Exploiting the Symmetry of $\mathbb{Z}^n$: Randomization and the Automorphism Problem

Kaijie Jiang[1], Anyu Wang[1,5,6(✉)], Hengyi Luo[2,3], Guoxiao Liu[4], Yang Yu[1,5,6], and Xiaoyun Wang[1,5,6,7,8]

[1] Institute for Advanced Study, BNRist, Tsinghua University, Beijing, China
jkj21@mails.tsinghua.edu.cn,
{anyuwang,yu-yang,xiaoyunwang}@tsinghua.edu.cn,
[2] Key Laboratory of Mathematics Mechanization, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, China
luohengyi23@mails.ucas.ac.cn
[3] University of Chinese Academy of Sciences, Beijing, China
[4] Institute for Network Sciences and Cyberspace, Tsinghua University, Beijing, China
lgx22@mails.tsinghua.edu.cn
[5] Zhongguancun Laboratory, Beijing, China
[6] National Financial Cryptography Research Center, Beijing, China
[7] Shandong Institute of Blockchain, Jinan, China
[8] Key Laboratory of Cryptologic Technology and Information Security, School of Cyber Science and Technology, Shandong University, Qingdao, China

Abstract. $\mathbb{Z}^n$ is one of the simplest types of lattices, but the computational problems on its rotations, such as $\mathbb{Z}$SVP and $\mathbb{Z}$LIP, have been of great interest in cryptography. Recent advances have been made in building cryptographic primitives based on these problems, as well as in developing new algorithms for solving them. However, the theoretical complexity of $\mathbb{Z}$SVP and $\mathbb{Z}$LIP are still not well understood.

In this work, we study the problems on rotations of $\mathbb{Z}^n$ by exploiting the symmetry property. We introduce a randomization framework that can be roughly viewed as 'applying random automorphisms' to the output of an oracle, without accessing the automorphism group. Using this framework, we obtain new reduction results for rotations of $\mathbb{Z}^n$. First, we present a reduction from $\mathbb{Z}$LIP to $\mathbb{Z}$SCVP. Here $\mathbb{Z}$SCVP is the problem of finding the shortest characteristic vectors, which is a special case of CVP where the target vector is a deep hole of the lattice. Moreover, we prove a reduction from $\mathbb{Z}$SVP to γ-$\mathbb{Z}$SVP for any constant $\gamma = O(1)$ in the same dimension, which implies that $\mathbb{Z}$SVP is as hard as its approximate version for any constant approximation factor. Second, we investigate the problem of finding a nontrivial automorphism for a given lattice, which is called LAP. Specifically, we use the randomization framework to show that $\mathbb{Z}$LAP is as hard as $\mathbb{Z}$LIP. We note that our result can be viewed as a $\mathbb{Z}^n$-analogue of Lenstra and Silverberg's result in [JoC2017], but with a different assumption: they assume the G-lattice structure, while we assume the access to an oracle that outputs a nontrivial automorphism.

Keywords: Lattice automorphism · Randomized reduction · $\mathbb{Z}$LIP · Gradient descent · Characteristic vectors of the unimodular lattice

1 Introduction

Lattices are fundamental mathematical concept that represent discrete additive subgroups of $\mathbb{R}^m$. A lattice is usually defined by a set of n linearly independent basis vectors $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n \in \mathbb{R}^m$, such that any point in the lattice can be expressed as an integer linear combination of the basis vectors. Lattices offer a rich geometric structure that can be used to define various computationally hard problems. Two of the famous problems are the *Shortest Vector Problem* (SVP), which involves finding the shortest non-zero vector in a given lattice, and the *Closest Vector Problem* (CVP), which involves finding the lattice point closest to a given target point. Both of these problems are known to be NP-hard, and their theoretical complexity and solving algorithms have been extensively studied [8,10,1,5]. In recent decades, lattices have played a crucial role in cryptography, with numerous cryptographic schemes being constructed based on the lattice-related computationally hard problems [45].

In addition to SVP and CVP, there are also other important lattice-related problems that have gained considerable attention. One such problem is the *Lattice Isomorphism Problem* (LIP). Two lattices $\mathcal{L}_1$ and $\mathcal{L}_2$ are said to be isomorphic if there exists an orthogonal transformation that maps $\mathcal{L}_1$ to $\mathcal{L}_2$. The LIP is to find such an orthogonal transformation given the lattice bases of $\mathcal{L}_1$ and $\mathcal{L}_2$. Research on the LIP dates back to the 1990s, with the development of algorithms for solving low-dimensional LIP [46]. Then a subsequent work studies the asymptotic complexity of LIP and proves that LIP is at least as hard as the *Graph Isomorphism Problem* (GIP) [50]. In [28], Haviv and Regev propose an $n^{O(n)}$-time algorithm for the general LIP, which remains the fastest known algorithm for solving LIP. There are also works that study LIP from different perspectives. Sikirić et al. [21] demonstrate that with access to an SVP oracle, an LIP instance can be converted to a GIP instance. Although GIP has a quasi-polynomial time algorithm as shown in [7], the worst-case number of shortest vectors may be exponential, which can lead to a potentially exponential-sized graph in [21]. Recently, Ducas and Gibbons have adapted the notion of the hull of a code and showed that it could be used to launch geometric attacks on certain special lattices [17]. Another line of research focuses on constructing cryptographic schemes based on the LIP. The proposed schemes include public-key encryption, signature, key encapsulation mechanism, and identification [9,18,19]. Notably, the security of some of these schemes relies on a special case of the LIP, i.e., the $\mathbb{Z}$LIP.

The $\mathbb{Z}$LIP involves finding an orthogonal transformation that maps $\mathbb{Z}^n$ to $\mathcal{L}$, provided that $\mathcal{L}$ is isomorphic to $\mathbb{Z}^n$. Initially, the $\mathbb{Z}$LIP is studied for cryptanalysis purposes of GGH [26] and NTRUSign [30]. In [25], Gentry and Szydlo extract the secret key of NTRUSign by solving an special form of the $\mathbb{Z}$LIP, i.e., solving a structured $\mathbf{U}$ from its Gram matrix $\mathbf{G} = \mathbf{U}^\top\mathbf{U}$ up to a signed permutation. Then Nguyen and Regev propose an alternative method for GGH by tackling a learning a parallelepiped problem using gradient descent [43]. Additionally, an in-depth analysis of the algorithm proposed by Gentry and Szydlo is provided in [32,33]. For the theoretic complexity of $\mathbb{Z}$LIP, Szydlo [53] provides a reduction from search $\mathbb{Z}$LIP to decision LIP, and results from [31] suggest that $\mathbb{Z}$LIP is in co-NP. On the other hand, solving algorithms and experiments for $\mathbb{Z}$LIP are proposed in [23,11]. Recent progress has also been made in [20], where Ducas provides a reduction from n-dimensional $\mathbb{Z}$LIP to $\frac{n}{2}$-dimensional SVP. Plugging in the fastest known algorithm for SVP from [2], it results in a $2^{n/2}$-time algorithm for $\mathbb{Z}$LIP. In addition, Bennett et al. [9] provide a reduction from $\mathbb{Z}$SVP to $O(1)$-uSVP, which leads a $2^{n/2}$ time algorithm for $\mathbb{Z}$SVP. Due to the well-known reduction from $\mathbb{Z}$LIP to $\mathbb{Z}$SVP, the results of [9] imply a reduction from $\mathbb{Z}$LIP to $O(1)$-uSVP and a $2^{n/2}$-time algorithm for $\mathbb{Z}$LIP.

1.1 Our Results and Techniques

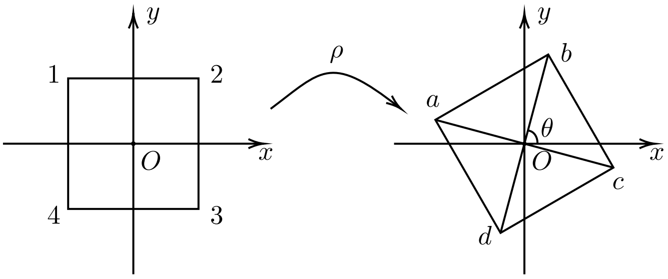
The basis observation of this work is that $\mathbb{Z}^n$ (and its rotations) possesses a remarkable degree of symmetry. For a lattice $\mathcal{L}$ isomorphic to $\mathbb{Z}^n$, the automorphism group $\mathrm{Aut}(\mathcal{L})$ is isomorphic to the signed permutation group $\mathcal{S}_n^{\pm}$ (see Section 2), which is known to be the largest possible for any lattice in $\mathbb{R}^n$ when $n > 10$.[1] Leveraging this powerful property of symmetry, we delve into the $\mathbb{Z}$LIP and focus on two key questions, i.e.,

Q1: Can the symmetry be used to assist in the solving or the reduction of the computational problems associated with $\mathbb{Z}^n$?

Q2: Is it feasible to efficiently obtain a nontrivial automorphism for a lattice isomorphic to $\mathbb{Z}^n$?

Centered on these two questions, we present the following results.

A Randomization Framework. To address the first question, we provide a *randomization framework*, which can be roughly viewed as 'applying random automorphisms' in $\mathrm{Aut}(\mathcal{L})$ to the output of an oracle, without knowing the specific elements in $\mathrm{Aut}(\mathcal{L})$. The framework utilizes the fact the $\mathrm{Aut}(\mathcal{L})$ is a subgroup of the orthogonal group $O_n(\mathbb{R})$, and the latter can be efficiently sampled uniformly at random.[2] The following toy example illustrates how the randomization framework operates.



[1] In fact, the signed permutation group $\mathcal{S}_n^{\pm}$ is the largest possible automorphism group among all lattices in $\mathbb{R}^n$, with the exception of dimensions $n = 2, 4, 6, 7, 8, 9, 10$ [44].

[2] Strictly speaking, we can efficiently generate matrices in $O_n(\mathbb{R})$ distributed with Haar measure. We refer to Section 3 for a detailed discussion.

Denote the square on the left-hand side as $\square_0$, and define $G = \mathbb{R}/(2\pi\mathbb{Z})$. Consider the action of G on $\square_0$ as rotations, i.e., $\rho(\square_0) = \square_\rho, \forall \rho \in G$, where $\square_\rho$ is the rotation of $\square_0$ around the origin O by ρ. In terms of rotations, the automorphism group of $\square_0$ can be expressed as $\mathrm{Aut}(\square_0) = \frac{\pi}{2}\mathbb{Z}_4$, which is a subgroup of $G = \mathbb{R}/(2\pi\mathbb{Z})$. We assume there is an oracle $\mathcal{O}$ that takes as input any $\square_\rho$ and outputs an arbitrary vertex of $\square_\rho$. The oracle does not know the specific rotation ρ and the correspondence of the vertices between $\square_0$ and $\square_\rho$. Next, we show how the randomization framework can obtain random vertices of $\square_0$ without accessing $\mathrm{Aut}(\square_0)$. Specifically, the randomization framework 1) generates a $\rho \in G$ uniformly at random; 2) invokes the oracle $\mathcal{O}$ with input $\rho(\square_0) = \square_\rho$ and obtains an arbitrary vertex of $\square_\rho$; 3) applies ρ^{-1} to the obtained vertex and outputs a vertex of $\square_0$. Using the randomness of ρ, it can be proved that the obtained vertex is uniformly distributed with respect to the action of $\mathrm{Aut}(\square_0)$ (see Appendix A).

The randomization framework for lattices generalizes the above example. Specifically, given a lattice $\mathcal{L}$ and an oracle defined for any rotations of $\mathcal{L}$, the framework randomizes the oracle's output such that the resulting samples follow a distribution that is invariant under the action of $\mathrm{Aut}(\mathcal{L})$. Another challenge should be addressed by the randomization framework is how to 'conceal' the information of the random orthogonal matrix from the oracle's input. This is achieved by using the method introduced in [28,9,19], which samples a basis via a discrete Gaussian distribution.

New Reduction Results for $\mathbb{Z}$LIP. The randomization framework enables us to derive new reduction results for $\mathbb{Z}$LIP or $\mathbb{Z}$SVP.

Theorem 1.1 *There is an efficient randomized reduction from $\mathbb{Z}$LIP to $\mathbb{Z}$SCVP.*

In Theorem 1.1, we introduce a new problem, $\mathbb{Z}$SCVP, which requires finding the shortest characteristic vector of a given lattice $\mathcal{L} \cong \mathbb{Z}^n$. We note that the set of characteristic vectors forms a coset $\mathbf{w} + 2\mathcal{L}$, and a characteristic vector can be efficiently computed for a given basis (see Lemma 2.6). Thus $\mathbb{Z}$SCVP can be viewed as a CVP in the lattice $2\mathcal{L}$. Previous studies on $\mathbb{Z}$LIP mainly focused on reductions to SVP or its variants [9,18,20]. To the best of our knowledge, Theorem 1.1 is the first direct reduction from $\mathbb{Z}$LIP to CVP. Moreover, $\mathbb{Z}$SCVP is a very special case of CVP, where the target vector is a deep hole in the lattice $2\mathcal{L}$. We believe this is a non-trivial observation that could facilitate further research on $\mathbb{Z}$LIP, as finding or verifying a deep hole for a lattice is generally hard [27].

The proof of Theorem 1.1 relies on the fact that $\mathrm{Aut}(\mathcal{L})$ acts transitively on the set of shortest characteristic vectors. This allows us to sample uniformly from this set using the randomization framework. Then we can show that with polynomial many samples, we can efficiently find the shortest vectors of $\mathcal{L}$ by using the gradient descent method adopted in [43].

Theorem 1.2 *For any constant $\gamma = O(1)$, there is an efficient randomized reduction from $\mathbb{Z}SVP$ to γ-$\mathbb{Z}SVP$ in the same dimension.*

Theorem 1.2 shows that $\mathbb{Z}$SVP is as hard as its approximate version for any constant approximation factor. Plugging the best known algorithm for $O(1)$-SVP in [39,6] gives a $2^{0.802n}$-time algorithm for $\mathbb{Z}$SVP. However, γ-$\mathbb{Z}$SVP is a special case of γ-SVP, so a more efficient algorithm for $\mathbb{Z}$SVP might exist if we can exploit its special structure, which can be an open problem for future research.

