IACR Communications in Cryptology
ISSN 3006-5496, Vol. 2, No. 2, 12 pages.

https://doi.org/10.62056/a3qjp2w9p

Check for updates

HAWK: Having Automorphisms Weakens Key

Daniël M. H. van Gent and Ludo N. Pulles

Centrum Wiskunde & Informatica, Cryptology Group, Amsterdam, the Netherlands

Abstract. The search rank-2 module Lattice Isomorphism Problem (smLIP), over a cyclotomic ring of degree a power of two, can be reduced to an instance of the Lattice Isomorphism Problem (LIP) of at most half the rank if an adversary knows a nontrivial automorphism of the underlying integer lattice. Knowledge of such a nontrivial automorphism speeds up the key recovery attack on HAWK at least quadratically, which would halve the number of security bits.
Luo *et al.* (ASIACRYPT 2024) recently found an automorphism that breaks omSVP, the initial underlying hardness assumption of HAWK. The team of HAWK amended the definition of omSVP to include this so-called symplectic automorphism in their submission to the second round of NIST's standardization of additional signatures. This work provides confidence in the soundness of this updated definition, assuming smLIP is hard, since there are plausibly no more trivial automorphisms that allow winning the omSVP game easily.
Although this work does not affect the security of HAWK, it opens up a new attack avenue involving the automorphism group that may be theoretically interesting on its own.

Keywords: Automorphism · Cryptanalysis · Lattice Isomorphism Problem · HAWK

1 Introduction

The *Lattice Isomorphism Problem* (LIP) has recently been introduced as a building block for cryptography [DvW22, BGPS23], and has already inspired the creation of a fast and compact signature scheme named HAWK [DPPvW22]. LIP for the integer lattice ($\mathbb{Z}$LIP) has been well-studied [Szy03, BM21, Duc24, BN24], and LIP for *ideal lattices* can be solved in polynomial time with the Gentry–Szydlo algorithm [GS02, LS17, LS19]. However, SUF-CMA security of HAWK is based on a new problem, called *one more Shortest Vector Problem* (omSVP). Since omSVP has received limited attention so far [DPPvW22, LJPW24], it requires more extensive study to increase confidence in HAWK.

Private key recovery for HAWK has received significantly more attention than omSVP. The former requires solving the so-called *search module LIP* (smLIP) between free modules of rank 2 over a (totally complex) cyclotomic number field. A recent line of work [MPPW24, LJPW24, APvW25] has developed a polynomial-time attack on smLIP over a number field with at least one real embedding, which remarkably is not the case with HAWK. smLIP for HAWK reduces uniformly to a principal ideal problem in a quaternion algebra [CME+25], and it remains unknown whether Gentry–Szydlo, the algorithm for the case of number fields, generalizes to such algebras. Thus far, it seems smLIP is not much easier than $\mathbb{Z}$LIP despite the extra module structure.

The signature distribution of HAWK cannot be simulated as easily as that of NTRU-based signatures, so it is not known how to instantiate the framework of [GPV08], which prevents leakage of the trapdoor basis [NR09, DN12]. Instead, security of HAWK is based on omSVP, in which an adversary, given an oracle that produces short vectors, needs to

E-mail: daniel.van.gent@cwi.nl (Daniël M. H. van Gent), lnp@cwi.nl (Ludo N. Pulles)

This work is licensed under a "CC BY 4.0" license.
Received: 2025-04-07 Accepted: 2025-06-02

output a short vector that is not a 'trivial transformation', e.g., multiplication by -1, of the previous outputs of the oracle. The parameters of HAWK are chosen based on practical cryptanalysis. For these parameters, the security reduction to omSVP produces a trivial instance of omSVP. Nevertheless, the reduction shows soundness of the design, and larger parameters reduce to a presumably hard instance of omSVP but are unfavorable for the compactness of HAWK.

The formulation of omSVP is a delicate matter, because its specification needs to include all the 'trivial transformations' that an adversary can be expected to compute. The module structure in HAWK already provides some of those, namely multiplication by roots of unity, and were considered in the original formulation [DPPvW22]. The work of [LJPW24], however, produces an additional transformation from the public information that was not considered. This transformation was a so-called *symplectic automorphism* and stems from the self-duality of the module lattice. Since then, HAWK has been amended to include the symplectic automorphism in the definition of omSVP in the submission to the second round of NIST's standardization process of additional digital signature schemes [BBD+24]. In other words, two vectors are deemed equivalent if they are in the same orbit under the group G_n generated by the roots of unity and the symplectic automorphism. The question remains whether there are more transformations publicly known which trivially solve omSVP.

1.1 Our contribution

Our main result is the following theorem, which regards $\mathbb{Z}^n$ as a module lattice R_n^2 over the n-th cyclotomic ring R_n with $n > 2$ a power of 2. The group G_n consists of the to-be-defined trivial automorphisms of R_n^2, and we write $G_{n,\mathbf{Q}} \subseteq \mathrm{GL}_n(\mathbb{Z})$ for the corresponding action of G on a Hermitian form $\mathbf{Q}$ isomorphic to R_n^2.

Theorem 1. *Given a Hermitian form $\mathbf{Q}$ of the module lattice R_n^2, and a $\mathbb{Z}$-automorphism $\mathbf{U} \in \mathrm{GL}_n(\mathbb{Z}) \setminus G_{n,\mathbf{Q}}$ of $\mathbf{Q}$, then, using standard lattice reduction heuristics, one can solve smLIP for $\mathbf{Q}$ by running BKZ-β with $\beta = n/4 + 1$ on some sublattice Λ constructed in polynomial time from $\mathbf{U}$ and that has rank at most $n/2$.*

Informally, one may think of Theorem 1 as follows: if one has a rotation of the module lattice R_n^2 and a nontrivial $\mathbb{Z}$-automorphism of it, one can recover that rotation by finding a shortest vector in a sublattice of half the rank and containing an unusually short vector.

Theorem 1 shows that with a nontrivial automorphism one can construct a specific lattice Λ of rank at most $n/2$. In Section 4, we show that BKZ-β heuristically recovers a shortest vector in such Λ for $\beta = n/4 + 1$, basically because this lattice is similarly as unusual as $\mathbb{Z}^n$. The heuristics for $\mathbb{Z}^n$ have been experimentally verified [DPPvW22], and it is proven [Duc24] that BKZ-β recovers a unit vector when $\beta = n/2 + o(n)$. Thus, Theorem 1 provides a *quadratic speed up* in solving smLIP, since BKZ-β runs in time exponential in β. Roughly speaking, if finding non-trivial automorphisms is easy, then so is smLIP. We view this as evidence that computing non-trivial automorphisms is hard, although it may just as well be that smLIP is easier than is currently assumed.

