ is a prime ideal. In what follows, assume that $q'\mathcal{O}_K$ is square-free as an ideal of $\mathcal{O}_K$.[8]

Suppose that we are given a principal right ideal $\mathcal{I} \leq \mathcal{O}$ and an element $q' \in \mathcal{O}_K$ for which $\mathrm{nrd}(\mathcal{I}) = q'\mathcal{O}_K$. In this section, we show that one can compute a two-element representation $\mathcal{I} = (\beta_0, q')\mathcal{O}$ in probabilistic polynomial time.

Suppose that $\mathfrak{p} \leq \mathcal{O}_K$ is a prime ideal dividing $q'\mathcal{O}_K$, and let $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_{p^r}$ where p is the rational prime lying under $\mathfrak{p}$ and $r \in \mathbb{N}$. Observe that $\mathcal{O}/\mathfrak{p}\mathcal{O}$ can be viewed as an order of the quaternion algebra

$$\left(\frac{-1,-1}{\mathbb{F}_{p^r}}\right),$$

under (canonical) isomorphism. By [43, Section 4], we can explicitly compute an isomorphism $\chi_\mathfrak{p} : \mathcal{O}/\mathfrak{p}\mathcal{O} \xrightarrow{\sim} M_2(\mathcal{O}_K/\mathfrak{p})$ in probabilistic polynomial time. Compute the image $\mathcal{J}$ of $\mathcal{I}$ under the chain of morphisms

$$\mathcal{O} \xrightarrow{\pi} \mathcal{O}/\mathfrak{p}\mathcal{O} \xrightarrow{\chi_\mathfrak{p}} M_2(\mathbb{F}_{p^r}),$$

where $\pi : \mathcal{O} \to \mathcal{O}/\mathfrak{p}\mathcal{O}$ is the quotient map. Note that $\mathcal{J}$ is a non-trivial right ideal of $M_2(\mathbb{F}_{p^r})$, which is a principal ideal ring. Therefore, any non-zero element of $\mathcal{J}$ is a principal generator, and we can compute such a generator $g_\mathfrak{p}$ in polynomial time. Let $\widetilde{g_\mathfrak{p}}$ denote a lift of $g_\mathfrak{p}$ to $\mathcal{I}$. By the Chinese remainder theorem, we can compute $\delta_\mathfrak{p} \in \mathcal{O}_K$ such that for any $\mathfrak{q} \,|\, (q')$,

$$\delta_\mathfrak{p} \equiv \mathbf{1}_{\mathfrak{p}=\mathfrak{q}} \pmod{\mathfrak{q}}.$$

We then exhibit

$$\beta_0 := \sum_{\mathfrak{q} \,|\, (q')} \delta_\mathfrak{q} \widetilde{g_\mathfrak{q}}.$$

By considering reduced norms, one finds that $\mathcal{I} = (\beta_0, q')\mathcal{O}$.

6 Bounding Norms

Setting: In Algorithm 2, we begin by sampling $x_r \leftarrow \mathcal{D}_{\mathbb{Z},\sigma}$ for $1 \leq r \leq n/2$, where $\sigma \approx 2$. We then form the element $x = \sum_{r=1}^{n/2} x_r \zeta_n^r$ and define the unimod-

[8] One can assume Heuristic 1 with α replaced with q' to see that q' is square-free with high probability.

ular matrix

$$U := \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \in M_2(\mathcal{O}_L).$$

In this section, we would like to bound the entries of $G' := U^* G U$.[9] This will allow us to find a 'short' two-element representation of $\mathcal{I} := \Phi(\mathbf{G}') \leq \mathcal{O}$ where $\mathbf{G}' = (G', \mathcal{O}_L, \mathcal{O}_L)$. In turn, this will ensure that the parameters passed to the Lenstra-Silverberg algorithm on line 25 of Algorithm 2 are of polynomial size.

6.1 HAWK Key Generation

We begin by studying the distribution of the HAWK private basis B and the corresponding public Gram matrix G as generated in [11, Algorithm 1] which will allow us to bound the entries of B. Loosely following the notation of [11], we define the number ring

$$R := \frac{\mathbb{Z}[X]}{(X^{n/2} + 1)},$$

which may be naturally identified with $\mathcal{O}_L$ by 'replacing' X with ζ_n. Throughout the rest of the paper, R and $\mathcal{O}_L$ are interchangeable, and we will use the notation that best fits the local context.

In the first step of [11, Algorithm 1], one samples $f, g \in R$ with coefficients from $\mathcal{D}_{\mathbb{Z},\sigma_{pk}}$ where $\sigma_{pk} \lesssim 2$ for all suggested HAWK parameters [11, Section 5.1]. We then set

$$(F_0, G_0)^\intercal = \mathsf{TowerSolveI}_{n/2,1}(f, g),$$

using [36, Algorithm 4], which is given below (Algorithm 3), largely in the notation of the original paper.[10] Here, $(F_0, G_0) \in \mathbb{Z}^n$ denotes the concatenation of the coefficient vectors of F_0 and G_0. Crucially, as in [36, Proof of Lemma 3],

$$\|(F_0, G_0)\|_2^2 = O(n^2 \|(f, g)\|_2^2).$$

Since $\|(f, g)\|_2^2 = O(n)$ with overwhelming probability, it follows that

$$\|(F_0, G_0)\|_2^2 = O(n^3),$$

with overwhelming probability. In step 6 of the HAWK key generation procedure [11, Algorithm 1], the second private basis vector $(F_0, G_0)^\intercal$ is subsequently reduced using fast Babai reduction [12], but this only decreases the Euclidean norm of $(F_0, G_0)^\intercal$. We conclude that, upon completion of [11, Algorithm 1],

$$\|(F_0, G_0)\|_2^2 = O(n^3), \tag{1}$$

with overwhelming probability. The HAWK private basis is defined as

$$B := \begin{pmatrix} f & F_0 \\ g & G_0 \end{pmatrix},$$

with corresponding public Gram matrix $G := B^* B$.

[9] In the 2-norm with respect to the usual power basis of $\mathcal{O}_L$.

[10] We have replaced the use of 'n' in the original paper with 'k' to avoid confusion.