The proof of Theorem 1.2 relies on an analysis of the orbits of the vectors in $\mathcal{L} \cap \gamma\mathcal{B}_2^n$ under the action of $\mathrm{Aut}(\mathcal{L})$. We show that we can sample uniformly from one orbit using the randomization framework. The shortest vectors can then be obtained by doing pairwise subtraction on a polynomial number of vectors in the same orbit.

The Lattice Automorphism Problem. To answer the second question, we introduce a new problem, $\mathbb{Z}$LAP, which requires finding a nontrivial automorphism in $\mathrm{Aut}(\mathcal{L})$. Our main result is the following reduction.

Theorem 1.3 *There is an efficient randomized reduction from $\mathbb{Z}LIP$ to $\mathbb{Z}LAP$.*

According to Theorem 1.3, it has $\mathbb{Z}\mathrm{LIP} \leq \mathbb{Z}\mathrm{LAP}$. On the other hand, a simple deduction gives $\mathbb{Z}\mathrm{LAP} \leq \mathbb{Z}\mathrm{LIP}$ by using Lemma 2.8. Therefore, we can conclude that $\mathbb{Z}\mathrm{LAP} = \mathbb{Z}\mathrm{LIP}$ with respect to the randomized reduction.

The key idea to prove Theorem 1.3 is still to use the randomization framework to sample automorphisms for a lattice $\mathcal{L} \cong \mathbb{Z}^n$, such that they are uniformly distributed with respect to the conjugate action of $\mathrm{Aut}(\mathcal{L})$. However, the number of conjugacy classes of $\mathrm{Aut}(\mathcal{L})$ is exponential in n, which makes direct application of the randomization framework inefficient. To overcome this, we devise a preprocessing method and a two-level randomization technique, which effectively transform the automorphisms into some specific conjugacy classes, while maintaining the uniformity. Then our problem turns to how to use these random automorphisms to recover the shortest vectors of $\mathcal{L}$. To solve this problem, we consider the distribution of $\langle \mathbf{x}, \phi\mathbf{x} \rangle$ for a random automorphism ϕ uniformly distributed over a conjugacy class and a fixed $\mathbf{x} \in \mathbb{R}^n$. This distribution captures the geometric information of the automorphisms, and we show that the shortest vectors of $\mathcal{L}$ can be recovered from this distribution using the gradient descent method.

Additionally, we can use the hardness of $\mathbb{Z}$LAP to link $\mathbb{Z}$LIP with the hidden subgroup problem (HSP) on $GL_n(\mathbb{Z})$. To see this, let $\mathcal{L}$ be a lattice with a basis $\mathbf{B}$. Then $\mathrm{Aut}(\mathcal{L})$ is isomorphic to the stabilizer group $\mathrm{Stab}(\mathbf{G})$, where $\mathbf{G} = \mathbf{B}^\top \mathbf{B}$. Hence, LAP of $\mathcal{L}$ is equivalent to finding a nontrivial element in $\mathrm{Stab}(\mathbf{G})$ (see Lemma 2.9). Since $\mathrm{Stab}(\mathbf{G})$ is a subgroup of $GL_n(\mathbb{Z})$, we can formulate a corresponding HSP on $GL_n(\mathbb{Z})$. By Theorem 1.3, we eventually obtain the following result. The only previous relation between lattice problems and HSP that we are aware of is due to Regev [47], who shows that HSP on the dihedral group is harder than $\sqrt{n}$-uSVP.

Corollary 1.1 *There exists an efficient randomized reduction from $\mathbb{Z}$LIP to a variant of HSP on $GL_n(\mathbb{Z})$.*

1.2 Related Works

Reduction from $\mathbb{Z}$SVP to Approximate SVP. In [9], Bennet et al. present a reduction from $\mathbb{Z}$SVP to γ-uSVP for any constant $\gamma = O(1)$ using lattice sparsification techniques [34,51]. They also propose a simple projection-based reduction from $\mathbb{Z}$SVP to $\sqrt{2}$-SVP, and suggest that this result may be extended to a more general case. Our result in Theorem 1.2 provides a different perspective on the reduction from $\mathbb{Z}$SVP to approximate SVP, and includes the $\sqrt{2}$-SVP result in [9] as a special case.

Graph Automorphism Problem (GAP). The GAP, which requires to find a generating set of the automorphism group of a given graph,[3] is a well-studied problem that has a close connection to the GIP. It is known that GAP and GIP are computationally equivalent [40]. Our result shows that $\mathbb{Z}$LIP and $\mathbb{Z}$LAP are also equivalent in the sense of randomized reduction. For general lattices, we further prove that LAP $\leq$ LIP (Corollary 4.2), while the reverse direction remains open.

LIP for *G*-Lattices. In [33], Lenstra and Silverberg investigate the isomorphism problem between a G-lattice and $\mathbb{Z}\langle G\rangle = \mathbb{Z}[G]/(u+1)$, where G is a finite abelian group containing an element u of order 2. A G-lattice is defined as a lattice $\mathcal{L}$ equipped with a homomorphism $f : G \to \mathrm{Aut}(\mathcal{L})$ such that $f(u) = -1$. The authors propose a deterministic polynomial time algorithm for solving the isomorphism problem between a G-lattice and $\mathbb{Z}\langle G\rangle$. Our results on LAP can be viewed as a $\mathbb{Z}^n$-analogue of Lenstra and Silverberg's result, but there are two key differences. Firstly, Lenstra and Silverberg's algorithm assumes the G-lattice structure, whereas in our reduction we assume access to an oracle that returns an arbitrary nontrivial automorphism. Secondly, they focus on deterministic algorithms, where we employ a randomization framework that produces randomized reductions.

1.3 Outline

The rest of the paper is organized as follows. Section 2 provides basic definitions and preliminaries. In Section 3, we present the randomization framework and use it to prove Theorem 1.1 and Theorem 1.2, along with some corollaries. In Section 4, we show the proof of Theorem 1.3 and some corollaries. Section 5 concludes the paper.

[3] This differs slightly from our definition of LAP, which only asks to find a nontrivial automorphism. We remark that for $\mathbb{Z}$LAP, finding a nontrivial automorphism and finding a generating set of the automorphism group are equivalent by Theorem 1.3.

2 Preliminary

2.1 Notations

- Matrices and column vectors are denoted by bold letters, such as $\mathbf{A}$ and $\mathbf{a}$. For a matrix $\mathbf{A} = (\mathbf{a}_1, \ldots, \mathbf{a}_n)$ we denote its Gram-Schmidt orthogonalisation by $\tilde{\mathbf{A}} = (\tilde{\mathbf{a}}_1, \ldots, \tilde{\mathbf{a}}_n)$. The Euclidean norm of $\mathbf{a} \in \mathbb{R}^n$ is denoted by $\|\mathbf{a}\|$. The transpose of $\mathbf{A}$ is denoted by $\mathbf{A}^\top$, and $(\mathbf{A}^{-1})^\top$ is abbreviated as $\mathbf{A}^{-\top}$.
- Let $[n] = \{1, 2, \ldots, n\}$ for a positive integer n. The size of a finite set A is denoted by $|A|$. For $a, b \in \mathbb{Z}$, $a \mid b$ means that b is divisible by a.
- Let $GL_n(\mathbb{R})$ and $GL_n(\mathbb{Z})$ be the general linear group of rank n over $\mathbb{R}$ and $\mathbb{Z}$ respectively. We use $O_n(\mathbb{R})$ to represent the group of orthogonal matrices $\mathbf{O} \in GL_n(\mathbb{R})$ such that $\mathbf{O}^\top \mathbf{O} = \mathbf{I}_n$, where $\mathbf{I}_n$ is the identity matrix.
- For a matrix $\mathbf{B} \in GL_n(\mathbb{R})$, we denote $\mathcal{L}(\mathbf{B})$ as the lattice generated by $\mathbf{B}$. We denote the standard basis of $\mathbb{Z}^n$ as $\{\mathbf{e}_i\}_{i \in [n]}$. We use $\mathcal{L}_1 \cong \mathcal{L}_2$ to represent that two lattices $\mathcal{L}_1$ and $\mathcal{L}_2$ are isomorphic.
- We denote the group of permutation matrices of size $n \times n$ as $\mathcal{S}_n$, and denote the group of signed permutation matrices of size $n \times n$ as $\mathcal{S}_n^{\pm}$, where a signed permutation matrix is a type of generalized permutation matrix, where the nonzero entries are ± 1. We use $\mathbf{P}_n$ to represent the permutation matrix $\left(\begin{smallmatrix} 0 & 1 \\ \mathbf{I}_{n-1} & 0 \end{smallmatrix}\right)$. For two groups G and H, we use $H \leq G$ to represent H is a subgroup of G.

2.2 Lattice and Related

A lattice $\mathcal{L}$ of rank n and dimension m is a set of points in $\mathbb{R}^m$ that can be expressed as integer combinations of n linearly independent basis vectors $\mathbf{b}_1, ..., \mathbf{b}_n$. Denote $\mathbf{B} = (\mathbf{b}_1, ..., \mathbf{b}_n)$ as the basis of the lattice $\mathcal{L}$, and then $\mathcal{L} = \{\mathbf{B}\mathbf{z} : \mathbf{z} \in \mathbb{Z}^n\}$. In the rest of this paper, we will consider only full-rank lattices, where $m = n$ and $\mathbf{B} \in GL_n(\mathbb{R})$. The dual lattice of $\mathcal{L}$ is defined as $\mathcal{L}^* \overset{\text{def}}{=} \{\mathbf{u} \in \mathbb{R}^n : \langle \mathbf{u}, \mathbf{v} \rangle \in \mathbb{Z} \text{ for all } \mathbf{v} \in \mathcal{L}\}$, and the dual basis of a lattice basis $\mathbf{B}$ is defined as $\mathbf{B}^* = \mathbf{B}^{-\top}$. Let $\lambda_i(\mathcal{L})$ denote the i-th successive minimum of the lattice $\mathcal{L}$, and let $bl(\mathcal{L})$ denote the minimum value of $\max_{i \in [n]} \|\mathbf{b}_i\|$ taken over all bases of $\mathcal{L}$. It is known that $\lambda_n(\mathcal{L}) \leq bl(\mathcal{L}) \leq \frac{\sqrt{n}}{2} \lambda_n(\mathcal{L})$ [13].

For the lattice $\mathbb{Z}^n$, a bound on the number of integer points contained in a ball of radius r centered at the origin is established in [48].

Lemma 2.1 **([48])** *Suppose r satisfies $1 \leq r \leq \sqrt{n}$ and $r^2 \in \mathbb{Z}$, then it has*

$$\left(2n/r^2\right)^{r^2} \leq |\mathbb{Z}^n \cap r\mathcal{B}_2^n| \leq \left(2e^3 n/r^2\right)^{r^2}, \tag{1}$$

where $\mathcal{B}_2^n$ is the closed Euclidean unit ball. Then for $r = O(1)$, it has $|\mathbb{Z}^n \cap r\mathcal{B}_2^n| \leq n^{O(1)}$.

Lattice Problems. In addition to SVP and CVP, the following approximate lattice problem is also involved in our reduction.

Definition 2.1 (γ-SVP) *Given a basis* $\mathbf{B}$ *of a lattice* $\mathcal{L}$ *as input, the* γ*-SVP is to find a nonzero short vector in* $\mathcal{L}$ *of length at most* $\gamma\lambda_1(\mathcal{L})$*. If* $\mathcal{L} \cong \mathbb{Z}^n$*, we call this problem* γ*-*$\mathbb{Z}$*SVP.*

γ-SVP has been extensively studied in the literature, see, e.g., [39,54,6,3,4]. The lemma below states the best-known result for γ-SVP with $\gamma = O(1)$.

Lemma 2.2 ([39]) *For every constant* $\epsilon > 0$*, there exists a constant* $\gamma = \gamma(\epsilon) \geq 1$ *depending only on* ϵ *such that there is a randomized algorithm that solves* γ*-SVP on lattices of dimension* n *in* $2^{(0.802+\epsilon)n} poly(n)$ *time.*

Gaussian Measure over Lattices. Let $\rho_s(\boldsymbol{y}) = \exp\left(-\pi\|\boldsymbol{y}\|^2/s^2\right), \boldsymbol{y} \in \mathbb{R}^n$, to be the Gaussian function centered at origin with parameter s, then the discrete Gaussian distribution with parameter s on a lattice $\mathcal{L}$ of rank n defined by

$$\mathcal{D}_{\mathcal{L},s}(\boldsymbol{y}) = \rho_s(\boldsymbol{y})/\rho_s(\mathcal{L}), \boldsymbol{y} \in \mathcal{L}. \tag{2}$$

For a set $A \subseteq \mathcal{L}$, we denote $\rho_s(A) = \sum_{\boldsymbol{x}\in A} \rho_s(\boldsymbol{x})$. The following results will be used in our reduction.

Lemma 2.3 ([28]) *Let* $\mathcal{L}$ *be a lattice of dimension* n *with* $det(\mathcal{L}) \geq 1$*. Then for any* $s \geq bl(\mathcal{L})$*, the probability that a set of* $\left(n^2 + n(n + 20\log\log(s\sqrt{n}))\log(s\sqrt{n})\right)$ *vectors chosen independently according to* $\mathcal{D}_{\mathcal{L},s}$ *does not generate* $\mathcal{L}$ *is* $2^{-\Omega(n)}$*.*

In [24], Gentry et al. present an efficient approach that produces a sample distribution that is statistically close to the $\mathcal{D}_{\mathcal{L},s}$ for sufficiently large parameter s. Furthermore, Brakerski et al. provide an algorithm that samples exactly according to $\mathcal{D}_{\mathcal{L},s}$ [12].