If we have an oracle for a *random* automorphism, then [JWL+23] solves SVP significantly faster. Even without the oracle, if the automorphism is random we can with high probability obtain a much better result. It is unreasonable to assume, however, that if an attacker obtains a nontrivial automorphism it will be a truly random one. More likely, it will be highly structured, like the symplectic automorphism. Hence, Theorem 1 justifies the choice for G_n, *the group of trivial automorphisms*, in the definition of omSVP [BBD+24]. We know that G_n must include the roots of unity *and*, by [LJPW24], the symplectic automorphism, because one can trivially win omSVP otherwise. Conversely, the theorem shows that smLIP and hence omSVP becomes much easier if one knows an additional

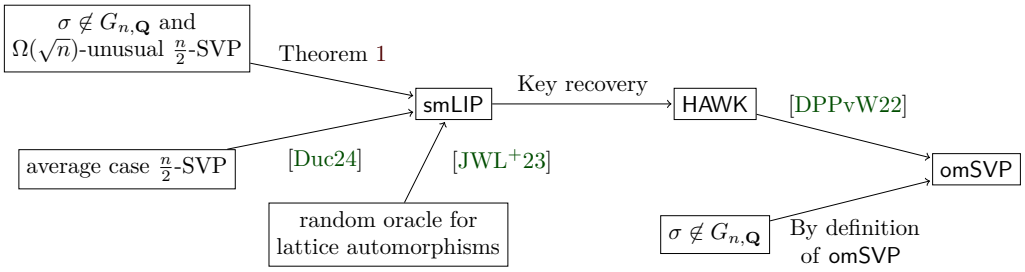

Figure 1: Reductions between problems related to the SUF-CMA security of HAWK. An arrow $A \to B$ indicates B reduces to A, i.e. B can be solved in polynomial time by making multiple queries to an algorithm that solves A.

automorphism $\sigma \notin G_n$. If there is any choice of G_n that would make omSVP hard, then the current G_n is the smallest such choice.

The situation is summarized in Figure 1.

Acknowledgments

We would like to thank Léo Ducas for the helpful discussion on the practical hardness of finding a short vector in our constructed lattices. Author Daniël van Gent is supported by the Quantum Software Consortium project (file number 024.003.037) of the Zwaartekracht research programme which is (partly) financed by the Dutch Research Council (NWO). Author Ludo Pulles is supported by ERC Starting Grant 947821 (ARTICULATE).

2 Preliminaries

Notation. Variable names for vectors and matrices are written in bold, and written in lower case and upper case respectively. The identity matrix on an n dimensional space is denoted $\mathbb{I}_n$. For a commutative ring R we define the group of *orthogonal matrices* $\mathcal{O}_n(R) = \left\{\mathbf{O} \in R^{n\times n} \,\middle|\, \mathbf{O}^\mathsf{T}\mathbf{O} = \mathbb{I}_n\right\}$, and the group $\mathrm{GL}_n(R) = \{\mathbf{M} \in R^{n\times n} \mid \exists \mathbf{N} \in R^{n\times n} \colon \mathbf{MN} = \mathbb{I}_n\}$ of *invertible matrices*.

Lattices. A *lattice* is a discrete subgroup of $\mathbb{R}^n$, and its *rank*, denoted by $\operatorname{rk}\Lambda$, is equal to the dimension of its $\mathbb{R}$-linear span. For $1 \le i \le \operatorname{rk}\Lambda$, the i-th *successive minimum* of Λ, denoted by $\lambda_i(\Lambda)$, is the smallest $r \in \mathbb{R}_{>0}$ such that the $\mathbb{R}$-linear span of $\{\mathbf{x} \in \Lambda \mid \|\mathbf{x}\| \le r\}$ has dimension at least i. Any rank-k lattice $\Lambda \subset \mathbb{R}^n$ is computationally represented by a basis $\mathbf{B} \in \mathbb{R}^{n\times k}$ for which $\Lambda = \mathbf{B} \cdot \mathbb{Z}^k$ holds. The *volume* of a lattice Λ with basis $\mathbf{B}$ is $\mathrm{Vol}(\Lambda) = \sqrt{\det(\mathbf{B}^\mathsf{T}\mathbf{B})}$. The *Gaussian Heuristic*, denoted by $\mathrm{GH}(n)$, is the expectation value of $\lambda_1(\Lambda)$ for a random lattice Λ of volume 1 and rank n. It is known that $\mathrm{GH}(n) \approx \sqrt{n/(2\pi e)}$ for $n \ge 50$ [Che13].

For an integer $k > 0$ we define the *root lattice of type A*,

$$A_k = \left\{\mathbf{x} \in \mathbb{Z}^{k+1} \,\middle|\, \sum_i \mathbf{x}_i = 0\right\}.$$

It has rank k, volume $\sqrt{k+1}$, successive minima $\lambda_1(A_k) = \cdots = \lambda_k(A_k) = \sqrt{2}$, and $k(k+1)$ shortest vectors of this length [CS98].

An *isomorphism* between lattices $\Lambda, \Lambda' \subset \mathbb{R}^n$ is an orthogonal matrix $\mathbf{O} \in \mathcal{O}_n(\mathbb{R})$ such that $\mathbf{O}\Lambda = \Lambda'$. We define the *orthogonal group* of Λ to be

$$O(\Lambda) = \{\mathbf{O} \in \mathcal{O}_n(\mathbb{R}) \mid \mathbf{O}\Lambda = \Lambda\},$$

the group consisting of all *automorphisms* of Λ, i.e., the isomorphisms from Λ to Λ. The automorphisms of the *integer lattice*, $\mathbb{Z}^n$, are precisely the *signed permutations*: a permutation of the coordinates followed by a possible sign change on each coordinate independently. Abstractly we have $O(\mathbb{Z}^n) \cong \{\pm 1\}^n \rtimes S_n$, and the group contains $2^n \cdot n!$ elements.

Equivalently, we may think of a lattice as a quadratic form on $\mathbb{R}^k$. Given a basis $\mathbf{B}$ of the lattice, the Gram matrix $\mathbf{Q} = \mathbf{B}^\mathsf{T}\mathbf{B}$ is a positive-definite symmetric bilinear form on $\mathbb{R}^k$, and conversely Cholesky decomposition provides for $\mathbf{Q}$ a basis $\mathbf{B}$ of a lattice such that $\mathbf{B}^\mathsf{T}\mathbf{B} = \mathbf{Q}$. An *isomorphism* of quadratic forms $\mathbf{Q}$ and $\mathbf{Q}'$ on $\mathbb{R}^k$ is a $\mathbf{U} \in \mathrm{GL}_k(\mathbb{Z})$ such that $\mathbf{U}^\mathsf{T}\mathbf{Q}\mathbf{U} = \mathbf{Q}'$. Analogously, we define the *orthogonal group* of a quadratic form $\mathbf{Q}$ to be

$$O(\mathbf{Q}) = \left\{ \mathbf{U} \in \mathrm{GL}_n(\mathbb{Z}) \,\middle|\, \mathbf{U}^\mathsf{T}\mathbf{Q}\mathbf{U} = \mathbf{Q} \right\}.$$

If full-rank lattices with bases $\mathbf{B}_1$ and $\mathbf{B}_2$ are isomorphic, then $\mathbf{B}_1^{-1} \cdot \mathbf{B}_2$ is an isomorphism between the corresponding quadratic forms. Conversely, if $\mathbf{U}$ is an isomorphism between the quadratic forms $\mathbf{B}_1^\mathsf{T}\mathbf{B}_1$ and $\mathbf{B}_2^\mathsf{T}\mathbf{B}_2$, then $\mathbf{B}_1\mathbf{U}\mathbf{B}_2^{-1}$ is an isomorphism between the corresponding lattices.

