Adjoint-Lattice Reduction for the HAWK Gram-Factor Problem

A Reduction to γ-SVP in Dimension $3n/4 + 1$

Anonymous research draft

17 July 2026

Abstract

Let $n \geq 4$ be a power of two, let

$$R = \mathbb{Z}[X]/(X^n + 1), \qquad K = \mathbb{Q}[X]/(X^n + 1),$$

and let $\star$ denote the involution induced by $X \mapsto X^{-1}$ together with matrix transposition. Given $Q \in \mathrm{Herm}_2(R)$ promised to satisfy $Q = B^\star B$ for some $B \in \mathrm{GL}_2(R)$, the goal is to recover any equivalent factor $\widetilde{B} \in \mathrm{GL}_2(R)$ with $\widetilde{B}^\star \widetilde{B} = Q$.

From Q we construct the public self-adjoint module $\mathcal{H}_Q$, remove its scalar center by the exact image $\mathcal{T}_Q = (A \mapsto 2A - \mathrm{tr}(A)I_2)(\mathcal{H}_Q)$, and take the scaled dual $\Gamma_Q = 2\mathcal{T}_Q^\vee$. We prove that Γ_Q has rank $3n/2$ and, under conjugation by the hidden factor B, is exactly isometric to

$$\mathbb{Z}^n \perp \sqrt{2}\,\mathbb{Z}^{n/2-1} \perp 2\mathbb{Z}.$$

Hence both primal and dual shortest shells are explicit, their next-shell gaps are $\sqrt{2}$, and

$$\lambda_1(\Gamma_Q)\lambda_1(\Gamma_Q^\vee) = \frac{1}{2}.$$

Applying the half-dimensional primal–dual blockwise reduction of Bambury and Nguyen [BN24] therefore finds a primal or dual shortest vector using polynomially many calls to γ-SVP in dimension at most $3n/4 + 1$, for every fixed $1 \leq \gamma < \sqrt{2}$. The resulting vector yields a non-scalar R-linear automorphism of the Hermitian form Q. We then apply the instance-preserving reduction from rank-two module-LIP to rank-two module-LAP proved in *Commitment Schemes Based on Module-LIP* [Luo+25, Theorem 3.1], specialized to the base form I_2. Since the required module-LAP witness has already been recovered from the shortest shell, the reduction deterministically reconstructs an equivalent factor $\widetilde{B}$ in polynomial time.

Keywords: rank-two module lattice isomorphism; adjoint lattice; shortest vector problem; primal–dual descent; CM-orders.

Contents

1 Problem statement and main theorem

Fix a power of two $n \geq 4$ and set

$$R = \mathbb{Z}[X]/(X^n + 1), \qquad K = \mathbb{Q}[X]/(X^n + 1).$$

Let $\star$ be induced by $X \mapsto X^{-1}$ on K and include transpose on matrices. Write $\mathrm{Herm}_2(R) = \{Q \in M_2(R) : Q^\star = Q\}$.

Definition 1.1 (Gram-factor recovery problem)**.** Given $Q \in \mathrm{Herm}_2(R)$, promised that $Q = B^\star B$ for some $B \in \mathrm{GL}_2(R)$, output any $\widetilde{B} \in \mathrm{GL}_2(R)$ satisfying

$$\widetilde{B}^\star \widetilde{B} = Q.$$

Theorem 1.2 (Main result)**.** *For every fixed $1 \leq \gamma < \sqrt{2}$, the problem in definition 1.1 admits a deterministic Turing reduction to polynomially many γ-SVP instances of dimension at most*

$$\boxed{\frac{3n}{4} + 1},$$

together with deterministic polynomial-time exact linear algebra. The oracle-rank bound is obtained by applying the primal–dual blockwise reduction of Bambury and Nguyen [BN24] to the public adjoint lattice. The resulting nontrivial automorphism is converted into an equivalent Gram factor by the instance-preserving module-LIP-to-module-LAP self-reduction of Luo–Jiang–Jin–Pan–Wang [Luo+25, Theorem 3.1].

Remark 1.3. The output is an equivalent Gram factor; it need not equal the promised factor B.

2 Technique overview

The proof architecture is summarized in Figure 1.