Lemma 2.4 ([12]) *Suppose* $\mathcal{L}$ *is a lattice of dimension* n *with a basis* $\mathbf{B}$*. Then there exists an efficient algorithm* **SampleD** *which inputs* $\mathbf{B}$ *and outputs a vector from* $\mathcal{D}_{\mathcal{L},s}$ *for any* $s \geq \sqrt{\ln(2n+4)/\pi} \cdot \max_i \left\|\tilde{\boldsymbol{b}}_i\right\|$*.*

Lemma 2.5 (Chernoff-Hoeffding Bound [29]) *Let* $X_1, \ldots, X_M \in [0,1]$ *be independent and identically distributed random variables. Then for* $s > 0$ *it has*

$$\Pr\left[\left|M \cdot \mathbb{E}\left[X_i\right] - \sum X_i\right| \geq sM\right] \leq 2e^{-Ms^2/10}. \tag{3}$$

2.3 Characteristic Vector of Unimodular Lattices

A lattice $\mathcal{L}$ is said to be unimodular if $\mathcal{L} = \mathcal{L}^*$. Equivalently, the Gram matrix of $\mathbf{B}$ is unimodular, i.e., $\mathbf{B}^\top\mathbf{B} \in GL_n(\mathbb{Z})$, where $\mathbf{B} \in GL_n(\mathbb{R})$ is a basis of $\mathcal{L}$. Clearly, any rotation of $\mathbb{Z}^n$ is unimodular. However, a lattice being unimodular does not necessarily imply that it is isomorphic to $\mathbb{Z}^n$, e.g., the unimodular lattice E_8 is not isomorphic to $\mathbb{Z}^8$.

Definition 2.2 (Characteristic Vector) *Suppose $\mathcal{L}$ is a unimodular lattice. A vector $\mathbf{w} \in \mathcal{L}$ is called a characteristic vector of $\mathcal{L}$ if it has $\langle \mathbf{w}, \mathbf{v} \rangle \equiv \langle \mathbf{v}, \mathbf{v} \rangle \mod 2$ for all $\mathbf{v} \in \mathcal{L}$.*

We denote the set of characteristic vectors as $\chi(\mathcal{L})$. For any unimodular lattice $\mathcal{L}$, the following properties hold for the characteristic vector, and their proofs can be found in [41] and Appendix B.

Lemma 2.6 *Assume $\mathbf{B} = (\mathbf{b}_1, ..., \mathbf{b}_n)$ is a basis of a unimodular lattice $\mathcal{L}$ and $\mathbf{B}^{-\top} = (\mathbf{d}_1, ..., \mathbf{d}_n)$, then it has:*

1) $\mathbf{w} = \sum_{i=1}^{n} \|\mathbf{d}_i\|^2 \mathbf{b}_i$ *is a characteristic vector of $\mathcal{L}$.*
2) $\chi(\mathcal{L}) = \mathbf{w} + 2\mathcal{L}$ *for any characteristic vector $\mathbf{w} \in \chi(\mathcal{L})$.*
3) $\mathbf{w} \in \mathcal{L}$ *is a characteristic vector if and only if $\langle \mathbf{w}, \mathbf{b}_i \rangle \equiv \langle \mathbf{b}_i, \mathbf{b}_i \rangle \mod 2$ for $i \in [n]$.*

Lemma 2.6 indicates that for a given basis $\mathbf{B}$, we can efficiently compute a characteristic vector of $\mathcal{L}$, as well as efficiently verify whether a given vector is a characteristic vector. For a lattice $\mathcal{L}$ that is isomorphic to $\mathbb{Z}^n$, the characteristic vector has the following more particular properties.

Lemma 2.7 *Suppose $\mathcal{L} \cong \mathbb{Z}^n$. Assume $\mathbf{B} = \mathbf{OU}$ is a basis of $\mathcal{L}$, where $\mathbf{O} \in O_n(\mathbb{R})$ and $\mathbf{U} \in GL_n(\mathbb{Z}^n)$. Then it has:*

1) $\chi(\mathcal{L}) = \{\mathbf{Oz} : \mathbf{z} \in \mathbb{Z}^n$ *such that* $\mathbf{z}_i \equiv 1 \mod 2, \forall i \in [n]\}$.
2) *The shortest characteristic vectors are exactly* $\{\mathbf{Oz} : \mathbf{z}_i = \pm 1, \forall i \in [n]\}$.

The problem of finding the shortest characteristic vector plays a crucial role in our reduction. We note that this problem is equivalent to the CVP in the lattice $2\mathcal{L}$, with the target point being any characteristic vector $\mathbf{w} \in \chi(\mathcal{L})$.

Definition 2.3 (Shortest Characteristic Vector Problem (SCVP)) *Given a basis $\mathbf{B} \in GL_n(\mathbb{R})$ of a unimodular lattice $\mathcal{L}$ as input, SCVP is to find a shortest characteristic vector $\mathbf{w} \in \chi(\mathcal{L})$. In particular, if $\mathcal{L} \cong \mathbb{Z}^n$, we call this problem $\mathbb{Z}$SCVP.*

2.4 Lattice Isomorphism and Automorphism

Two n-dimensional lattices $\mathcal{L}_1$ and $\mathcal{L}_2$ are said to be isomorphic if there exists an orthogonal matrix $\mathbf{O} \in \mathcal{O}_n(\mathbb{R})$ such that $\mathcal{L}_2 = \{\mathbf{Ov} : \mathbf{v} \in \mathcal{L}_1\}$. The automorphism group $\mathrm{Aut}(\mathcal{L})$ of an n-dimensional lattice $\mathcal{L}$ consists of all orthogonal matrices that preserve $\mathcal{L}$, i.e.,

$$\mathrm{Aut}(\mathcal{L}) = \{\mathbf{O} \in \mathcal{O}_n(\mathbb{R}) : \mathbf{Ov} \in \mathcal{L} \text{ for all } \mathbf{v} \in \mathcal{L}\}. \tag{4}$$

It is clear that $\mathrm{Aut}(\mathcal{L})$ contains the automorphisms $\pm\mathbf{I}_n$, which are called *trivial automorphisms* of $\mathcal{L}$.

Lemma 2.8 *For any two isomorphic lattices $\mathcal{L}_1$ and $\mathcal{L}_2$, it has:*

1) $\mathrm{Aut}(\mathcal{L}_1) \cong \mathrm{Aut}(\mathcal{L}_2)$. *For any $\mathbf{O} \in \mathcal{O}_n(\mathbb{R})$ such that $\mathcal{L}_2 = \mathbf{O}\mathcal{L}_1$, the map ϕ defined by $\phi(\mathbf{O}_1) = \mathbf{O}\mathbf{O}_1\mathbf{O}^{-1}, \forall \mathbf{O}_1 \in \mathrm{Aut}(\mathcal{L}_1)$, is an isomorphism from $\mathrm{Aut}(\mathcal{L}_1)$ to $\mathrm{Aut}(\mathcal{L}_2)$.*
2) *There is a one-to-one correspondence between $\mathrm{Aut}(\mathcal{L}_1)$ and the set all isomorphisms between $\mathcal{L}_1$ and $\mathcal{L}_2$. For any $\mathbf{O} \in \mathcal{O}_n(\mathbb{R})$ such that $\mathcal{L}_2 = \mathbf{O}\mathcal{L}_1$, the map ψ defined by $\psi(\mathbf{O}_1) = \mathbf{O}\mathbf{O}_1, \forall \mathbf{O}_1 \in \mathrm{Aut}(\mathcal{L}_1)$, is a bijection between $\mathrm{Aut}(\mathcal{L}_1)$ and the isomorphisms from $\mathcal{L}_1$ to $\mathcal{L}_2$.*

For a lattice $\mathcal{L}$ with a basis $\mathbf{B}$, $\mathrm{Aut}(\mathcal{L})$ is closely related to the stabilizer of $\mathbf{G} = \mathbf{B}^\top\mathbf{B}$. Particularly, for a positive definite $n \times n$ matrix $\mathbf{G}$, the stabilizer of $\mathbf{G}$ is a finite group defined by $\mathrm{Stab}(\mathbf{G}) = \{\mathbf{U} \in \mathrm{GL}_n(\mathbb{Z}) : \mathbf{U}^\top\mathbf{G}\mathbf{U} = \mathbf{G}\}$.

Lemma 2.9 *Let $\mathcal{L}$ be a lattice with a basis $\mathbf{B}$. Then it has $\mathrm{Stab}(\mathbf{B}^\top\mathbf{B}) \cong \mathrm{Aut}(\mathcal{L})$, and the map ϕ defined by $\phi(\mathbf{U}) = \mathbf{B}\mathbf{U}\mathbf{B}^{-1}, \forall \mathbf{U} \in \mathrm{Stab}(\mathbf{B}^\top\mathbf{B})$, is an isomorphism from $\mathrm{Stab}(\mathbf{B}^\top\mathbf{B})$ to $\mathrm{Aut}(\mathcal{L})$.*

Proof. For any $\mathbf{U} \in \mathrm{Stab}(\mathbf{B}^\top\mathbf{B})$, it has $(\phi(\mathbf{U}))^\top(\phi(\mathbf{U})) = \mathbf{B}^{-\top}\mathbf{U}^\top(\mathbf{B}^\top\mathbf{B})\mathbf{U}\mathbf{B}^{-1} = \mathbf{I}_n$ and $\phi(\mathbf{U})\mathbf{B} = \mathbf{B}\mathbf{U}$. Thus it has $\phi(\mathbf{U}) \in \mathrm{Aut}(\mathcal{L})$. On the other hand, for any $\mathbf{O} \in \mathrm{Aut}(\mathcal{L})$, there exists a $\mathbf{U}' \in \mathrm{GL}_n(\mathbb{Z})$ such that $\mathbf{O}\mathbf{B} = \mathbf{B}\mathbf{U}'$. Thus $\mathbf{B}^{-1}\mathbf{O}\mathbf{B} \in \mathrm{GL}_n(\mathbb{Z})$ and it can be easily verified that $\phi^{-1}(\mathbf{O}) \in \mathrm{Stab}(\mathbf{B}^\top\mathbf{B})$. Besides, it is clear that ϕ defines a homomorphism, which completes the proof. □

A natural problem related to lattice automorphism is how to find a nontrivial automorphism for a given lattice $\mathcal{L}$, which is defined as follows.

Definition 2.4 (Lattice Automorphism Problem (LAP)) *Given a basis $\mathbf{B}$ of a lattice $\mathcal{L}$, such that $\mathrm{Aut}(\mathcal{L}) \neq \{\pm\mathbf{I}_n\}$. The LAP is to find an automorphism $\mathbf{O} \in \mathrm{Aut}(\mathcal{L})$ such that $\mathbf{O} \neq \pm\mathbf{I}_n$. In particular, If $\mathcal{L} \cong \mathbb{Z}^n$, we call this problem $\mathbb{Z}$LAP.*

Automorphisms of Rotations of $\mathbb{Z}^n$. It is known that $\mathrm{Aut}(\mathbb{Z}^n) = \mathcal{S}_n^{\pm}$. Then for any $\mathcal{L} \cong \mathbb{Z}^n$, it has $\mathrm{Aut}(\mathcal{L}) \cong \mathcal{S}_n^{\pm}$. Specifically, from Lemma 2.8 it has $\mathrm{Aut}(\mathcal{L}) = \mathbf{O}\mathcal{S}_n^{\pm}\mathbf{O}^{-1}$ for any isomorphism $\mathbf{O}$ such that $\mathcal{L} = \mathbf{O}\mathbb{Z}^n$. Besides, suppose $\mathbf{w} \in \chi(\mathcal{L})$ is a shortest characteristic vector of $\mathcal{L}$, then the set of shortest characteristic vectors of $\mathcal{L}$ can be expressed as $\{\mathbf{O}\mathbf{w} : \mathbf{O} \in \mathrm{Aut}(\mathcal{L})\}$.

Besides, it is worth noting that finding a shortest vector of $\mathcal{L} \cong \mathbb{Z}^n$ directly yields a non-trivial automorphism of $\mathcal{L}$. Assume that we have a shortest vector $\mathbf{v} \in \mathcal{L}$. Let $\mathcal{L}' = \pi_{\mathrm{span}(\mathbf{v})^\perp}(\mathcal{L}) \cong \mathbb{Z}^{n-1}$, then $\mathcal{L} = \mathbf{v}\mathbb{Z} \oplus \mathcal{L}'$. From this, we can easily construct an $\mathbf{O} \in O_n(\mathbb{R})$ such that $\mathbf{O}\mathbf{v} = -\mathbf{v}$ and $\mathbf{O}\mathbf{x} = \mathbf{x}$ for all $\mathbf{x} \in \mathcal{L}'$. Thus $\mathbf{O} \in \mathrm{Aut}(\mathcal{L})$ and $\mathbf{O} \neq \pm\mathbf{I}_n$.

3 Randomized Reduction Framework for Rotations of $\mathbb{Z}^n$

This section demonstrates how the randomization framework can be used to obtain specific reductions for rotations in $\mathbb{Z}^n$. In Section 3.1, we explain the randomization framework and discuss how it can be used to get a reduction from $\mathbb{Z}$LIP to $\mathbb{Z}$SCVP. Then we prove the reduction from $\mathbb{Z}$SVP to γ-$\mathbb{Z}$SVP in Section 3.2. Additionally, Section 3.3 presents some other interesting results that can be obtained using the randomization framework.

3.1 A Reduction from $\mathbb{Z}$LIP to $\mathbb{Z}$SCVP

Suppose that $\mathcal{L} \cong \mathbb{Z}^n$ and $\mathbf{B}$ is a basis of $\mathcal{L}$. Given a $\mathbb{Z}$SCVP oracle $\mathcal{O}$, which takes a lattice basis $\mathbf{B}$ as input and returns a shortest characteristic vector in $\chi(\mathcal{L})$. We first show that the randomization framework enables us to sample uniformly and independently from the set of shortest characteristic vectors of $\mathcal{L}$. We then prove that, with a polynomial number of such samples, we can effectively recover the shortest vectors in $\mathcal{L}$ and thus solve the $\mathbb{Z}$LIP.

