

Poisoned Cryptography: Solving Direct-Sum LIP in Half the Dimension

Aleksandr Bakharev^{2,3} and Artyom Kuninets¹

¹QApp, Bolshoy blvd 30b1, Moscow, 121205, Russian Federation.

²JSRPC Kryptonite, Shlyuzovaya Naberezhnaya 4, Moscow, 115114, Russian Federation.

³Novosibirsk State University, 2 Pirogov Street, Novosibirsk, 630090, Russian Federation.

Contributing authors: a.bakharev@g.nsu.ru; artkuninets@yandex.ru;

Abstract

We analyse the Lattice Isomorphism Problem framework of Ducas and van Woerden when it is instantiated with the direct sum of two rescaled integral Barnes–Wall lattices, $\Lambda_S = gBW_m^Z \oplus (g+1)BW_m^Z$. All primitives of the framework share the same key pair, a public form $\mathbf{P} = \mathbf{U}^\top \mathbf{S} \mathbf{U}$ and a secret unimodular matrix $\mathbf{U}$, so recovering $\mathbf{U}$ from $\mathbf{P}$ breaks each of them. We take the hash-and-sign signature scheme as an example, whose security rests on distinguishing the class of $\mathbf{S} = \text{diag}(g^2\mathbf{R}, (g+1)^2\mathbf{R})$ from that of the auxiliary form $\mathbf{Q}^{-1} = \text{diag}(\mathbf{R}, g^2(g+1)^2\mathbf{R})$. We show that the g^2 -hull maps each of the two classes onto the other, is computable from the public key alone, and rescales the two blocks from $(g, g+1)$ to $(1, g(g+1))$ without changing the automorphism group, so that solutions of the transformed instance lift back. The transformed instance then splits into two isomorphism problems for the public Barnes–Wall lattice in half the dimension. At $d = 1024$, $g = 43$ the estimated cost of key recovery drops from **220** to **124** classical bits.

1 Introduction

In recent years, the Lattice Isomorphism Problem (LIP) has attracted increasing attention as a foundation for post-quantum cryptography. The framework proposed by Ducas and van Woerden [1] uses a lattice equipped with efficient decoding or sampling algorithms, applies a secret unimodular transformation of basis, and publishes the resulting Gram matrix. The change of basis serves as the secret key and the Gram matrix as the public key. The HAWK signature scheme [2] follows the same principle in a module setting. Since then, a number of further primitives have been built within this framework. They include a concrete key encapsulation mechanism on Barnes–Wall lattices [3], public-key encryption [4], fully homomorphic encryption [5, 6], identity-based encryption [7], and commitment schemes obtained by viewing LIP as a group action [8]. The security of all these schemes relies on the hardness of either the search or the distinguishing variant of LIP for a direct sum lattice masked by a unimodular transformation.

Despite increasing activity, cryptanalysis of concrete LIP instantiations remains comparatively limited. Ducas and Gibbons [9] examined the cryptanalytic role of s -hulls for LIP and showed that these sublattices, computable directly from a Gram matrix, yield effective reductions for several families of instances. Their analysis also identifies a case in which the s -hull construction provides no useful information. For a unimodular lattice, every s -hull is a scaled copy of the original lattice, so the transformation does not alter the underlying geometry. This explains the preference for unimodular lattices in [1, 9].

The instantiations considered in this work fall outside this case. The secret lattice is a direct sum of two differently scaled copies of the same unimodular lattice. Although each individual block is therefore unaffected by the unimodular-lattice argument of [9], the direct sum is not. The s -hull acts on the two blocks with different scaling factors to them, so that the resulting lattice is not a scaled copy of the original one. Thus, an appropriate

choice of s modifies the geometry of the lattice while preserving the relevant structural information. This change in geometry creates a sharp separation between the two blocks and makes the underlying direct-sum decomposition reachable by lattice reduction.

Our contribution. We consider the instantiation in which the remarkable lattice in the framework [1] is the direct sum of two rescaled copies of the integral Barnes–Wall lattice $BW_m^{\mathbb{Z}}$ of dimension m ,

$$\Lambda_{\mathbf{S}} = gBW_m^{\mathbb{Z}} \oplus (g+1)BW_m^{\mathbb{Z}} \subset \mathbb{R}^d, \quad d = 2m, \quad \mathbf{S} = \text{diag}(g^2\mathbf{R}, (g+1)^2\mathbf{R}),$$

where $\mathbf{R}$ denotes the Gram matrix of $BW_m^{\mathbb{Z}}$, and the distinguishing problem is stated with respect to the auxiliary form $\mathbf{Q}^{-1} = \text{diag}(\mathbf{R}, g^2(g+1)^2\mathbf{R})$. The scaling factors g and $g+1$ are consecutive, so the two blocks of $\Lambda_{\mathbf{S}}$ have close first minimum. Moreover, the two forms have the same determinant and kissing number. The g^2 -hull does not separate the classes either: it maps each form to a scaled representative of the other class.

We present an attack that exploits s -hulls to expose the hidden direct-sum structure of the public form. Passing to the g^2 -hull changes the scaling factors from $(g, g+1)$ to $(1, g(g+1))$. The automorphism groups remain equal to $\text{Aut}(\mathbf{R}) \times \text{Aut}(\mathbf{R})$, which allows a solution of the transformed LIP instance to be lifted to a solution for the original forms. The resulting scale separation implies that vectors below $g(g+1)\lambda_1(\mathbf{R})$ belong to the first Barnes–Wall block. Consequently, short-vector reduction can be used to identify the hidden decomposition, after which the search problem decomposes into two LIP instances for the public form $\mathbf{R}$ of dimension $d/2$.

Organization of the paper. Section 2 introduces the notation for integral forms and LIP, recalls the relevant properties of s -hulls and Barnes–Wall lattices, and specifies the considered signature instantiation. Section 3 gives the reduction, proves its correctness, describes the corresponding algorithms, and evaluates the resulting search and distinguishing costs.

2 Preliminaries

2.1 Lattices

A *lattice* $\Lambda \subset \mathbb{R}^d$ is a discrete subgroup of the additive group $\mathbb{R}^d$. It is closed under addition and subtraction, and there is a radius $r > 0$ such that any two distinct vectors $\mathbf{v}, \mathbf{w} \in \Lambda$ satisfy $\|\mathbf{v} - \mathbf{w}\| \geq r$, where $\|\cdot\|$ denotes the Euclidean norm on $\mathbb{R}^d$.

Every lattice admits a *basis*, a set of linearly independent vectors $\mathbf{b}_1, \dots, \mathbf{b}_n \in \mathbb{R}^d$ that generates it over $\mathbb{Z}$. Arranging them as the columns of $\mathbf{B} = [\mathbf{b}_1, \dots, \mathbf{b}_n]$, we write

$$\Lambda(\mathbf{B}) = \mathbf{B} \cdot \mathbb{Z}^n = \left\{ \sum_{i=1}^n x_i \mathbf{b}_i \mid x_i \in \mathbb{Z} \right\}.$$

The number n of basis vectors is the *rank* of Λ , equal to the dimension of the real subspace spanned by Λ . The lattice is *full-rank* if $n = d$, and we restrict to this case throughout. Two bases $\mathbf{B}$ and $\mathbf{B}'$ generate the same lattice if and only if $\mathbf{B}' = \mathbf{B}\mathbf{U}$ for some $\mathbf{U} \in GL_d(\mathbb{Z})$, which is why unimodular transformations play the role of secret keys in the constructions considered below.

The *dual lattice* of Λ consists of the vectors of its span having integer inner product with every lattice vector,

$$\Lambda^* = \{ \mathbf{x} \in \text{span}(\Lambda) \mid \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z} \text{ for all } \mathbf{y} \in \Lambda \}.$$

If $\mathbf{B}$ is a basis of a full-rank lattice Λ , then $\mathbf{B}^{-\top}$ is a basis of Λ^* . A lattice is *integral* if $\Lambda \subseteq \Lambda^*$, that is, if all inner products of lattice vectors are integers, and *unimodular* if $\Lambda = \Lambda^*$.

The *Gram matrix* of a basis $\mathbf{B}$ is the symmetric positive definite matrix of pairwise inner products

$$\mathbf{B}^{\top} \mathbf{B} = (\langle \mathbf{b}_i, \mathbf{b}_j \rangle)_{1 \leq i, j \leq d},$$

and the *volume* of Λ is $\text{vol}(\Lambda) = \det(\mathbf{B}^{\top} \mathbf{B})^{1/2}$. The volume does not depend on the choice of basis and measures the density of the lattice, a larger volume corresponding to sparser lattice points.

The *first minimum* of Λ is the length of a shortest nonzero lattice vector,

$$\lambda_1(\Lambda) = \min_{\mathbf{v} \in \Lambda \setminus \{\mathbf{0}\}} \|\mathbf{v}\|.$$

More generally, the i -th successive minimum $\lambda_i(\Lambda)$ is the smallest $r > 0$ such that the lattice vectors of norm at most r span a subspace of dimension at least i . The first minimum is bounded in terms of the volume.

Theorem 2.1 (Minkowski bound). *For a lattice Λ of rank d ,*

$$\lambda_1(\Lambda) \leq \sqrt{d} \cdot \text{vol}(\Lambda)^{1/d}.$$

For a random lattice the first minimum is predicted by the *Gaussian heuristic*

$$\text{gh}(\Lambda) = \frac{\text{vol}(\Lambda)^{1/d}}{\text{vol}(\mathcal{B}_1^d)^{1/d}} \approx \sqrt{\frac{d}{2\pi e}} \cdot \text{vol}(\Lambda)^{1/d},$$

where $\mathcal{B}_1^d$ is the unit ball in $\mathbb{R}^d$. The ratio $\lambda_1(\Lambda)/\text{gh}(\Lambda)$ compares the first minimum of a lattice with that of a random lattice of the same volume. It enters both the hull analysis and the cost estimates of Section 3.2.

2.2 Quadratic forms and the Lattice Isomorphism Problem

Throughout, vectors are columns, $GL_d(\mathbb{Z})$ denotes the group of unimodular integer matrices, and $O_d(\mathbb{R})$ the group of orthogonal transformations.

Definition 2.2 (Lattice Isomorphism Problem). *Given bases $\mathbf{B}, \mathbf{B}' \in \mathbb{R}^{d \times d}$ of two isomorphic lattices, compute an orthogonal transformation $\mathbf{O} \in O_d(\mathbb{R})$ and a unimodular transformation $\mathbf{U} \in GL_d(\mathbb{Z})$ such that $\mathbf{B}' = \mathbf{O}\mathbf{B}\mathbf{U}$.*

It is more convenient to work with quadratic forms. A *quadratic form* of rank d is a positive definite symmetric matrix $\mathbf{M} \in \mathcal{S}_d^{>0}(\mathbb{R})$ and the form is *integral* if $\mathbf{M} \in \mathbb{Z}^{d \times d}$. We write $q_{\mathbf{M}}(\mathbf{x}) = \mathbf{x}^\top \mathbf{M} \mathbf{x}$ for the associated quadratic map, $\|\mathbf{x}\|_{\mathbf{M}} = \sqrt{q_{\mathbf{M}}(\mathbf{x})}$ for the induced norm, and $\text{vol}(\mathbf{M}) = \sqrt{\det \mathbf{M}}$. A basis $\mathbf{B}$ of a lattice Λ gives the quadratic form $\mathbf{M} = \mathbf{B}^\top \mathbf{B}$, its Gram matrix, and conversely every $\mathbf{M} \in \mathcal{S}_d^{>0}(\mathbb{R})$ arises in this way from a lattice $\Lambda_{\mathbf{M}}$ determined up to isometry. Lattice invariants therefore transfer to quadratic forms, and we write

$$\lambda_1(\mathbf{M}) = \min_{\mathbf{x} \in \mathbb{Z}^d \setminus \{\mathbf{0}\}} \|\mathbf{x}\|_{\mathbf{M}}, \quad \min(\mathbf{M}) = \lambda_1(\mathbf{M})^2, \quad \text{Min}(\mathbf{M}) = \{\mathbf{x} \in \mathbb{Z}^d : q_{\mathbf{M}}(\mathbf{x}) = \min(\mathbf{M})\},$$

with $\lambda_i(\mathbf{M})$ the i -th successive minimum.