Algorithm 3 $\mathsf{TowerSolve}l_{k,q}(f, g)$

Require: $-$ $f, g \in \mathbb{Z}[x]/(x^k + 1)$ with k a power of two
$-$ $\mathbb{L} = \mathbb{Z}[x]/(x^k + 1)$ and $\mathbb{K} = \mathbb{Z}[x]/(x^{k/2} + 1)$
Ensure: Polynomials F_0, G_0 such that $fG_0 - gF_0 = q$

$(f', g') \leftarrow (f, g)$
for $i \leftarrow 1, \ldots, \log k$ **do**
  $(f', g') \leftarrow (N_{\mathbb{L}/\mathbb{K}}(f'), N_{\mathbb{L}/\mathbb{K}}(g'))$ ▷ At that point, f' and g' have degree 0
end for
Compute $u, v \in \mathbb{Z}$ such that $uf' - vg' = \mathrm{GCD}(f, g)$
if $\delta = \mathrm{GCD}(f, g)$ is not a divisor of q **then**
  abort
end if
$(F_0, G_0) \leftarrow (vq/\delta, uq/\delta)$
for $i \leftarrow \log k, \ldots, 1$ **do**
  $(f', g') \leftarrow (f, g)$
  for $j \leftarrow 1, \ldots, i - 1$ **do**
    $(f', g') \leftarrow (N_{\mathbb{L}/\mathbb{K}}(f'), N_{\mathbb{L}/\mathbb{K}}(g'))$
  end for
  $(F_0, G_0) \leftarrow (g'^{\times} F_0, f'^{\times} G_0)$
  $\mathsf{Reduce}(f', g', F_0, G_0)$ ▷ [36, Algorithm 1]
end for
return (F_0, G_0)

6.2 Bounding q'

Lemma 3. *Let $\|\cdot\|_2$ denote the 2-norm on L with respect to the usual power basis. Then for $x, y \in \mathcal{O}_L \backslash \{0\}$,*

$$\frac{\|xy\|_2}{\|x\|_2 \cdot \|y\|_2} \leq \sqrt{n}.$$

Proof. This is a restatement of [19, Lemma 7.4.3]. □

In the notation of Algorithm 2, write

$$G = \begin{pmatrix} q_{11} & q_{12} \\ q_{21} & q_{22} \end{pmatrix}, \; G' = \begin{pmatrix} q'_{11} & q'_{12} \\ q'_{21} & q'_{22} \end{pmatrix}.$$

One can compute the entries of G directly:

$$\begin{aligned} q_{11} &= f^* f + g^* g, \\ q_{12} &= f^* F_0 + g^* G_0, \\ q_{21} &= \overline{q_{12}} = F_0^* f + G_0^* g, \\ q_{22} &= F_0^* F_0 + G_0^* G_0. \end{aligned}$$

Lemma 3 allows us to bound the entries of G. For example, by equation (1),

$$\begin{aligned}\|q_{22}\|_2 &\leq \|F_0^* F_0\|_2 + \|G_0^* G_0\|_2 \\ &\leq \sqrt{n}\,(\|F_0\|_2\|F_0^*\|_2 + \|G_0\|_2\|G_0^*\|_2) \\ &\lesssim O(n^{7/2}).\end{aligned}$$

Since $\|(f,g)\|_2^2 = O(n)$, we obtain the corresponding bounds on all entries:

$$\|q_{rs}\|_2 < O(n^{7/2}),$$

for $r, s \in \{1, 2\}$. We will also want to bound the (absolute) algebraic norm of each q_{rs}, which can be achieved using the following result:

Lemma 4. *Suppose that $y \in L$ and define $\|y\|_2$ with respect to the usual power basis of $\mathcal{O}_L$. Then*

$$N_{L/\mathbb{Q}}(y)^{\frac{1}{[L:\mathbb{Q}]}} \leq \|y\|_2.$$

Proof. By definition,

$$N_{L/\mathbb{Q}}(y) = \prod_{\sigma \in \mathrm{Gal}(L/\mathbb{Q})} \sigma(y).$$

The result is now an immediate consequence of the AM-GM inequality, since

$$\|\sigma(y)\|_2 = \|y\|_2$$

for all $y \in L$ and $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$. □

A direct computation shows that

$$G'_{11} := q' = q_{11} + \overline{xq_{12}} + xq_{12} + x\overline{x}q_{22}.$$

By the triangle inequality for $\|\cdot\|_2$, we deduce that

$$\|q'\|_2 \leq \|q_{11}\|_2 + 2\|xq_{12}\|_2 + \|x\overline{x}q_{22}\|_2.$$

Repeatedly applying Lemma 3, we find that

$$\|q'\|_2 < O\left(\sqrt{n} \cdot \sqrt{n} \cdot \|x\|_2^2 \cdot \|q_{22}\|_2\right).$$

Since we sample each coefficient of x from $\mathcal{D}_{\mathbb{Z},\sigma}$, it follows that $\|x\|_2^2 < O(n)$ with overwhelming probability. Combining this with the above discussion, we conclude that $\|q'\|_2 < O(n^{11/2})$ with overwhelming probability. By Lemma 4, we also have

$$|N_{K/\mathbb{Q}}(q')|^{1/[K:\mathbb{Q}]} < O(n^{11/2})$$

with overwhelming probability.

6.3 Reducing the Length of β_0

We now detail step 18 of GuessingGame: given a right ideal $\mathcal{I} \leq \mathcal{O}$ with explicit two-element generation $\mathcal{I} = (\beta_0, q')\mathcal{O}$, find $\beta \in \mathcal{O}$ with $\mathcal{I} = (\beta, q')\mathcal{O}$ and

$$\|\beta\|_2 < O(n^{13/2}).$$

We will accomplish this using Babai's rounding off algorithm (Algorithm 1). We define the *natural order* $\Lambda \subset \mathcal{A}$ as the lattice contained in $\mathcal{A}$ with $\mathbb{Z}$-basis

$$\widetilde{\mathcal{B}} := \{\zeta_n^r, j\zeta_n^r : 1 \leq r \leq n/2\}.$$

We define the 2-norm on $\mathcal{A}$ with respect to this basis $\widetilde{\mathcal{B}}$. Note that $q'\Lambda \subset q'\mathcal{O}$ and $q'\Lambda$ has $\mathbb{Z}$-basis $q'\widetilde{\mathcal{B}}$ in which every basis vector has 2-norm at most

$$\|q'\|_2 < O(n^{11/2}).$$

Therefore, using Babai's rounding off algorithm, one can compute $u \in q'\Lambda$ with

$$\|\beta_0 - u\|_2 < O(n^{13/2}).$$

We define $\beta := \beta_0 - u$. By construction, $\beta_0 \equiv \beta \bmod q'\mathcal{O}$ so

$$(\beta_0, q')\mathcal{O} = (\beta, q')\mathcal{O}.$$

6.4 Bounding α

Lemma 5. *Let $\|\cdot\|_2$ denote the 2-norm on $\mathcal{A}$ with respect to the $\mathbb{Q}$-basis*

$$\mathcal{B} = \{\zeta_n^r, j\zeta_n^r : 1 \leq r \leq n/2\}.$$

Suppose that $a, b \in \mathcal{A}\backslash\{0\}$. Then

$$\frac{\|ab\|_2}{\|a\|_2 \cdot \|b\|_2} \leq \sqrt{8n}.$$

Proof. Following [29], we define

$$\delta_2 = \sup\left\{\frac{\|cd\|_2}{\|c\|_2\|d\|_2} : c, d \in \mathcal{O}_L\backslash 0\right\},$$
$$\delta_2^{quat} = \sup\left\{\frac{\|cd\|_2}{\|c\|_2\|d\|_2} : c, d \in \Lambda\backslash 0\right\}.$$