$\mathbb{Z}$LIP is a problem that asks, given a lattice isomorphic to $\mathbb{Z}^n$, to produce such an isomorphism. In terms of the quadratic form, that problem reads as follows.

Problem 1 ($\mathbb{Z}$LIP)**.** *Given a matrix $\mathbf{Q} \in \mathrm{GL}_n(\mathbb{Z})$ for which there exist $\mathbf{B} \in \mathrm{GL}_n(\mathbb{Z})$ such that $\mathbf{Q} = \mathbf{B}^\mathsf{T} \cdot \mathbf{B}$, compute any such $\mathbf{B}$.*

If given such a $\mathbf{B}$, it becomes easy to compute $O(\mathbf{Q})$ since we know $O(\mathbb{Z}^n)$. Without $\mathbf{B}$, we may compute the trivial automorphisms $\pm\mathbb{I}_n$. It is believed to be difficult, however, to construct any other automorphism of $\mathbf{Q}$ without solving $\mathbb{Z}$LIP.

Module Lattices. We consider the ring of integers $R_n = \mathbb{Z}[\zeta]$ of the n-th cyclotomic field, where $n \geq 4$ is a power of 2 and ζ is a primitive n-th root of unity (so $\zeta^{n/2} = -1$). Moreover, R_n comes with a complex conjugation that maps ζ to ζ^{-1}, which we denote by $(-)^\star$. For any matrix $\mathbf{M} \in R_n^{l \times m}$ we write $\mathbf{M}^\star$ for the *Hermitian adjoint* of $\mathbf{M}$, obtained by applying $(-)^\star$ coefficient-wise to $\mathbf{M}^\mathsf{T}$.

As an abelian group, R_n has a basis $(\zeta^0, \zeta^1, \ldots, \zeta^{n/2-1})$. Through the *coefficient embedding* $\mathrm{vec}\colon R_n \to \mathbb{Z}^{n/2}$ given by

$$x_0 + x_1\zeta + \cdots + x_{n/2-1}\zeta^{n/2-1} \mapsto \begin{pmatrix} x_0 \\ \vdots \\ x_{n/2-1} \end{pmatrix}$$

we may identify R_n with the lattice $\mathbb{Z}^{n/2} \subset \mathbb{R}^{n/2}$. We also consider the map $\mathrm{rot}\colon R_n \to \mathbb{Z}^{(n/2)\times(n/2)}$ given by

$$x \mapsto [\mathrm{vec}(\zeta^0 x), \mathrm{vec}(\zeta^1 x), \ldots, \mathrm{vec}(\zeta^{n/2-1} x)],$$

which satisfies $\mathrm{vec}(xy) = \mathrm{rot}(x)\mathrm{vec}(y)$ and $\mathrm{rot}(xy) = \mathrm{rot}(x)\mathrm{rot}(y)$. In particular, rot is a ring homomorphism. The names of these maps have been taken from the HAWK specification document.

An *R_n-basis* of R_n^2 is a matrix in $\mathrm{GL}_2(R_n)$. We extend the definitions to $\mathrm{vec}\colon R_n^2 \to \mathbb{Z}^n$ and $\mathrm{rot}\colon \mathrm{GL}_2(R_n) \to \mathrm{GL}_n(\mathbb{Z})$ by applying these maps coefficient-wise. In particular, we treat R_n^2 as a lattice isomorphic to $\mathbb{Z}^n$ and may associate to each R_n-basis of R_n^2 a $\mathbb{Z}$-basis of $\mathbb{Z}^n$. Note that not every $\mathbb{Z}$-basis is of this form.

To an R_n-basis $\mathbf{B}$ we associate the R_n-Gram-matrix $\mathbf{Q} = \mathbf{B}^\star\mathbf{B}$, which is in some well-defined way that we will not go into, a Hermitian form. The corresponding $\mathbb{Z}$-Gram-matrix is $\mathrm{rot}(\mathbf{Q})$. An *isomorphism* of Hermitian forms $\mathbf{Q}$ and $\mathbf{Q}'$ is a matrix $\mathbf{U} \in \mathrm{GL}_2(R_n)$ such

that $\mathbf{U}^\star\mathbf{Q}\mathbf{U} = \mathbf{Q}'$ holds, and we analogously write $O(\mathbf{Q})$ for the *group of automorphisms* of $\mathbf{Q}$. Note that rot maps $O(\mathbf{Q})$ into $O(\mathrm{rot}(\mathbf{Q}))$.

The analog to $\mathbb{Z}$LIP for R_n^2 is the following.

Problem 2 (smLIP)**.** *Given a matrix $\mathbf{Q} \in \mathrm{GL}_2(R_n)$ for which there exist $\mathbf{B} \in \mathrm{GL}_2(R_n)$ such that $\mathbf{Q} = \mathbf{B}^\star\mathbf{B}$, compute any such $\mathbf{B}$.*

Note that smLIP is not harder than $\mathbb{Z}$LIP in dimension n.

Trivial automorphisms. The *group of R_n-automorphisms* of $\mathbb{I}_2$ is equal to

$$\left\{ \begin{pmatrix} \zeta^a & 0 \\ 0 & \zeta^b \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^c \;\middle|\; 0 \le a, b < n,\ 0 \le c < 2 \right\}.$$

It has size $2n^2$, which is very little compared to $2^n \cdot n!$, the number of $\mathbb{Z}$-automorphisms. We identify ζ with the matrix $\zeta \cdot \mathbb{I}_2 \in \mathrm{GL}_2(R_n)$. The automorphism ζ of the Hermitian form $\mathbb{I}_2$ provides the following $\mathbb{Z}$-automorphism with respect to the standard basis $\mathrm{rot}(\mathbb{I}_2) = \mathbb{I}_n$:

$$(x_0, \dots, x_{n-1})^\mathsf{T} \mapsto (-x_{n/2-1}, x_0, x_1, \dots, x_{n/2-2},\ -x_{n-1}, x_{n/2}, x_{n/2+1}, \dots, x_{n-2})^\mathsf{T}.$$

In fact, ζ is an automorphism for every Hermitian form, similar to how -1 is an automorphism for every lattice. An important question is the following:

> **Question:** Given a Hermitian form $\mathbf{Q}$, which automorphisms of $\mathrm{rot}(\mathbf{Q})$ are *easier* to compute than to solve $\mathbb{Z}$LIP?