Step 1: pass to an adjoint representation. Conjugation by the hidden B sends Q-self-adjoint matrices to ordinary self-adjoint matrices. Ordinary 2×2 Hermitian matrices have two scalar diagonal degrees of freedom and one cyclotomic off-diagonal coordinate. Removing the scalar center leaves a trace-zero Hermitian space of $\mathbb{Z}$-rank $3n/2$.

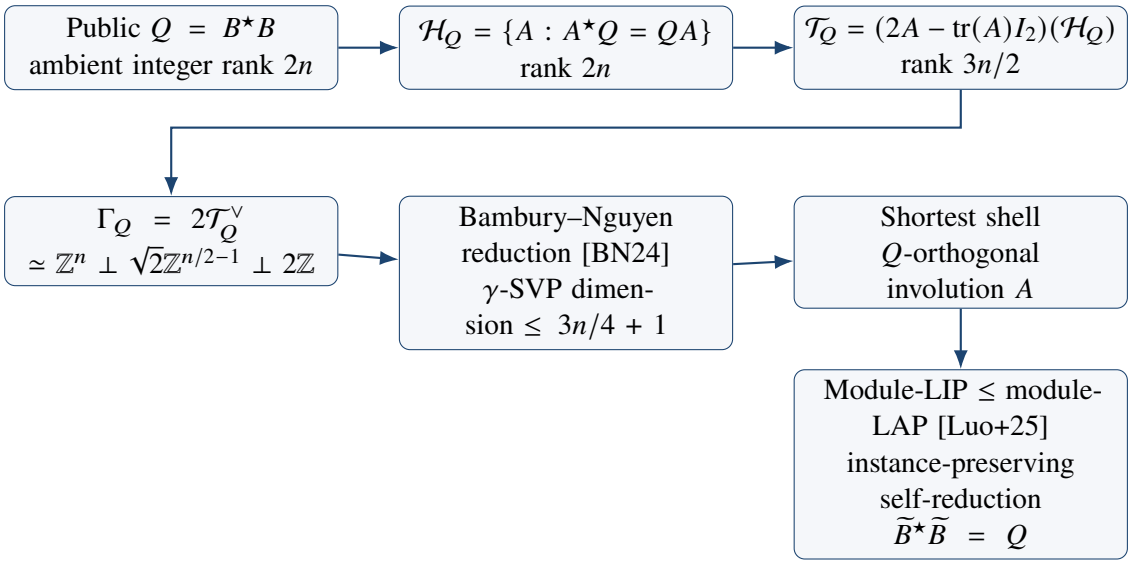

Figure 1: The adjoint-lattice reduction. Algebra reduces the representation dimension and exposes exact geometry; the half-dimensional primal–dual reduction of Bambury and Nguyen [BN24] finds a nontrivial automorphism; the instance-preserving module-LIP-to-module-LAP reduction of [Luo+25] recovers a factor.

Step 2: choose the scaled dual, not merely the trace-zero image. The trace-zero image $\mathcal{T}_Q$ already has reduced rank, but its shortest shell is small. Passing to $\Gamma_Q = 2\mathcal{T}_Q^\vee$ exchanges the large off-diagonal scale with a unit scale. In hidden coordinates, Γ_Q has $2n$ primal shortest vectors and exactly two dual shortest vectors. More importantly, the product of minima is $1/2$.

Step 3: apply the Bambury–Nguyen half-dimensional reduction. The dimension-halving mechanism is the primal–dual blockwise reduction of Bambury and Nguyen [BN24], which extends Ducas's reduction for the hypercubic lattice [Duc24]. Their reduction alternates a short-vector call in a projected primal block with a short-vector call in the corresponding dual block; in an unsuccessful round, the covolume multiplier is bounded by the product of the two block minima. For the present adjoint lattice, the explicitly proved shell gaps permit the required shortest-shell tests with a γ-SVP oracle, and the contraction factor is

$$\gamma^2 \lambda_1(\Gamma_Q)\lambda_1(\Gamma_Q^\vee) = \frac{\gamma^2}{2} < 1.$$

Thus the Bambury–Nguyen result gives the $3n/4 + 1$ oracle-rank bound. The dimension-halving reduction and its covolume-descent analysis are imported from [BN24]; the manuscript-specific step is the construction of Γ_Q and the proof that it satisfies the required minima and shell-gap hypotheses.