Suppose that we are given $c, d \in \Lambda$. Write

$$c = c_1 + jc_2,$$
$$d = d_1 + jd_2,$$

where $c_1, c_2, d_1, d_2 \in \mathcal{O}_L$. After a straightforward computation, we find that

$$\|cd\|_2^2 = \|(c_1d_1 - \overline{c_2}d_2) + j(\overline{c_1}d_2 + c_2d_1)\|_2^2 = \|c_1d_1 - \overline{c_2}d_2\|_2^2 + \|\overline{c_1}d_2 + c_2d_1\|_2^2.$$

By the triangle inequality, this is at most

$$\|c_1d_1\|_2^2 + 2\|c_1d_1\|_2 \cdot \|\overline{c_2}d_2\|_2 + \|\overline{c_2}d_2\|_2^2 + \|\overline{c_1}d_2\|_2^2 + 2\|\overline{c_1}d_2\|_2 \cdot \|c_2d_1\|_2 + \|c_2d_1\|_2^2.$$

By Lemma 3, we therefore have

$$\|cd\|_2^2 \leq n(\|c_1\|_2^2 \cdot \|d_1\|_2^2 + \|c_2\|_2^2 \cdot \|d_2\|_2^2 + \|c_1\|_2^2 \cdot \|d_2\|_2^2 + \|c_2\|_2^2 \cdot \|d_1\|_2^2 + 4\|c_1\|_2 \cdot \|d_1\|_2 \cdot \|c_2\|_2 \cdot \|d_2\|_2).$$

Note that $\|c_1\|_2, \|c_2\|_2 \leq \|c\|_2$ and $\|d_1\|_2, \|d_2\|_2 \leq \|d\|_2$. We conclude that

$$\|cd\|_2^2 \leq 8n\|c\|_2^2 \cdot \|d\|_2^2.$$

In other words, we have shown that, for any $c, d \in \Lambda \backslash 0$,

$$\frac{\|cd\|_2}{\|c\|_2 \cdot \|d\|_2} \leq \sqrt{8n}.$$

One can extend this result to general elements $a, b \in \mathcal{A}$ using the fact that there exists $d \in \mathbb{Z}$ such that $da, db \in \Lambda$. □

Recall that we define

$$\alpha = -\mathrm{nrd}(\beta) + \frac{\mathrm{trd}(\beta)^2}{4} = -\beta\overline{\beta} + \frac{(\beta + \overline{\beta})^2}{4} = \frac{\beta^2 + \overline{\beta}^2}{4} - \frac{1}{2}\beta\overline{\beta}.$$

Since $\|\beta\|_2 < O(n^{13/2})$ with overwhelming probability, by Lemma 5,

$$\|\beta^2\|_2 \leq \delta_2^{quat}\|\beta\|_2^2 \leq \sqrt{8n}\,\|\beta\|_2^2 < O(n^{27/2}),$$

with overwhelming probability. We deduce that, with overwhelming probability,

$$\|\alpha\|_2 < O(n^{27/2}). \tag{2}$$

By Lemma 4, we conclude that

$$N_{K/\mathbb{Q}}(\alpha)^{\frac{1}{[K:\mathbb{Q}]}} < O(n^{27/2}), \tag{3}$$

again with overwhelming probability.

7 'Monogenic' Generation

Sample $\alpha \in \mathcal{O}_K$ as in GuessingGame and form the totally complex K-extension $F := K(\sqrt{\alpha})$. In this section, we estimate the probability that $\mathcal{O}_F = \mathcal{O}_K[\sqrt{\alpha}]$.

Lemma 6. *Let $F := K(\sqrt{\alpha})$ where $\alpha \in \mathcal{O}_K$ is square-free and let $\mathfrak{d}$ denote the unique prime ideal of $\mathcal{O}_K$ lying over 2. Assume that the image of α in $\mathcal{O}_K/\mathfrak{d}^2$ is not a square, and that $\mathfrak{d} \nmid \alpha\mathcal{O}_K$. Then $\mathcal{O}_F = \mathcal{O}_K[\sqrt{\alpha}]$.*

Proof. If $\mathcal{O}_F \neq \mathcal{O}_K[\sqrt{\alpha}]$ then we may choose $y \in \mathcal{O}_F \backslash \mathcal{O}_K[\sqrt{\alpha}]$ and write

$$y = a + b\sqrt{\alpha},$$

where $a, b \in K$. Since $y \in \mathcal{O}_F$, we have

$$\mathrm{Tr}(y) = 2a,\ N_{F/K}(y) = a^2 - \alpha b^2 \in \mathcal{O}_F \cap K = \mathcal{O}_K.$$

Therefore, $a' := 2a \in \mathcal{O}_K$. As $a^2 - \alpha b^2 \in \mathcal{O}_K$, we have that $4\alpha b^2 = \alpha(2b)^2 \in \mathcal{O}_K$. Since α is square-free, assuming Weber's conjecture ($\mathcal{O}_K$ is a UFD), we deduce that $2b \in \mathcal{O}_K$. Therefore, we can set $b' := 2b \in \mathcal{O}_K$ and therefore write

$$y = \frac{a' + b'\sqrt{\alpha}}{2},$$

where $a', b' \in \mathcal{O}_K$. By the well-ordering principle, there exists $\delta \in \mathcal{O}_K$ such that

$$y = \frac{e + f\sqrt{\alpha}}{\delta},$$

where $v_{\mathfrak{d}}(\delta)$ is chosen to be minimal. Again, since $N_{F/K}(y) \in \mathcal{O}_K$, we find that $e^2 - \alpha f^2 \equiv 0 \bmod \delta^2\mathcal{O}_K$. We claim that f is invertible modulo $\delta^2\mathcal{O}_K$. Indeed, if $\mathfrak{d} | f\mathcal{O}_K$, then $e^2 \equiv 0 \bmod \mathfrak{d}$, and therefore $e \in \mathfrak{d}$. This contradicts the minimality of $v_{\mathfrak{d}}(\delta)$, proving the claim. Since $e^2 = \alpha f^2 \bmod \delta^2\mathcal{O}_K$ and f is invertible modulo $\delta^2\mathcal{O}_K$, we conclude that α is a square modulo $\mathfrak{d}^2$, which is a contradiction. □