As noted before, the answer includes the powers of ζ. However, it was shown by Luo *et al.* that there are more $\mathbb{Z}$-automorphisms that are easy to compute [LJPW24]. Namely, since R_n^2 is equal to its dual, the so-called *symplectic automorphism*

$$\omega \colon R_n^2 \to R_n^2, \qquad \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} y^\star \\ -x^\star \end{pmatrix},$$

yields a map $\omega_\mathbf{Q} \colon \mathbf{z} \mapsto \mathbf{Q}^{-1}\omega(\mathbf{z})$, which *is not* an automorphism of $\mathbf{Q}$, but *is* an automorphism of $\mathrm{rot}(\mathbf{Q})$. We consider the group $G_{n,\mathbf{Q}}$ generated by ζ and $\omega_\mathbf{Q}$, which we call the group of *trivial automorphisms*.

HAWK. The signature scheme HAWK [DPPvW22] has an R_n-basis $\mathbf{B} = [\mathbf{b}_1, \mathbf{b}_2]$ of R_n^2 as its private key, obtained by sampling $\mathbf{b}_1$ from a discrete Gaussian and finding a not too long $\mathbf{b}_2$ such that $\det(\mathbf{B}) = 1$. The public key in HAWK is the Hermitian form $\mathbf{Q} = \mathbf{B}^\star\mathbf{B}$. A message msg, and salt $\mathbf{r}$ are hashed to a target coset $\mathbf{h} \in R_n^2/2R_n^2$ publicly. A valid signature for msg consists of a salt $\mathbf{r}$ and a vector $\mathbf{s}$ that is near $\frac{1}{2}\mathbf{h}$ with respect to the Hermitian form $\mathbf{Q}$.

A reduction in the quantum random oracle model from SUF-CMA security of HAWK to omSVP is discussed in Section 6 of the specification document [BBD+24]. This problem is defined as follows.

Problem 3 (omSVP)**.** *After an interactive phase with access to an oracle $\mathcal{O}$, that outputs a vector $\mathbf{x} \leftarrow D_{\mathbf{Q},\sigma}$ such that $\|\mathbf{B}\mathbf{x}\|^2$ is short, output a* new *vector*

$$\mathbf{x}_{N+1} \in R_n^2 \setminus \left\{ \sigma(\mathbf{x}_i) \;\middle|\; 1 \le i \le N,\ \sigma \in G_{n,\mathbf{Q}} \right\},$$

such that $\|\mathbf{B}\mathbf{x}_{N+1}\|^2$ is short, where $\mathbf{x}_1, \dots, \mathbf{x}_N \in R_n^2$ are all previous outputs from $\mathcal{O}$.

A precise formulation of how short $\mathbf{x}_{N+1}$ needs to be and how short $\mathbf{x}_1, \ldots, \mathbf{x}_N \in R_n^2$ are, can be found in the HAWK specification.

In the initial submission of HAWK to NIST, omSVP was formulated with $G_{n,\mathbf{Q}} = \langle \zeta \rangle$, but was amended to $G_{n,\mathbf{Q}} = \langle \zeta, \omega_{\mathbf{Q}} \rangle$ in round 2. Access to any $\mathbb{Z}$-automorphism $\sigma \in O(\mathrm{rot}(\mathbf{Q})) \setminus G_{n,\mathbf{Q}}$ trivially breaks omSVP by querying the oracle until it outputs some $\mathbf{x}$ such that $\mathbf{x} \neq \sigma(\mathbf{x})$, and then returning $\sigma(\mathbf{x})$. We will show that given any such $\sigma \in O(\mathrm{rot}(\mathbf{Q})) \setminus G_{n,\mathbf{Q}}$, the smLIP problem for HAWK can be solved more easily, and in turn the private key can be recovered.

3 Main Result

In this section we will prove the main result. Recall that G_n is the group of linear automorphisms of R_n^2 generated by the group $\mu = \langle \zeta \rangle$ of roots of unity and the symplectic automorphism ω.

Lemma 1. *The group $G = G_n$*

1. *acts regularly (i.e., transitively and freely) on the shortest vectors of the lattice R_n^2;*
2. *has exactly one element of order 2, namely $-1 = \zeta^{n/2} = \omega^2$, and*
3. *is isomorphic to $(\mu \rtimes \langle \omega \rangle)/\langle -1 \rangle \cong (C_n \rtimes C_4)/C_2$, where ω acts on μ by $\zeta \mapsto \zeta^\star = \zeta^{-1}$.*
4. *The multiplication map $\mu \times \{1, \omega\} \to G$ is a bijection.*

Proof. For all $x, y \in R_n$ we have

$$\omega\zeta \begin{pmatrix} x \\ y \end{pmatrix} = \omega \begin{pmatrix} \zeta x \\ \zeta y \end{pmatrix} = \begin{pmatrix} +\zeta^\star \cdot y^\star \\ -\zeta^\star \cdot x^\star \end{pmatrix} = \zeta^\star \begin{pmatrix} +y^\star \\ -x^\star \end{pmatrix} = \zeta^\star \omega \begin{pmatrix} x \\ y \end{pmatrix},$$

so $\omega\zeta\omega^{-1} = \zeta^\star$. It follows that $\mu \rtimes \langle \omega \rangle \to G$ is a (surjective) group homomorphism. Its kernel consists of all pairs (ζ^i, ω^j) such that $\zeta^i = \omega^{-j}$. Since $\omega^2 = -1 \in \mu$ and $\omega \notin \mu$, we conclude that the kernel is generated by $(-1, -1)$, establishing the group structure. It follows that the multiplication map $\mu \times \{1, \omega\} \to G$ is a bijection.

In μ, the only element of order 2 is -1. As $(\zeta^i\omega)^2 = \zeta^i\omega\zeta^i\omega = \zeta^i\zeta^{-i}\omega\omega = \omega^2 = -1$, we conclude that -1 is the only element of G of order 2.

The set S of shortest vectors of R_n^2 equals $(\mu \times \mathbf{0}) \sqcup (\mathbf{0} \times \mu)$. It is easy to see that the action of G on S is transitive: under $\mu \subseteq G$ there are the two orbits $\mu \times \mathbf{0}$ and $\mathbf{0} \times \mu$, while ω interchanges the two. Suppose $\mathbf{x} \in S$ is fixed by $\zeta^i\omega^j$ with $j \in \{0, 1\}$. Then $j = 0$, otherwise $\mathbf{x}$ and $\omega^j\mathbf{x}$ are in different orbits under μ. It follows that $\zeta^i\mathbf{x} = \mathbf{x}$, which is only possible if $\zeta^i = 1$. Hence the action is free. □

Lemma 2. *There exists a polynomial time algorithm that, given a Hermitian form $\mathbf{Q}$ of R_n^2 and $\mathbf{x} \in R_n^2$ of length 1 or $\sqrt{2}$, computes all shortest vectors of $\mathbf{Q}$.*

Proof. By [LJPW24] we may compute $G = G_{n,\mathbf{Q}}$. If $\|\mathbf{x}\| = 1$, we may compute by Lemma 1 all shortest vectors as the orbit of $\mathbf{x}$ under G. Now assume $\|\mathbf{x}\| = \sqrt{2}$. Compute for each $\sigma \in G \setminus \{1\}$ the element

$$\mathbf{y}_\sigma = \Big(\sum_{i=0}^{k_\sigma - 1} \sigma^i \Big)(\mathbf{x}), \quad \text{where } k_\sigma = \mathrm{ord}(\sigma)/2.$$