Two quadratic forms $\mathbf{M}, \mathbf{M}'$ are *equivalent*, written $\mathbf{M} \simeq \mathbf{M}'$, if $\mathbf{M}' = \mathbf{U}^\top \mathbf{M} \mathbf{U}$ for some $\mathbf{U} \in GL_d(\mathbb{Z})$. Denote the equivalence class of $\mathbf{M}$ as

$$[\mathbf{M}] = \{\mathbf{U}^\top \mathbf{M} \mathbf{U} \mid \mathbf{U} \in GL_d(\mathbb{Z})\}.$$

For a pair of forms we denote by

$$\text{Iso}(\mathbf{M}, \mathbf{M}') = \{\mathbf{X} \in GL_d(\mathbb{Z}) \mid \mathbf{X}^\top \mathbf{M} \mathbf{X} = \mathbf{M}'\}, \quad \text{Aut}(\mathbf{M}) = \text{Iso}(\mathbf{M}, \mathbf{M})$$

the set of equivalences between them and the automorphism group of $\mathbf{M}$.

Definition 2.3 (Worst-case search LIP, wc-sLIP^M). *For a quadratic form $\mathbf{M}$, the worst-case search lattice isomorphism problem consists of finding, for a given $\mathbf{M}' \in [\mathbf{M}]$, a unimodular transformation $\mathbf{U} \in GL_d(\mathbb{Z})$ such that $\mathbf{M}' = \mathbf{U}^\top \mathbf{M} \mathbf{U}$.*

This is equivalent to Definition 2.2, since the orthogonal part is recovered as $\mathbf{O} = \mathbf{B}'(\mathbf{B}\mathbf{U})^{-1}$ once $\mathbf{U}$ is known. For a form $\mathbf{M}$ and $\mathbf{M}' \in [\mathbf{M}]$ we write $\text{LIP}^{(\mathbf{M}, \mathbf{M}')}$ for the instance of wc-sLIP^M with input $\mathbf{M}'$, that is, the task of finding an element of $\text{Iso}(\mathbf{M}, \mathbf{M}')$, and $\text{LIP}^{(\mathbf{M}, \cdot)}$ when $\mathbf{M}' \in [\mathbf{M}]$ is left unspecified.

Definition 2.4 (Worst-case distinguishing LIP, wc-ΔLIP^{M₀, M₁}). *For two quadratic forms $\mathbf{M}_0, \mathbf{M}_1$ with $[\mathbf{M}_0] \neq [\mathbf{M}_1]$, the worst-case distinguishing lattice isomorphism problem is the following: given an arbitrary $\mathbf{M}' \in [\mathbf{M}_b]$, where $b \in \{0, 1\}$ is a uniformly random bit, recover b .*

Cryptographic schemes sample their public key from a fixed distribution rather than adversarially, so security is stated against the average-case variants. Let $\mathcal{D}_\sigma([\mathbf{M}])$ denote a distribution supported on $[\mathbf{M}]$, parametrised by

a width s . In $\text{ac-sLIP}_s^{\mathbf{M}}$ the instance $\mathbf{M}'$ is drawn from $\mathcal{D}_\sigma([\mathbf{M}])$, and in $\text{ac-}\Delta\text{LIP}_s^{\mathbf{M}_0, \mathbf{M}_1}$ the instance is drawn from $\mathcal{D}_\sigma([\mathbf{M}_b])$ for a uniform bit b . Worst-case to average-case reductions for both are given in [1].

Fact 2.5. *If $\mathbf{X}_0 \in \text{Iso}(\mathbf{M}, \mathbf{M}') \neq \emptyset$, then $\text{Iso}(\mathbf{M}, \mathbf{M}') = \text{Aut}(\mathbf{M}) \cdot \mathbf{X}_0$.*

Proof. If $\mathbf{A} \in \text{Aut}(\mathbf{M})$ then $(\mathbf{A}\mathbf{X}_0)^\top \mathbf{M} (\mathbf{A}\mathbf{X}_0) = \mathbf{X}_0^\top \mathbf{M} \mathbf{X}_0 = \mathbf{M}'$. Conversely, if $\mathbf{X} \in \text{Iso}(\mathbf{M}, \mathbf{M}')$ then, using $\mathbf{M} = (\mathbf{X}_0^\top)^{-1} \mathbf{M}' \mathbf{X}_0^{-1}$, the matrix $\mathbf{A} = \mathbf{X} \mathbf{X}_0^{-1}$ satisfies $\mathbf{A}^\top \mathbf{M} \mathbf{A} = \mathbf{M}$. $\square$

The solutions of a search instance thus form a coset of $\text{Aut}(\mathbf{M})$, and any element of the corresponding coset is sufficient for the successful key-recovery attack.

2.3 Hulls for lattices and quadratic forms

One of the main cryptanalytic techniques against LIP is the hull attack of Ducas and Gibbons [9]. It exploits s -hulls computable from the public Gram matrix whose geometry can make the associated LIP instances easier than the original instance. Unimodular lattices, those with $\Lambda = \Lambda^*$, avoid this source of geometric weakness, since every rational s -hull is a scaled copy of the original lattice [9].

Definition 2.6 (Hull and s -hull). *For a lattice Λ with dual Λ^* , the hull is $H(\Lambda) = \Lambda \cap \Lambda^*$. For $s \in \mathbb{Q}_{>0}$, the s -hull of Λ is the sublattice*

$$\mathcal{H}_s(\Lambda) = \Lambda \cap s\Lambda^*.$$

For an integral lattice, $\Lambda \subseteq \Lambda^*$ and hence $H(\Lambda) = \Lambda$. The ordinary hull therefore provides no nontrivial invariant, which motivates the parametrized construction. The behaviour of the s -hull on unimodular lattices is completely characterized by [9, Lemma 8]: for $s = a/b$ with $\gcd(a, b) = 1$ it coincides with the scaled lattice $a\Lambda$. Up to scaling there is thus a single s -hull, namely Λ itself, however s is chosen. More generally, for an integral lattice with Gram matrix $\mathbf{M}$, the same argument shows that $\mathcal{H}_{a/b}(\Lambda) = a\Lambda$ whenever a is coprime to $\det \mathbf{M}$, so only the values of s whose numerator shares a prime factor with $\det \mathbf{M}$ can yield a lattice that is not a scalar multiple of Λ .

Scaling is what removes any cryptanalytic value from these hulls in the case of unimodular lattices. The difficulty of LIP for a lattice is determined by its gap

$$\text{gap}(\Lambda) = \max \left\{ \frac{\text{gh}(\Lambda)}{\lambda_1(\Lambda)}, \frac{\text{gh}(\Lambda^*)}{\lambda_1(\Lambda^*)} \right\}, \quad (1)$$

where gh denotes the Gaussian heuristic. Since $\text{gap}(s\Lambda) = \text{gap}(\Lambda)$ for every s , replacing a unimodular lattice Λ by any of its s -hulls yields an instance of exactly the same difficulty. In particular, whenever the s -hull is merely a scaled copy of Λ , the technique of [9] provides no advantage. Barnes–Wall lattices are unimodular up to scaling over $\mathbb{Z}[i]$ and their integral versions have determinant a power of two, so all odd s values yield scaled copies, while the remaining s values were shown in [10] to be ineffective as well.

Section 3 shows that this classification does not extend to the case when the lattice is a direct sum whose blocks are scaled by different factors. Even when both blocks are unimodular, the s -hull of the resulting lattice need not be a scaled copy of it, because a single modulus s can act differently on blocks carrying different scaling factors. This permits to reduce $\text{LIP}^{(\mathbf{S}, \mathbf{P})}$ to a simpler problem considering the hulls of the original lattice $\Lambda_{\mathbf{S}}$. For a nonsingular $\mathbf{M} \in \mathbb{Z}^{d \times d}$ put

$$\Lambda_s^\perp(\mathbf{M}) = \{\mathbf{x} \in \mathbb{Z}^d : \mathbf{M}\mathbf{x} \equiv 0 \pmod{s}\},$$

a lattice of full rank d , since it contains $s\mathbb{Z}^d$.

Lemma 2.7 ([9, Lemma 3]). *Let Λ be an integral lattice with basis matrix $\mathbf{B}$ and Gram matrix $\mathbf{M} = \mathbf{B}^\top \mathbf{B}$. Then $\mathcal{H}_s(\Lambda) = \mathbf{B} \Lambda_s^\perp(\mathbf{M})$, and if $\mathbf{K}$ is a basis matrix of $\Lambda_s^\perp(\mathbf{M})$, the Gram matrix of $\mathcal{H}_s(\Lambda)$ in the basis $\mathbf{BK}$ is*

$$\mathbf{M}_{\mathcal{H}_s} = (\mathbf{BK})^\top (\mathbf{BK}) = \mathbf{K}^\top \mathbf{M} \mathbf{K}. \quad (2)$$

Proof. A vector $\mathbf{B}\mathbf{y}$ with $\mathbf{y} \in \mathbb{Z}^d$ lies in $s\Lambda^* = s\mathbf{B}^{-\top} \mathbb{Z}^d$ if and only if $\mathbf{B}\mathbf{y} = s\mathbf{B}^{-\top} \mathbf{z}$ for some $\mathbf{z} \in \mathbb{Z}^d$, that is, if and only if $\mathbf{M}\mathbf{y} = s\mathbf{z}$. Hence $\mathcal{H}_s(\Lambda) = \mathbf{B} \Lambda_s^\perp(\mathbf{M})$, and (2) is immediate. $\square$

The form $\mathbf{K}^\top \mathbf{M} \mathbf{K}$ depends on the choice of $\mathbf{K}$ only up to $\mathbb{Z}$ -equivalence. Replacing $\mathbf{K}$ by $\mathbf{KW}$ with $\mathbf{W} \in GL_d(\mathbb{Z})$ replaces it by $\mathbf{W}^\top (\mathbf{K}^\top \mathbf{M} \mathbf{K}) \mathbf{W}$. The class $[\mathbf{K}^\top \mathbf{M} \mathbf{K}]$ is therefore a well-defined invariant of $[\mathbf{M}]$, and s -hulls may

be used either as distinguishers, through this invariant, or as reductions, through the transformation itself. The second use is based on the following equivariance.

Lemma 2.8. *Let $\mathbf{M} \in \mathbb{Z}^{d \times d}$ be nonsingular and $\mathbf{M}' = \mathbf{U}^\top \mathbf{M} \mathbf{U}$ with $\mathbf{U} \in GL_d(\mathbb{Z})$. Then $\Lambda_s^\perp(\mathbf{M}') = \mathbf{U}^{-1} \Lambda_s^\perp(\mathbf{M})$ for every $s \in \mathbb{N}$.*

Proof. The matrix $\mathbf{U}^\top$ is unimodular, hence invertible modulo s . Therefore

$$\mathbf{M}' \mathbf{x} \equiv 0 \iff \mathbf{U}^\top \mathbf{M} (\mathbf{U} \mathbf{x}) \equiv 0 \iff \mathbf{M} (\mathbf{U} \mathbf{x}) \equiv 0 \pmod{s} \iff \mathbf{U} \mathbf{x} \in \Lambda_s^\perp(\mathbf{M}). \quad \square$$

2.4 Barnes–Wall lattices

Definition 2.9 (Barnes–Wall lattice). *Let N be a power of two and $\theta = 1 + i$. The Barnes–Wall lattice BW_N of dimension N over $\mathbb{Z}[i]$ is the lattice generated by the columns of the basis matrix*

$$\mathbf{B}(BW_1) = (1), \quad \mathbf{B}(BW_N) = \begin{pmatrix} \mathbf{B}(BW_{N/2}) & \mathbf{0} \\ \mathbf{B}(BW_{N/2}) & \theta \mathbf{B}(BW_{N/2}) \end{pmatrix},$$

or, equivalently,

$$\mathbf{B}(BW_N) = \begin{pmatrix} 1 & 0 \\ 1 & \theta \end{pmatrix}^{\otimes \log_2 N}.$$

We write $BW_m^\mathbb{Z} \subset \mathbb{Z}^m$, with m a power of two, for the integral lattice obtained from $BW_{m/2}$ by replacing each entry $a + ib \in \mathbb{Z}[i]$ of $\mathbf{B}(BW_{m/2})$ with the block

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix},$$

whose columns are the real embeddings of $a + ib$ and of $i(a + ib)$. The resulting matrix is a basis $\mathbf{B}(BW_m^\mathbb{Z})$ of $BW_m^\mathbb{Z}$, and we denote by $\mathbf{R} = \mathbf{B}(BW_m^\mathbb{Z})^\top \mathbf{B}(BW_m^\mathbb{Z})$ its Gram matrix. This is the form the attack works with, so we record its parameters in the notation used throughout. Every column of $\mathbf{B}(BW_{m/2})$ has squared norm $m/2$, since both columns of the 2×2 factor have squared norm 2, and the real embedding preserves norms. Hence

$$\lambda_1(\mathbf{R})^2 = m/2,$$

so the squared minimum of $BW_m^\mathbb{Z}$ is half its dimension, all basis vectors of $BW_m^\mathbb{Z}$ are minimal, and $\text{Min}(\mathbf{R})$ generates $\mathbb{Z}^m$. Table 1 lists the quantities invoked throughout this work. Note that the gap of Barnes–Wall lattices differs from the Minkowski bound by $\Theta(\sqrt[m]{m})$, which makes them unusually dense for structured lattices and permits smaller parameters at a given security level [1, 10].