Note that $\mathcal{O}_K/\mathfrak{d}^2 \cong \mathbb{F}_2[X]/(X^2)$. Since $\mathbb{F}_2[X]/(X^2)$ contains the non-square element $X + 1 \bmod X^2$, $\mathcal{O}_K/\mathfrak{d}^2$ contains a non-square element γ corresponding to $X + 1 \bmod X^2$. If $\overline{\gamma}$ is a lift of γ to $\mathcal{O}_K$ via the quotient map $\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{d}^2$, then $\mathfrak{d} \nmid \gamma\mathcal{O}_K$. Therefore, we propose the following heuristic:

Heuristic 2 *Let $\mathfrak{d} \leq \mathcal{O}_K$ be the unique prime ideal of $\mathcal{O}_K$ lying over 2. There is a natural isomorphism $\mathcal{O}_K/\mathfrak{d}^2 \cong \mathbb{F}_2[X]/(X^2)$. The image of α in the quotient $\mathcal{O}_K/\mathfrak{d}^2$ corresponds to $X + 1 \in \mathbb{F}_2[X]/(X^2)$ with probability around $1/4$.*

Assuming Heuristic 2 and applying Lemma 6, we deduce that $\mathcal{O}_F = \mathcal{O}_K[\sqrt{\alpha}]$ with high probability.

8 Solving Norm Equations

8.1 The Number of Primes Dividing q' and α

Assuming that $\|q'\|_2 < O(n^{11/2})$, which holds with overwhelming probability, by Lemma 4, we have

$$N_{K/\mathbb{Q}}(q')^{\frac{1}{[K:\mathbb{Q}]}} < O(n^{11/2}).$$

Equivalently, there exists a constant $D > 0$ such that

$$N_{K/\mathbb{Q}}(q') < D^{\frac{n}{4}} n^{\frac{11n}{8}}.$$

The number of prime ideals dividing $q'\mathcal{O}_K$ is at most the number of rational primes dividing $N_{K/\mathbb{Q}}(q')$, including multiplicity. By the Erdős-Kac Theorem (Theorem 1), the number of primes dividing $N_{K/\mathbb{Q}}(q')$ is at most

$$(1 + o(1)) \log\log(N_{K/\mathbb{Q}}(q')) < (1 + o(1)) \log\log(D^{\frac{n}{4}} n^{\frac{11n}{8}}) = (1 + o(1)) \log(n),$$

with overwhelming probability. Similarly, the number of primes dividing $N_{K/\mathbb{Q}}(\alpha)$ is at most $(1 + o(1)) \log(n)$ with overwhelming probability.

8.2 Our Third Heuristic

By the Hasse Norm Theorem (Theorem 3), if $q' \in N_{F_v/K_v}(F_v^\times)$ for every $v \in \mathrm{Pl}(K)$ then there exists $g \in F$ with

$$N_{F/K}(g) = q'.$$

We first compute the index of the local norms $N_{F_v/K_v}(F_v^\times)$ in $K_v^\times$ at each place v of K. Let $v \in \mathrm{Pl}(K)$ and split into cases according to the nature of v:

1. v is an infinite place. Since q' is totally positive, q' is a local norm at v.

2. v is a finite place that does not divide q' and v is unramified in F. Then $N_{F_v/K_v}(\mathcal{O}_{F,v}^\times) = \mathcal{O}_{K,v}^\times$ and $q' \in \mathcal{O}_{K,v}^\times$ so q' is a local norm at v.

3. v is a finite place that ramifies in F. By local Artin reciprocity (Theorem 4),

   $$[K_v^\times : N_{F_v/K_v}(F_v^\times)] = |\mathrm{Gal}(F_v/K_v)| = 2.$$

   Since all ramified primes divide $2\alpha\mathcal{O}_K$, there are at most $(1 + o(1)) \log(n)$ such primes.

4. v is an unramified finite place dividing q'. By local Artin reciprocity (Theorem 4),

   $$[K_v^\times : N_{F_v/K_v}(F_v^\times)] \leq 2.$$

   Note that $q'\mathcal{O}_K$ has at most $(1 + o(1)) \log(n)$ prime ideal factors with overwhelming probability, so there are at most $(1 + o(1)) \log(n)$ such primes, again, with overwhelming probability.

In order to state our next heuristic, we reformulate the above in the language of log S-unit lattices.

Theorem 7 (S-Unit Theorem). *Let K be a number field, and let S be a finite set of places of K including all of the archimedean ones. Let $U_{K,S}$ denote the S-unit group of K, given by*

$$U_{K,S} = \{y \in K^\times : \|y\|_v = 1 \ \forall v \notin S\}.$$

The S-unit group $U_{K,S}$ is a finitely generated abelian group of rank $\#S - 1$. Let $\mathrm{Tor}(U_{K,S})$ denote the finite-order elements of $U_{K,S}$. Under the embedding $\mathrm{Log} : U_{K,S}/\mathrm{Tor}(U_{K,S}) \to \mathbb{R}^{\#S}$ given by

$$\xi \mapsto \left(\frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log \|\xi\|_v \right)_v,$$

the image of Log *is a lattice which spans the trace zero hyperplane*

$$\left\{ y \in \mathbb{R}^{\#S} : \sum_v y_v = 0 \right\}.$$

Proof. This formulation is given in [16, Introduction], although the theorem is due to Dirichlet, Hasse, and Chevalley [16]. □

Consider the following set of places of K:

$$\begin{aligned} S := \{v \in \mathrm{Pl}(K) \text{ finite}, \ v \,|\, q'\mathcal{O}_K\} \cup \{v \in \mathrm{Pl}(K) \text{ finite, ramified in } F\} \\ \cup \{v \in \mathrm{Pl}(K) \text{ archimedean}\}. \end{aligned}$$