We will show that $\mathbf{y}_\sigma$ is twice a shortest vector for some σ, in which case we may reduce to the previous case with $\mathbf{x} \leftarrow \mathbf{y}_\sigma/2$. Note that $\mathbf{x} = \mathbf{x}_1 - \mathbf{x}_2$ for some shortest vectors $\mathbf{x}_1 \neq \mathbf{x}_2$. By Lemma 1 there is some $\sigma \in G$ such that $\sigma(\mathbf{x}_1) = \mathbf{x}_2$, and $\sigma^{k_\sigma} = -1$. Then

$$\mathbf{y}_\sigma = \sum_{i=0}^{k_\sigma - 1} \sigma^i(\mathbf{x}_1) - \sum_{i=0}^{k_\sigma - 1} \sigma^i(\mathbf{x}_2) = \sum_{i=0}^{k_\sigma - 1} \sigma^i(\mathbf{x}_1) - \sum_{i=0}^{k_\sigma - 1} \sigma^{i+1}(\mathbf{x}_1) = \mathbf{x}_1 - \sigma^{k_\sigma}(\mathbf{x}_1) = 2\mathbf{x}_1,$$

as was to be shown. □

Proposition 1. *There is a polynomial-time reduction from* smLIP *on a Hermitian form* $\mathbf{Q}$ *of* R_n^2 *to finding a nonzero vector of length at most* $\sqrt{2}$ *of* $\mathbf{Q}$.

Proof. Let $\mathbf{Q}$ be a Hermitian form of R_n^2 and suppose we have such a vector. By Lemma 2 we may compute the shortest vectors. The action of μ partitions them into two orbits, and let $\mathbf{b}_1$ and $\mathbf{b}_2$ be elements of the two orbits. With $\mathbf{B} = [\mathbf{b}_1, \mathbf{b}_2]$ we have $\mathbf{B}^\star\mathbf{Q}\mathbf{B} = \mathbb{I}_2$, so we may return $\mathbf{B}^{-1}$. □

Lemma 3. *Let* $\sigma \in O(\mathbb{Z}^n)$ *with order dividing a prime* p *and let* $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + 1$. *Then the sublattices* $\Lambda_1 = \ker(\sigma - 1)$ *and* $\Lambda_2 = \ker(\Phi_p(\sigma))$ *of* $\mathbb{Z}^n$ *satisfy* $\operatorname{rk}(\Lambda_1) + \operatorname{rk}(\Lambda_2) = n$. *Moreover, we have*

$$\Lambda_1 \cong \mathbb{Z}^a \times \sqrt{p} \cdot \mathbb{Z}^c \quad \text{and} \quad \Lambda_2 \cong \mathbb{Z}^b \times A_{p-1}^c, \tag{1}$$

for some $a, b, c \in \mathbb{Z}_{\geq 0}$, *with* $b = 0$ *if* $p > 2$. *If* $\sigma \neq \pm 1$, *we have* $\Lambda_1, \Lambda_2 \neq \mathbf{0}$.

Proof. Since σ is a signed permutation, it partitions the coordinates of $\mathbb{Z}^n$. This gives a decomposition $\mathbb{Z}^n = L_1 \oplus \cdots \oplus L_k$ into pairwise orthogonal sublattices, with each L_i isomorphic to either $\mathbb{Z}$ or $\mathbb{Z}^p$. With $\pi_i : \mathbb{Z}^n \to L_i$ the corresponding projections, we have $\sigma \circ \pi_i = \pi_i \circ \sigma$. It follows from linear algebra that $\Lambda_j = (L_1 \cap \Lambda_j) \oplus \cdots \oplus (L_k \cap \Lambda_j)$ $(j = 1, 2)$. Hence, it is sufficient to prove the lemma for the case $\mathbb{Z}^n = L_1$.

If $n = 1$, then $\sigma = \pm 1$. Hence, (Λ_1, Λ_2) equals $(\mathbb{Z}, \mathbf{0})$, or if $p = 2$ possibly $(\mathbf{0}, \mathbb{Z})$. In particular, they are of the prescribed forms.

Suppose now that $n = p$. Additionally assume that σ is just a permutation without sign flips, which is automatic when p is odd. Let

$$B_1 = \mathbb{Z}\mathbf{z} \quad \text{and} \quad B_2 = \left\{\mathbf{x} \in \mathbb{Z}^n \mid \mathbf{z}^\mathsf{T}\mathbf{x} = 0\right\},$$

where $\mathbf{z}$ is the all-1 vector in $\mathbb{Z}^n$. It is easy to verify that $B_1 \subseteq \Lambda_1$ and $B_2 \subseteq \Lambda_2$. Since $\mathbb{Q}B_1 + \mathbb{Q}B_2 = \mathbb{Q}^n$, we have by linear algebra that $\Lambda_j = (\mathbb{Q}B_j) \cap \mathbb{Z}^n = B_j$ $(j = 1, 2)$. Hence, $\Lambda_1 = \mathbb{Z}\mathbf{z} \cong \sqrt{p} \cdot \mathbb{Z}$ and $\Lambda_2 = A_{p-1}$.

Suppose now that $n = 2$ and σ is not a permutation. Then $-\sigma$ is a permutation, otherwise $\sigma^2 \neq 1$. Compared to σ, this results in interchanging the corresponding lattices Λ_1 and Λ_2. Since $A_1 \cong \sqrt{2} \cdot \mathbb{Z}$, we are done. □

Proposition 2. *There exists a polynomial-time algorithm that, given a Hermitian form* $\mathbf{Q}$ *of* R_n^2 *and* $\sigma \in O(\operatorname{rot}(\mathbf{Q})) \setminus G_{n,\mathbf{Q}}$, *computes a nonzero sublattice* Λ *of* $\operatorname{rot}(\mathbf{Q})$ *of rank at most* $n/2$ *such that* $\lambda_1(\Lambda) \leq \sqrt{2}$.

Proof. We may compute in polynomial time, e.g. using the characteristic polynomial of σ, the multiplicative order of σ. In particular, we may test whether $-1 \in \langle\sigma\rangle$.

Assume first that this is not the case. Then by replacing σ by some power, we may assume σ has prime order p and $\sigma \neq \pm 1$. Let Λ_1 and Λ_2 be the lattices obtained from Lemma 3, which we may compute by linear algebra, and let Λ to be the one of minimal rank. Since $\operatorname{rk}(\Lambda_1) + \operatorname{rk}(\Lambda_2) = n$, we have $\operatorname{rk}\Lambda \leq n/2$. It remains to show that $\lambda_1(\Lambda_1), \lambda_1(\Lambda_2) \leq \sqrt{2}$. For Λ_2, this immediately follows from Lemma 3 and $\lambda_1(A_{p-1}) = \sqrt{2}$. If $p = 2$, then the same follows for Λ_1. Suppose p is odd. Then $\Lambda_1 \cong \mathbb{Z}^a \times \sqrt{p} \cdot \mathbb{Z}^c$ and $\Lambda_2 \cong A_{p-1}^c$ for some a, c. As $a + pc = \operatorname{rk}(\Lambda_1) + \operatorname{rk}(\Lambda_2) = n$ is a power of 2 and p is odd, we conclude that $a > 0$. Hence, $\lambda_1(\Lambda_1) = 1$ and we are done.