Table 1 Parameters of the integral Barnes–Wall lattice $BW_m^\mathbb{Z}$.

parameter	general	$m = 512$
dimension	m	512
first minimum	$\lambda_1(\mathbf{R}) = \sqrt{m/2}$	16
Gram determinant	$\det \mathbf{R} = (m/2)^{m/2}$	256^{256}
volume	$\text{vol}(\mathbf{R}) = (m/2)^{m/4}$	256^{128}
normalized volume	$\text{vol}(\mathbf{R})^{1/m} = \sqrt{\lambda_1(\mathbf{R})}$	4
density relative to gh	$\lambda_1(\mathbf{R}) / \text{gh}(\mathbf{R}) = \sqrt{\pi e / \lambda_1(\mathbf{R})}$	0.73
kissing number	$\kappa = \prod_{i=1}^{\log_2 m} (2^i + 2)$	$\approx 2^{47.2}$

2.5 Schemes from ΔLIP framework and the key-recovery problem

The framework of [1] yields several primitives: a key encapsulation mechanism, a zero-knowledge proof of knowledge and the identification scheme derived from it, and a hash-and-sign signature. They differ in how the secret is used,

but not in how it is generated. In each case one fixes a quadratic form $\mathbf{S}$ whose lattice admits an efficient decoder or Gaussian sampler, samples $\mathbf{P} \leftarrow \mathcal{D}_\sigma([\mathbf{S}])$ together with a unimodular $\mathbf{U}$ satisfying $\mathbf{P} = \mathbf{U}^\top \mathbf{S} \mathbf{U}$, and publishes $\mathbf{P}$ while keeping $\mathbf{U}$ secret.

The security of these schemes is stated in terms of $\text{ac-sLIP}_s^{\mathbf{S}}$ and of $\text{ac-}\Delta\text{LIP}^{\mathbf{S}, \mathbf{Q}^{-1}}$ with an auxiliary class $[\mathbf{Q}^{-1}]$. The choice of that class is constrained by the arithmetic invariants of a quadratic form, which are computable in polynomial time and would otherwise separate the two classes at once. The auxiliary form must therefore agree with $\mathbf{S}$ on all of them.

The role of the auxiliary class depends on the primitive, so we take the hash-and-sign signature of [1, §6] as an example. The auxiliary form is chosen so that, in the last game of the security proof, signature forgery is statistically impossible. Once the public key has been replaced by a form of $[\mathbf{Q}^{-1}]$, which the distinguishing assumption makes undetectable, an overwhelming fraction of targets admit no valid signature at all. To achieve this, the form $\mathbf{Q}^{-1}$ must admit a sparse projection or, equivalently, its dual must contain a dense sublattice of rank k . A uniform target then has no lattice point within the acceptance radius ρ , except with probability at most 2^{-k} .

Theorem 2.10 ([1, Theorem 6.2]). *Consider the signature scheme $\mathcal{S} := (\text{Gen}, \text{Sign}, \text{Verify})$ of [1, §6] instantiated with a quadratic form $\mathbf{S} \in \mathcal{S}_d^{>0}(\mathbb{Z})$, sampling parameter ρ , and public key parameter $s > 0$. Let $\mathbf{Q} \in \mathcal{S}_d^{>0}(\mathbb{Z})$ be a quadratic form with a dense rank $k = \Theta(d)$ sublattice $\mathbf{D}\mathbb{Z}^k \subset \mathbb{Z}^d$, in particular such that*

$$\frac{2\rho}{\sqrt{k}} \leq \left(\sqrt{8\pi e} \cdot \det(\mathbf{D}^\top \mathbf{Q} \mathbf{D})^{1/k} \right)^{-1}.$$

Then $\mathcal{S}$ is EUF-CMA secure if $\text{ac-}\Delta\text{LIP}_s^{\mathbf{S}, \mathbf{Q}^{-1}}$ is hard.

We analyse the instantiation in which $\mathbf{S}$ and $\mathbf{Q}^{-1}$ are block-diagonal forms whose blocks are differently scaled quadratic forms $\mathbf{R}$ of the Barnes–Wall lattice $BW_m^{\mathbb{Z}}$. For an integer $g \geq 2$ we set

$$d = 2m, \quad \mathbf{S} = \begin{pmatrix} g^2 \mathbf{R} & 0 \\ 0 & (g+1)^2 \mathbf{R} \end{pmatrix}, \quad \mathbf{Q}^{-1} = \begin{pmatrix} \mathbf{R} & 0 \\ 0 & g^2(g+1)^2 \mathbf{R} \end{pmatrix}. \quad (3)$$

The value $g = 1$ is excluded because the two forms then coincide. Geometric invariants of a quadratic form, such as the successive minima, the kissing number and the theta series, are hard to compute, and the design relies on this. For $\mathbf{S}$ and $\mathbf{Q}^{-1}$ they do not all coincide. The kissing numbers agree, since in both lattices the minimal vectors are exactly those of one Barnes–Wall block, but the first minimum differs by the factor g ,

$$\lambda_1(\mathbf{S}) = g \lambda_1(\mathbf{R}), \quad \lambda_1(\mathbf{Q}^{-1}) = \lambda_1(\mathbf{R}),$$

since in each case the shorter block attains the minimum, and the theta series differ as well. The first minimum is an invariant of $\mathbb{Z}$ -equivalence, so $[\mathbf{S}] \neq [\mathbf{Q}^{-1}]$ for every $g \geq 2$, and the two classes are distinguished by any algorithm that computes it. This is no contradiction with the assumed hardness of $\Delta\text{LIP}^{\mathbf{S}, \mathbf{Q}^{-1}}$, since computing the first minimum of a d -dimensional form is itself exponential in d . The security of the scheme rests on the claim that no such invariant is accessible within the claimed security level.

The search problem considered in this work is

$$\text{given the public } \mathbf{P} \text{ and } \mathbf{S}, \text{ find } \mathbf{U}' \in GL_d(\mathbb{Z}) \text{ with } \mathbf{U}'^\top \mathbf{S} \mathbf{U}' = \mathbf{P},$$

and by Fact 2.5 every element of $\text{Iso}(\mathbf{S}, \mathbf{P})$ is an equivalent secret key. The remaining parameters, including the Gaussian widths, the acceptance bound ρ , the modulus q and the sampling distribution $\mathcal{D}_\sigma([\mathbf{S}])$, do not enter the reductions below.

3 The attack

3.1 Reduction and splitting

We present the argument for odd g , and Remark 1 explains the modification for even g . The starting point is the g^2 -hull of the two forms, which we compute explicitly.

Proposition 3.1. *Let $s = g^2$, with g odd. Then $\mathbf{K}_\mathbf{S} = \text{diag}(\mathbf{I}_m, g^2 \mathbf{I}_m)$ is a basis matrix of $\Lambda_{g^2}^\perp(\mathbf{S})$, the matrix $\mathbf{K}_\mathbf{Q} = \text{diag}(g^2 \mathbf{I}_m, \mathbf{I}_m)$ is one of $\Lambda_{g^2}^\perp(\mathbf{Q}^{-1})$, and*

$$\mathbf{K}_\mathbf{S}^\top \mathbf{S} \mathbf{K}_\mathbf{S} = \begin{pmatrix} g^2 \mathbf{R} & 0 \\ 0 & g^4 (g+1)^2 \mathbf{R} \end{pmatrix} = g^2 \mathbf{Q}^{-1}, \quad \mathbf{K}_\mathbf{Q}^\top \mathbf{Q}^{-1} \mathbf{K}_\mathbf{Q} = \begin{pmatrix} g^4 \mathbf{R} & 0 \\ 0 & g^2 (g+1)^2 \mathbf{R} \end{pmatrix} = g^2 \mathbf{S}. \quad (4)$$

Proof. Write $\mathbf{x} = (\mathbf{x}_1, \mathbf{x}_2)$ with $\mathbf{x}_1, \mathbf{x}_2 \in \mathbb{Z}^m$. For $\mathbf{S}$ the condition $\mathbf{S}\mathbf{x} \equiv 0 \pmod{g^2}$ splits into $g^2 \mathbf{R}\mathbf{x}_1 \equiv 0$, which holds for every $\mathbf{x}_1$, and $(g+1)^2 \mathbf{R}\mathbf{x}_2 \equiv 0 \pmod{g^2}$. As $\gcd(g+1, g) = 1$, the factor $(g+1)^2$ is invertible modulo g^2 , and as g is odd, $\mathbf{R}$ is invertible modulo g^2 by Section 2.4. The condition is therefore $\mathbf{x}_2 \equiv 0 \pmod{g^2}$. Hence $\Lambda_{g^2}^\perp(\mathbf{S}) = \mathbb{Z}^m \oplus g^2 \mathbb{Z}^m$ with basis matrix $\mathbf{K}_\mathbf{S}$. For $\mathbf{Q}^{-1}$ the second condition, $g^2 (g+1)^2 \mathbf{R}\mathbf{x}_2 \equiv 0 \pmod{g^2}$, is void, while the first, $\mathbf{R}\mathbf{x}_1 \equiv 0 \pmod{g^2}$, forces $\mathbf{x}_1 \equiv 0 \pmod{g^2}$. Hence $\Lambda_{g^2}^\perp(\mathbf{Q}^{-1}) = g^2 \mathbb{Z}^m \oplus \mathbb{Z}^m$ with basis matrix $\mathbf{K}_\mathbf{Q}$. Both identities in (4) are direct computations. $\square$

Remark 1. *If g is even, then $g+1$ is odd and the modulus $s = (g+1)^2$ plays the role of g^2 . The proof of Proposition 3.1, with the two blocks exchanged, shows that $\mathbf{K}_\mathbf{S} = \text{diag}((g+1)^2 \mathbf{I}_m, \mathbf{I}_m)$ is a basis matrix of $\Lambda_{(g+1)^2}^\perp(\mathbf{S})$ and*

$$\mathbf{K}_\mathbf{S}^\top \mathbf{S} \mathbf{K}_\mathbf{S} = (g+1)^2 \begin{pmatrix} g^2 (g+1)^2 \mathbf{R} & 0 \\ 0 & \mathbf{R} \end{pmatrix}.$$

Up to the permutation exchanging the two blocks, which is unimodular, this is $(g+1)^2 \mathbf{Q}^{-1}$. All subsequent statements and algorithms therefore hold for even g after replacing g^2 by $(g+1)^2$ and exchanging the blocks, so the parity of g does not affect the subsequent arguments.