By Theorem 7,

$$\mathcal{L} := \mathrm{Log}(U_{K,S} \bmod \mathrm{Tor}(U_{K,S})) \subset \mathbb{R}^{\#S}$$

is a lattice spanning the trace-zero hyperplane in $\mathbb{R}^{\#S}$. Since K is totally real, $\mathrm{Tor}(U_{K,S}) = \{\pm 1\}$. Let $U^+_{K,S}$ denote the subgroup of totally positive elements, and let H be the subgroup of $U_{K,S}$ defined as the union of totally positive and totally negative elements. We can define the lattices

$$\begin{aligned} \mathcal{L}' &:= \mathrm{Log}(H), \\ \mathcal{L}'' &:= \mathrm{Log}(\pm N_{F/K}(F^\times) \cap U_{K,S}). \end{aligned}$$

Let S' denote the finite places of S and consider the natural map

$$\xi : U^+_{K,S} \to \prod_{v \in S'} \frac{K_v^\times}{N_{F_v/K_v}(F_v^\times)}.$$

By the Hasse Norm Theorem (Theorem 3), $\ker(\xi) \subset U^+_{K,S} \cap N_{F/K}(F^\times)$. We immediately deduce that

$$\left| \frac{U^+_{K,S}}{U^+_{K,S} \cap N_{F/K}(F^\times)} \right| \leq \left| \prod_{v \in S'} \frac{K_v^\times}{N_{F_v/K_v}(F_v^\times)} \right| \leq 2^{\#S'},$$

which allows us to obtain

$$[\mathcal{L}' : \mathcal{L}''] = [U_{K,S}^{+} : N_{F/K}(F^{\times}) \cap U_{K,S}] \leq \prod_{v \in S'} [K_v^{\times} : N_{F_v/K_v}(F_v^{\times})] < O(n^{2+o(1)}),$$

with overwhelming probability. This naturally leads to the following heuristic:

Heuristic 3 *Note that* $\mathrm{Log}(q') \in \mathcal{L}'$ *and* $\mathcal{L}''$ *is an index* $O(n^{2+o(1)})$ *sub-lattice of* $\mathcal{L}'$. *The image of* $\mathrm{Log}(q')$ *in* $\mathcal{L}'/\mathcal{L}''$ *is* 0 *with probability* $\Omega(n^{-2-o(1)})$.

9 The Coup de Grâce

Recall that we define

$$\alpha = -\mathrm{nrd}(\beta) + \frac{\mathrm{trd}(\beta)^2}{4}.$$

Note that β satisfies the quadratic equation

$$\beta^2 - \mathrm{trd}(\beta)\beta + \mathrm{nrd}(\beta) = 0,$$

and by completing the square, one finds that

$$\left(\beta - \frac{\mathrm{trd}(\beta)}{2}\right)^2 = \alpha.$$

Therefore, $K(\beta) \cong K(\sqrt{\alpha})$ as fields, and this isomorphism can be explicitly defined by sending

$$\beta - \frac{\mathrm{trd}(\beta)}{2} \mapsto \sqrt{\alpha}.$$

We will denote this (field) isomorphism as $\chi : K(\beta) \to K(\sqrt{\alpha})$. Define $\mathfrak{a} := (\mathrm{trd}(\beta)/2 + \sqrt{\alpha}, q') \leq \mathcal{O}_F$ and note that $\mathcal{I} = \chi^{-1}(\mathfrak{a})\mathcal{O}$ if $\mathcal{O}_F = \mathcal{O}_K[\sqrt{\alpha}]$ (and therefore $\mathcal{O}_{K(\beta)} = \mathcal{O}_K[\beta]$), which occurs with high probability, assuming Heuristics 1 and 2. Assume that there exists $h \in F := K(\sqrt{\alpha}) \cong K(\beta)$ with

$$N_{F/K}(h) = q',$$

which under Heuristic 3, occurs with non-negligible probability. We observe that $h\mathcal{O}_F$ and $\mathfrak{a}$ are both ideals of $\mathcal{O}_F$ with relative norm $q'\mathcal{O}_K$ (over the extension F/K). Since $q'\mathcal{O}_K$ has at most $\log(n^{1+o(1)})$ prime factors, there are at most $O(n^{1+o(1)})$ ideals of $\mathcal{O}_F$ with relative norm $q'\mathcal{O}_K$, with overwhelming probability. Therefore, we propose the following heuristic:

Heuristic 4 *Let* α *be sampled as in our main algorithm (Algorithm 2) and define* $F := K(\sqrt{\alpha})$. *Form the ideal* $\mathfrak{a} := (\mathrm{trd}(\beta)/2 + \sqrt{\alpha}, q') \leq \mathcal{O}_F$ *and note that* $N_{F/K}(\mathfrak{a}) = q'\mathcal{O}_K$. *There are at most* $O(n^{1+o(1)})$ *ideals of* $\mathcal{O}_F$ *with relative norm* $q'\mathcal{O}_K$ *with overwhelming probability. Given that one of these ideals is principal, the probability that* $\mathfrak{a}$ *itself is principal is* $\Omega(n^{-1-o(1)})$.

In what follows, we assume that $\mathfrak{a}$ is principal, which holds with non-negligible probability under Heuristics 3 and 4. Since F/K is a CM extension, we can compute an element $h \in \mathfrak{a}$ with

$$N_{F/K}(h) = \mathrm{nrd}(\chi^{-1}(h)) = q',$$

in deterministic polynomial time using the Lenstra-Silverberg Algorithm (Theorem 5). Define $g := \chi^{-1}(h)$. Since $g \in \mathcal{I}$ and $\mathrm{nrd}(g) = q'$, it immediately follows that $\mathcal{I} = g\mathcal{O}$.

10 Completing the Key Recovery Attack

Assume that we reach line 35 (win = 1) in GuessingGame. Let U denote the current unimodular matrix 'guess', and let $G' = U^*GU$ be the corresponding Gram matrix. Assume that we have found $g \in \mathcal{O}$ such that $g\mathcal{O} = \mathcal{I}$ where $\mathbf{G}' := (G', \mathcal{O}_L, \mathcal{O}_L)$ and $\mathcal{I} := \Phi(\mathbf{G}')$ is the right $\mathcal{O}$-ideal attached to G'.