Step 4: turn the shortest vector into an involution. Every primal shortest vector is conjugate to an off-diagonal matrix

$$E_u = \begin{pmatrix} 0 & u \\ u^\star & 0 \end{pmatrix}, \qquad u \in \{\pm X^j\},$$

while twice every dual shortest vector is conjugate to $D = \mathrm{diag}(1, -1)$. Both square to I_2 and are non-scalar Q-orthogonal automorphisms. This is exactly the type of module-LAP witness required by the instance-preserving module-LIP-to-module-LAP reduction of Luo–Jiang–Jin–Pan–Wang [Luo+25, Theorem 3.1]. Their proof treats the diagonal and anti-diagonal hidden automorphisms separately [Luo+25, Propositions 3.1–3.2], using eigensubmodules and Lenstra–Silverberg reconstruction [HS19].

3 Preliminaries

3.1 The cyclotomic order and its involution

Fix a power of two $n \geq 4$ and set

$$R = \mathbb{Z}[X]/(X^n + 1), \qquad K = \mathbb{Q}[X]/(X^n + 1).$$

We use the same symbol X for the residue class. It is a primitive $2n$-th root of unity. The order R is stable under complex conjugation. The involution

$$a \longmapsto a^\star, \qquad X^\star = X^{-1} = -X^{n-1},$$

is complex conjugation. Its fixed field and fixed order are

$$F = K^\star, \qquad R^+ = R \cap F,$$

with $[K : \mathbb{Q}] = n$ and $[F : \mathbb{Q}] = d = n/2$.

For vectors and matrices, $\star$ applies entrywise and includes transpose. Thus $Q \in M_2(R)$ is Hermitian when $Q^\star = Q$. Scalar multiplication on R^2 is on the left; commutativity of R makes this convention harmless.

The coefficient inner product on R is

$$\langle a, b \rangle_{\text{coeff}} = \frac{1}{n} \operatorname{Tr}_{K/\mathbb{Q}}(ab^\star).$$

The basis $1, X, \ldots, X^{n-1}$ is orthonormal. Indeed, multiplication by X^k in this basis is a signed cyclic shift and has trace zero for $0 < |k| < n$.

For a Hermitian Q, define on R^2

$$\langle x, y \rangle_Q = \frac{1}{n} \operatorname{Tr}_{K/\mathbb{Q}}(x^\star Q y).$$

Under the promise $Q = B^\star B$ with $B \in \mathrm{GL}_2(R)$, this is a positive definite integral lattice form and

$$\langle x, y \rangle_Q = \langle Bx, By \rangle_{\text{coeff}}.$$

3.2 Lattices, duals, shortest shells, and SVP

A lattice Λ is a free abelian group equipped with a positive definite real inner product. Its dual is

$$\Lambda^\vee = \{y \in \operatorname{span}_{\mathbb{R}}(\Lambda) : \langle y, x \rangle \in \mathbb{Z} \text{ for all } x \in \Lambda\}.$$

It is *integral* if $\Lambda \subseteq \Lambda^\vee$. Its first minimum and first shell are

$$\lambda_1(\Lambda) = \min_{0 \neq x \in \Lambda} \|x\|, \qquad S_1(\Lambda) = \{x \in \Lambda : \|x\| = \lambda_1(\Lambda)\}.$$

For $\gamma \geq 1$, a γ-SVP oracle returns a nonzero vector $v \in \Lambda$ satisfying

$$\|v\| \leq \gamma \lambda_1(\Lambda).$$

We say that the first shell has multiplicative gap $\Delta > 1$ if every vector outside $S_1(\Lambda)$ has norm at least $\Delta\lambda_1(\Lambda)$. When $\gamma < \Delta$, any γ-SVP output of norm below the second shell necessarily lies in $S_1(\Lambda)$. Rational lattice descriptions may be cleared of denominators without changing their dimension or approximation factor.

3.3 CM-order lattice isomorphism

An R-lattice in the sense of Lenstra and Silverberg is an integral lattice L with an R-module structure satisfying

$$\langle ax, y\rangle = \langle x, a^\star y\rangle \qquad (a \in R,\ x, y \in L).$$

The standard R-lattice is R with inner product

$$(a, b) \longmapsto \mathrm{Tr}_{K/\mathbb{Q}}(a^\star b).$$

We use the following theorem as a black box.