The Randomization Step. To begin with, we establish the following lemma, which states we can efficiently sample a basis according to some distribution, such that the distribution is invariant under the action of $\mathrm{Aut}(\mathcal{L})$ on the input. The primary technique used in this lemma is to sample a basis via a discrete Gaussian distribution over $\mathcal{L}$, which has been commonly utilized in existing lattice literature. e.g., [14,28,9,19].

Lemma 3.1 *There is an efficient algorithm that takes as input a basis* $\mathbf{B}$ *for a lattice* $\mathcal{L}$ *and outputs a basis according to a distribution* $\mathcal{A}(\mathbf{B})$*, such that the distribution* $\mathcal{A}(\mathbf{B})$ *is identical to* $\mathcal{A}(\mathbf{OB})$ *for any* $\mathbf{O} \in \mathit{Aut}(\mathcal{L})$*.*

Proof. We assume that $\det(\mathcal{L}) = 1$. If this is not the case, we can consider $\mathcal{L}/\det(\mathcal{L})^{\frac{1}{n}}$ instead of $\mathcal{L}$. To start with, we apply LLL algorithm to $\mathbf{B}$ and obtain a reduced basis $\mathbf{B}' = [\mathbf{b}'_1, \dots, \mathbf{b}'_n]$ of $\mathcal{L}$ such that $\|\mathbf{b}'_i\| \leq 2^{n/2}$. Then using Lemma 2.4, we can efficiently sample $p(n)$ vectors $\mathbf{v}_1, \dots, \mathbf{v}_{p(n)}$ according $\mathcal{D}_{\mathcal{L},s}$, where $s = 2^n$ and $p(n)$ is the number of vectors required in Lemma 2.3. We note that the vectors $\mathbf{v}_1, \dots, \mathbf{v}_{p(n)}$ generate $\mathcal{L}$ with overwhelming probability by Lemma 2.3. Finally, we run LLL algorithm on $\mathbf{v}_1, \dots, \mathbf{v}_{p(n)}$ to get a basis $\mathbf{B}_1$ of $\mathcal{L}$ and output it. Observe that applying $\mathrm{Aut}(\mathcal{L})$ to the input basis has no effect on the distribution $\mathcal{D}_{\mathcal{L},s}$, and thus has no effect on the output distribution $\mathcal{A}(\mathbf{B})$. □

An intuitive explanation of Lemma 3.1 is that the input basis is 'concealed' within the output basis. This is a crucial point in our randomization framework.

Proposition 3.1 (Randomization) *Given a $\mathbb{Z}$SCVP oracle* $\mathcal{O}$*, which takes a lattice basis* $\tilde{\mathbf{B}}$ *as input, subject to the condition that* $\mathcal{L}(\tilde{\mathbf{B}}) \cong \mathbb{Z}^n$*, and returns a shortest characteristic vector in* $\chi(\mathcal{L}(\tilde{\mathbf{B}}))$*. Then for a lattice* $\mathcal{L} \cong \mathbb{Z}^n$*, we can sample uniformly and independently from the set of shortest characteristic vectors of* $\mathcal{L}$*.*

Proof. Let $\mathbf{B}$ be a basis of the lattice $\mathcal{L}$. To start with, we sample an orthogonal matrix $\mathbf{O}_1$ from $O_n(\mathbb{R})$ uniformly at random. Here the term "uniform" refers to the *Haar measure*, which ensures that the distribution of the matrix remains unchanged when multiplied by any orthogonal matrix [15]. Please refer to the discussion following this proof for the sampling method. Using Lemma 3.1 we can obtain a basis $\mathbf{B}_1 \leftarrow \mathcal{A}(\mathbf{O_1 B})$ of the lattice $\mathcal{L}_1 = \mathbf{O}_1\mathcal{L}$. Then we call the $\mathbb{Z}$SCVP oracle $\mathcal{O}$, taking $\mathbf{B}_1$ as input to obtain a shortest characteristic vector $\mathbf{w}_1 \in \chi(\mathcal{L}_1)$. Finally, we compute $\mathbf{O}_1^{-1}\mathbf{w}_1 \in \chi(\mathcal{L})$.

We claim that $\mathbf{O}_1^{-1}\mathbf{w}_1$ is uniformly distributed in the set of shortest characteristic vectors of $\mathcal{L}$. In other words, the probability

$$\Pr_{\mathbf{O}_1 \leftarrow O_n(\mathbb{R}); \mathbf{B}_1 \leftarrow \mathcal{A}(\mathbf{O}_1\mathbf{B})}[\mathbf{O}_1^{-1}\mathcal{O}(\mathbf{B}_1) = \mathbf{w}] \tag{5}$$

is identical for any shortest characteristic vector $\mathbf{w} \in \chi(\mathcal{L})$. Note that the set of shortest characteristic vectors of $\mathcal{L}$ can be written as $\{\mathbf{Ow} : \mathbf{O} \in \mathrm{Aut}(\mathcal{L})\}$. Then it suffices to show that $\Pr[\mathbf{O}_1^{-1}\mathcal{O}(\mathbf{B}_1) = \mathbf{w}] = \Pr[\mathbf{O}_1^{-1}\mathcal{O}(\mathbf{B}_1) = \mathbf{Ow}]$ for any $\mathbf{O} \in \mathrm{Aut}(\mathcal{L})$. Note that

$$\begin{aligned}
&\Pr_{\mathbf{O}_1 \leftarrow O_n(\mathbb{R}); \mathbf{B}_1 \leftarrow \mathcal{A}(\mathbf{O}_1\mathbf{B})}[\mathbf{O}_1^{-1}\mathcal{O}(\mathbf{B}_1) = \mathbf{Ow}] \\
=\ &\Pr_{\mathbf{O}_1 \leftarrow O_n(\mathbb{R}); \mathbf{B}_1 \leftarrow \mathcal{A}(\mathbf{O}_1\mathbf{B})}[(\mathbf{O}_1\mathbf{O})^{-1}\mathcal{O}(\mathbf{B}_1) = \mathbf{w}] \\
=\ &\Pr_{(\mathbf{O}_1\mathbf{O}) \leftarrow O_n(\mathbb{R}); \mathbf{B}_1 \leftarrow \mathcal{A}(\mathbf{O}_1\mathbf{B})}[(\mathbf{O}_1\mathbf{O})^{-1}\mathcal{O}(\mathbf{B}_1) = \mathbf{w}] \\
=\ &\Pr_{(\mathbf{O}_1\mathbf{O}) \leftarrow O_n(\mathbb{R}); \mathbf{B}_1 \leftarrow \mathcal{A}(\mathbf{O}_1\mathbf{OB})}[(\mathbf{O}_1\mathbf{O})^{-1}\mathcal{O}(\mathbf{B}_1) = \mathbf{w}] \\
=\ &\Pr_{\mathbf{O}_1 \leftarrow O_n(\mathbb{R}); \mathbf{B}_1 \leftarrow \mathcal{A}(\mathbf{O}_1\mathbf{B})}[\mathbf{O}_1^{-1}\mathcal{O}(\mathbf{B}_1) = \mathbf{w}].
\end{aligned}$$

The second equality follows from the property of Haar measure. The third equality can be deduced from the fact that $\mathbf{O}_1\mathbf{OB} = (\mathbf{O}_1\mathbf{OO}_1^{-1})\mathbf{O}_1\mathbf{B}$ and $\mathbf{O}_1\mathbf{OO}_1^{-1} \in \mathrm{Aut}(\mathcal{L}_1)$ using Lemma 3.1. The last equality is simply a substitution of the variable. Thus $\mathbf{O}_1^{-1}\mathbf{w}_1$ is uniformly distributed in the set of shortest characteristic vectors of $\mathcal{L}$.

To establish the independence of $\mathbf{O}_1^{-1}\mathbf{w}_1$ for each trial, we can consider the joint distribution by leveraging the above method and taking into account that the choice of $\mathbf{O}_1$ is independent. The detailed proof is in Appendix C. □

To carry out the randomization framework, it is necessary to generate a uniformly distributed random orthogonal matrix, i.e., with respect to the Haar measure. Random orthogonal matrices are important in various fields, such as multivariate analysis, directional statistics, and physical systems modeling. There have been numerous studies on efficiently generating random orthogonal matrices. One method is to perform a QR decomposition on a matrix whose entries are independently drawn from a standard normal distribution, with the resulting orthogonal matrix distributed according to the Haar measure [42]. Another approach involves constructing a Householder reflection from a uniformly distributed unit vector of dimension n, and then applying it to an $(n-1) \times (n-1)$ uniformly distributed orthogonal matrix [16,52].

Remark 1. It appears that we need to tackle the precision issue in our approach because matrices over $\mathbb{R}$ are involved. Precision is a subtle issue for LIP because orthogonal matrices often involve irrational numbers that cannot be represented exactly. This issue has been explored in the literature on lattices, such as [28,9]. In our paper, we follow their approach of ignoring the precision issue and focus on the core aspects of reduction. We note that the precision issue is not a critical concern in our reduction. As demonstrated in the recovery step, it is possible to efficiently reconstruct the shortest vectors from their approximations. Furthermore, the connection between the automorphism group and the stabilizer group, as described in Lemma 2.9, allows us to transform our reductions using the Gram matrix (as adopted in [18,19,21]). For a detailed discussion, please see Appendix D.

The Recovery Step. In this step, we demonstrate how to recover the shortest vectors in $\mathcal{L}$ from a polynomial number of shortest characteristic vectors in $\chi(\mathcal{L})$ obtained in the previous step. Essentially, our task is to solve the following problem.

Problem 3.1 *Given a basis* $\mathbf{B}$ *of a lattice* $\mathcal{L} \cong \mathbb{Z}^n$*, and* $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_{poly(n)} \in \chi(\mathcal{L})$ *that are drawn uniformly and independently from the set of shortest characteristic vectors of* $\mathcal{L}$*. The goal is to find the shortest vectors of* $\mathcal{L}$*.*

Suppose that $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is a set of n linearly independent shortest vectors of $\mathcal{L}$, and denote $\mathbf{O} = (\mathbf{v}_1, \ldots, \mathbf{v}_n) \in O_n(\mathbb{R})$. Then by Lemma 2.7, the set of shortest characteristic vectors of $\mathcal{L}$ can be expressed as $\{z_1\mathbf{v}_1 + \cdots + z_n\mathbf{v}_n : z_i = \pm 1, \forall i \in [n]\}$. Define the function

$$M_k(\mathbf{x}) = \mathbb{E}[\langle \mathbf{w}, \mathbf{x} \rangle^k], x \in \mathbb{R}^n, \tag{6}$$

where $k \in \mathbb{Z}^+$, and $\mathbf{w}$ is uniformly distributed over the set of shortest characteristic vectors of $\mathcal{L}$. From Chernoff-Hoeffding bound, we can effectively approximate $M_k(\mathbf{x})$ by making use of a polynomials number of shortest characteristic vector as provided in Problem 3.1. As the set of shortest characteristic vectors is symmetric around the origin, it has $M_k(\mathbf{x}) = 0$ for any odd k. On the other hand, a straightforward calculation shows that

$$M_4(\mathbf{x}) = 3\left\|\mathbf{x}\right\|^4 - 2\sum_{i=1}^{n} \langle \mathbf{v}_i, \mathbf{x} \rangle^4 \tag{7}$$

Next, we focus on the $\mathbf{x}$ that is on the unit sphere and define

$$f(\mathbf{x}) = -\frac{1}{2}(M_4(\mathbf{x}) - 3) = \sum_{i=1}^{n} \langle \mathbf{v}_i, \mathbf{x} \rangle^4. \tag{8}$$

Then the following lemma is clear.

Lemma 3.2 *The global maximum of* $f(\mathbf{x})$ *over the unit sphere is attained at* $\{\pm\mathbf{v}_1, \ldots, \pm\mathbf{v}_n\}$*, which is exactly the set of shortest vectors of* $\mathcal{L}$*.*

Lemma 3.2 allows us to convert Problem 3.1 into the problem of maximizing $f(\mathbf{x})$ over the unit sphere. One widely-used approach to solve this problem is via gradient descent as that adopted in [43]. Taking into account the approximation error of $M_k(x)$, we present Algorithm 1 as a solution to Problem 3.1, as well as an analysis of the algorithm in Proposition 3.2.

Algorithm 1: Solve Problem 3.1 via Gradient Descent.

```
Require: A polynomial number of samples uniformly distributed over the shortest
    characteristic vectors of a lattice $\mathcal{L} \cong \mathbb{Z}^n$
Ensure: An approximation a shortest vector of $\mathcal{L}$
 1: Choose $\mathbf{x}$ uniformly at random from the unit sphere of $\mathbb{R}^n$
 2: Compute an approximation of the gradient $\nabla f(\mathbf{x})$
 3: $\mathbf{x}_{new} \leftarrow \nabla f(\mathbf{x})$
 4: $\mathbf{x}_{new} \leftarrow \mathbf{x}_{new} / \|\mathbf{x}_{new}\|$
 5: Compute the approximations of $f(\mathbf{x}_{new})$ and $f(\mathbf{x})$
 6: if $f(\mathbf{x}_{new}) \leq f(\mathbf{x})$ then
 7:     return $\mathbf{x}$
 8: else
 9:     Replace $\mathbf{x}$ by $\mathbf{x}_{new}$ and go to step 2
10: end if
```

In step 2 of Algorithm 1, we need to approximate the gradient $\nabla f(x)$, which can be done via two methods. The first method involves using the equations $\nabla M_4(\mathbf{x}) = \mathbb{E}[\nabla(\langle \mathbf{w}, \mathbf{x}\rangle^4)] = 4\mathbb{E}[\langle \mathbf{w}, \mathbf{x}\rangle^3 \mathbf{w}]$, and $\nabla f(\mathbf{x}) = -\frac{1}{2}(\nabla M_4(\mathbf{x}) - 12\mathbf{x})$. Alternatively, the second method involves approximating $f(\mathbf{x}+t\mathbf{y}) = \sum_{i=1}^{n} \langle \mathbf{v}_i, \mathbf{x}+t\mathbf{y}\rangle^4$ for $0 \leq t \leq 4$, and then computing $\sum_{i=1}^{n} \langle \mathbf{v}_i, \mathbf{x}\rangle^k \langle \mathbf{v}_i, \mathbf{y}\rangle^{4-k}, 0 \leq k \leq 4$, using linear algebra. Specifically, by setting $k = 3$, we get $\sum_{i=1}^{n} \langle \mathbf{v}_i, \mathbf{x}\rangle^3 \langle \mathbf{v}_i, \mathbf{y}\rangle = \langle \sum_{i=1}^{n} \langle \mathbf{v}_i, \mathbf{x}\rangle^3 \mathbf{v}_i, \mathbf{y}\rangle$, and by letting $\mathbf{y}$ run over the standard basis $\mathbf{e}_i$, $i \in [n]$, we can obtain an approximation of $\nabla f(\mathbf{x}) = 4\sum_{i=1}^{n} \langle \mathbf{v}_i, \mathbf{x}\rangle^3 \mathbf{v}_i$.