Remark 2 (lattice form of Proposition 3.1). *The proposition also follows directly from the corresponding lattice representations. Write $\Lambda = BW_m^\mathbb{Z}$. For lattices L_1, M_1 in a subspace V and L_2, M_2 in its orthogonal complement,*

$$(L_1 \oplus L_2)^\star = L_1^\star \oplus L_2^\star, \quad (L_1 \oplus L_2) \cap (M_1 \oplus M_2) = (L_1 \cap M_1) \oplus (L_2 \cap M_2),$$

and $(c\Lambda)^\star = c^{-1}\Lambda^\star$ for every $c > 0$, so that $\mathcal{H}_s(c\Lambda) = c\mathcal{H}_{s/c^2}(\Lambda)$. The hull of $\Lambda_\mathbf{S} = g\Lambda \oplus (g+1)\Lambda$ is therefore computed block by block,

$$\mathcal{H}_s(\Lambda_\mathbf{S}) = g\mathcal{H}_{s/g^2}(\Lambda) \oplus (g+1)\mathcal{H}_{s/(g+1)^2}(\Lambda).$$

It remains to determine the s -hulls of Λ for rational s . Since Λ is integral and $\det \mathbf{R}$ is a power of two, the quotient $\Lambda^\star/\Lambda$ is a 2-group and $\Lambda \subseteq \Lambda^\star \subseteq 2^{-e}\Lambda$ for some $e \geq 0$. Let p, q be positive integers with p odd and $\gcd(p, q) = 1$. If $\mathbf{x} \in \Lambda$ and $\mathbf{x} = (p/q)\mathbf{y}$ with $\mathbf{y} \in \Lambda^\star$, then $2^e q \mathbf{x} = p 2^e \mathbf{y} \in p\Lambda$, and since $2^e q$ is invertible modulo p , this gives $\mathbf{x} \in p\Lambda$. Conversely $p\Lambda = (p/q)q\Lambda \subseteq (p/q)\Lambda^\star$. Thus

$$\mathcal{H}_{p/q}(\Lambda) = p\Lambda$$

for all such p and q . In particular $\mathcal{H}_1(\Lambda) = \Lambda \cap \Lambda^\star = \Lambda$, which only uses that Λ is integral. For $s = g^2$ with g odd, the first block of $\Lambda_\mathbf{S}$ therefore gives $g\mathcal{H}_1(\Lambda) = g\Lambda$, and the second gives $(g+1)\mathcal{H}_{g^2/(g+1)^2}(\Lambda) = g^2(g+1)\Lambda$, since g^2 is odd and coprime to $(g+1)^2$. Hence

$$\mathcal{H}_{g^2}(\Lambda_\mathbf{S}) = g\Lambda \oplus g^2(g+1)\Lambda = g\Lambda_{\mathbf{Q}^{-1}}.$$

The same computation for $\Lambda_{\mathbf{Q}^{-1}} = \Lambda \oplus g(g+1)\Lambda$ uses $\mathcal{H}_{g^2}(\Lambda) = g^2\Lambda$ and $\mathcal{H}_{1/(g+1)^2}(\Lambda) = \Lambda$, and gives $\mathcal{H}_{g^2}(\Lambda_{\mathbf{Q}^{-1}}) = g^2\Lambda \oplus g(g+1)\Lambda = g\Lambda_\mathbf{S}$. Each block is multiplied by its own factor, here 1 for the first block of $\Lambda_\mathbf{S}$ and g^2 for the second. This is why, in contrast with the unimodular case, the s -hull of $\Lambda_\mathbf{S}$ is not a scaled copy of $\Lambda_\mathbf{S}$, even when Λ itself is unimodular.

Both hulls are thus scaled copies of the other form in the pair. The next statement rewrites this in lattice terms and shows that $s = g^2$ is the least favourable choice for the scheme, in the sense that it separates the two blocks most strongly.

Corollary 3.2. *Let g be odd, write $g+1 = 2^t w$ with w odd and $t \geq 1$, and put $\Lambda = BW_m^\mathbb{Z}$.*

1. The g^2 -hull exchanges the two lattices up to the scaling factor g ,

$$\mathcal{H}_{g^2}(\Lambda_{\mathbf{S}}) = g\Lambda_{\mathbf{Q}^{-1}}, \quad \mathcal{H}_{g^2}(\Lambda_{\mathbf{Q}^{-1}}) = g\Lambda_{\mathbf{S}}.$$

In particular, the associated invariant takes the same pair of values on $[\mathbf{S}]$ and on $[\mathbf{Q}^{-1}]$, so it does not separate the two classes.

2. For every odd positive integer s ,

$$\mathcal{H}_s(\Lambda_{\mathbf{S}}) = c_1(s)\Lambda \oplus c_2(s)\Lambda, \quad c_1(s) = \frac{g s}{\gcd(s, g^2)}, \quad c_2(s) = \frac{(g+1)s}{\gcd(s, w^2)},$$

and the ratio of the block scalings $\text{sep}(s) = \max\{c_1(s)/c_2(s), c_2(s)/c_1(s)\}$ satisfies $\text{sep}(s) \leq g(g+1)$. Equality holds if and only if $g^2 \mid s$ and $\gcd(s, w) = 1$, and in that case $\mathcal{H}_s(\Lambda_{\mathbf{S}}) = (s/g^2) \mathcal{H}_{g^2}(\Lambda_{\mathbf{S}})$.

Proof. (1). Apply Lemma 2.7 to (4). The forms $g^2\mathbf{Q}^{-1}$ and $g^2\mathbf{S}$ are the Gram matrices of $g\Lambda_{\mathbf{Q}^{-1}}$ and $g\Lambda_{\mathbf{S}}$.

(2). By Remark 2,

$$\mathcal{H}_s(\Lambda_{\mathbf{S}}) = g \mathcal{H}_{s/g^2}(\Lambda) \oplus (g+1) \mathcal{H}_{s/(g+1)^2}(\Lambda),$$

and $\mathcal{H}_{p/q}(\Lambda) = p\Lambda$ whenever p/q is in lowest terms with p odd. In lowest terms s/g^2 has numerator $s/\gcd(s, g^2)$, which is odd because s is odd, so the first block equals $c_1(s)\Lambda$. Since s is odd, no power of two cancels in $s/(g+1)^2 = s/(2^{2t}w^2)$, so its numerator in lowest terms is $s/\gcd(s, w^2)$, again odd, and the second block equals $c_2(s)\Lambda$. The two ratios are

$$\frac{c_2(s)}{c_1(s)} = \frac{g+1}{g} \cdot \frac{\gcd(s, g^2)}{\gcd(s, w^2)}, \quad \frac{c_1(s)}{c_2(s)} = \frac{g}{g+1} \cdot \frac{\gcd(s, w^2)}{\gcd(s, g^2)}.$$

Since $\gcd(s, g^2) \leq g^2$ and $\gcd(s, w^2) \geq 1$, the first ratio is at most $g(g+1)$, with equality exactly when $g^2 \mid s$ and $\gcd(s, w) = 1$. The second ratio is at most $gw^2/(g+1) = gw/2^t$, which is strictly smaller than $g(g+1)$ because $w \leq g+1$ and $t \geq 1$. In the case of equality $s = g^2r$ with r odd and coprime to w , so $c_1(s) = gr$ and $c_2(s) = g^2(g+1)r$, and $\mathcal{H}_s(\Lambda_{\mathbf{S}}) = r \mathcal{H}_{g^2}(\Lambda_{\mathbf{S}})$ by part (1). $\square$

For comparison, $s = 1$ returns $\Lambda_{\mathbf{S}}$ itself with $\text{sep}(1) = 1 + 1/g$. Even values of s bring in the 2-adic structure of $BW_m^{\mathbb{Z}}$ and are not covered by part (2). For even g the same argument applies with the roles of g and $g+1$ exchanged, the optimal value being $s = (g+1)^2$ as in Remark 1.

Thus the g^2 -hull does not by itself provide a distinguishing invariant. Its relevance to key recovery is of a different nature. It changes the ratio of the block scalings from $1 + 1/g$ for $\mathbf{S}$ to $g(g+1)$ for $\mathbf{Q}^{-1}$, and this scale separation is the structural property exploited by the short-vector step below. The hull computation is polynomial-time and, as shown further on, preserves the automorphism group relevant to the lifting of solutions. Since the hull is computed from a Gram matrix alone, the same transformation can be applied to the public key, where the secret $\mathbf{U}$ is unavailable. Lemma 2.8 shows that the result is the hull of $\mathbf{S}$ transported by $\mathbf{U}$, which gives the following reduction.

Theorem 3.3. *Let $\mathbf{P} = \mathbf{U}^{\top} \mathbf{S} \mathbf{U}$, let $\mathbf{K}_{\mathbf{P}}$ be any basis matrix of $\Lambda_{g^2}^{\perp}(\mathbf{P})$, and set $\mathbf{G} = g^{-2} \mathbf{K}_{\mathbf{P}}^{\top} \mathbf{P} \mathbf{K}_{\mathbf{P}}$. Then $\mathbf{G}$ is integral, the matrix $\mathbf{V}_0 = \mathbf{K}_{\mathbf{S}}^{-1} \mathbf{U} \mathbf{K}_{\mathbf{P}}$ lies in $GL_d(\mathbb{Z})$, and $\mathbf{G} = \mathbf{V}_0^{\top} \mathbf{Q}^{-1} \mathbf{V}_0$. In particular $\mathbf{G} \in [\mathbf{Q}^{-1}]$.*

Proof. By Lemma 2.8, $\Lambda_{g^2}^{\perp}(\mathbf{P}) = \mathbf{U}^{-1} \Lambda_{g^2}^{\perp}(\mathbf{S})$. Hence $\mathbf{K}_{\mathbf{P}}$ and $\mathbf{U}^{-1} \mathbf{K}_{\mathbf{S}}$ are bases of the same lattice and differ by a unimodular factor, that is $\mathbf{K}_{\mathbf{P}} = \mathbf{U}^{-1} \mathbf{K}_{\mathbf{S}} \mathbf{V}_0$ with $\mathbf{V}_0 = \mathbf{K}_{\mathbf{S}}^{-1} \mathbf{U} \mathbf{K}_{\mathbf{P}}$. Then

$$\mathbf{K}_{\mathbf{P}}^{\top} \mathbf{P} \mathbf{K}_{\mathbf{P}} = \mathbf{V}_0^{\top} \mathbf{K}_{\mathbf{S}}^{\top} \mathbf{S} \mathbf{K}_{\mathbf{S}} \mathbf{V}_0 = \mathbf{V}_0^{\top} (g^2 \mathbf{Q}^{-1}) \mathbf{V}_0$$

by Proposition 3.1, and the right-hand side is g^2 times an integral matrix. $\square$

An instance of $\text{LIP}^{(\mathbf{S}, \cdot)}$ is therefore transformed into an instance of $\text{LIP}^{(\mathbf{Q}^{-1}, \cdot)}$ in polynomial time. The cryptanalytic relevance of this transformation follows from the increased separation between the scaling factors of the two blocks in the resulting instance. To obtain a reduction to lower-dimensional LIP instances, we must first identify the corresponding block decomposition from the transformed form and then establish that a solution to the transformed instance can be mapped back to a solution of the original one. Both properties follow from the structure of sufficiently short vectors in the transformed lattice.

Lemma 3.4. Let $\Lambda = c_1 BW_m^{\mathbb{Z}} \oplus c_2 BW_m^{\mathbb{Z}}$ with $0 < c_1 < c_2$. Every vector $\mathbf{x} = (\mathbf{x}_1, \mathbf{x}_2) \in \Lambda$ with

$$\|\mathbf{x}\|^2 < c_2^2 \lambda_1(\mathbf{R})^2$$

satisfies $\mathbf{x}_2 = 0$ and hence lies entirely in the first block. In particular $\lambda_1(\Lambda) = c_1 \lambda_1(\mathbf{R})$ and

$$\text{Min}(\Lambda) = \text{Min}(c_1 BW_m^{\mathbb{Z}}) \oplus \{\mathbf{0}\}, \quad \langle \text{Min}(\Lambda) \rangle = c_1 BW_m^{\mathbb{Z}} \oplus \{\mathbf{0}\}.$$

Proof. We have $\|\mathbf{x}\|^2 = c_1^2 \mathbf{x}_1^\top \mathbf{R} \mathbf{x}_1 + c_2^2 \mathbf{x}_2^\top \mathbf{R} \mathbf{x}_2$ with both terms nonnegative, and $\mathbf{x}_2 \neq 0$ forces $\mathbf{x}_2^\top \mathbf{R} \mathbf{x}_2 \geq \lambda_1(\mathbf{R})^2$. The value $c_1^2 \lambda_1(\mathbf{R})^2$ is attained in the first block and is smaller, so every minimal vector has $\mathbf{x}_2 = 0$. These vectors generate $c_1 BW_m^{\mathbb{Z}} \oplus \{\mathbf{0}\}$ because $\text{Min}(\mathbf{R})$ generates $\mathbb{Z}^m$. $\square$

The threshold $c_2 \lambda_1(\mathbf{R})$ exceeds the first minimum by the factor c_2/c_1 . For $\mathbf{S}$ this factor equals $1 + 1/g$, whereas for $\mathbf{Q}^{-1}$ it equals $g(g+1)$. The same block-separation argument is therefore substantially more accessible after the hull transformation, and the corresponding BKZ estimates are given in Section 3.2. The lemma has a second consequence, which does not depend on the size of the separation but only on its existence. Since the minimal vectors span exactly one block, no isometry can interchange the two.