Applying Theorem 6 to the two pseudo-Gram matrices $(I_2, \mathcal{O}_L, \mathcal{O}_L)$ and $(G', \mathcal{O}_L, \mathcal{O}_L)$, we find that one call to a nrdPIP oracle $\mathfrak{O}$ is sufficient to compute

$$\mathrm{Cong}((I_2, \mathcal{O}_L, \mathcal{O}_L), (G', \mathcal{O}_L, \mathcal{O}_L)).$$

We claim that the relevant call to $\mathfrak{O}$ is parameterised by $(q', \mathcal{I})$. There is a clash of notation between [8] and this work, so we must take care when checking this. In [8, Algorithm 3], on line 8, we pass the parameters

$$(\mathbf{B}, \mathbf{G}', \delta_0, \mathcal{O}, I_M, \mathcal{O}', \mathcal{O}'^1) := ((I_2, \mathcal{O}_L, \mathcal{O}_L), (G', \mathcal{O}_L, \mathcal{O}_L), 1, \mathcal{O}, \mathcal{O}, \mathcal{O}, \langle \zeta_n, j \rangle)$$

to [8, Algorithm 1], where the left hand side of the above equation is written in the notation of [8], while the right hand side is written in our notation. The nrdPIP oracle is then called on line 7 of [8, Algorithm 1] for the fractional right $\mathcal{O}$-ideal, $\Phi(\mathbf{G}')$, with corresponding reduced norm q'_{11}, where q'_{rs} denote the entries of G'. By Lemma 2, this right ideal is equal to $\mathcal{I}$. Since $\mathrm{nrd}(\mathcal{I}) = q'_{11}$, we may replace this instance of the oracle $\mathfrak{O}$ with the output from GuessingGame.

11 The Complexity Class: PPT

There are three main considerations in deducing the complexity of GuessingGame:

1. The expected number of 'guesses' until 'win = 1'.
2. Verifying that the Lenstra-Silverberg Algorithm (Theorem 5) call on line 25 of Algorithm 2 indeed runs in deterministic polynomial time.
3. The complexity of [8, Algorithm 1] when recovering B' (line 33).

Theorem 8 (Heuristic Full Key Recovery Attack on HAWK). *Suppose that $B \in M_2(\mathcal{O}_L)$ is a basis of $\mathcal{O}_L^2$ and $G := B^*B$. There exists a probabilistic polynomial-time algorithm that returns $C \in M_2(\mathcal{O}_L)$ with $C^*C = G$, assuming Weber's conjecture and Heuristics 1, 2, 3, 4.*

Proof. We look at the three main considerations, as outlined above:

1. We expect to re-sample U around $O(n\log(n))$ times before $q'\mathcal{O}_K$ is a prime ideal. Combining this with Heuristics 1, 2, 3, 4, the probability that we set 'win = 1' for a given 'guess' $U \in M_2(\mathcal{O}_L)$ is $\Omega(n^{-4-o(1)})$. Therefore, we expect a total of around
$$O(n^{4+o(1)}\log(n))$$
guesses before we set 'win = 1'.[11]

2. It suffices to show that the parameters $(\mathrm{trd}(\beta)/2 + \sqrt{\alpha}, q') \leq \mathcal{O}_F$ and $q'\mathcal{O}_K = \mathcal{I}\overline{\mathcal{I}}$ passed to the Lenstra-Silverberg algorithm on line 25 of Algorithm 2 are of polynomial size. This is clear since $\|q'\|_2 < O(n^{11/2})$ and $\|\beta\|_2 < O(n^{13/2})$ with overwhelming probability.

3. By Theorem 6, the complexity of step 33 of GuessingGame is polynomial in
$$n, \mathrm{size}(I_2, \mathcal{O}_L, \mathcal{O}_L), \text{ and } \mathrm{size}(G', \mathcal{O}_L, \mathcal{O}_L).$$
We first note that
$$\mathrm{size}(I_2, \mathcal{O}_L, \mathcal{O}_L) = \mathrm{size}(I_2) + \mathrm{size}(\mathcal{O}_L) + \mathrm{size}(\mathcal{O}_L) = n + n < O(n).$$
Moreover, for $y, z \in \mathcal{O}_L$, $\mathrm{size}(y\cdot z) < \mathrm{poly}(\mathrm{size}(y), \mathrm{size}(z), \log|\Delta_L|)$ [8, pp.34]. By [44, Proposition 2.1], since $L = \mathbb{Q}(\zeta_n)$ with $n = 2^l$, we have
$$\Delta_L = 2^{2^{l-1}(l-1)}.$$
We conclude that $\log|\Delta_L| < O(n\log(n))$. Next, for $G' = U^*GU$, we have
$$G' = \begin{pmatrix} q_{11} + q_{12}x + q_{21}x^* + q_{22}xx^* & q_{12} + x^*q_{22} \\ q_{21} + q_{22}x & q_{22} \end{pmatrix}.$$
Therefore, in order to show that $\mathrm{size}(G') < \mathrm{poly}(n)$, it suffices to show that $\mathrm{size}(f), \mathrm{size}(g), \mathrm{size}(F_0), \mathrm{size}(G_0) < \mathrm{poly}(n)$, that is, $\mathrm{size}(G) < \mathrm{poly}(n)$. Since $f, g, F_0, G_0 \in R \cong \mathcal{O}_L$ and
$$\|f\|_2^2, \|g\|_2^2, \|F_0\|_2^2, \|G_0\|_2^2 < O(n^3),$$
we deduce that $\mathrm{size}(G) < \mathrm{poly}(n)$ as required.

□

[11] We don't need to run the Lenstra-Silverberg algorithm before checking that $q'\mathcal{O}_K$ is prime. Therefore, we estimate the expected number of calls to the Lenstra-Silverberg algorithm as $O(n^{3+o(1)})$ as opposed to $O(n^{4+o(1)}\log(n))$.

12 Conclusion and Further Work

We conclude by remarking that the security of LIP is in part provided by the size of $\mathrm{GL}_n(\mathbb{Z})$, the haystack, which hides the congruence matrix, the needle. However, it is this very property that allows us to conduct our attack; we are able to find enough 'short straws' which in turn reveal the needle. We have given an algorithm, Algorithm 2, to solve the specific case of rank-2 module-LIP underpinning HAWK, which after avoiding the multitude of attacks launched at it, may have finally suffered a blow. Moreover, under seemingly reasonable number-theoretic heuristics, our algorithm runs in polynomial-time. Naturally, we flag the experimental verification of these heuristics as an interesting open question.

Again, we reiterate that this attack does *not* break nrdPIP in quaternion orders, and may in fact point us towards building cryptography using this as the hardness assumption, as is done in [31]. It also raises the matter of whether similar reductions may be hiding similar re-sampling attacks that may be useful for the analysis of other problems and schemes.