Proposition 3.2 *Suppose that $\mathcal{L} \cong \mathbb{Z}^n$. For any $c_0 > 0$, there exists a constant $c_1 > 0$ such that Algorithm 1 inputs n^{c_1} samples that are independently and uniformly distributed over the shortest characteristic vectors of $\mathcal{L}$, and outputs a vector $\mathbf{x}$ such that $\|\mathbf{x} - \mathbf{v}\| \leq n^{-c_0}$ for some shortest vector $\mathbf{v} \in \mathcal{L}$, with $O(\log\log n)$ descent steps and a constant probability. Moreover, $O(n \log n)$ calls to Algorithm 1 will find all shortest vectors of $\mathcal{L}$ with an overwhelming probability.*

Proof. We start by ignoring the approximation error and analyzing Algorithm 1. In this proof, we use the coordinate representation of vectors under the orthogonal basis $\{\mathbf{v}_i\}_{1\leq i\leq n}$, i.e., $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n$, where $x_i = \langle \mathbf{x}, \mathbf{v}_i\rangle$. Then by

$$\nabla f(\mathbf{x}) = 4\sum_{i=1}^{n} \langle \mathbf{v}_i, \mathbf{x}\rangle^3 \mathbf{v}_i, \tag{9}$$

we can deduce that a single iteration transforms the the vector $\mathbf{x} = (x_1, \ldots, x_n)$ into $\alpha \cdot (x_1^3, \ldots, x_n^3)$ for some normalization factor α. Thus after r iterations, a vector $(x_1, \ldots, x_n)$ becomes a vector $\alpha \cdot (x_1^{3^r}, \ldots, x_n^{3^r})$ for some normalization factor α. We note that the original vector $(x_1, \ldots, x_n)$ is uniformly sampled from the unit sphere. It can be proved that with some constant probability, there exits a $k \in [n]$ such that $|x_k| \geq (1 + \Omega(1/\log n))|x_i|, \forall i \neq k$ [43]. For such a vector, $r = O(\log\log n)$ iterations are enough to increase this gap to more than $n^{\log n}$, which means that we have one coordinate very close to ±1, and all others are at most $n^{-\log n}$ in absolute value.

Next, we take into account the approximation error. By Chernoff-Hoeffding bound, for any $c > 0$, there exits a c_1 such that with overwhelming probability all gradients in $r < poly(n)$ iterations have errors at most n^{-c} in the Euclidean norm. In one iteration, let $\mathbf{x} = (x_1, \ldots, x_n)$ be such that $|x_k| \geq (1 + \Omega(1/\log n))|x_i|, \forall i \neq k$. Then clearly $|x_k| > n^{-1/2}$ since $\|\mathbf{x}\| = 1$. Let $(y_1, \ldots, y_n) = \nabla f(\mathbf{x})$ and hence $|y_k| = 4|x_k|^3 > n^{-2}$.

Let $(\tilde{y}_1, \ldots, \tilde{y}_n)$ be an approximation of $\nabla f(\mathbf{x})$. By our assumption on the approximation $\nabla f(\mathbf{x})$, for each i, we have $|\tilde{y}_i - y_i| \leq n^{-c}$. Then, for any $i \neq k$, we have

$$\frac{|\tilde{y}_k|}{|\tilde{y}_i|} \geq \frac{|y_k| - n^{-c}}{|y_i| + n^{-c}} \geq \frac{|y_k|\left(1 - n^{-(c-2)}\right)}{|y_i| + n^{-c}}. \tag{10}$$

Hence, if $|y_i| > n^{-(c-1)}$, then $\frac{|\tilde{y}_k|}{|\tilde{y}_i|}$ is at least $(1 - O(1/n))(x_k/x_i)^3$. Otherwise, $\frac{|\tilde{y}_k|}{|\tilde{y}_i|}$ is at least $\Omega(n^{c-3})$. After $r = O(\log\log n)$ steps, the gap x_k/x_i becomes $\Omega(n^{c-3})$. Therefore, for any $c_0 > 0$, we can choose c appropriately such that the Euclidean distance between the output vector and one of $\pm\mathbf{v}_i$'s is less than n^{-c_0}.

Finally, from the Coupon Collector's problem, $O(n\log n)$ calls to Algorithm 1 will find all shortest vectors of $\mathcal{L}$ with overwhelming probability. □

Given approximations of the shortest vectors of $\mathcal{L}$ as in Proposition 3.1, there is an effective way to recover the exact shortest vectors $\{\mathbf{v}_i\}_{1\leq i\leq n}$ from its approximations $\{\tilde{\mathbf{v}}_i\}_{1\leq i\leq n}$ using a set of n linearly independent shortest characteristic vectors. Specifically, let $\mathbf{W} = \{\mathbf{w}_1, \ldots, \mathbf{w}_n\}$ be a set of n linearly independent shortest characteristic vectors, where $\mathbf{w}_i = z_{i1}\mathbf{v}_1 + \ldots + z_{in}\mathbf{v}_n$ and $z_{ij} = \pm 1$, and suppose $\tilde{\mathbf{v}}_i = \mathbf{v}_i + \boldsymbol{\epsilon}_i$ such that $\|\boldsymbol{\epsilon}_i\| \leq n^{-c}$. Observe that $\langle \mathbf{w}_i, \tilde{\mathbf{v}}_j\rangle = z_{ij} + \sum_{l=1}^{n} z_{il}\langle \mathbf{v}_l, \boldsymbol{\epsilon}_j\rangle$, and $\langle \mathbf{v}_l, \boldsymbol{\epsilon}_j\rangle \leq \|\mathbf{v}_l\| \cdot \|\boldsymbol{\epsilon}_j\| \leq n^{-c}$. It follows that $|\langle \mathbf{w}_i, \tilde{\mathbf{v}}_j\rangle - z_{ij}| \leq n^{-(c-1)} < \frac{1}{2}$ for $c > 2, n > 2$. Thus z_{ij} can be recovered by just taking $\text{sign}(\langle \mathbf{w}_i, \tilde{\mathbf{v}}_j\rangle)$, and $\{\mathbf{v}_i\}_{1\leq i\leq n}$ can be exactly recovered consequently.

Proof of the Reduction. By combining the above two steps, we can conclude the following reduction.

Theorem 3.1 *There is an efficient randomized reduction from $\mathbb{Z}$LIP to $\mathbb{Z}$SCVP.*

Proof. The theorem is a direct result of Proposition 3.1 and Proposition 3.2. □

For a unimodular lattice $\mathcal{L}$, it has $\chi(\mathcal{L}) = \mathbf{w} + 2\mathcal{L}$ for any characteristic vector $\mathbf{w} \in \chi(\mathcal{L})$ according to Lemma 2.6. Therefore, SCVP can be considered as a CVP in the lattice $2\mathcal{L}$, with the target vector being $\mathbf{w}$. Furthermore, for

$\mathcal{L} \cong \mathbb{Z}^n$, the $\mathbb{Z}$SCVP is a very special case of CVP. Lemma 2.6 tells us the target $\mathbf{w}$ is completely dependent on the given basis and Lemma 2.7 tells us that the distance between $\mathbf{w}$ and $2\mathcal{L}$ is $\sqrt{n}$, and the deep holes of $2\mathcal{L}$ are exactly $\chi(\mathcal{L})$. Therefore, the $\mathbb{Z}$SCVP can be viewed as a CVP in the lattice $2\mathcal{L}$, with a deep hole as the target vector. We believe this is a non-trivial observation that could aid in further study of $\mathbb{Z}$LIP, as it is known that calculating or verifying a deep hole for a lattice is a difficult problem in general [27].

3.2 A Reduction from $\mathbb{Z}$SVP to γ-$\mathbb{Z}$SVP

The randomization framework can be readily adapted to other oracles for rotations of $\mathbb{Z}^n$. In this subsection, we explore the approximate $\mathbb{Z}$SVP and establish the following reduction.

Theorem 3.2 *There is an efficient randomized reduction from $\mathbb{Z}$SVP to γ-$\mathbb{Z}$SVP for any constant $\gamma = O(1)$.*

Proof. Suppose that $\mathcal{L} \cong \mathbb{Z}^n$. Denote $A = \mathcal{L} \cap \gamma\mathcal{B}_2^n$, then by Lemma 2.1 it has $|A| = |\mathbb{Z}^n \cap \gamma\mathcal{B}_2^n| \leq n^c$ for some constant c. Consider the action of $\mathrm{Aut}(\mathcal{L})$ on A. Write $A = \cup_{\mathbf{v}\in\bar{A}} A_{\mathbf{v}}$ to be the disjoint union of distinct orbits, where $A_{\mathbf{v}} = \{\mathbf{Ov} : \mathbf{O} \in \mathrm{Aut}(\mathcal{L})\}$ and $\bar{A}$ is a set of representative vectors with respect to the action of $\mathrm{Aut}(\mathcal{L})$ on A.

Using the randomization framework, we can invoke the γ-$\mathbb{Z}$SVP oracle $m = poly(n)$ times, with $m > n^c$, yielding a vector set $X = \{\mathbf{x}_1, \ldots, \mathbf{x}_m\} \subseteq A$. Then through a deduction similar to Proposition 3.1, it can be shown that, if $X \cap A_{\mathbf{v}}$ is nonempty, the vectors in $X \cap A_{\mathbf{v}}$ are independently and uniformly distributed over $A_{\mathbf{v}}$. Since $m > n^c \geq |\bar{A}|$, there must exist two $\mathbf{x}_i$ and $\mathbf{x}_j$ fall in a same orbit $A_{\mathbf{v}}$. We claim that the probability that $\mathbf{x}_i - \mathbf{x}_j$ is a multiple of a shortest vector of $\mathcal{L}$, (i.e., $\frac{\mathbf{x}_i - \mathbf{x}_j}{\|\mathbf{x}_i - \mathbf{x}_j\|}$ is a shortest vector), is at least $1/|A_{\mathbf{v}}| \geq 1/n^c$. To prove the claim, suppose that $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are n linearly independent shortest vectors of $\mathcal{L}$, and write $\mathbf{x}_i = x_{i,1}\mathbf{v}_1 + \cdots + x_{i,n}\mathbf{v}_n$. Without loss of generality, we assume $x_{i,1} \neq 0$. It is evident that $x_{i,1}(-\mathbf{v}_1) + x_{i,2}\mathbf{v}_2 + \cdots + x_{i,n}\mathbf{v}_n \in A_{\mathbf{v}}$. Moreover, with probability $1/|A_{\mathbf{v}}|$, it has $\mathbf{x}_j = x_{i,1}(-\mathbf{v}_1) + x_{i,2}\mathbf{v}_2 + \cdots + x_{i,n}\mathbf{v}_n$ for a randomly chosen $\mathbf{x}_j$ from $A_{\mathbf{v}}$. Thus $\mathbf{x}_i - \mathbf{x}_j = 2x_{i,1}\mathbf{v}_1$, which is a multiple of the shortest vector $\mathbf{v}_1$.

Then we compute $\mathbf{x}_i - \mathbf{x}_j$ for all $i, j \in [m]$, and check if it is a multiple of a shortest vector. This step requires at most m^2 checks. Finally, repeating the whole process $O(n^{c+1})$ times, we can get a shortest vector in $\mathcal{L}$ with an overwhelming probability. □

Using the fastest known algorithm for $O(1)$-SVP as stated in Lemma 2.2, we can obtain a $2^{0.802n}$-time algorithm for the $\mathbb{Z}$SVP. It is worth noting that γ-$\mathbb{Z}$SVP is a special case of γ-SVP, so there is potential for a better algorithm for the $\mathbb{Z}$SVP problem if we can develop a more specialized algorithm for γ-$\mathbb{Z}$SVP. However, further research is needed to establish such an algorithm.

The approach used in Theorem 3.2 can be extended to handle general values of γ, but the resulting reduction may not have a guaranteed polynomial-time complexity. Specifically, denote $\ell(\gamma, n) = |\bar{A}|$ and $\xi(\gamma, n) = \max_{\mathbf{v}\in\bar{A}} |A_{\mathbf{v}}|$. Let $T_{\mathbb{Z}\mathrm{SVP}}(\gamma, n)$ be the run time of an algorithm for γ-ℤSVP on lattices of dimension n.