Theorem 3.5. Let $\mathbf{T} \in \{\mathbf{S}, \mathbf{Q}^{-1}\}$ and $\mathbf{A} \in GL_d(\mathbb{Z})$ with $\mathbf{A}^\top \mathbf{T} \mathbf{A} = \mathbf{T}$. Then $\mathbf{A} = \text{diag}(\mathbf{A}_1, \mathbf{A}_2)$ with $\mathbf{A}_1, \mathbf{A}_2 \in \text{Aut}(\mathbf{R})$, and

$$\text{Aut}(\mathbf{S}) = \text{Aut}(\mathbf{Q}^{-1}) = \text{Aut}(\mathbf{R}) \times \text{Aut}(\mathbf{R}) \quad (5)$$

as block-diagonal subgroups of $GL_d(\mathbb{Z})$.

Proof. Both forms are of the shape $\mathbf{T} = \text{diag}(c_1^2 \mathbf{R}, c_2^2 \mathbf{R})$ with $0 < c_1 < c_2$, namely $(c_1, c_2) = (g, g+1)$ for $\mathbf{S}$ and $(c_1, c_2) = (1, g(g+1))$ for $\mathbf{Q}^{-1}$. Let $\Lambda_1 = \mathbb{Z}^m \oplus \{\mathbf{0}\}$ and $\Lambda_2 = \{\mathbf{0}\} \oplus \mathbb{Z}^m$ be the coordinate blocks of $\mathbb{Z}^d$.

Since $\mathbf{A}^\top \mathbf{T} \mathbf{A} = \mathbf{T}$, the map $\mathbf{x} \mapsto \mathbf{A} \mathbf{x}$ preserves $q_{\mathbf{T}}$ and hence permutes $\text{Min}(\mathbf{T})$. By Lemma 3.4 these vectors lie in Λ_1 and generate it, so $\mathbf{A} \Lambda_1 = \Lambda_1$. Moreover Λ_2 is the orthogonal complement of Λ_1 with respect to $\mathbf{T}$, because $\mathbf{T}$ is block diagonal and $\mathbf{R}$ is nonsingular. Let $\mathbf{y} \in \Lambda_2$ and $\mathbf{x} \in \Lambda_1$. Since $\mathbf{A} \Lambda_1 = \Lambda_1$, we may write $\mathbf{x} = \mathbf{A} \mathbf{x}'$ with $\mathbf{x}' \in \Lambda_1$, and then

$$\mathbf{x}^\top \mathbf{T}(\mathbf{A} \mathbf{y}) = \mathbf{x}'^\top \mathbf{A}^\top \mathbf{T} \mathbf{A} \mathbf{y} = \mathbf{x}'^\top \mathbf{T} \mathbf{y} = 0.$$

Hence $\mathbf{A} \mathbf{y}$ is orthogonal to Λ_1 , and $\mathbf{A} \Lambda_2 = \Lambda_2$ as well.

From $\mathbb{Z}^d = \Lambda_1 \oplus \Lambda_2$ and $\mathbf{A} \Lambda_i = \Lambda_i$ we get $\mathbf{A} = \text{diag}(\mathbf{A}_1, \mathbf{A}_2)$ with $\mathbf{A}_1, \mathbf{A}_2 \in GL_m(\mathbb{Z})$. Substituting into $\mathbf{A}^\top \mathbf{T} \mathbf{A} = \mathbf{T}$ gives $c_i^2 \mathbf{A}_i^\top \mathbf{R} \mathbf{A}_i = c_i^2 \mathbf{R}$, that is, $\mathbf{A}_i \in \text{Aut}(\mathbf{R})$. Conversely, every $\text{diag}(\mathbf{A}_1, \mathbf{A}_2)$ with $\mathbf{A}_i \in \text{Aut}(\mathbf{R})$ satisfies $\mathbf{A}^\top \mathbf{T} \mathbf{A} = \mathbf{T}$, the scalings c_i^2 cancelling. The resulting condition does not involve c_1 and c_2 , so the two automorphism groups coincide. $\square$

The two automorphism groups therefore coincide, and the hull transformation does not enlarge the set of solutions. This differs from the Construction-A instantiations considered in [9, §5], where the hull may collapse to $p\mathbb{Z}^d$ for generic instances and the subsequent reduction proceeds through code equivalence. In the present setting the transformed lattice retains both Barnes–Wall blocks, so the correspondence between the two LIP instances is exact and can be written down explicitly.

Theorem 3.6. In the setting of Theorem 3.3, the map $\varphi : \mathbf{X} \mapsto \mathbf{K}_{\mathbf{S}} \mathbf{X} \mathbf{K}_{\mathbf{P}}^{-1}$ is a bijection from $\text{Iso}(\mathbf{Q}^{-1}, \mathbf{G})$ onto $\text{Iso}(\mathbf{S}, \mathbf{P})$.

Proof. Let $\mathbf{V} \in \text{Iso}(\mathbf{Q}^{-1}, \mathbf{G})$. The set is nonempty by Theorem 3.3, so $\mathbf{V} = \mathbf{A} \mathbf{V}_0$ with $\mathbf{V}_0 = \mathbf{K}_{\mathbf{S}}^{-1} \mathbf{U} \mathbf{K}_{\mathbf{P}}$ and $\mathbf{A} \in \text{Aut}(\mathbf{Q}^{-1})$ by Fact 2.5, and $\mathbf{A} = \text{diag}(\mathbf{A}_1, \mathbf{A}_2)$ by Theorem 3.5. Since $\mathbf{K}_{\mathbf{S}} = \text{diag}(\mathbf{I}, g^2 \mathbf{I})$ is scalar on each block, it commutes with $\mathbf{A}$, whence

$$\varphi(\mathbf{V}) = \mathbf{K}_{\mathbf{S}} \mathbf{A} \mathbf{V}_0 \mathbf{K}_{\mathbf{P}}^{-1} = (\mathbf{K}_{\mathbf{S}} \mathbf{A} \mathbf{K}_{\mathbf{S}}^{-1}) (\mathbf{K}_{\mathbf{S}} \mathbf{V}_0 \mathbf{K}_{\mathbf{P}}^{-1}) = \mathbf{A} \mathbf{U},$$

an integral unimodular matrix satisfying $(\mathbf{A} \mathbf{U})^\top \mathbf{S} (\mathbf{A} \mathbf{U}) = \mathbf{U}^\top (\mathbf{A}^\top \mathbf{S} \mathbf{A}) \mathbf{U} = \mathbf{P}$ by (5). Injectivity follows from the invertibility of $\mathbf{K}_{\mathbf{S}}$ and $\mathbf{K}_{\mathbf{P}}$ over $\mathbb{Q}$. Conversely, for any $\mathbf{U}' \in \text{Iso}(\mathbf{S}, \mathbf{P})$, the matrix $\mathbf{A} = \mathbf{U}' \mathbf{U}^{-1}$ belongs to $\text{Aut}(\mathbf{S}) = \text{Aut}(\mathbf{Q}^{-1})$, and $\varphi(\mathbf{A} \mathbf{V}_0) = \mathbf{U}'$. $\square$

Any solution of the transformed instance therefore yields a secret key for the original one, and it remains to solve the transformed instance itself. Here the enlarged scaling of the second block becomes decisive. By Lemma 3.4

the vectors below the threshold identify one block of $\Lambda_{\mathbf{Q}^{-1}}$, and the orthogonal complement identifies the other, which reduces the problem to two instances of half the dimension for the public form $\mathbf{R}$.

Theorem 3.7. *Let $\mathbf{G} = \mathbf{V}^\top \mathbf{Q}^{-1} \mathbf{V}$ for an unknown $\mathbf{V} \in GL_d(\mathbb{Z})$ and put*

$$\Lambda^{(1)} = \text{Span}_{\mathbb{Q}}\{\mathbf{x} \in \mathbb{Z}^d \mid \mathbf{x}^\top \mathbf{G} \mathbf{x} < g^2(g+1)^2 \lambda_1(\mathbf{R})^2\} \cap \mathbb{Z}^d, \quad \Lambda^{(2)} = \{\mathbf{y} \in \mathbb{Z}^d \mid \mathbf{x}^\top \mathbf{G} \mathbf{y} = 0 \ \forall \mathbf{x} \in \Lambda^{(1)}\}. \quad (6)$$

Then the following hold.

1. $\Lambda^{(1)}$ and $\Lambda^{(2)}$ have rank m and $\mathbb{Z}^d = \Lambda^{(1)} \oplus \Lambda^{(2)}$.
2. For basis matrices $\mathbf{C}_1, \mathbf{C}_2 \in \mathbb{Z}^{d \times m}$ the matrix $\mathbf{C} = [\mathbf{C}_1 \mid \mathbf{C}_2]$ is unimodular, and the forms

$$\mathbf{R}_1 = \mathbf{C}_1^\top \mathbf{G} \mathbf{C}_1, \quad \mathbf{R}_2 = g^{-2}(g+1)^{-2} \mathbf{C}_2^\top \mathbf{G} \mathbf{C}_2 \quad (7)$$

are integral and $\mathbb{Z}$ -equivalent to $\mathbf{R}$, say $\mathbf{F}_i^\top \mathbf{R} \mathbf{F}_i = \mathbf{R}_i$ with $\mathbf{F}_i \in GL_m(\mathbb{Z})$.

3. For any such $\mathbf{F}_1, \mathbf{F}_2$, the matrix $\mathbf{V}' = \text{diag}(\mathbf{F}_1, \mathbf{F}_2) \mathbf{C}^{-1}$ lies in $GL_d(\mathbb{Z})$ and satisfies $\mathbf{V}'^\top \mathbf{Q}^{-1} \mathbf{V}' = \mathbf{G}$.

Proof. Let $\Lambda_1 = \mathbb{Z}^m \oplus \{\mathbf{0}\}$ and $\Lambda_2 = \{\mathbf{0}\} \oplus \mathbb{Z}^m$, with respect to which $\mathbf{Q}^{-1}$ is orthogonal, and let $\mathcal{W} = \{\mathbf{x} \in \mathbb{Z}^d \mid \mathbf{x}^\top \mathbf{G} \mathbf{x} < g^2(g+1)^2 \lambda_1(\mathbf{R})^2\}$, so that $\Lambda^{(1)} = \text{Span}_{\mathbb{Q}} \mathcal{W} \cap \mathbb{Z}^d$. The map $\mathbf{x} \mapsto \mathbf{V} \mathbf{x}$ is an isometry from $\mathbf{G}$ to $\mathbf{Q}^{-1}$.

(1). First, $\mathbf{V}^{-1} \Lambda_1$ is saturated. Indeed $\mathbb{Z}^d = \mathbf{V}^{-1} \Lambda_1 \oplus \mathbf{V}^{-1} \Lambda_2$, so the quotient by $\mathbf{V}^{-1} \Lambda_1$ is free and

$$\text{Span}_{\mathbb{Q}}(\mathbf{V}^{-1} \Lambda_1) \cap \mathbb{Z}^d = \mathbf{V}^{-1} \Lambda_1. \quad (8)$$

By Lemma 3.4 with $c_1 = 1$ and $c_2 = g(g+1)$, every $\mathbf{x} \in \mathcal{W}$ has $\mathbf{V} \mathbf{x} \in \Lambda_1$. Hence $\mathcal{W} \subseteq \mathbf{V}^{-1} \Lambda_1$ and, taking spans and intersecting with $\mathbb{Z}^d$, $\Lambda^{(1)} \subseteq \mathbf{V}^{-1} \Lambda_1$ by (8). For the reverse inclusion it is enough that $\mathcal{W}$ have rank m , since then the two $\mathbb{Q}$ -spans are nested of equal dimension, hence equal. That holds because $BW_m^{\mathbb{Z}}$ contains m independent minimal vectors, of squared norm $\lambda_1(\mathbf{R})^2 < g^2(g+1)^2 \lambda_1(\mathbf{R})^2$, whose preimages lie in $\mathcal{W}$.