Theorem 3.1 (Lenstra–Silverberg [HS19])**.** *There is a deterministic polynomial-time algorithm that, given a CM-order A and an A-lattice L, decides whether L is A-isomorphic to the standard A-lattice and, if so, computes an A-isomorphism.*

The theorem is stronger than ordinary ideal principality testing because it incorporates the prescribed positive form. The instance-preserving rank-two module-LIP-to-module-LAP reduction in *Commitment Schemes Based on Module-LIP* [Luo+25, Theorem 3.1] uses this reconstruction principle after extracting eigensubmodules of a non-scalar automorphism; its diagonal and anti-diagonal branches are given in Propositions 3.1 and 3.2 of that work.

4 The public adjoint lattice

4.1 The Q-self-adjoint module

Define

$$\mathcal{H}_Q = \{A \in M_2(R) : A^\star Q = QA\}.$$

It is public: after expanding entries in the coefficient basis of R, it is the integer kernel of a linear map on $4n$ variables.

Proposition 4.1 (Hidden standard form)**.** *Let $Q = B^\star B$ with $B \in \mathrm{GL}_2(R)$. Conjugation by B gives*

$$\mathcal{H}_Q = B^{-1}\mathcal{H}_0 B,$$

where

$$\mathcal{H}_0 = \left\{ \begin{pmatrix} a & z \\ z^\star & c \end{pmatrix} : a, c \in R^+,\ z \in R \right\}.$$

In particular, $\mathrm{rank}_{\mathbb{Z}} \mathcal{H}_Q = 2n$.

Proof. For $A \in M_2(R)$ put $Y = BAB^{-1}$. The equality $A^\star B^\star B = B^\star BA$ is equivalent to

$$(B^\star)^{-1} A^\star B^\star = BAB^{-1},$$

that is, $Y^\star = Y$. The displayed description of $\mathcal{H}_0$ is the general form of a Hermitian 2×2 matrix over R. Its rank is $2\,\mathrm{rank}_{\mathbb{Z}} R^+ + \mathrm{rank}_{\mathbb{Z}} R = 2d + n = 2n$. □

4.2 Removing the scalar center

Define the $\mathbb{Z}$-linear map

$$\tau(A) = 2A - \mathrm{tr}(A) I_2, \qquad \mathcal{T}_Q = \tau(\mathcal{H}_Q).$$

The factor two is essential: $\mathcal{T}_Q$ is the exact image lattice, not its saturation.

For $a \in R^+$ and $z \in R$, write

$$X(a, z) = \begin{pmatrix} a & z \\ z^\star & -a \end{pmatrix}.$$

Proposition 4.2 (Trace-zero image)**.** *One has*

$$\ker(\tau|_{\mathcal{H}_Q}) = R^+ I_2, \qquad \operatorname{rank}_{\mathbb{Z}} \mathcal{T}_Q = \frac{3n}{2},$$

and

$$\mathcal{T}_Q = B^{-1}\mathcal{T}_0 B, \qquad \mathcal{T}_0 = \{X(\delta, 2z) : \delta \in R^+,\ z \in R\}.$$

Proof. If $\tau(A) = 0$, then A is scalar; the Q-self-adjoint condition forces the scalar to lie in R^+. Conversely every such scalar lies in the kernel. Thus

$$\operatorname{rank} \mathcal{T}_Q = 2n - d = 3n/2.$$

For a standard Hermitian matrix,

$$\tau\begin{pmatrix} a & z \\ z^\star & c \end{pmatrix} = X(a - c, 2z),$$

and every $\delta \in R^+$ occurs as $a - c$. Finally, τ commutes with conjugation. □

4.3 The adjoint inner product and public construction

On $\mathcal{T}_Q \otimes \mathbb{Q}$ define

$$\langle A, C\rangle_{\mathrm{ad}} = \frac{1}{2n} \operatorname{Tr}_{K/\mathbb{Q}} \operatorname{tr}(AC).$$

Matrix trace is invariant under conjugation, so $Y \mapsto B^{-1}YB$ is an isometry for this form. Positivity follows from the standard coordinates computed in Section 5.

Define the scaled dual

$$\boxed{\Gamma_Q = 2\mathcal{T}_Q^\vee}.$$

The lattice is public even though its convenient diagonal basis is hidden.

Algorithm 1 Public construction of Γ_Q

Require: $Q \in \mathrm{Herm}_2(R)$ promised to equal $B^\star B$ for some $B \in \mathrm{GL}_2(R)$.
Ensure: A rational matrix basis of the integral lattice Γ_Q and its Gram matrix.