Corollary 3.1 *There is a randomized algorithm that solves ℤSVP on lattices of dimension n in $\xi(\gamma, n) \cdot (\ell(\gamma, n) \cdot T_{\mathbb{Z}SVP}(\gamma, n) + \ell(\gamma, n)^2) \cdot poly(n)$ time.*

3.3 Other Corollaries from the Randomization Framework

Another advantage of the randomization framework is the suitability for using fixed-dimensional oracles, which makes it useful for fixed-dimensional reduction. As a simple example, we demonstrate how to use the randomization framework to establish a reduction from ℤLIP to ℤSVP for a fixed dimension in the following corollary. Note that without the fixed dimension restriction, a reduction from ℤLIP to ℤSVP can be established by employing the projecting method [9]. Specifically, suppose that $\mathcal{L} \cong \mathbb{Z}^n$. We call an n-dimensional ℤSVP oracle to obtain a shortest vector $\mathbf{v}_1 \in \mathcal{L}$, from which we can efficiently obtain a basis for the $(n-1)$-dimensional sublattice $\mathcal{L}_1 \subseteq \mathcal{L}$ that is orthogonal to $\mathbf{v}_1$. Then we call an $(n-1)$-dimensional ℤSVP oracle to obtain a shortest vector in $\mathcal{L}_1$, and then we recursively find n linearly independent shortest vectors of $\mathcal{L}$.

Corollary 3.2 *There is an efficient randomized reduction from ℤLIP to ℤSVP in the same dimension.*

Proof. Suppose that $\mathcal{L} \cong \mathbb{Z}^n$. Note that $\mathrm{Aut}(\mathcal{L})$ acts transitively on the set of shortest vectors of $\mathcal{L}$. By invoking the ℤSVP oracle with the randomization framework, we can obtain vectors that are independently and uniformly distributed over the set of shortest vectors of $\mathcal{L}$. Then we just need to sample $O(n \log n)$ shortest vectors to get a set of linearly independent ones, e.g., $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$. This gives the matrix $\mathbf{O} = (\mathbf{v}_1, \ldots, \mathbf{v}_n) \in O_n(\mathbb{R})$ which is an isomorphism from $\mathcal{L}$ to $\mathbb{Z}^n$. □

It is worth noting that, like Corollary 3.1, the reductions in Theorem 3.1 and Theorem 3.2 can also be modified to fixed-dimensional reductions. Another simple application of the randomization framework is demonstrated by the following result.

Corollary 3.3 *In the sense of randomized reduction, the $(n-1)$-dimensional ℤSVP is easier than the n-dimensional ℤSVP.*

Proof. Suppose that $\mathcal{L} \cong \mathbb{Z}^{n-1}$. We first embed $\mathcal{L}$ into an n-dimensional lattice $\mathcal{L}_1 \cong \mathbb{Z}^n$ by adding $\mathbf{e}_n$ to the basis of $\mathcal{L}$. Then we invoke the n-dimensional ℤSVP oracle using the randomization framework to obtain vectors that are independently and uniformly distributed over the set of shortest vectors of $\mathcal{L}_1$. The probability of such a vector falling into $\mathcal{L}$ is $1 - \frac{1}{n}$. By invoking the n-dimensional ℤSVP oracle $O(\log n)$ times, we can obtain a shortest vector in $\mathcal{L}(\mathbf{B})$ with an overwhelming probability. □

4 A Reduction from ℤLIP to ℤLAP

This section focuses on the ℤLAP, which involves finding a nontrivial automorphism in $\mathrm{Aut}(\mathcal{L})$ for a given lattice $\mathcal{L} \cong \mathbb{Z}^n$ (Definition 2.4). Although the effect of 'applying random automorphisms' to the output of an oracle can be achieved via the randomization framework, the ℤLAP still seems difficult. In fact, we can prove that the ℤLAP is as hard as ℤLIP. Note that ℤLAP $\leq$ ℤLIP follows directly from Lemma 2.8. Therefore, in this section, we focus on the reduction from ℤLIP to ℤLAP, which is achieved in two steps. The first step shows how to efficiently sample automorphisms independently and uniformly from a special conjugacy class by invoking the ℤLAP oracle using the randomization framework (Section 4.1). The second step demonstrates how to use these automorphisms to recover the shortest vectors (Section 4.2). Besides, in Section 4.3 we introduce other results related to ℤLAP.

4.1 Random Sample from a Conjugacy Class

To begin with, we give a brief introduction to the conjugation of the automorphism group $\mathrm{Aut}(\mathcal{L})$ for any lattice $\mathcal{L} \cong \mathbb{Z}^n$. For convenience, lowercase Greek letters such as ϕ are used to represent automorphisms in $\mathrm{Aut}(\mathcal{L})$ throughout this section. In $\mathrm{Aut}(\mathcal{L})$, two automorphisms ϕ_1 and ϕ_2 are conjugate if there exists an automorphism $\phi \in \mathrm{Aut}(\mathcal{L})$ such that $\phi_1 = \phi\phi_2\phi^{-1}$, which is denoted by $\phi_1 \sim \phi_2$. Conjugation is an equivalence relation that divides $\mathrm{Aut}(\mathcal{L})$ into disjoint conjugacy classes, which are denoted by $\mathfrak{C}_\phi = \{\phi_1 \in \mathrm{Aut}(\mathcal{L}) : \phi_1 \sim \phi\}$. For two lattices $\mathcal{L}_1 \cong \mathcal{L}_2$, from Lemma 2.8 it has $\mathrm{Aut}(\mathcal{L}_1) \cong \mathrm{Aut}(\mathcal{L}_2)$. This implies that the isomorphisms between $\mathcal{L}_1$ and $\mathcal{L}_2$ induce a canonical bijection between the conjugacy classes of $\mathcal{L}_1$ and those of $\mathcal{L}_2$, i.e., $\tau : \mathfrak{C}_\phi \to \mathfrak{C}_{\mathbf{O}\phi\mathbf{O}^{-1}}$ for any $\phi \in \mathrm{Aut}(\mathcal{L}_1)$ and any $\mathbf{O} \in O_n(\mathbb{R})$ such that $\mathcal{L}_2 = \mathbf{O}\mathcal{L}_1$. Thus by an abuse of notation, we also use $\phi_1 \sim \phi_2$ to represent $\tau(\mathfrak{C}_{\phi_1}) = \mathfrak{C}_{\phi_2}$ for any $\phi_1 \in \mathrm{Aut}(\mathcal{L}_1)$ and $\phi_2 \in \mathrm{Aut}(\mathcal{L}_2)$.

For the lattice $\mathbb{Z}^n$, it has $\mathrm{Aut}(\mathbb{Z}^n) = S_n^{\pm}$ and we are particularly interested in the conjugacy classes defined by the following types of matrices in $S_n^{\pm}$.

- $\mathbf{T}_{i,j,k} = \mathrm{diag}\{\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), \dots, \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), -\mathbf{I}_i, \mathbf{I}_j\}$, where there are k $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$'s on the diagonal such that $2k + i + j = n$ and $i, j < n$.
- $\mathbf{T}_{p,k} = \mathrm{diag}\{\mathbf{P}_p, \dots, \mathbf{P}_p, \mathbf{I}_{n-pk}\}$, where there are k $\mathbf{P}_p$'s on the diagonal and $p > 2$ is an odd prime number. We remind that $\mathbf{P}_p = \left(\begin{smallmatrix} 0 & 1 \\ \mathbf{I}_{p-1} & 0 \end{smallmatrix}\right)$.
- $\mathbf{T}_n = \mathrm{diag}\{\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right), \dots, \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\}$, where n is even.

The aim of this subsection is to prove the following statement, which claims that we can efficiently sample automorphisms from one conjugacy class.

Proposition 4.1 *Assume that n is odd and the lattice $\mathcal{L} \cong \mathbb{Z}^n$. Given a ℤLAP oracle $\mathcal{O}$ for dimension n. Then there exists i, j, k such that we efficiently obtain $poly(n)$ samples $\phi_1, \phi_2, \dots, \phi_{poly(n)} \in Aut(\mathcal{L})$ that are independently and uniformly distributed over the conjugacy class $\{\phi \in Aut(\mathcal{L}) | \, \phi \sim \mathbf{T}_{i,j,k}\}$.*

The main approach for proving the proposition is still utilizing the randomization framework to generate samples uniformly distributed over each conjugacy class. However, due to the total number of conjugacy classes being exponential in n, we can not effectively sample from one class as that in Theorem 3.2. To address this, we modify the randomization procedure by preprocessing the outputs of the oracle to ensure that the resulting automorphisms belong to one of the conjugacy classes corresponding to $\mathbf{T}_{i,j,k}$, $\mathbf{T}_{p,k}$ or $\mathbf{T}_n$. The number of these types of conjugacy classes is a polynomial of n, allowing for efficient sampling from one conjugacy class.

Preprocessing and Randomization. Firstly, we give an efficient preprocessing algorithm that transforms the output of the oracle into specific conjugacy classes.

Lemma 4.1 (Preprocessing) *Suppose that $\mathcal{L} \cong \mathbb{Z}^n$. Then there exists an efficient algorithm $\mathcal{P}$ that takes a nontrivial automorphism $\phi \in Aut(\mathcal{L})$ as input and returns an automorphism $\mathcal{P}(\phi) \in Aut(\mathcal{L})$ falling into one of the conjugacy classes corresponding to $\mathbf{T}_{i,j,k}$, $\mathbf{T}_{p,k}$, or $\mathbf{T}_n$. Additionally, it can be efficiently identified which conjugacy class $\mathcal{P}(\phi)$ belongs to.*

Proof. The algorithm begins by computing $\mathrm{ord}(\phi) := \min\{i \in \mathbb{Z}^+ : \phi^i = \mathbf{I}_n\}$. It is clear that $\mathrm{ord}(\phi) \mid |S_n^{\pm}|$. We note that $\mathrm{ord}(\phi)$ can be computed in a polynomial time of n, which is proved in Lemma 4.2. In the following, the algorithm processes ϕ according to its order.

(1) $\mathrm{ord}(\phi)$ is odd. Let p be the smallest odd prime factor of $\mathrm{ord}(\phi)$.[4] Then the algorithm outputs $\mathcal{P}(\phi) = \phi^{\mathrm{ord}(\phi)/p}$. It can be deduced that $\mathcal{P}(\phi) \sim \mathbf{T}_{p,k}$, where $k = (n-d)/(p-1)$ and d is the dimension of the eigenspace associated with the eigenvalue 1 of $\mathcal{P}(\phi)$. The proof is given in Lemma 4.3.

(2) $\mathrm{ord}(\phi)$ is even and $\phi^{\mathrm{ord}(\phi)/2} = -\mathbf{I}_n$. If $4 \nmid \mathrm{ord}(\phi)$, it can be deduced that $\mathrm{ord}(-\phi) = \mathrm{ord}(\phi)/2$ is odd. Thus, we can preprocess ϕ by multiplying it with $-\mathbf{I}_n$, which transforms it into the case of (1). If $4 \mid \mathrm{ord}(\phi)$, then the algorithm outputs $\mathcal{P}(\phi) = \phi^{\mathrm{ord}(\phi)/4}$, and it can be deduced that $\mathcal{P}(\phi) \sim \mathbf{T}_n$. The proof is given in Lemma 4.3.

(3) $\mathrm{ord}(\phi)$ is even and $\phi^{\mathrm{ord}(\phi)/2} \neq -\mathbf{I}_n$. The algorithm outputs $\mathcal{P}(\phi) = \phi^{\mathrm{ord}(\phi)/2}$. Let V_1 be the eigenspace associated with the eigenvalue 1 of $\mathcal{P}(\phi)$, and let d be the dimension of V_1. Define $\mathcal{L}_1 = V_1 \cap \mathcal{L}$. It can be deduced that $\mathcal{P}(\phi) \sim \mathbf{T}_{n-d-k,d-k,k}$, where $k = \log_2(\det(\mathcal{L}_1)^2)$. The proof is given in Lemma 4.3. □

Lemma 4.2 *Suppose that $\mathcal{L} \cong \mathbb{Z}^n$. Then there is an efficient algorithm that takes any $\phi \in \mathrm{Aut}(\mathcal{L})$ as input and computes $\mathrm{ord}(\phi)$.*

Proof. Suppose that $\lambda_\phi(x) \in \mathbb{Z}[x]$ is the characteristic polynomial of ϕ. Then $\lambda_\phi(x)$ can be factorized into the product of integer irreducible polynomials using

[4] Note that $\mathrm{ord}(\phi) \mid |S_n^{\pm}|$, then each prime divisor of $\mathrm{ord}(\phi)$ is no more than n. Therefore p can be computed efficiently.

LLL algorithm [38]. Since the eigenvalues of ϕ are roots of unity, it follows that these irreducible polynomials are cyclotomic polynomials of degrees no more than n. Next, we turn to determine the order of these cyclotomic polynomials. For a cyclotomic polynomial $\Phi_m(x)$ of order m, its degree is the Euler's totient function $\varphi(m)$. It is known that $\varphi(m) \geq \sqrt{m/2}$, then the orders of these cyclotomic polynomials are no more than $2n^2$, and thus can be efficiently determined. Finally, $\mathrm{ord}(\phi)$ is computed by just taking the least common multiple of the orders of these cyclotomic polynomials. □

Lemma 4.3 *Suppose that $\psi \in S_n^{\pm}$. Let V_1 be the eigenspace associated with the eigenvalue 1 of ψ, $d = dim(V_1)$, and let $\mathcal{L}_1 = V_1 \cap \mathbb{Z}^n$. Then*

- *If $ord(\psi) = p$ for a odd prime p, it has $\psi \sim \mathbf{T}_{p,k}$, where $k = (n-d)/(p-1)$.*
- *If $ord(\psi) = 4$ and $\psi^2 = -\mathbf{I}_n$, it has $\psi \sim \mathbf{T}_n$.*
- *If $ord(\psi) = 2$ and $\psi \neq -\mathbf{I}_n$, it has $\psi \sim \mathbf{T}_{n-d-k,d-k,k}$ for $det(\mathcal{L}_1) > 1$, where $k = \log_2(det(\mathcal{L}_1)^2)$.*

Proof. As ψ is a signed permutation, we focus on the action of ψ on the set of vectors $E = \{\pm\mathbf{e}_1, \ldots, \pm\mathbf{e}_n\}$.