Finally, we again point out that as it stands, this does not break general rank-2 module-LIP. We acknowledge that there are places in which we must use certain remarkable properties of cyclotomic fields, and specifically power-of-two cyclotomic fields. We believe that the extension of the methods used and presented here may extend to cover the general case, and leave this for future work.

References

1. Allombert, B., Pellet-Mary, A., van Woerden, W.P.J.: Cryptanalysis of rank-2 module-LIP: A single real embedding is all it takes. In: Fehr, S., Fouque, P.A. (eds.) Advances in Cryptology – EUROCRYPT 2025, Part II. Lecture Notes in Computer Science, vol. 15602, pp. 184–212. Springer, Cham, Switzerland, Madrid, Spain (May 4–8, 2025). https://doi.org/10.1007/978-3-031-91124-8_7
2. Biasse, J.F., Song, F.: Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. In: Krauthgamer, R. (ed.) 27th Annual ACM-SIAM Symposium on Discrete Algorithms. pp. 893–902. ACM-SIAM, Arlington, VA, USA (Jan 10–12, 2016). https://doi.org/10.1137/1.9781611974331.ch64
3. Bos, J.W., Bronchain, O., Ducas, L., Fehr, S., Huang, Y.H., Pornin, T., Postlethwaite, E.W., Prest, T., Pulles, L.N., van Woerden, W.: HAWK. Tech. rep., National Institute of Standards and Technology (2026), round 3 specification. Available at https://csrc.nist.gov/Projects/pqc-dig-sig/round-3-additional-signatures
4. Campbell, P., Groves, M., Shepherd, D.: Soliloquy: A cautionary tale. In: ETSI 2nd Quantum-Safe Crypto Workshop (2014), https://docbox.etsi.org/Workshop/2014/201410_CRYPTO/S07_Systems_and_Attacks/S07_Groves_Annex.pdf
5. Cassels, J.W.S., Fröhlich, A. (eds.): Algebraic Number Theory. Academic Press (1967)

6. Chevignard, C., Fouque, P.A., Mureau, G., Pellet-Mary, A., Wallet, A.: A reduction from hawk to the principal ideal problem in a quaternion algebra. Cryptology ePrint Archive, Report 2024/1147 (2024), https://eprint.iacr.org/2024/1147
7. Chevignard, C., Mureau, G.: Ideally HAWKward: How not to break module-LIP. Cryptology ePrint Archive, Report 2025/1095 (2025), https://eprint.iacr.org/2025/1095
8. Chevignard, C., Mureau, G., Espitau, T., Pellet-Mary, A., Pliatsok, H., Wallet, A.: A reduction from hawk to the principal ideal problem in a quaternion algebra. In: Fehr, S., Fouque, P.A. (eds.) Advances in Cryptology – EUROCRYPT 2025, Part II. Lecture Notes in Computer Science, vol. 15602, pp. 154–183. Springer, Cham, Switzerland, Madrid, Spain (May 4–8, 2025). https://doi.org/10.1007/978-3-031-91124-8_6
9. Cramer, R., Ducas, L., Peikert, C., Regev, O.: Recovering short generators of principal ideals in cyclotomic rings. In: Fischlin, M., Coron, J.S. (eds.) Advances in Cryptology – EUROCRYPT 2016, Part II. Lecture Notes in Computer Science, vol. 9666, pp. 559–585. Springer Berlin Heidelberg, Germany, Vienna, Austria (May 8–12, 2016). https://doi.org/10.1007/978-3-662-49896-5_20
10. Diffie, W., Hellman, M.E.: New directions in cryptography. IEEE Transactions on Information Theory **22**(6), 644–654 (1976). https://doi.org/10.1109/TIT.1976.1055638
11. Ducas, L., Postlethwaite, E.W., Pulles, L.N., van Woerden, W.P.J.: Hawk: Module LIP makes lattice signatures fast, compact and simple. In: Agrawal, S., Lin, D. (eds.) Advances in Cryptology – ASIACRYPT 2022, Part IV. Lecture Notes in Computer Science, vol. 13794, pp. 65–94. Springer, Cham, Switzerland, Taipei, Taiwan (Dec 5–9, 2022). https://doi.org/10.1007/978-3-031-22972-5_3
12. Ducas, L., Prest, T.: Fast Fourier orthogonalization. Cryptology ePrint Archive, Report 2015/1014 (2015), https://eprint.iacr.org/2015/1014
13. Ducas, L., van Woerden, W.P.J.: On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography. In: Dunkelman, O., Dziembowski, S. (eds.) Advances in Cryptology – EUROCRYPT 2022, Part III. Lecture Notes in Computer Science, vol. 13277, pp. 643–673. Springer, Cham, Switzerland, Trondheim, Norway (May 30 – Jun 3, 2022). https://doi.org/10.1007/978-3-031-07082-2_23
14. Erdős, P., Kac, M.: The Gaussian Law of Errors in the Theory of Additive Number Theoretic Functions. American Journal of Mathematics **62**(1), 738–742 (1940). https://doi.org/10.2307/2371483
15. Espitau, T., Pliatsok, H.: On hermitian decomposition lattices and the module-LIP problem in rank 2. Cryptology ePrint Archive, Report 2024/1148 (2024), https://eprint.iacr.org/2024/1148
16. Fili, P., Miner, Z.: A generalization of dirichlet's unit theorem. Acta Arithmetica **162**(4), 355–368 (2014). https://doi.org/10.4064/aa162-4-3
17. Fukuda, T., Komatsu, K.: Weber's class number problem in the cyclotomic z2-extension of q, ii. Journal de Théorie des Nombres de Bordeaux (2010)
18. van Gent, D.M.H., Pulles, L.N.: HAWK: Having automorphisms weakens key. IACR Communications in Cryptology (CiC) **2**(2), 20 (2025). https://doi.org/10.62056/a3qjp2w9p
19. Gentry, C.: A Fully Homomorphic Encryption Scheme. Ph.D. thesis, Stanford University (2009), https://crypto.stanford.edu/craig/
20. Gentry, C., Szydlo, M.: Cryptanalysis of the revised NTRU signature scheme. In: Knudsen, L.R. (ed.) Advances in Cryptology – EUROCRYPT 2002. Lecture Notes