1: Expand $A^\star Q - QA = 0$ in the coefficient basis and compute a $\mathbb{Z}$-basis of $\mathcal{H}_Q$ by HNF/SNF.
2: Apply $\tau(A) = 2A - \operatorname{tr}(A)I_2$ to this basis and compute a basis of the exact image $\mathcal{T}_Q$; do not saturate.
3: Form the Gram matrix G_T under $\langle\cdot,\cdot\rangle_{\mathrm{ad}}$.
4: Express a dual basis as G_T^{-1}-linear combinations of the basis of $\mathcal{T}_Q$.
5: Multiply the dual basis by 2 and return it as a basis of Γ_Q.

All operations in algorithm 1 are exact integer or rational linear algebra. Under the Gram-factor promise, theorem 5.2 below additionally shows $\Gamma_Q \subseteq M_2(R)$.

5 Exact geometry of the adjoint lattice

5.1 An orthogonal basis of the fixed order

Let $d = n/2$ and, for $1 \le i < d$, set

$$s_i = X^i + X^{-i} = X^i - X^{n-i}.$$

Lemma 5.1. *The elements*

$$1, s_1, \dots, s_{d-1}$$

form a $\mathbb{Z}$-basis of R^+. They are orthogonal for the coefficient inner product, with squared norms

$$1, 2, \dots, 2.$$

Proof. Write $a = \sum_{j=0}^{n-1} a_j X^j$. The condition $a = a^\star$ gives

$$a_j = -a_{n-j} \quad (1 \le j < n),$$

and in particular $a_d = 0$. Hence

$$a = a_0 + \sum_{j=1}^{d-1} a_j (X^j - X^{n-j}) = a_0 + \sum_{j=1}^{d-1} a_j s_j.$$

The supports of these coefficient vectors are disjoint, giving the stated orthogonality and norms. □

For $X(a, z)$ one computes

$$X(a, z)^2 = (a^2 + zz^\star) I_2.$$

Therefore

$$\|X(a, z)\|_{\text{ad}}^2 = \frac{1}{n} \operatorname{Tr}_{K/\mathbb{Q}}(a^2 + zz^\star) = \|a\|_{\text{coeff}}^2 + \|z\|_{\text{coeff}}^2 . \tag{1}$$

5.2 Diagonalization, determinant, and shells

Define

$$D = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad E_j = \begin{pmatrix} 0 & X^j \\ X^{-j} & 0 \end{pmatrix} \quad (0 \le j < n).$$

Theorem 5.2 (Exact adjoint geometry)**.** *Under $Q = B^\star B$, conjugation by B gives isometries*

$$\mathcal{T}_Q = B^{-1} \mathcal{T}_0 B, \qquad \Gamma_Q = B^{-1} \Gamma_0 B,$$

where

$$\mathcal{T}_0 \simeq \mathbb{Z} \perp \sqrt{2}\,\mathbb{Z}^{d-1} \perp 2\mathbb{Z}^n,$$
$$\Gamma_0 \simeq \mathbb{Z}^n \perp \sqrt{2}\,\mathbb{Z}^{d-1} \perp 2\mathbb{Z}.$$

More explicitly, Γ_0 has the orthogonal basis

$$E_0, \dots, E_{n-1}, \quad X(s_1, 0), \dots, X(s_{d-1}, 0), \quad 2D.$$

Consequently,

$$\det G_{\mathcal{T}_Q} = 2^{5n/2-1}, \qquad \det G_{\Gamma_Q} = 2^{n/2+1}.$$

Moreover,

$$\lambda_1(\Gamma_Q) = 1, \qquad S_1(\Gamma_Q) = \{\pm B^{-1} E_j B : 0 \le j < n\},$$
$$\lambda_1(\Gamma_Q^\vee) = \frac{1}{2}, \qquad S_1(\Gamma_Q^\vee) = \left\{\pm \frac{1}{2} B^{-1} D B\right\}.$$

Every non-shortest primal vector has norm at least $\sqrt{2}$, and every non-shortest dual vector has norm at least $1/\sqrt{2}$.