If $\mathrm{ord}(\psi) = p$ for a odd prime p. For any $\mathbf{e}_i \in E$, it has either $\psi\mathbf{e}_i = \mathbf{e}_i$ or the vectors $\mathbf{e}_i, \psi\mathbf{e}_i, \ldots, \psi^{p-1}\mathbf{e}_i \in E$ are linearly independent. Thus $\psi \sim \mathbf{T}_{p,k}$. It follows that $d = \dim(V_1) = k + (n - pk)$, i.e., $k = (n-d)/(p-1)$.

If $\mathrm{ord}(\psi) = 4$ and $\psi^2 = -\mathbf{I}_n$. For any $\mathbf{e}_i \in E$, there is a $\mathbf{v} \in E$ such that $\mathbf{v} \neq \pm\mathbf{e}_i$ and $\psi\mathbf{e}_i = \mathbf{v}, \psi\mathbf{v} = -\mathbf{e}_i$. It follows that $\psi \sim \mathbf{T}_n$.

If $\mathrm{ord}(\psi) = 2$ and $\psi \neq -\mathbf{I}_n$. Then the vectors in E can be divided into three categories. The first catergry consists of the $\mathbf{v} \in E$ such that $\psi\mathbf{v} = \mathbf{v}$, and the second catergry consists of the $\mathbf{v} \in E$ such that $\psi\mathbf{v} = -\mathbf{v}$. The third catergry contains all $\mathbf{u}, \mathbf{v} \in E$ such that $\mathbf{u} \neq \mathbf{v}$, $\psi\mathbf{u} = \mathbf{v}$ and $\psi\mathbf{v} = \mathbf{u}$. It follows that $\psi \sim \mathbf{T}_{i,j,k}$. Since $\psi \neq \pm\mathbf{I}_n$, it has $i, j < n$. Moreover, observe that for $\mathbf{T}_{i,j,k}$, a basis of V_1 is $\{\mathbf{e}_1+\mathbf{e}_2, \mathbf{e}_3+\mathbf{e}_4, \ldots, \mathbf{e}_{2k-1}+\mathbf{e}_{2k}\} \cup \{\mathbf{e}_{n-j+1}, \ldots, \mathbf{e}_n\}$. Thus $d = k+j$ and $\det(\mathcal{L}_1) = 2^{\frac{k}{2}}$, which implies that $k = \log_2(\det(\mathcal{L}_1)^2)$, $i = n-d-k$ and $j = d-k$. □

Next, we integrate the randomization framework (Proposition 3.1) and the preprocessing technique (Lemma 4.1) to establish the following proposition.

Lemma 4.4 (Randomization) *Given a $\mathbb{Z}$LAP oracle $\mathcal{O}$, which takes a lattice basis $\tilde{\mathbf{B}}$ as input, subject to the condition that $\mathcal{L}(\tilde{\mathbf{B}}) \cong \mathbb{Z}^n$, and returns a nontrivial automorphism in $\mathrm{Aut}(\mathcal{L}(\tilde{\mathbf{B}}))$. Then for a lattice $\mathcal{L} \cong \mathbb{Z}^n$, we can efficiently sample automorphisms in $\mathrm{Aut}(\mathcal{L})$ such that they are uniformly and independently distributed in each of the conjugacy classes corresponding to $\mathbf{T}_{i,j,k}$, $\mathbf{T}_{p,k}$, or $\mathbf{T}_n$.*

Proof. Let $\mathbf{B}$ be a basis of $\mathcal{L}$. Similar to Proposition 3.1, we sample an orthogonal matrix $\mathbf{O}_1$ from $O_n(\mathbb{R})$ uniformly at random, and obtain a basis $\mathbf{B}_1 \leftarrow \mathcal{A}(\mathbf{O_1B})$ of the lattice $\mathcal{L}_1 = \mathbf{O}_1\mathcal{L}$. Then we call the $\mathbb{Z}$LAP oracle, taking $\mathbf{B}_1$ as input to obtain a nontrivial automorphism $\phi_1 \in \mathrm{Aut}(\mathcal{L}_1)$. Applying the preprocessing technique in Lemma 4.1 to ϕ_1, we obtain an automorphism $\psi_1 \in \mathrm{Aut}(\mathcal{L}_1)$ in one of the conjugacy classes corresponding to $\mathbf{T}_{i,j,k}$, $\mathbf{T}_{p,k}$, or $\mathbf{T}_n$. Finally, we compute $\mathbf{O}_1^{-1}\psi_1\mathbf{O}_1 \in \mathrm{Aut}(\mathcal{L})$.

Next we prove that for any conjugacy class $\mathfrak{C}_{\phi_0}, \phi_0 \in \mathrm{Aut}(\mathcal{L})$, the probability

$$\Pr_{\mathbf{O}_1 \leftarrow O_n(\mathbb{R}); \mathbf{B}_1 \leftarrow \mathcal{A}(\mathbf{O}_1\mathbf{B})}[\mathbf{O}_1^{-1}\psi_1\mathbf{O}_1 = \phi] \tag{11}$$

is identical for each $\phi \in \mathfrak{C}_{\phi_0}$. Note that for each $\phi' \in \mathrm{Aut}(\mathcal{L})$, it has

$$\begin{aligned}
&\Pr_{\mathbf{O}_1 \leftarrow O_n(\mathbb{R}); \mathbf{B}_1 \leftarrow \mathcal{A}(\mathbf{O}_1\mathbf{B})}[\mathbf{O}_1^{-1}\psi_1\mathbf{O}_1 = \phi'\phi\phi'^{-1}] \\
&= \Pr_{(\mathbf{O}_1\phi') \leftarrow O_n(\mathbb{R}); \mathbf{B}_1 \leftarrow \mathcal{A}(\mathbf{O}_1\mathbf{B})}[(\mathbf{O}_1\phi')^{-1}\psi_1(\mathbf{O}_1\phi') = \phi] \\
&= \Pr_{\mathbf{O}_1 \leftarrow O_n(\mathbb{R}); \mathbf{B}_1 \leftarrow \mathcal{A}(\mathbf{O}_1\mathbf{B})}[\mathbf{O}_1^{-1}\psi_1\mathbf{O}_1 = \phi].
\end{aligned}$$

Moreover, it is clear that $\mathbf{O}_1^{-1}\psi_1\mathbf{O}_1$ is in one of the conjugacy classes corresponding to $\mathbf{T}_{i,j,k}$, $\mathbf{T}_{p,k}$, or $\mathbf{T}_n$, which proves the uniformity. The independence of each trial follows from the same reason as in Proposition 3.1. □

Conversion to a Special Conjugacy Class. Observe that the total number of conjugacy classes corresponding to $\mathbf{T}_{i,j,k}$, $\mathbf{T}_{p,k}$ and $\mathbf{T}_n$ is $O(n^2)$. Then by Lemma 4.1 and Lemma 4.4, we can efficiently sample $poly(n)$ automorphisms in $\mathrm{Aut}(\mathcal{L})$ such that they are independently and uniformly distributed in a conjugacy class corresponding to one of the $\mathbf{T}_{i,j,k}$, $\mathbf{T}_{p,k}$ and $\mathbf{T}_n$. In order to ease the analysis of the shortest vector recovery, we further introduce a technique that transforms the automorphisms into a conjugacy class that corresponds to $\mathbf{T}_{i,j,k}$. For the sake of simplicity, we will focus on the case where n is odd, which excludes $\mathbf{T}_n$. To begin with, we establish the following lemma.

Lemma 4.5 *Assume that n is odd and $\mathcal{L} \cong \mathbb{Z}^n$. Let $\phi \in \mathrm{Aut}(\mathcal{L})$ be an automorphism such that $\phi \sim \mathbf{T}_{p,k}$, and let ϕ_1 be an automorphism that is uniformly distributed over $\mathfrak{C}_\phi$. Then the probability that $2 \mid \mathrm{ord}(\phi_1\phi)$ and $(\phi_1\phi)^{\mathrm{ord}(\phi_1\phi)/2} \neq -\mathbf{I}_n$ is at least $1/n^4$.*

Proof. Suppose $\mathbf{O} \in O_n(\mathbb{R})$ is an isomorphism from $\mathbb{Z}^n$ to $\mathcal{L}$ such that $\phi = \mathbf{O}\mathbf{T}_{p,k}\mathbf{O}^{-1}$. Then we can express ϕ_1 as $\mathbf{O}\mathbf{S}\mathbf{T}_{p,k}\mathbf{S}^{-1}\mathbf{O}^{-1}$, where $\mathbf{S}$ is uniformly distributed over $S_n^{\pm}$. Therefore $\phi_1\phi = \mathbf{O}\mathbf{S}\mathbf{T}_{p,k}\mathbf{S}^{-1}\mathbf{T}_{p,k}\mathbf{O}^{-1}$. In the following, we analyze the probability that $\mathbf{S}\mathbf{T}_{p,k}\mathbf{S}^{-1}\mathbf{T}_{p,k}$ contains a 2-cycle. There are two cases.

(1) $p > 3$ or $k \geq 2$. In this case there exist four distinct integers $i_1, i_2, i_3, i_4 \in [n]$ such that $\mathbf{T}_{p,k}\mathbf{e}_{i_1} = \mathbf{e}_{i_2}$ and $\mathbf{T}_{p,k}\mathbf{e}_{i_3} = \mathbf{e}_{i_4}$. We are interested in the probability that $\mathbf{S}\mathbf{T}_{p,k}\mathbf{S}^{-1}\mathbf{T}_{p,k}\mathbf{e}_{i_1} = \mathbf{e}_{i_3}$ and $\mathbf{S}\mathbf{T}_{p,k}\mathbf{S}^{-1}\mathbf{T}_{p,k}\mathbf{e}_{i_3} = \mathbf{e}_{i_1}$, i.e., (i_1, i_3) is a 2-cycle with respect to the action of $\mathbf{S}\mathbf{T}_{p,k}\mathbf{S}^{-1}\mathbf{T}_{p,k}$. Note that the above conditions can be written as $\mathbf{T}_{p,k}(\mathbf{S}^{-1}\mathbf{e}_{i_2}) = \mathbf{S}^{-1}\mathbf{e}_{i_3}$ and $\mathbf{T}_{p,k}(\mathbf{S}^{-1}\mathbf{e}_{i_4}) = \mathbf{S}^{-1}\mathbf{e}_{i_1}$. Since $\mathbf{S}$ is uniformly distributed over $S_n^{\pm}$, it can be deduced that the probability is as least $\frac{1}{4} \cdot \frac{kp(kp-3)}{n^4} \geq \frac{1}{n^4}$.

(2) $p = 3, k = 1$. In this case we are interested on the probability that $(1, 2)$ is a 2-cycle with respect to the action of $\mathbf{S}\mathbf{T}_{p,k}\mathbf{S}^{-1}\mathbf{T}_{p,k}$, i.e., $\mathbf{S}\mathbf{T}_{p,k}\mathbf{S}^{-1}\mathbf{T}_{p,k}\mathbf{e}_1 = \mathbf{e}_2$ and $\mathbf{S}\mathbf{T}_{p,k}\mathbf{S}^{-1}\mathbf{T}_{p,k}\mathbf{e}_2 = \mathbf{e}_1$. The conditions can be written as $\mathbf{T}_{p,k}(\mathbf{S}^{-1}\mathbf{e}_2) =$

$\mathbf{S}^{-1}\mathbf{e}_2$ and $\mathbf{T}_{p,k}(\mathbf{S}^{-1}\mathbf{e}_3) = \mathbf{S}^{-1}\mathbf{e}_1$. It can be deduced that the probability is at least $\frac{n-pk}{n} \cdot \frac{1}{2} \cdot \frac{pk}{n^2} > \frac{1}{n^4}$.

Observe that $\mathbf{S}\mathbf{T}_{p,k}\mathbf{S}^{-1}\mathbf{T}_{p,k}$ contains a 2-cycle implies that $2 \mid \mathrm{ord}(\phi_1\phi)$ and $(\phi_1\phi)^{\mathrm{ord}(\phi_1\phi)/2} \neq -\mathbf{I}_n$. Therefore we can conclude the lemma. □

In the rest of this subsection, we give the proof of Proposition 4.1. Particularly, we present a two-level randomization technique for generating automorphisms that are uniformly and independently distributed over a conjugacy class associated with $\mathbf{T}_{i,j,k}$.

Proof of Proposition 4.1. To begin with, we randomly select $\mathbf{O}_1 \in O_n(\mathbb{R})$ and create the lattice $\mathcal{L}_1 = \mathbf{O}_1\mathcal{L}$ (first-level randomization). Using Lemma 4.4, we can efficiently obtain $poly(n)$ samples in $\phi_1, \dots, \phi_{poly(n)} \in \mathrm{Aut}(\mathcal{L}_1)$ that are uniformly and independently distributed in one of the conjugacy classes corresponding to $\mathbf{T}_{i,j,k}$ or $\mathbf{T}_{p,k}$ (second-level randomization). Note that we exclude $\mathbf{T}_n$ since n is odd. There are two cases.

(1) These $poly(n)$ samples are in a conjugacy class corresponding to $\mathbf{T}_{i,j,k}$. We just apply $\mathbf{O}_1^{-1}\phi_i\mathbf{O}_1$ and obtain $poly(n)$ samples in $\mathrm{Aut}(\mathcal{L})$.

(2) These $poly(n)$ samples are in a conjugacy class corresponding to $\mathbf{T}_{p,k}$. Using Lemma 4.5, we can show that, with a probability of at least $1/n^4$, the automorphisms $\phi_2\phi_1, \phi_3\phi_1 \dots, \phi_{poly(n)}\phi_1 \in \mathrm{Aut}(\mathcal{L}_1)$ satisfy the conditions $2 \mid \mathrm{ord}(\phi_i\phi)$ and $(\phi_1\phi)^{\mathrm{ord}(\phi_i\phi)/2} \neq -\mathbf{I}_n$. By properly defining $poly(n)$, we can obtain such an automorphism $\phi_i\phi$ with overwhelming probability. We can then apply the preprocessing procedure (Lemma 4.1) to $\phi_i\phi$ to get an automorphism in a conjugacy class corresponding to $\mathbf{T}_{i,j,k}$, resulting in a desired random automorphism in $\mathrm{Aut}(\mathcal{L})$.