Note that $\mathcal{W}$ need not generate $\mathbf{V}^{-1} \Lambda_1$. Only the independence of m of its elements is used, and any finite index is absorbed by the saturation in (6). Nor is minimality of length needed, since everything below the threshold qualifies and the threshold is itself the certificate of membership in the first block.

For $\Lambda^{(2)}$, the condition $\mathbf{x}^\top \mathbf{G} \mathbf{y} = 0$ for all $\mathbf{x} \in \Lambda^{(1)}$ says that $\mathbf{V} \mathbf{y}$ is $\mathbf{Q}^{-1}$ -orthogonal to Λ_1 , which for a nonsingular block-diagonal form means $\mathbf{V} \mathbf{y} \in \Lambda_2$. Hence $\Lambda^{(2)} = \mathbf{V}^{-1} \Lambda_2$ and $\Lambda^{(1)} \oplus \Lambda^{(2)} = \mathbf{V}^{-1} \mathbb{Z}^d = \mathbb{Z}^d$.

(2). Unimodularity of $\mathbf{C}$ follows from (1). As $\mathbf{V} \mathbf{C}_1$ is a basis matrix of Λ_1 , it has the form $\begin{pmatrix} \mathbf{F}_1 \\ \mathbf{0} \end{pmatrix}$ with $\mathbf{F}_1 \in GL_m(\mathbb{Z})$, and likewise $\mathbf{V} \mathbf{C}_2 = \begin{pmatrix} \mathbf{0} \\ \mathbf{F}_2 \end{pmatrix}$. Then $\mathbf{R}_1 = (\mathbf{V} \mathbf{C}_1)^\top \mathbf{Q}^{-1} (\mathbf{V} \mathbf{C}_1) = \mathbf{F}_1^\top \mathbf{R} \mathbf{F}_1$ and $\mathbf{C}_2^\top \mathbf{G} \mathbf{C}_2 = g^2(g+1)^2 \mathbf{F}_2^\top \mathbf{R} \mathbf{F}_2$.

(3). From $\mathbf{V} \mathbf{C} = \text{diag}(\mathbf{F}_1, \mathbf{F}_2)$ we get $\mathbf{V} = \text{diag}(\mathbf{F}_1, \mathbf{F}_2) \mathbf{C}^{-1}$ for the true $\mathbf{F}_i$. Given other solutions $\mathbf{F}'_i$, the matrices $\mathbf{D}_i = \mathbf{F}'_i \mathbf{F}_i^{-1}$ lie in $\text{Aut}(\mathbf{R})$, so

$$\mathbf{V}' = \text{diag}(\mathbf{F}'_1, \mathbf{F}'_2) \mathbf{C}^{-1} = \text{diag}(\mathbf{D}_1, \mathbf{D}_2) \mathbf{V},$$

and $\text{diag}(\mathbf{D}_1, \mathbf{D}_2) \in \text{Aut}(\mathbf{Q}^{-1})$ by Theorem 3.5, whence $\mathbf{V}'^\top \mathbf{Q}^{-1} \mathbf{V}' = \mathbf{G}$. $\square$

3.2 Algorithms and cost estimates

Key recovery

Algorithm 1 $\text{HULLBASIS}(\mathbf{M}, s)$ — a basis matrix of $\Lambda_s^\perp(\mathbf{M})$

Require: nonsingular $\mathbf{M} \in \mathbb{Z}^{d \times d}$, modulus $s \in \mathbb{N}$

Ensure: $\mathbf{K} \in \mathbb{Z}^{d \times d}$, a basis matrix of $\Lambda_s^\perp(\mathbf{M})$

- 1: $(\mathbf{D}, \mathbf{A}, \mathbf{B}) \leftarrow \text{SNF}(\mathbf{M})$ $\triangleright \mathbf{D} = \mathbf{A} \mathbf{M} \mathbf{B}, \mathbf{A}, \mathbf{B} \in GL_d(\mathbb{Z}), \mathbf{D}$ diagonal
 - 2: **for** $i = 1, \dots, d$ **do**
 - 3: $c_i \leftarrow s / \gcd(s, D_{ii})$
 - 4: $\mathbf{K} \leftarrow \mathbf{B} \cdot \text{diag}(c_1, \dots, c_d)$
 - 5: $\mathbf{K} \leftarrow \text{HNF}(\mathbf{K})$
 - 6: **return** $\mathbf{K}$
-

Lemma 3.8. *Algorithm 1 is correct and polynomial in d , $\log s$ and the bit size of $\mathbf{M}$.*

Proof. The matrix $\mathbf{A}$ is invertible modulo s , so $\mathbf{M}\mathbf{x} \equiv 0$ is equivalent to $\mathbf{A}\mathbf{M}\mathbf{x} \equiv 0$. With $\mathbf{y} = \mathbf{B}^{-1}\mathbf{x}$ this reads $D_{ii}y_i \equiv 0 \pmod s$ for each i , that is $y_i \equiv 0 \pmod{c_i}$. Hence $\Lambda_s^\perp(\mathbf{M}) = \mathbf{B} \operatorname{diag}(c_1, \dots, c_d) \mathbb{Z}^d$, and the Hermite normal form (HNF) only changes the basis. Both normal forms are computable in polynomial time [11]. $\square$

Algorithm 2 REDUCETO AUXILIARY($\mathbf{P}, g$) — from $\operatorname{LIP}(\mathbf{S}, \cdot)$ to $\operatorname{LIP}(\mathbf{Q}^{-1}, \cdot)$

Require: public key $\mathbf{P} = \mathbf{U}^\top \mathbf{S} \mathbf{U}$, integer $g \geq 2$

Ensure: $(\mathbf{K}_\mathbf{S}, \mathbf{K}_\mathbf{P}, \mathbf{G})$ with $\mathbf{G} \in [\mathbf{Q}^{-1}]$

1: **if** g is odd **then**

2: $s \leftarrow g^2$, $\mathbf{K}_\mathbf{S} \leftarrow \operatorname{diag}(\mathbf{I}_m, g^2 \mathbf{I}_m)$

3: **else**

4: $s \leftarrow (g+1)^2$, $\mathbf{K}_\mathbf{S} \leftarrow \begin{pmatrix} \mathbf{0} & (g+1)^2 \mathbf{I}_m \\ \mathbf{I}_m & \mathbf{0} \end{pmatrix}$

$\triangleright$ see Remark 1

5: $\mathbf{K}_\mathbf{P} \leftarrow \operatorname{HULLBASIS}(\mathbf{P}, s)$

6: $\mathbf{G} \leftarrow s^{-1} \mathbf{K}_\mathbf{P}^\top \mathbf{P} \mathbf{K}_\mathbf{P}$

7: **return** $(\mathbf{K}_\mathbf{S}, \mathbf{K}_\mathbf{P}, \mathbf{G})$

Lemma 3.9. *With $\mathbf{K}_\mathbf{P}$ in Hermite normal form and $\mathbf{G} = g^{-2} \mathbf{K}_\mathbf{P}^\top \mathbf{P} \mathbf{K}_\mathbf{P}$,*

$$\log_2 \|\mathbf{G}\|_{\max} \leq \log_2 \|\mathbf{P}\|_{\max} + 2 \log_2 d + 2 \log_2 g.$$

Proof. The entries of $\mathbf{K}_\mathbf{P}$ are bounded by $s = g^2$ because $s\mathbb{Z}^d \subseteq \Lambda_s^\perp(\mathbf{P})$, so that $|(\mathbf{K}_\mathbf{P}^\top \mathbf{P} \mathbf{K}_\mathbf{P})_{ij}| \leq d^2 s^2 \|\mathbf{P}\|_{\max}$. Dividing by s gives the claim. $\square$

At $d = 1024$ and $g = 43$ this contributes at most 31 additional bits to the bound on each entry, which is negligible compared with the subsequent lattice-reduction steps.

Algorithm 3 SOLVEAUXILIARY($\mathbf{G}, g, \lambda_1(\mathbf{R})$) — solving $\operatorname{LIP}(\mathbf{Q}^{-1}, \mathbf{G})$

Require: $\mathbf{G} = \mathbf{V}^\top \mathbf{Q}^{-1} \mathbf{V}$ for an unknown $\mathbf{V} \in GL_d(\mathbb{Z})$

Ensure: some $\mathbf{V}' \in \operatorname{Iso}(\mathbf{Q}^{-1}, \mathbf{G})$

1: $\mathcal{W} \leftarrow m$ independent $\mathbf{x} \in \mathbb{Z}^d$ with $\mathbf{x}^\top \mathbf{G} \mathbf{x} < g^2(g+1)^2 \lambda_1(\mathbf{R})^2$, obtained by reducing $\mathbf{G}$

2: $\mathbf{C}_1 \leftarrow$ basis matrix of $\Lambda^{(1)} = \operatorname{Span}_{\mathbb{Q}}(\mathcal{W}) \cap \mathbb{Z}^d$

$\triangleright$ saturation, via HNF/SNF

3: $\mathbf{C}_2 \leftarrow$ basis matrix of $\ker_{\mathbb{Z}}(\mathbf{C}_1^\top \mathbf{G})$

$\triangleright \{\mathbf{y} \in \mathbb{Z}^d \mid \mathbf{x}^\top \mathbf{G} \mathbf{y} = 0 \ \forall \mathbf{x} \in \Lambda^{(1)}\}$

4: $\mathbf{C} \leftarrow [\mathbf{C}_1 \mid \mathbf{C}_2]$, $\mathbf{R}_1 \leftarrow \mathbf{C}_1^\top \mathbf{G} \mathbf{C}_1$, $\mathbf{R}_2 \leftarrow g^{-2}(g+1)^{-2} \mathbf{C}_2^\top \mathbf{G} \mathbf{C}_2$

5: $\mathbf{F}_1 \leftarrow \operatorname{SOLVELIP}(\mathbf{R}, \mathbf{R}_1)$, $\mathbf{F}_2 \leftarrow \operatorname{SOLVELIP}(\mathbf{R}, \mathbf{R}_2)$

$\triangleright$ dimension $d/2$

6: **return** $\mathbf{V}' \leftarrow \operatorname{diag}(\mathbf{F}_1, \mathbf{F}_2) \cdot \mathbf{C}^{-1}$

Remark 3. *Line 1 of Algorithm 3 does not require minimal vectors of $\mathbf{G}$. By the proof of the Theorem 3.7, any vector of norm below $g(g+1)\lambda_1(\mathbf{R})$ lies in the first block, so it suffices to find m linearly independent vectors below this threshold. If a single lattice reduction does not provide that many, the procedure can be iterated in the orthogonal complement of the vectors already found.*

The computations in Lines 2–3 are polynomial-time integer linear algebra. If $\mathbf{K}$ is a basis matrix of the integer kernel $\{\mathbf{y} \in \mathbb{Z}^d \mid \mathbf{W}^\top \mathbf{y} = \mathbf{0}\}$, where the columns of $\mathbf{W}$ are the vectors of $\mathcal{W}$, then $\Lambda^{(1)} = \operatorname{Span}_{\mathbb{Q}}(\mathcal{W}) \cap \mathbb{Z}^d$ is the integer kernel of $\mathbf{K}^\top$, since both consist of the integer vectors orthogonal to every vector orthogonal to $\mathcal{W}$. Line 3 is again an integer kernel computation. Integer kernels are computable in polynomial time via Hermite normal forms [11]. By Theorem 3.7, every entry of $\mathbf{C}_2^\top \mathbf{G} \mathbf{C}_2$ is divisible by $g^2(g+1)^2$, so the form $\mathbf{R}_2$ computed in Line 4 is integral. Line 5 invokes $\operatorname{LIP}(\mathbf{R}, \cdot)$ twice with the same reference form $\mathbf{R}$, so any precomputation for $BW_m^{\mathbb{Z}}$, including a canonical form [12] or the isometry test of Plesken and Souvignier [13], can be reused.