Now consider the case for general σ. By [LJPW24], we may compute $G = G_{n,\mathbf{Q}}$. It suffices to show that $-1 \notin \langle\tau\rangle$ for some $\tau \in G \cdot \sigma$, since we may then apply the above argument on τ in the rôle of σ. Let $\mathbf{x} \in R_n^2$ be a shortest vector. Then by Lemma 1 there exists some $\rho \in G$ such that $\rho(\mathbf{x}) = \sigma(\mathbf{x})$. Hence, $\tau = \rho^{-1} \cdot \sigma$ fixes $\mathbf{x}$, and $\tau \neq 1$ because otherwise $\sigma \notin G$. Since -1 fixes no shortest vectors, we conclude that $-1 \notin \langle\tau\rangle$. □

4 Heuristic Hardness of SVP

In this section, we analyze the hardness of recovering a shortest vector from a lattice Λ appearing in Proposition 2. Specifically, we determine the minimal block size β such that BKZ-β finds a shortest vector in Λ, using standard heuristics in lattice reduction.

We use the methodology based on the "2016 estimates" which were phrased for lattices related to *Learning with Errors* [ADPS16], and verified experimentally [AGVW17, DDGR20, PV21]. Here, we apply this methodology to a lattice of the form as in Eq. (1). These 2016 estimates have already been used to motivate the experimentally verified estimates that BKZ-β recovers the shortest vector in a rotation of $\mathbb{Z}^n$ when $\beta = n/2 + o(n)$ [DPPvW22].

Definition 1 ([DvW22])**.** A rank-n lattice Λ is an *f-unusual-SVP* instance if we have

$$f \cdot \lambda_1(\Lambda) \leq \mathrm{GH}(n) \cdot \mathrm{Vol}(\Lambda)^{1/n}.$$

For example, $\mathbb{Z}^n$ and A_n are $\Omega(\sqrt{n})$-unusual-SVP instances, as $n \to \infty$.

The hardness of recovering a shortest vector in an unusual-SVP lattice is mainly determined by the ratio $\mathrm{GH}(n)\mathrm{Vol}(\Lambda)^{1/n}/\lambda_1(\Lambda)$, rather than the so-called uSVP-factor $\lambda_2(\Lambda)/\lambda_1(\Lambda)$ [AD21]. For such f-unusual-SVP instance with an unusually short vector $\mathbf{v}$, a *threshold phenomenon* occurs in the terminal block of a BKZ-β tour once the projection of $\mathbf{v}$ onto this block is much shorter than the expected first minimum if that terminal block had been a random lattice. Now when this $\mathbf{v}$ is part of the basis at position $\mathrm{rk}(\Lambda) - \beta + 1$, subsequent tours of BKZ-β will then move $\mathbf{v}$ to the front of the basis with steps of $\beta - 1$ per tour [PV21].

The lattice computed in Proposition 2 is of the form $\mathbb{Z}^a \times \sqrt{p}\mathbb{Z}^c$ (with $a > 0$) or $\mathbb{Z}^b \times A_{p-1}^c$, and thus is an instance of the $\Omega(\sqrt{k})$-unusual-SVP, where $k = \mathrm{rk}(\Lambda) \leq n/2$. In the following heuristic, let $\delta_\beta = \mathrm{GH}(\beta)^{1/(\beta-1)}$ be the *root Hermite factor*, and note $\delta_\beta \approx (\beta/(2\pi e))^{\frac{1}{2(\beta-1)}}$ for $\beta > 50$.

Heuristic 1. *Suppose $\Lambda \subseteq R_n^2$ is a nonzero rank-k lattice with $\lambda_1(\Lambda) \leq \sqrt{2}$. If $\beta \in \mathbb{Z}_{\geq 2}$ satisfies*

$$\sqrt{2\beta/k} \leq \delta_\beta^{2\beta-k-1}, \tag{2}$$

then BKZ-β will recover a shortest vector of Λ. In particular, this condition holds asymptotically for $\beta = k/2 + 1$.

Justification. Because Λ can be identified with a sublattice of $\mathbb{Z}^n$, by [Duc24, Lemma 2], its volume is at least 1. Note that the projection of a shortest vector of Λ onto the terminal block of a BKZ-β tour has an expected norm of $\lambda_1(\Lambda) \cdot \sqrt{\beta/k} \leq \sqrt{2\beta/k}$. Moreover, if the terminal block during a BKZ-β tour would be a random block, its first minimum would be $\delta_\beta^{2\beta-k+1} \cdot \mathrm{Vol}(\Lambda)^{1/k} \geq \delta_\beta^{2\beta-k+1}$. Thus, if Eq. (2) holds, then the [ADPS16] success condition

$$\lambda_1(\Lambda) \cdot \sqrt{\beta/k} \leq \delta_\beta^{2\beta-k+1} \cdot \mathrm{Vol}(\Lambda)^{1/k}$$

is satisfied, and we expect a threshold phenomenon to occur. For the last statement, note the left hand side of Eq. (2) is equal to $\sqrt{1 + 2/k} \leq e^{1/k}$, and the right hand side of Eq. (2) is at least $(k/(4\pi e))^{1/k}$, which is larger than $e^{1/k}$ once $k > 100$. △

Note that we use the *Geometric Series Assumption* (GSA) for this estimate, i.e., we assume the lengths of the Gram–Schmidt basis vectors follow a geometric series, and there are better simulators for these lengths [CN11, BSW18], Still, the GSA gives a decent approximation. In addition, there is a more refined simulator that can take multiple shortest vectors of a lattice (e.g. n for $\mathbb{Z}^n$) into account [DDGR20], which expects a slightly lower required block size. However, because we are interested in the worst-case instance of Λ occurring in Proposition 2, such a refined simulator does not help in cases when there is a single shortest vector.

5 Group-theoretic Heuristics

Our results are strong in that they impose no conditions on the automorphism, besides being nontrivial, but they 'only' halve the security parameter of HAWK. As [JWL+23] shows, under the stronger assumption that an attacker has access to an oracle giving automorphisms of a lattice, SVP can be (probabilistically) solved in polynomial time. If instead of having an oracle, the attacker generates a single uniformly random automorphism, then we can, as we will argue, heuristically break HAWK with high probability.