Proof. By lemma 5.1 and Equation (1), an orthogonal basis of $\mathcal{T}_0$ is

$$D = X(1,0), \quad X(s_i,0)\ (1 \le i < d), \quad 2E_j = X(0,2X^j)\ (0 \le j < n),$$

with squared norms 1, 2, and 4, respectively. This proves the first diagonalization and its determinant.

The dual basis is

$$D, \quad \frac{1}{2}X(s_i,0), \quad \frac{1}{2}E_j.$$

Multiplying by two gives the stated basis of $\Gamma_0 = 2\mathcal{T}_0^\vee$, with squared norms 1 on the E_j, 2 on the $X(s_i,0)$, and 4 on $2D$. This proves the second diagonalization, determinant, and primal shell.

Since $\Gamma_0^\vee = \frac{1}{2}\mathcal{T}_0$, its orthogonal scales have shortest vector $D/2$ of norm $1/2$, followed by $X(s_i,0)/2$ of norm $1/\sqrt{2}$. Conjugation transfers all statements to Q. Finally, $B, B^{-1} \in M_2(R)$ and $\Gamma_0 \subseteq M_2(R)$, so $\Gamma_Q \subseteq M_2(R)$. □

Corollary 5.3. *The adjoint lattice satisfies*

$$\lambda_1(\Gamma_Q)\lambda_1(\Gamma_Q^\vee) = \frac{1}{2},$$

and both primal and dual first shells have multiplicative gap $\sqrt{2}$.

5.3 Shortest vectors are orthogonal involutions

For $u \in R$ with $u^\star u = 1$, put

$$E_u = \begin{pmatrix} 0 & u \\ u^\star & 0 \end{pmatrix}.$$

Then $E_u^2 = I_2$. The primal shell in theorem 5.2 consists of conjugates of E_u for $u \in \{\pm X^j\}$; twice the dual shell consists of conjugates of $\pm D$. Thus either shell supplies a nontrivial module-LAP witness for the same public form Q, precisely the input required by the instance-preserving self-reduction of [Luo+25, Theorem 3.1].

Corollary 5.4. *From any vector in* $S_1(\Gamma_Q)$*, or twice any vector in* $S_1(\Gamma_Q^\vee)$*, one obtains a matrix* $A \in M_2(R)$ *satisfying*

$$A^2 = I_2, \qquad A^\star Q = QA, \qquad A^\star QA = Q.$$

Proof. The first two identities hold in the hidden standard form and are preserved by conjugation. The third follows from $A^\star Q = QA$ and $A^2 = I_2$. □

6 The Bambury–Nguyen half-dimensional reduction

The dimension-halving component is the primal–dual blockwise reduction of Bambury and Nguyen [BN24], not a new reduction of the present work. Their framework extends Ducas's half-dimensional reduction for the hypercubic lattice [Duc24]: it alternates reduction of a projected primal block and of a dual block, and measures progress by the resulting decrease of the covolume of a half-rank sublattice. We record the specialization needed for the adjoint lattice.

Theorem 6.1 (Bambury–Nguyen reduction, specialized form [BN24])**.** *Let* Λ *be an integral lattice of rank* r*. Suppose that*

$$a = \lambda_1(\Lambda), \qquad b = \lambda_1(\Lambda^\vee)$$

are known, and suppose that the primal and dual first shells have known multiplicative gaps at least $\Delta > 1$*. If*

$$1 \le \gamma < \Delta, \qquad \gamma^2 ab < 1,$$

then the primal–dual blockwise reduction of [BN24], with its shortest-shell tests instantiated using the known gap Δ, finds a vector in $S_1(\Lambda)$ or $S_1(\Lambda^\vee)$ using polynomially many γ-SVP calls. Every oracle lattice has dimension at most

$$\left\lfloor \frac{r}{2} \right\rfloor + 1.$$

For a fixed contraction margin $1 - \gamma^2 ab > 0$, the number of calls and all exact auxiliary lattice operations are polynomial in the input length.

Remark 6.2 (What is imported from [BN24])**.** The alternating projected-primal/dual-block algorithm, the half-dimensional oracle bound, and the covolume-descent termination argument are precisely the Bambury–Nguyen framework. The displayed hypotheses only spell out its specialization here. The shell gap makes the required first-shell tests valid with a γ-SVP oracle, while an unsuccessful primal–dual round contracts the maintained covolume by at most $\gamma^2 ab < 1$; see [BN24]. No independent dimension-halving lemma is claimed in this work.