Algorithm 4 HULLATTACK($\mathbf{P}, g$) — recovering a secret key

Require: public key $\mathbf{P} = \mathbf{U}^\top \mathbf{S} \mathbf{U}$, integer $g \geq 2$

Ensure: $\mathbf{U}' \in GL_d(\mathbb{Z})$ with $\mathbf{U}'^\top \mathbf{S} \mathbf{U}' = \mathbf{P}$

- 1: $(\mathbf{K}_\mathbf{S}, \mathbf{K}_\mathbf{P}, \mathbf{G}) \leftarrow \text{REDUCETO AUXILIARY}(\mathbf{P}, g)$
 - 2: $\mathbf{V}' \leftarrow \text{SOLVEAUXILIARY}(\mathbf{G}, g, \lambda_1(\mathbf{R}))$
 - 3: **return** $\mathbf{U}' \leftarrow \mathbf{K}_\mathbf{S} \mathbf{V}' \mathbf{K}_\mathbf{P}^{-1}$
-

Theorem 3.10. Suppose SOLVELIP is correct and Line 1 of Algorithm 3 returns m independent vectors below the threshold. Then Algorithm 4 outputs $\mathbf{U}' \in GL_d(\mathbb{Z})$ with $\mathbf{U}'^\top \mathbf{S} \mathbf{U}' = \mathbf{P}$.

Proof. By Theorem 3.3 the form $\mathbf{G}$ is integral and lies in $[\mathbf{Q}^{-1}]$, so $\text{Iso}(\mathbf{Q}^{-1}, \mathbf{G}) \neq \emptyset$. Theorem 3.7 makes SOLVEAUXILIARY correct. The saturation of $\langle \mathcal{W} \rangle$ is $\Lambda^{(1)}$, the forms $\mathbf{R}_1$ and $\mathbf{R}_2$ are $\mathbb{Z}$ -equivalent to $\mathbf{R}$ so that both oracle calls have solutions, and the assembled $\mathbf{V}'$ lies in $\text{Iso}(\mathbf{Q}^{-1}, \mathbf{G})$. Theorem 3.6 then sends $\mathbf{V}'$ to an element of $\text{Iso}(\mathbf{S}, \mathbf{P})$. $\square$

Apart from the short-vector computation in Line 1 and the two calls to SOLVELIP, the attack consists of Smith and Hermite normal forms and products of $d \times d$ integer matrices. These operations are polynomial in d and $\log_2 \|\mathbf{P}\|_{\max}$ [11], with coefficient growth bounded by Lemma 3.9.

Remark 4. Note that the transformed instance $\mathbf{G}$ is needed only to identify the preimages of the two blocks in the coordinates of $\mathbf{P}$, after which $\mathbf{P}$ itself decomposes. Let $\Lambda_1 = \mathbb{Z}^m \oplus \{\mathbf{0}\}$ and $\Lambda_2 = \{\mathbf{0}\} \oplus \mathbb{Z}^m$. By Theorem 3.3 and Theorem 3.7, $\mathbf{K}_\mathbf{P} = \mathbf{U}^{-1} \mathbf{K}_\mathbf{S} \mathbf{V}_0$ and $\Lambda^{(1)} = \mathbf{V}_0^{-1} \Lambda_1$. Since $\mathbf{K}_\mathbf{S} = \text{diag}(\mathbf{I}_m, g^2 \mathbf{I}_m)$ maps Λ_1 onto itself, this gives

$$\mathbf{K}_\mathbf{P} \Lambda^{(1)} = \mathbf{U}^{-1} \Lambda_1.$$

Hence the lattices

$$M_1 = \text{Span}_{\mathbb{Q}}(\mathbf{K}_\mathbf{P} \Lambda^{(1)}) \cap \mathbb{Z}^d = \mathbf{U}^{-1} \Lambda_1, \quad M_2 = \{\mathbf{y} \in \mathbb{Z}^d \mid \mathbf{x}^\top \mathbf{P} \mathbf{y} = 0 \ \forall \mathbf{x} \in M_1\} = \mathbf{U}^{-1} \Lambda_2$$

are computable from $\mathbf{P}$, the second equality using that $\mathbf{S}$ is block diagonal. For basis matrices $\mathbf{T}_1, \mathbf{T}_2$ of M_1, M_2 the matrix $\mathbf{T} = [\mathbf{T}_1 \mid \mathbf{T}_2]$ is unimodular, and $\mathbf{T}^\top \mathbf{P} \mathbf{T} = \text{diag}(g^2 \mathbf{R}'_1, (g+1)^2 \mathbf{R}'_2)$ with $\mathbf{R}'_i \in [\mathbf{R}]$. For arbitrary solutions $\mathbf{F}_i'^\top \mathbf{R} \mathbf{F}_i' = \mathbf{R}'_i$ the matrix $\mathbf{U}' = \text{diag}(\mathbf{F}'_1, \mathbf{F}'_2) \mathbf{T}^{-1}$ then satisfies

$$\mathbf{U}'^\top \mathbf{S} \mathbf{U}' = \mathbf{T}^{-\top} (\mathbf{T}^\top \mathbf{P} \mathbf{T}) \mathbf{T}^{-1} = \mathbf{P}.$$

This yields a secret key directly, without Theorem 3.6 or Theorem 3.5, and at the same cost, since the short-vector step and the two instances of $\text{LIP}^{(\mathbf{R}, \cdot)}$ are unchanged. Theorems 3.5 and 3.6 nevertheless retain their structural significance, since they establish an explicit bijection between the solution sets of $\text{LIP}^{(\mathbf{S}, \mathbf{P})}$ and $\text{LIP}^{(\mathbf{Q}^{-1}, \mathbf{G})}$, so that the reduction to the g^2 -hull is lossless.

ΔLIP

The block structure also settles the distinguishing problem, and here no hull transformation is needed. The determinant and the kissing number coincide for the two classes, whereas their first minimum differ by the factor g .

Proposition 3.11. We have $\min(\mathbf{S}) = g^2 \lambda_1(\mathbf{R})^2$ and $\min(\mathbf{Q}^{-1}) = \lambda_1(\mathbf{R})^2$. Moreover, exactly κ vectors of $\mathbb{Z}^d$ satisfy $\mathbf{x}^\top \mathbf{Q}^{-1} \mathbf{x} = \lambda_1(\mathbf{R})^2$, while none satisfies $\mathbf{x}^\top \mathbf{S} \mathbf{x} < g^2 \lambda_1(\mathbf{R})^2$. Both quantities are $\mathbb{Z}$ -equivalence invariants.

Proof. Apply Lemma 3.4 with $(c_1, c_2) = (g, g+1)$ and with $(c_1, c_2) = (1, g(g+1))$, and read the kissing number from Table 1. Invariance holds because congruence by a unimodular matrix is a bijection of $\mathbb{Z}^d$ preserving the quadratic form. $\square$

Any vector of squared norm below $g^2 \lambda_1(\mathbf{R})^2$ therefore certifies that a form lies in $[\mathbf{Q}^{-1}]$, which gives the following distinguisher.

Algorithm 5 DISTINGUISH($\mathbf{P}, g, \lambda_1(\mathbf{R})$) — solving $\text{ac-}\Delta\text{LIP}^{\mathbf{S}, \mathbf{Q}^{-1}}$

Require: $\mathbf{P} \leftarrow \mathcal{D}_\sigma([\mathbf{S}])$ or $\mathbf{P} \leftarrow \mathcal{D}_\sigma([\mathbf{Q}^{-1}])$, parameters g and $\lambda_1(\mathbf{R})$

Ensure: a guess for the class of $\mathbf{P}$

- 1: $\beta \leftarrow$ smallest block size satisfying (11) with $n = d$, $\|\mathbf{v}\| = \lambda_1(\mathbf{R})$ and $\text{vol}^{1/d} = \sqrt{g(g+1)\lambda_1(\mathbf{R})}$
 - 2: $\mathbf{v} \leftarrow \text{BKZ}_\beta(\mathbf{P})$
 - 3: **if** $\mathbf{v}^\top \mathbf{P} \mathbf{v} < g^2 \lambda_1(\mathbf{R})^2$ **then**
 - 4: **return** $[\mathbf{Q}^{-1}]$
 - 5: **else**
 - 6: **return** $[\mathbf{S}]$
-

The distinguisher depends only on a class invariant and is therefore independent of the key-generation distribution.

Remark 5 (auxiliary forms from [14]). *The auxiliary form need not be built from $\mathbf{R}$ itself. By [14, Lemma 15], the signature scheme can be instantiated with the same $\mathbf{S}$ and the auxiliary form*

$$\mathbf{Q}'^{-1} = \begin{pmatrix} \mathbf{R}' & 0 \\ 0 & g^2(g+1)^2 \mathbf{R}' \end{pmatrix},$$

where $\mathbf{R}'$ is the Gram matrix of a lattice in the genus of $BW_m^{\mathbb{Z}}$ whose first minimum and that of its dual are within a constant factor of the Minkowski bound. Such a lattice exists by [14, Theorem 1], under a mild condition on the genus. The gap (1) of the auxiliary lattice then grows only linearly in the gap of $BW_m^{\mathbb{Z}}$, so that a considerably smaller scaling factor g suffices.

This modification does not restore the security of the scheme. Key recovery is unaffected, because Algorithm 4 never uses the auxiliary form of the scheme. It relies on the fact that the g^2 -hull of $\mathbf{S}$ is $g^2 \mathbf{Q}^{-1}$ with $\mathbf{Q}^{-1} = \text{diag}(\mathbf{R}, g^2(g+1)^2 \mathbf{R})$, which is a property of $\mathbf{S}$ alone. Moreover, Table 3 shows that reducing g does not remove the gap between key recovery and the direct attack. For $g \geq 7$ the cost of key recovery is determined by the two instances of $\text{LIP}^{(\mathbf{R}, \cdot)}$ and equals 124 classical and 112 quantum bits independently of g . For $g = 3$ the splitting step becomes dominant and the cost rises to 139 classical and 126 quantum bits, still far below the 209 classical and 189 quantum bits of the direct attack.

Finally, any key-recovery algorithm immediately yields a distinguisher with essentially the same complexity and one-sided error. Let $\mathcal{A}$ be an algorithm that, for a sample $\mathbf{P} \leftarrow \mathcal{D}_\sigma([\mathbf{S}])$, outputs a matrix $\mathbf{U}' \in \text{Iso}(\mathbf{S}, \mathbf{P})$ with probability ε . Define a distinguisher that runs $\mathcal{A}$ on the input $\mathbf{P}$, verifies whether $\mathbf{U}'^\top \mathbf{S} \mathbf{U}' = \mathbf{P}$, and outputs $[\mathbf{S}]$ if and only if the verification succeeds. The verification requires $\mathcal{O}(d^3)$ operations.

For a sample from $[\mathbf{Q}^{-1}]$, the verification condition can never be satisfied, and hence the distinguisher never outputs $[\mathbf{S}]$, independently of the output or behavior of $\mathcal{A}$. For a sample from $[\mathbf{S}]$, the verification succeeds with probability ε . Consequently, the distinguishing advantage is ε , while the computational cost is that of $\mathcal{A}$ plus an $\mathcal{O}(d^3)$ verification overhead.