Suppose σ is uniformly sampled from $O(\mathrm{rot}(\mathbf{Q}))$, and let $g \in S_n$ be the corresponding permutation on the shortest vectors of $\mathrm{rot}(\mathbf{Q}) \cong \mathbb{Z}^n$ modulo sign, i.e., on the coordinates of the lattice. Then, g is a uniformly random permutation. Each orbit $\Omega/\{\pm 1\}$ of g comes with a sign which is negative if the corresponding action of σ on Ω is transitive. Let c_k^s be the number of orbits of g of length k and sign s. One can show, analogously to Lemma 3, that the characteristic polynomial of σ equals

$$\prod_{s=\pm 1}\prod_{k=1}^{n}(X^n - s)^{c_k^s}, \quad \text{and that} \quad \Lambda_1 = \ker(\sigma - 1) \cong \prod_{k=1}^{n}(\sqrt{k}\cdot\mathbb{Z})^{c_k^+}.$$

We will now argue that with high probability $\Lambda_1 \neq 0$ and $\operatorname{rk}\Lambda_1 = O(\log n)$. In particular, smLIP reduces, given σ, to a comparatively trivial instance of SVP.

The probability that g has no fixed points is approximately $1/e$, so we may assume that g *has* a fixed point. Alternatively, one notes that if we multiply σ by the unique element of $G_{n,\mathbf{Q}}$ such that the result g' fixes some preselected shortest vector $\mathbf{x}$, then g' is a uniformly random permutation among all permutations fixing $\mathbf{x}$. Multiplying σ by -1 if necessary, we may assume $c_1^+ > 0$. In particular, $\Lambda_1 \neq \{\mathbf{0}\}$ and $\lambda_1(\Lambda_1) = 1$. The expected number of orbits of g is $\sum_{k=1}^{n} 1/k \approx \log(n)$. Hence, the expected rank of Λ_1 is at most $\log(n)$.

On a less rigorous note, the group generated by $G_{n,\mathbf{Q}}$ and σ will often be significantly larger than $\#G_{n,\mathbf{Q}} \cdot \#\langle\sigma\rangle$. It is also not unlikely that it maps surjectively to S_n. In this case it becomes possible to sample random-enough automorphisms, bringing us in the regime of [JWL+23].

6 Conclusion

Theorem 1 now easily follows from combining Proposition 2 and Heuristic 1. Namely, given a Hermitian form $\mathbf{Q}$ of R_n^2 and a nontrivial $\mathbb{Z}$-automorphism σ, Proposition 2 computes in polynomial time a basis for a lattice Λ of rank at most $n/2$, such that recovering a shortest vector of Λ allows solving smLIP for $\mathbf{Q}$. Then, Heuristic 1 shows, heuristically, that BKZ-β recovers a shortest vector of Λ when $\beta = \mathrm{rk}(\Lambda)/2 + 1 \leq n/4 + 1$.

Based on the results of Section 5, it is reasonable to suspect that Λ is of much lower rank in the average case. Indeed, sampling σ uniformly at random likely gives a lattice of rank at most $\log(n)$, for which directly solving SVP only takes polynomial time in n.

In practice, if one happens to find a nontrivial automorphism σ, it may be worthwhile to take a random composition of σ, ζ and $\omega_{\mathbf{Q}}$'s until finding a lattice of rank at most $\log(n)$, since $\langle\sigma, \zeta, \omega_{\mathbf{Q}}\rangle = O(\mathrm{rot}(\mathbf{Q}))$ may happen. Although we prove a worst-case result that block size $n/4 + 1$ is heuristically sufficient given a nontrivial automorphism, in practice, we expect one could find a lattice of extremely low rank, and subsequently solve smLIP and break HAWK. In this light, we believe that smLIP is *practically* as hard as finding a nontrivial automorphism, but theoretically not harder than finding a nontrivial automorphism and solving SVP on an easier lattice.

References

[AD21] Martin R. Albrecht and Léo Ducas. *Lattice Attacks on NTRU and LWE: A History of Refinements*, pages 15–40. London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, United Kingdom, 2021. doi:10.1017/9781108854207.

[ADPS16] Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum key exchange - A new hope. In Thorsten Holz and Stefan Savage, editors, *USENIX Security 2016: 25th USENIX Security Symposium*, pages 327–343, Austin, TX, USA, August 10–12, 2016. USENIX Association. URL: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/alkim.

[AGVW17] Martin R. Albrecht, Florian Göpfert, Fernando Virdia, and Thomas Wunderer. Revisiting the expected cost of solving uSVP and applications to LWE. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology – ASIACRYPT 2017, Part I*, volume 10624 of *Lecture Notes in Computer Science*, pages 297–322, Hong Kong, China, December 3–7, 2017. Springer, Cham, Switzerland. doi:10.1007/978-3-319-70694-8_11.

[APvW25] Bill Allombert, Alice Pellet-Mary, and Wessel P. J. van Woerden. Cryptanalysis of rank-2 module-LIP: A single real embedding is all it takes. In Serge Fehr and Pierre-Alain Fouque, editors, *Advances in Cryptology – EUROCRYPT 2025, Part II*, volume 15602 of *Lecture Notes in Computer Science*, pages 184–212, Madrid, Spain, May 4–8, 2025. Springer, Cham, Switzerland. doi:10.1007/978-3-031-91124-8_7.

[BBD+24] Joppe W. Bos, Olivier Bronchain, Léo Ducas, Serge Fehr, Yu-Hsuan Huang, Thomas Pornin, Eamonn W. Postlethwaite, Thomas Prest, Ludo N. Pulles, and Wessel van Woerden. HAWK. Technical report, National Institute of Standards and Technology, 2024. available at https://csrc.nist.gov/Projects/pqc-dig-sig/round-2-additional-signatures.

[BGPS23] Huck Bennett, Atul Ganju, Pura Peetathawatchai, and Noah Stephens-Davidowitz. Just how hard are rotations of $\mathbb{Z}^n$? algorithms and cryptography with the simplest lattice. In Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology – EUROCRYPT 2023, Part V*, volume 14008 of *Lecture Notes in Computer Science*, pages 252–281, Lyon, France, April 23–27, 2023. Springer, Cham, Switzerland. doi:10.1007/978-3-031-30589-4_9.

[BM21] Tamar Lichter Blanks and Stephen D. Miller. Generating cryptographically-strong random lattice bases and recognizing rotations of $\mathbb{Z}^n$. In Jung Hee Cheon and Jean-Pierre Tillich, editors, *Post-Quantum Cryptography - 12th International Workshop, PQCrypto 2021*, pages 319–338, Daejeon, South Korea, July 20–22, 2021. Springer, Cham, Switzerland. doi:10.1007/978-3-030-81293-5_17.

[BN24] Henry Bambury and Phong Q. Nguyen. Improved provable reduction of NTRU and hypercubic lattices. In Markku-Juhani Saarinen and Daniel Smith-Tone, editors, *Post-Quantum Cryptography - 15th International Workshop, PQCrypto 2024, Part I*, pages 343–370, Oxford, UK, June 12–14, 2024. Springer, Cham, Switzerland. doi:10.1007/978-3-031-62743-9_12.