Theorem 6.3 (Main oracle-rank theorem)**.** *Let $n \geq 4$ be a power of two and $R = \mathbb{Z}[X]/(X^n + 1)$. Given $Q \in \mathrm{Herm}_2(R)$ promised to satisfy $Q = B^\star B$ for some $B \in \mathrm{GL}_2(R)$, and any fixed $1 \leq \gamma < \sqrt{2}$, one can find a Q-orthogonal involution of the form described in corollary 5.4 using polynomially many γ-SVP calls, each in dimension at most*

$$\boxed{\frac{3n}{4} + 1}.$$

Proof. Apply the Bambury–Nguyen reduction in theorem 6.1 to $\Lambda = \Gamma_Q$. By theorem 5.2 and corollary 5.3,

$$r = \frac{3n}{2}, \qquad a = 1, \qquad b = \frac{1}{2}, \qquad \Delta = \sqrt{2}.$$

For every fixed $\gamma < \sqrt{2}$, the shell tests are valid and

$$\gamma^2 ab = \frac{\gamma^2}{2} < 1.$$

The cited reduction therefore uses oracle lattices of dimension at most

$$\left\lfloor \frac{r}{2} \right\rfloor + 1 = \frac{3n}{4} + 1.$$

A primal shortest vector is already the required involution; twice a dual shortest vector is the required involution. □

7 Gram-factor recovery via the module-LIP self-reduction

The shortest-shell computation has already produced a nontrivial automorphism of the public Hermitian form. We now use the instance-preserving module-LIP-to-module-LAP reduction proved in *Commitment Schemes Based on Module-LIP* [Luo+25, Theorem 3.1]. We state exactly the specialization needed here. In the notation of the cited paper, we take $k = 0$, so its base form $Q_0^{(0)}$ is exactly I_2.

Definition 7.1 (Rank-two module-LIP and module-LAP at I_2)**.** For a positive-definite Hermitian form $Q \in \mathrm{Herm}_2(R)$ in the orbit of I_2, write

$$\mathrm{Aut}_R(Q) = \{P \in \mathrm{GL}_2(R) : P^\star Q P = Q\}, \qquad \mu(R) = \{\pm X^j : 0 \leq j < n\}.$$

The search module-LIP instance asks for a matrix $U \in \mathrm{GL}_2(R)$ satisfying $Q = U^\star U$. A module-LAP witness is any

$$P_Q \in \mathrm{Aut}_R(Q) \setminus \mu(R) I_2.$$

Theorem 7.2 (Instance-preserving module-LIP-to-module-LAP reduction [Luo+25])**.** *Let $Q = U^\star U$ with $U \in \mathrm{GL}_2(R)$. Given Q and any nontrivial module-lattice automorphism*

$$P_Q \in \mathrm{Aut}_R(Q) \setminus \mu(R) I_2,$$

there is a deterministic polynomial-time algorithm that outputs an equivalent factor $\widetilde{B} \in \mathrm{GL}_2(R)$ satisfying

$$\widetilde{B}^\star \widetilde{B} = Q.$$

The reduction preserves the input instance Q. In the proof of the cited theorem, the possible hidden automorphism is enumerated inside the polynomial-size group $\mathrm{Aut}_R(I_2)$; the diagonal and anti-diagonal cases are handled by Propositions 3.1 and 3.2, respectively, using eigensubmodules and CM-order lattice isomorphism.

Remark 7.3 (Specialization of the anti-diagonal branch)**.** For a primal shortest vector, the hidden standard automorphism is

$$E_u = \begin{pmatrix} 0 & u \\ u^\star & 0 \end{pmatrix}, \qquad u \in \mu(R).$$

In the notation of the anti-diagonal branch of [Luo+25, Proposition 3.2], the product of the two off-diagonal roots of unity is $uu^\star = 1$. Hence its eigenvalues are already $\pm 1 \in K$; the field-extension step needed for a general anti-diagonal automorphism is unnecessary in the present specialization. The dual shortest shell gives the diagonal branch of [Luo+25, Proposition 3.1].