Complexity estimate

We estimate the lattice-reduction components of the attack using the core-SVP model. $\text{BKZ-}\beta$ [15, 16] is represented by a polynomial number of SVP calls on projected blocks of dimension β . In the core-SVP model [17], one such call is assigned cost 2^{c_β} , with $c_C = \log_2 \sqrt{3/2} \approx 0.292$ in the classical setting [18] and $c_Q = \log_2 \sqrt{13/9} \approx 0.265$ in the quantum setting [19]. Under the geometric series assumption [20] the root-Hermite factor is

$$\delta_\beta = \left(\frac{\beta}{2\pi e} (\pi\beta)^{1/\beta} \right)^{\frac{1}{2(\beta-1)}}, \quad (9)$$

and $\text{BKZ-}\beta$ returns a vector of norm about $\delta_\beta^n \text{vol}(\mathcal{L})^{1/n}$. A vector of norm below a bound T is therefore obtained once

$$\delta_\beta^n \cdot \text{vol}(\mathcal{L})^{1/n} < T. \quad (10)$$

If the lattice contains an unusually short vector $\mathbf{v}$, the estimate of [17] predicts that it is found once

$$\sqrt{\frac{\beta}{n}} \cdot \|\mathbf{v}\| < \delta_\beta^{2\beta-n-1} \cdot \text{vol}(\mathcal{L})^{1/n}. \quad (11)$$

For the splitting step, condition (10) with $T = g(g+1)\lambda_1(\mathbf{R})$ and $\text{vol}(\mathbf{G})^{1/d} = \sqrt{g(g+1)\lambda_1(\mathbf{R})}$ reads $\delta_\beta^d < \sqrt{g(g+1)\lambda_1(\mathbf{R})}$, whereas (11) is applied to the minimal vectors of $\mathbf{G}$, of norm $\lambda_1(\mathbf{R})$. In each case the block size is the smallest β satisfying the condition, and the corresponding classical and quantum costs are given as $\lfloor c_C \beta \rfloor$ and $\lfloor c_Q \beta \rfloor$ bits.

Applied to $BW_m^{\mathbb{Z}}$ itself these estimates give $\beta = 426$ at $m = 512$, that is 124 classical and 112 quantum bits, and $\beta = 816$ at $m = 1024$, see [10] for details. Note that these models work on random lattices, for which $\lambda_1 \approx \text{gh}$, whereas $BW_m^{\mathbb{Z}}$ is highly structured. Their use for Barnes–Wall lattices is therefore heuristic, as is customary for lattices and the same applies to the estimates below.

We compare three lattice-reduction problems. Recovering $\text{Min}(\mathbf{P})$ directly requires a vector of norm $g\lambda_1(\mathbf{R})$ in dimension d . The splitting step works in the transformed lattice $\mathbf{G} \in [\mathbf{Q}^{-1}]$ of the same dimension and volume, where it suffices either to recover a minimal vector, of norm $\lambda_1(\mathbf{R})$, or to reach the threshold $g(g+1)\lambda_1(\mathbf{R})$. Each of the two resulting instances of $\text{LIP}(\mathbf{R}, \cdot)$ requires the minimal vectors of a form in $[\mathbf{R}]$, of norm $\lambda_1(\mathbf{R})$ in dimension m , and is independent of g . Under the geometric series assumption the latter target is not reached for any $\beta < m$, so the corresponding estimate is an exact SVP computation in dimension m . The parameters and estimates are given in Tables 2 and 3.

Table 2 Parameters at $d = 1024$, $m = 512$ and $\lambda_1(\mathbf{R}) = 16$.

	$g = 3$	$g = 7$	$g = 9$	$g = 43$
$g(g+1)$	12	56	90	1892
$\text{vol}^{1/d} = \sqrt{g(g+1)\lambda_1(\mathbf{R})}$	13.86	29.93	37.95	173.99
$\lambda_1(\Lambda_{\mathbf{S}}) = g\lambda_1(\mathbf{R})$	48	112	144	688
$\lambda_1(\Lambda_{\mathbf{Q}^{-1}}) = \lambda_1(\mathbf{R})$	16	16	16	16
splitting threshold $g(g+1)\lambda_1(\mathbf{R})$	192	896	1440	30272

Table 3 Cost at $d = 1024$ as β and (classical bits / quantum bits) in the core-SVP model. The block size is estimated either by the condition of [17] for recovering an unusually short vector or by the geometric series assumption [20]. For LIP for $\mathbf{R}$ the latter is not met for any $\beta < 512$, so the entry marked * is an exact SVP computation in dimension 512.

step	estimate	dim.	$g = 3$	$g = 7$	$g = 9$	$g = 43$
direct attack on $\mathbf{P}$	[17]	1024	716 (209/189)	739 (215/195)	743 (216/196)	756 (220/200)
distinguishing	[17]	1024	479 (139/126)	377 (110/99)	352 (102/93)	237 (69/62)
splitting	[17]	1024	479 (139/126)	377 (110/99)	352 (102/93)	237 (69/62)
	[20]	1024	737 (215/195)	517 (150/137)	470 (137/124)	282 (82/74)
LIP for $\mathbf{R}$, twice	[17]	512	426 (124/112)	426 (124/112)	426 (124/112)	426 (124/112)
	[20]	512	512* (149/135)	512* (149/135)	512* (149/135)	512* (149/135)
key recovery	[17]		479 (139/126)	426 (124/112)	426 (124/112)	426 (124/112)
	[20]		737 (215/195)	517 (150/137)	512* (149/135)	512* (149/135)

At $d = 1024$ and $g = 43$ the estimated key-recovery cost decreases from 220 to 124 classical bits and from 200 to 112 quantum bits. The dominant component after the hull and block decomposition is the LIP for the Barnes–Wall form $\mathbf{R}$ in dimension m , so the remaining computational problem is determined by the corresponding half-dimensional instance.

The key-recovery estimate becomes independent of g once the block-splitting step is cheaper than the subsequent LIP instances. Under the geometric series assumption [20], the splitting step determines the key-recovery cost for $g = 3$ and $g = 7$, with 215 and 150 classical bits respectively, while for $g \geq 9$ the exact SVP computations for the two Barnes–Wall instances dominate at 149 classical bits. The distinguishing cost depends on g , since the first

minimum of the two classes differ by a factor of g . At $d = 1024$, the heuristic core-SVP estimate is 69 classical bits for $g = 43$ and 110 for $g = 7$.

4 Conclusion

The attack is not specific to Barnes–Wall lattices. It applies to the generic construction $\Lambda_{\mathbf{S}} = g\Lambda \oplus (g+1)\Lambda$ of [1, 14] for any integral lattice Λ with Gram matrix $\mathbf{R}$, provided that one of g and $g+1$, say u , is coprime to $\det \mathbf{R}$. Proposition 3.1 then holds with the modulus $s = u^2$, and the hull again rescales the blocks to $(1, g(g+1))$. The splitting argument of Theorem 3.7 holds for any $\mathbf{R}$ with $\lambda_m(\mathbf{R}) < g(g+1)\lambda_1(\mathbf{R})$, and the direct decomposition of Remark 4 yields a secret key without using the structure of $\text{Aut}(\mathbf{R})$. Key recovery therefore always reduces to two instances of LIP for Λ in half the dimension. For $\Lambda = \mathbb{Z}^m$, where $\det \mathbf{R} = 1$ and $\lambda_m = \lambda_1$, both conditions hold for every g . The remaining instances are then instances of $\mathbb{Z}\text{LIP}$ in dimension $d/2$, for which the heuristic analysis of [2] predicts that BKZ with block size $d/4 + o(d)$ suffices, and for which [21] gives a provable algorithm making polynomially many calls to an SVP oracle in dimension at most $d/4 + 1$. Direct sums of rescaled copies of a single lattice should thus be avoided in LIP-based constructions.

References

- [1] Ducas, L., van Woerden, W.: On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography. In: Dunkelman, O., Dziembowski, S. (eds.) *Advances in Cryptology – EUROCRYPT 2022*, pp. 643–673. Springer, Cham (2022)
- [2] Ducas, L., Postlethwaite, E.W., Pulles, L.N., van Woerden, W.: Hawk: Module LIP makes lattice signatures fast, compact and simple. In: Agrawal, S., Lin, D. (eds.) *Advances in Cryptology – ASIACRYPT 2022*, pp. 65–94. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-22972-5_3
- [3] Castro Biage, G., Zambonin, G., Idalino, T.B., Panario, D., Custodio, R.: A concrete lip-based kem with simple lattices. *IEEE Access* **12**, 16408–16420 (2024) <https://doi.org/10.1109/ACCESS.2024.3358670>
- [4] Ackermann, L., Roux-Langlois, A., Wallet, A.: Public-key encryption from the lattice isomorphism problem. In: *WCC 2024 – The Thirteenth International Workshop on Coding and Cryptography*, Perugia, Italy, pp. 1–11 (2024). <https://inria.hal.science/hal-04924507>
- [5] Branco, P., Malavolta, G., Maradni, Z.: Fully-homomorphic encryption from lattice isomorphism. In: Applebaum, B., Lin, H.R. (eds.) *Theory of Cryptography*, pp. 220–252. Springer, Cham (2026)
- [6] Leporati, A., Rovidia, L., van Woerden, Wessel: Beyond LWE: a Lattice Framework for Homomorphic Encryption. *Cryptology ePrint Archive*, Paper 2025/1171 (2025). <https://eprint.iacr.org/2025/1171>
- [7] Bennett, H., Lai, Z., Stephens-Davidowitz, N.: Advanced cryptography from lattice isomorphism—new constructions of ibe and fhe. In: Heninger, N., Rosulek, M. (eds.) *Advances in Cryptology – CRYPTO 2026*, pp. 446–476. Springer, Cham (2026)
- [8] Jiang, K., Wang, A., Luo, H., Liu, G., Tang, G., Pan, Y., Wang, X.: Re-randomize and extract: A novel commitment construction framework based on group actions. In: Fehr, S., Fouque, P.-A. (eds.) *Advances in Cryptology – EUROCRYPT 2025*, pp. 124–153. Springer, Cham (2025)
- [9] Ducas, L., Gibbons, S.: Hull attacks on the lattice isomorphism problem. In: Boldyreva, A., Kolesnikov, V. (eds.) *Public-Key Cryptography – PKC 2023*, pp. 177–204. Springer, Cham (2023). https://doi.org/10.1007/978-3-031-31368-4_7
- [10] Kuninets, A., Leevik, A., Malygina, E., Melnichuk, E., Nabokov, D.: On the construction of Barnes–Wall lattices and their application in cryptography. *Journal of Computer Virology and Hacking Techniques* **22**(1), 62 (2026) <https://doi.org/10.1007/s11416-026-00646-9>
- [11] Storjohann, A.: Algorithms for matrix canonical forms. PhD thesis, ETH Zürich (2000)

- [12] Dutour Sikirić, M., Haensch, A., Voight, J., van Woerden, W.: A canonical form for positive definite matrices. *The Open Book Series* **4**(1), 179–195 (2020) <https://doi.org/10.2140/obs.2020.4.179>
- [13] Plesken, W., Souvignier, B.: Computing isometries of lattices. *Journal of Symbolic Computation* **24**(3–4), 327–334 (1997) <https://doi.org/10.1006/jsco.1996.0130>
- [14] Woerden, W.: Dense and smooth lattices in any genus. In: Chung, K.-M., Sasaki, Y. (eds.) *Advances in Cryptology – ASIACRYPT 2024*, pp. 386–417. Springer, Singapore (2025)
- [15] Schnorr, C.-P., Euchner, M.: Lattice basis reduction: improved practical algorithms and solving subset sum problems. *Mathematical Programming* **66**, 181–199 (1994) <https://doi.org/10.1007/BF01581144>
- [16] Chen, Y., Nguyen, P.Q.: Bkz 2.0: Better lattice security estimates. In: Lee, D.H., Wang, X. (eds.) *Advances in Cryptology – ASIACRYPT 2011*, pp. 1–20. Springer, Berlin, Heidelberg (2011). https://doi.org/10.1007/978-3-642-25385-0_1
- [17] Alkim, E., Ducas, L., Pöppelmann, T., Schwabe, P.: Post-quantum key exchange — a new hope. In: *25th USENIX Security Symposium*, pp. 327–343 (2016)
- [18] Becker, A., Ducas, L., Gama, N., Laarhoven, T.: New directions in nearest neighbor searching with applications to lattice sieving. In: *Proceedings of the 2016 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pp. 10–24. <https://doi.org/10.1137/1.9781611974331.ch2>
- [19] Laarhoven, T.: Search problems in cryptography: from fingerprinting to lattice sieving. PhD thesis, Eindhoven University of Technology (2015)
- [20] Schnorr, C.P.: Lattice reduction by random sampling and birthday methods. In: Alt, H., Habib, M. (eds.) *STACS 2003*, pp. 145–156. Springer, Berlin, Heidelberg (2003). https://doi.org/10.1007/3-540-36494-3_14
- [21] Ducas, L.: Provable lattice reduction of $\mathbb{Z}^n$ with blocksize $n/2$. *Designs, Codes and Cryptography* **92**, 909–916 (2024) <https://doi.org/10.1007/s10623-023-01320-7>