in Computer Science, vol. 2332, pp. 299–320. Springer Berlin Heidelberg, Germany, Amsterdam, The Netherlands (Apr 28 – May 2, 2002). https://doi.org/10.1007/3-540-46035-7_20
21. Haviv, I., Regev, O.: On the lattice isomorphism problem. In: Chekuri, C. (ed.) 25th Annual ACM-SIAM Symposium on Discrete Algorithms. pp. 391–404. ACM-SIAM, Portland, OR, USA (Jan 5–7, 2014). https://doi.org/10.1137/1.9781611973402.29
22. Kirchner, P.: Algorithms on ideal over complex multiplication order. Cryptology ePrint Archive, Report 2016/220 (2016), https://eprint.iacr.org/2016/220
23. Kirschmer, M., Voight, J.: Algorithmic enumeration of ideal classes for quaternion orders. SIAM J. Comput. **39**, 1714–1747 (2008). https://doi.org/10.5555/1958016.1958018
24. Lenstra, H.W., Silverberg, A.: Revisiting the Gentry-Szydlo algorithm. In: Garay, J.A., Gennaro, R. (eds.) Advances in Cryptology – CRYPTO 2014, Part I. Lecture Notes in Computer Science, vol. 8616, pp. 280–296. Springer Berlin Heidelberg, Germany, Santa Barbara, CA, USA (Aug 17–21, 2014). https://doi.org/10.1007/978-3-662-44371-2_16
25. Lenstra, H.W., Silverberg, A.: Testing isomorphism of lattices over CM-orders. SIAM Journal on Computing **48**(4), 1300–1334 (2019). https://doi.org/10.1137/17M115390X
26. Lenstra, Jr., H.W., Silverberg, A.: Lattices with symmetry. Journal of Cryptology **30**(3), 760–804 (Jul 2017). https://doi.org/10.1007/s00145-016-9235-7
27. Luo, H., Jiang, K., Pan, Y., Wang, A.: Cryptanalysis of rank-2 module-LIP with symplectic automorphisms. In: Chung, K.M., Sasaki, Y. (eds.) Advances in Cryptology – ASIACRYPT 2024, Part IV. Lecture Notes in Computer Science, vol. 15487, pp. 359–385. Springer, Singapore, Singapore, Kolkata, India (Dec 9–13, 2024). https://doi.org/10.1007/978-981-96-0894-2_12
28. Lyubashevsky, V., Ducas, L., Kiltz, E., Lepoint, T., Schwabe, P., Seiler, G., Stehlé, D., Bai, S.: CRYSTALS-DILITHIUM. Tech. rep., National Institute of Standards and Technology (2022), available at https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022
29. Lyubashevsky, V., Micciancio, D.: Generalized compact Knapsacks are collision resistant. In: Bugliesi, M., Preneel, B., Sassone, V., Wegener, I. (eds.) ICALP 2006: 33rd International Colloquium on Automata, Languages and Programming, Part II. Lecture Notes in Computer Science, vol. 4052, pp. 144–155. Springer Berlin Heidelberg, Germany, Venice, Italy (Jul 10–14, 2006). https://doi.org/10.1007/11787006_13
30. Marcus, D.A.: Number Fields. Universitext, Springer, Cham (2018). https://doi.org/10.1007/978-3-319-90233-3
31. Mendelsohn, A., Nelson, B.: SoliloQuat: Throwing caution to the wind. Cryptology ePrint Archive, Paper 2026/859 (2026), https://eprint.iacr.org/2026/859
32. Mureau, G., Pellet-Mary, A., Pliatsok, G., Wallet, A.: Cryptanalysis of rank-2 module-LIP in totally real number fields. In: Joye, M., Leander, G. (eds.) Advances in Cryptology – EUROCRYPT 2024, Part VII. Lecture Notes in Computer Science, vol. 14657, pp. 226–255. Springer, Cham, Switzerland, Zurich, Switzerland (May 26–30, 2024). https://doi.org/10.1007/978-3-031-58754-2_9
33. National Institute of Standards and Technology: Post-quantum cryptography: Call for proposals. Tech. rep. (2016), https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/call-for-proposals

34. National Institute of Standards and Technology: Call for additional digital signature schemes for the post-quantum cryptography standardization process. Tech. rep. (2022), https://csrc.nist.gov/projects/pqc-dig-sig/standardization/call-for-proposals
35. Neukirch, J., Schmidt, A., Wingberg, K.: Cohomology of Number Fields, Grundlehren der mathematischen Wissenschaften, vol. 323. Springer, Berlin, Heidelberg, 2 edn. (2008). https://doi.org/10.1007/978-3-540-37889-1
36. Pornin, T., Prest, T.: More efficient algorithms for the NTRU key generation using the field norm. In: Lin, D., Sako, K. (eds.) PKC 2019: 22nd International Conference on Theory and Practice of Public Key Cryptography, Part II. Lecture Notes in Computer Science, vol. 11443, pp. 504–533. Springer, Cham, Switzerland, Beijing, China (Apr 14–17, 2019). https://doi.org/10.1007/978-3-030-17259-6_17
37. Prest, T., Fouque, P.A., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Ricosset, T., Seiler, G., Whyte, W., Zhang, Z.: FALCON. Tech. rep., National Institute of Standards and Technology (2022), available at https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022
38. Rivest, R.L., Shamir, A., Adleman, L.M.: A method for obtaining digital signatures and public-key cryptosystems. Communications of the Association for Computing Machinery **21**(2), 120–126 (Feb 1978). https://doi.org/10.1145/359340.359342
39. Schwabe, P., Avanzi, R., Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Seiler, G., Stehlé, D., Ding, J.: CRYSTALS-KYBER. Tech. rep., National Institute of Standards and Technology (2022), available at https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022
40. Shor, P.W.: Algorithms for quantum computation: Discrete logarithms and factoring. In: 35th Annual Symposium on Foundations of Computer Science. pp. 124–134. IEEE Computer Society Press, Santa Fe, NM, USA (Nov 20–22, 1994). https://doi.org/10.1109/SFCS.1994.365700
41. Smart, N.P., Vercauteren, F.: Fully homomorphic encryption with relatively small key and ciphertext sizes. In: Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010: 13th International Conference on Theory and Practice of Public Key Cryptography. Lecture Notes in Computer Science, vol. 6056, pp. 420–443. Springer Berlin Heidelberg, Germany, Paris, France (May 26–28, 2010). https://doi.org/10.1007/978-3-642-13013-7_25
42. Voight, J.: Quaternion Algebras. Graduate Texts in Mathematics, Springer International Publishing (2021)
43. Voight, J.: Identifying the matrix ring: algorithms for quaternion algebras and quadratic forms. arXiv preprint arXiv:1004.0994 (2010)
44. Washington, L.: Introduction to Cyclotomic Fields. Graduate Texts in Mathematics, Springer New York (1997)