Proposition 7.4 (The recovered involution is a valid LAP witness)**.** *Let A be obtained from a primal shortest vector of Γ_Q, or let $A = 2W$ for a dual shortest vector $W \in S_1(\Gamma_Q^\vee)$. Then*

$$A \in \mathrm{Aut}_R(Q) \setminus \mu(R) I_2.$$

Proof. By corollary 5.4, $A \in M_2(R)$ satisfies $A^\star Q A = Q$ and $A^2 = I_2$, so $A \in \mathrm{Aut}_R(Q)$. In hidden coordinates, A is conjugate either to some E_u or to $\pm D$, where $D = \mathrm{diag}(1, -1)$. All of these matrices have trace zero and are nonzero. A scalar matrix in $\mu(R) I_2$ has trace 2ξ with $\xi \in \mu(R)$, which is nonzero in characteristic zero. Thus A is not a trivial scalar automorphism. □

Algorithm 2 Factor recovery through the module-LIP-to-module-LAP self-reduction

Require: Q, and either $W \in S_1(\Gamma_Q)$ or $W \in S_1(\Gamma_Q^\vee)$.
Ensure: $\widetilde{B} \in \mathrm{GL}_2(R)$ with $\widetilde{B}^\star \widetilde{B} = Q$.

1: **if** $W \in S_1(\Gamma_Q)$ **then**
2: $\quad A \leftarrow W$.
3: **else**
4: $\quad A \leftarrow 2W$.
5: Apply the post-processing algorithm of theorem 7.2 to the module-LIP instance Q and the module-LAP witness A.
6: **return** the resulting equivalent factor $\widetilde{B}$.

Theorem 7.5 (Factor recovery)**.** *Under the promise in definition 1.1, algorithm 2 runs in deterministic polynomial time and returns $\widetilde{B} \in \mathrm{GL}_2(R)$ satisfying*

$$\widetilde{B}^\star \widetilde{B} = Q.$$

Proof. By proposition 7.4, the matrix A supplied to the self-reduction is a nontrivial element of $\mathrm{Aut}_R(Q)$. The conclusion therefore follows directly from theorem 7.2. No further shortest-vector computation is used in this post-processing step. □

Proof of theorem 1.2. By theorem 6.3, polynomially many γ-SVP calls of dimension at most $3n/4+1$ produce a primal or dual shortest-shell vector and hence, by corollary 5.4, a Q-orthogonal involution. By proposition 7.4, this involution is a nontrivial module-LAP witness for the same instance Q. The instance-preserving self-reduction of [Luo+25, Theorem 3.1], stated as theorem 7.2, then returns an equivalent factor $\widetilde{B}$ in deterministic polynomial time. All remaining operations are the exact constructions in algorithm 1, the Bambury–Nguyen reduction quoted in theorem 6.1, and the module-LIP self-reduction quoted in theorem 7.2. □

A Public formulas for the dual basis

Let $t_1, \dots, t_r$ be a $\mathbb{Z}$-basis of $\mathcal{T}_Q$, represented in a fixed rational basis of $M_2(K)$, and let

$$G = (\langle t_i, t_j \rangle_{\mathrm{ad}})_{i,j}.$$

Then

$$t_i^\vee = \sum_{j=1}^{r} (G^{-1})_{ij} t_j$$

is the dual basis, and $2t_i^\vee$ is a basis of Γ_Q. Under the promise, these rational matrices have integral coefficients in R, but integrality need not be assumed by the implementation: it can be checked exactly after construction.

References

[BN24] H. Bambury and P. Q. Nguyen. "Improved Provable Reduction of NTRU and Hypercubic Lattices". In: *Post-Quantum Cryptography – PQCrypto 2024, Part I*. Springer, 2024, pp. 343–370. DOI: 10.1007/978-3-031-62743-9_12. IACR ePrint: 2024/601.

[Duc24] L. Ducas. "Provable Lattice Reduction of $\mathbb{Z}^n$ with Blocksize $n/2$". In: *Designs, Codes and Cryptography* 92.4 (2024), pp. 909–916. DOI: 10.1007/s10623-023-01320-7.

[HS19] J. Hendrik W. Lenstra and A. Silverberg. "Testing Isomorphism of Lattices over CM-Orders". In: *SIAM Journal on Computing* 48.4 (2019), pp. 1300–1334. DOI: 10.1137/17M115390X. arXiv: 1706.07373.

[Luo+25] H. Luo, K. Jiang, R. Jin, Y. Pan, and A. Wang. *Commitment Schemes Based on Module-LIP*. Cryptology ePrint Archive, Paper 2025/431. 2025. URL: https://eprint.iacr.org/2025/431.