[BSW18] Shi Bai, Damien Stehlé, and Weiqiang Wen. Measuring, simulating and exploiting the head concavity phenomenon in BKZ. In Thomas Peyrin and

Steven Galbraith, editors, *Advances in Cryptology – ASIACRYPT 2018, Part I*, volume 11272 of *Lecture Notes in Computer Science*, pages 369–404, Brisbane, Queensland, Australia, December 2–6, 2018. Springer, Cham, Switzerland. doi:10.1007/978-3-030-03326-2_13.

[Che13] Yuanmi Chen. *Réduction de réseau et sécurité concrete du chiffrement completement homomorphe*. Phd thesis, Université Paris Diderot, November 13, 2013. Available at https://archive.org/details/PhDChen13.

[CME+25] 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 Serge Fehr and Pierre-Alain Fouque, editors, *Advances in Cryptology – EUROCRYPT 2025, Part II*, volume 15602 of *Lecture Notes in Computer Science*, pages 154–183, Madrid, Spain, May 4–8, 2025. Springer, Cham, Switzerland. doi:10.1007/978-3-031-91124-8_6.

[CN11] Yuanmi Chen and Phong Q. Nguyen. BKZ 2.0: Better lattice security estimates. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology – ASIACRYPT 2011*, volume 7073 of *Lecture Notes in Computer Science*, pages 1–20, Seoul, South Korea, December 4–8, 2011. Springer Berlin Heidelberg, Germany. doi:10.1007/978-3-642-25385-0_1.

[CS98] J.H. Conway and N.J.A. Sloane. *Sphere Packings, Lattices and Groups*, volume 3 of *Grundlehren der mathematischen Wissenschaften*. Springer New York, 1998. doi:10.1007/978-1-4757-6568-7.

[DDGR20] Dana Dachman-Soled, Léo Ducas, Huijing Gong, and Mélissa Rossi. LWE with side information: Attacks and concrete security estimation. In Daniele Micciancio and Thomas Ristenpart, editors, *Advances in Cryptology – CRYPTO 2020, Part II*, volume 12171 of *Lecture Notes in Computer Science*, pages 329–358, Santa Barbara, CA, USA, August 17–21, 2020. Springer, Cham, Switzerland. doi:10.1007/978-3-030-56880-1_12.

[DN12] Léo Ducas and Phong Q. Nguyen. Learning a zonotope and more: Cryptanalysis of NTRUSign countermeasures. In Xiaoyun Wang and Kazue Sako, editors, *Advances in Cryptology – ASIACRYPT 2012*, volume 7658 of *Lecture Notes in Computer Science*, pages 433–450, Beijing, China, December 2–6, 2012. Springer Berlin Heidelberg, Germany. doi:10.1007/978-3-642-34961-4_27.

[DPPvW22] 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, Part IV*, volume 13794 of *Lecture Notes in Computer Science*, pages 65–94, Taipei, Taiwan, December 5–9, 2022. Springer, Cham, Switzerland. doi:10.1007/978-3-031-22972-5_3.

[Duc24] Léo Ducas. Provable lattice reduction of $\mathbb{Z}^n$ with blocksize n/2. *Designs, Codes and Cryptography*, 92(4):909–916, 2024. doi:10.1007/s10623-023-01320-7.

[DvW22] Léo Ducas and Wessel P. J. van Woerden. On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography. In Orr Dunkelman and Stefan Dziembowski, editors, *Advances in Cryptology – EUROCRYPT 2022, Part III*, volume 13277 of *Lecture Notes in Computer Science*, pages 643–673, Trondheim, Norway, May 30 – June 3, 2022. Springer, Cham, Switzerland. doi:10.1007/978-3-031-07082-2_23.

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In Cynthia Dwork, editor, *Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17-20, 2008*, pages 197–206. ACM, 2008. doi:10.1145/1374376.1374407.

[GS02] Craig Gentry and Michael Szydlo. Cryptanalysis of the revised NTRU signature scheme. In Lars R. Knudsen, editor, *Advances in Cryptology – EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 299–320, Amsterdam, The Netherlands, April 28 – May 2, 2002. Springer Berlin Heidelberg, Germany. doi:10.1007/3-540-46035-7_20.

[JWL+23] Kaijie Jiang, Anyu Wang, Hengyi Luo, Guoxiao Liu, Yang Yu, and Xiaoyun Wang. Exploiting the symmetry of $\mathbb{Z}^n$: Randomization and the automorphism problem. In Jian Guo and Ron Steinfeld, editors, *Advances in Cryptology – ASIACRYPT 2023, Part IV*, volume 14441 of *Lecture Notes in Computer Science*, pages 167–200, Guangzhou, China, December 4–8, 2023. Springer, Singapore, Singapore. doi:10.1007/978-981-99-8730-6_6.

[LJPW24] Hengyi Luo, Kaijie Jiang, Yanbin Pan, and Anyu Wang. Cryptanalysis of rank-2 module-LIP with symplectic automorphisms. In Kai-Min Chung and Yu Sasaki, editors, *Advances in Cryptology – ASIACRYPT 2024, Part IV*, volume 15487 of *Lecture Notes in Computer Science*, pages 359–385, Kolkata, India, December 9–13, 2024. Springer, Singapore, Singapore. doi:10.1007/978-981-96-0894-2_12.

[LS17] Hendrik W. Lenstra, Jr. and Alice Silverberg. Lattices with symmetry. *Journal of Cryptology*, 30(3):760–804, July 2017. doi:10.1007/s00145-016-9235-7.

[LS19] Hendrik W. Lenstra Jr. and Alice Silverberg. Testing isomorphism of lattices over CM-Orders. *SIAM Journal on Computing*, 48(4):1300–1334, 2019. doi:10.1137/17M115390X.

[MPPW24] Guilhem Mureau, Alice Pellet-Mary, Georgii Pliatsok, and Alexandre Wallet. Cryptanalysis of rank-2 module-LIP in totally real number fields. In Marc Joye and Gregor Leander, editors, *Advances in Cryptology – EUROCRYPT 2024, Part VII*, volume 14657 of *Lecture Notes in Computer Science*, pages 226–255, Zurich, Switzerland, May 26–30, 2024. Springer, Cham, Switzerland. doi:10.1007/978-3-031-58754-2_9.

[NR09] Phong Q. Nguyen and Oded Regev. Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures. *Journal of Cryptology*, 22(2):139–160, April 2009. doi:10.1007/s00145-008-9031-0.

[PV21] Eamonn W. Postlethwaite and Fernando Virdia. On the success probability of solving unique SVP via BKZ. In Juan Garay, editor, *PKC 2021: 24th International Conference on Theory and Practice of Public Key Cryptography, Part I*, volume 12710 of *Lecture Notes in Computer Science*, pages 68–98, Virtual Event, May 10–13, 2021. Springer, Cham, Switzerland. doi:10.1007/978-3-030-75245-3_4.

[Szy03] Michael Szydlo. Hypercubic lattice reduction and analysis of GGH and NTRU signatures. In Eli Biham, editor, *Advances in Cryptology – EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 433–448, Warsaw, Poland, May 4–8, 2003. Springer Berlin Heidelberg, Germany. doi:10.1007/3-540-39200-9_27.