Then Proposition 4.1 can be proved by repeating the above procedure polynomial times. □

4.2 Recover the Shortest Vectors

Using Proposition 4.1, a reduction from $\mathbb{Z}$LIP to $\mathbb{Z}$LAP can be established by solving the following problem, which can be viewed as an analogue of Problem 3.1.

Problem 4.1 *Given a basis* $\mathbf{B}$ *of a lattice* $\mathcal{L} \cong \mathbb{Z}^n$*, and a set of automorphisms* $\phi_1, \phi_2, \dots, \phi_{poly(n)} \in \mathrm{Aut}(\mathcal{L})$ *that are drawn uniformly and independently from a conjugacy class* $\mathfrak{C}_{\phi_0}$*, where* $\phi_0 \sim \mathbf{T}_{k_1,k_2,l}$ *and* k_1, k_2, l *are fixed. The goal is to find the shortest vectors of* $\mathcal{L}$.

Define the function

$$g_k(\mathbf{x}) = \mathbb{E}[\langle \phi\mathbf{x}, \mathbf{x}\rangle^k], \mathbf{x} \in \mathbb{R}^n, \tag{12}$$

where $k \in \mathbb{Z}^+$ and ϕ is uniformly distributed over $\mathfrak{C}_{\phi_0}$. Similar to the deduction in Section 3, for any $x \in \mathbb{R}^n$, $g_k(\mathbf{x})$ can be effectively approximated by using the given samples in $\mathfrak{C}_{\phi_0}$ due to Chernoff bound. Suppose $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ is a set of independent shortest vectors of $\mathcal{L}$. Then any $\mathbf{x} \in \mathbb{R}^n$ can be expressed as a linear combination $\mathbf{x} = x_1\mathbf{v}_1 + \cdots + x_n\mathbf{v}_n$, i.e., $x_i = \langle \mathbf{x}, \mathbf{v}_i \rangle$ for $1 \leq i \leq n$. Then the following lemma can be derived.

Lemma 4.6 *For $k = 1, 2$, it has*

$$g_1(\mathbf{x}) = \frac{k_2 - k_1}{n} \sum_{i=1}^{n} {x_i}^2 = \frac{k_2 - k_1}{n} \|\mathbf{x}\|^2$$

$$g_2(\mathbf{x}) = \frac{n^2 - 2nl - (k_1 - k_2)^2 - 4l}{n(n-1)} \sum_{i=1}^{n} {x_i}^4 + \frac{6l + (k_1 - k_2)^2 - n}{n(n-1)} (\sum_{i=1}^{n} {x_i}^2)^2$$

Proof. We refer the proof to Appendix E. □

On the other hand, note that

$$\nabla \mathbb{E}[\langle \phi\mathbf{x}, \mathbf{x} \rangle^2] = \mathbb{E}[\nabla \langle \phi\mathbf{x}, \mathbf{x} \rangle^2] = 2\mathbb{E}[\langle \phi\mathbf{x}, \mathbf{x} \rangle \cdot (\phi + \phi^\top)\mathbf{x}]. \tag{13}$$

Thus the gradient

$$\nabla g_2(\mathbf{x}) = 4 \sum_{i=1}^{n} (\frac{n^2 - 2nl - (k_1 - k_2)^2 - 4l}{n(n-1)} x_i^3 + \frac{6l + (k_1 - k_2)^2 - n}{n(n-1)} x_i \|\mathbf{x}\|^2) \mathbf{v}_i$$

can be effectively approximated by using the given samples in $\mathfrak{C}_{\phi_0}$.

Observe that n is odd and $n = k_1 + k_2 + 2l$, it follows that the coefficient $n^2 - 2nl - (k_1 - k_2)^2 - 4l = 4k_1k_2 + 2l(k_1 + k_2 - 2) \neq 0$. Again we can use the gradient descent to solve Problem 4.1. Specifically, we assume that $\mathbf{x}$ is on the unit sphere, and define

$$f_2(\mathbf{x}) = (g_2(\mathbf{x}) - \frac{6l + (k_1 - k_2)^2 - n}{n(n-1)}) / \frac{n^2 - 2nl - (k_1 - k_2)^2 - 4l}{n(n-1)} = \sum_{i=1}^{n} \langle \mathbf{v}_i, \mathbf{x} \rangle^4.$$

Then $\nabla f_2(\mathbf{x}) = 4 \sum_{i=1}^{n} \langle \mathbf{v}_i, \mathbf{x} \rangle^3 \mathbf{v}_i$ can be computed from $\nabla g_2(x)$[5], and clearly the global maximum of $f_2(\mathbf{x})$ over the unit sphere is attained at $\{\pm\mathbf{v}_1, \ldots, \pm\mathbf{v}_n\}$. Taking into account the approximation error, we present Algorithm 2 as a solution to Problem 4.1, and an analysis of the algorithm in Proposition 4.2.

Proposition 4.2 *Suppose that n is odd and $\mathcal{L} \cong \mathbb{Z}^n$. For any $c_0 > 0$, there exists a constant $c_1 > 0$ such that Algorithm 2 inputs n^{c_1} samples that are independently and uniformly distributed over a conjugacy class $\mathfrak{C}_{\phi_0}$, where k_1, k_2, l are fixed and $\phi_0 \sim \mathbf{T}_{k_1,k_2,l}$. And Algorithm 2 outputs a vector $\mathbf{x}$ such that $\|\mathbf{x} - \mathbf{v}\| \leq n^{-c_0}$ for some shortest vector $\mathbf{v} \in \mathcal{L}$, with $O(\log\log n)$ descent steps and a constant probability. Moreover, $O(n \log n)$ calls to Algorithm 2 will find all shortest vectors of $\mathcal{L}$ with an overwhelming probability.*

[5] The second method described in Section 3 can also be used to approximate the gradient $\nabla g_2(\mathbf{x})$.

Algorithm 2: Solve Problem 4.1 via Gradient Descent

```
Require: A polynomial number of samples in $\mathrm{Aut}(\mathcal{L})$ that are uniformly and
    independently distributed over the conjugacy class $\mathfrak{C}_{\phi_0}$, where $k_1, k_2, l$ are fixed
    and $\phi_0 \sim \mathbf{T}_{k_1,k_2,l}$
Ensure: An approximation a shortest vector of $\mathcal{L}$
 1: Choose $\mathbf{x}$ uniformly at random from the unit sphere of $\mathbb{R}^n$
 2: Compute an approximation of the gradient $\nabla f_2(\mathbf{x})$
 3: $\mathbf{x}_{new} \leftarrow \nabla f_2(\mathbf{x})$
 4: $\mathbf{x}_{new} \leftarrow \mathbf{x}_{new} / \|\mathbf{x}_{new}\|$
 5: Compute the approximations of $f_2(\mathbf{x}_{new})$ and $f_2(\mathbf{x})$
 6: if $f_2(\mathbf{x}_{new}) \leq f_2(\mathbf{x})$ then
 7:     return $\mathbf{x}$
 8: else
 9:     Replace $\mathbf{x}$ by $\mathbf{x}_{new}$ and go to step 2
10: end if
```

Proof. The proof is similar to that of Proposition 3.2 and is omitted here. □

Similar to Proposition 3.2, we can also recover the exact shortest vectors through good enough approximations of the shortest vectors of $\mathcal{L}$ by using a set of random automorphisms. The details can be found in Appendix F.

Combining Proposition 4.1 and Proposition 4.2, we can prove our main result in this section.

Theorem 4.1 *There is an efficient randomized reduction from $\mathbb{Z}$LIP to $\mathbb{Z}$LAP.*

Proof. If the dimension n is odd, then the theorem follows directly from Proposition 4.1 and Proposition 4.2. For even n, we utilize Corollary 3.3 to convert the $\mathbb{Z}$LIP into an $n+1$ dimensional problem, which we can then solve using the same approach. □

Remark 2. It is worth mentioning that all reductions in this paper are dimension-preserving, except for Theorem 4.1. In Theorem 4.1, the condition that n is odd (required in Proposition 4.1 and Proposition 4.2) is primarily for ease of analysis and is not a fundamental requirement. We believe that for even n, similar results can be obtained through a more complex deduction process. However, we do not provide a detailed analysis in this paper and leave it as future work.

4.3 Related Corollaries of Lattice Automorphisms

To begin with, we show that the lattice automorphisms can be linked with the hidden subgroup problem (HSP) on $GL_n(\mathbb{Z})$. HSP is a fundamental problem in quantum computation that encompasses a variety of problems, including factoring, discrete logarithm [49], principal ideal [22], graph isomorphism [35], and unique shortest vector problem [47]. It is of great importance in the theory of quantum computing as virtually all known quantum algorithms that run superpolynomially faster than classical algorithms solve special cases of the HSP on abelian groups such as those presented in [49] and [22], while the other problems correspond to non-abelian groups. As far as we know, prior to this paper, there were no known applications of the HSP on $GL_n(\mathbb{Z})$.

Definition 4.1 (HSP) *Given a group G, a subgroup $H \leq G$, and a set X. Let $f : G \to X$ be a function that hides H, i.e., $\forall g_1, g_2 \in G$, $f(g_1) = f(g_2) \Leftrightarrow g_1 H = g_2 H$. The HSP is to find a generating set of H given the function f as an oracle.*

Typically G and X are required to be finite, allowing for a well-defined problem size and efficient solution strategies. Nevertheless, for certain special infinite groups G and sets X, well-defined problems can still be formulated and solved efficiently [36,37]. Additionally, the case where G is a continuous group is also addressed in [22].

Corollary 4.1 *There is an efficient randomized reduction from $\mathbb{Z}$LIP to a variant of HSP on $GL_n(\mathbb{Z})$.*

Proof. Given a basis $\mathbf{B}$ of lattice $\mathcal{L} \cong \mathbb{Z}^n$. Let $G = X = GL_n(\mathbb{Z})$ and $H = \mathrm{Stab}(\mathbf{B}^\top \mathbf{B}) \leq G$. Define $f : G \to X$ such that $f(\mathbf{U}) = \mathbf{U}^\top \mathbf{B}^\top \mathbf{B}\mathbf{U}, \forall \mathbf{U} \in GL_n(\mathbb{Z})$. Then clearly f can be computed efficiently, and f hides H. By Lemma 2.9 there is a direct connection between $H = \mathrm{Stab}(\mathbf{B}^\top \mathbf{B})$ and $\mathrm{Aut}(\mathcal{L})$, and thus the statement follows directly from Theorem 4.1. □

Another natural question is whether the randomization framework can be applied in the reduction of general lattices. The following conclusions demonstrate that it is still applicable to specific problems. However, we believe that the randomization framework is better suited to lattices with high symmetry, i.e., those with a large automorphism group.

Corollary 4.2 *There is an efficient randomized reduction from LAP to LIP in the same dimension.*

Proof. Let $\mathcal{L}$ be an n dimensional lattice with a basis $\mathbf{B}$. To begin with, we choose a random $\mathbf{O}_1 \in O_n(\mathbb{R})$. Using Lemma 3.1, we can obtain a basis $\mathbf{B}_1 \leftarrow \mathcal{A}(\mathbf{O}_1\mathbf{B})$. Then we call the LIP oracle $\mathcal{O}$ with input $\mathbf{B}$ and $\mathbf{B}_1$, and get an isomorphism $\mathbf{O} = \mathcal{O}(\mathbf{B}, \mathbf{B}_1)$ from $\mathcal{L}$ to $\mathcal{L}_1$. For any $\phi, \phi_0 \in \mathrm{Aut}(\mathcal{L})$, it can be deduced that

$$\begin{aligned}
&\Pr_{\mathbf{O}_1 \leftarrow O_n(\mathbb{R}); \mathbf{B}_1 \leftarrow \mathcal{A}(\mathbf{O}_1\mathbf{B})}[\mathbf{O}_1^{-1}\mathcal{O}(\mathbf{B}, \mathbf{B}_1) = \phi\phi_0] \\
=& \Pr_{\mathbf{O}_1\phi \leftarrow O_n(\mathbb{R}); \mathbf{B}_1 \leftarrow \mathcal{A}(\mathbf{O}_1\phi\mathbf{B})}[(\mathbf{O}_1\phi)^{-1}\mathcal{O}(\mathbf{B}, \mathbf{B}_1) = \phi_0] \\
=& \Pr_{\mathbf{O}_1 \leftarrow O_n(\mathbb{R}); \mathbf{B}_1 \leftarrow \mathcal{A}(\mathbf{O}_1\mathbf{B})}[\mathbf{O}_1^{-1}\mathcal{O}(\mathbf{B}, \mathbf{B}_1) = \phi_0],
\end{aligned}$$

which implies that $\mathbf{O}_1^{-1}\mathcal{O}(\mathbf{B}, \mathbf{B}_1)$ is uniformly distributed in $\mathrm{Aut}(\mathcal{L})$. Thus if $\mathrm{Aut}(\mathcal{L}) \neq \{\pm \mathbf{I}_n\}$, we can efficiently obtain a nontrivial automorphism from $\mathrm{Aut}(\mathcal{L})$ with an overwhelming probability by repeating the above process $O(n)$ times. □

5 Conclusion

We present a randomization framework for lattices that randomizes the output of an oracle in such a way that the resulting samples conform to a distribution that is invariant under the action of the automorphism group. Using this framework, we derive three randomized reductions related to the rotation of $\mathbb{Z}^n$: $\mathbb{Z}$LIP to $\mathbb{Z}$SCVP, $\mathbb{Z}$SVP to $O(1)$-$\mathbb{Z}$SVP, and $\mathbb{Z}$LIP to $\mathbb{Z}$LAP. These results offer new insights into the study of rotations of $\mathbb{Z}^n$, and we believe they will pave the way for further research into $\mathbb{Z}$LIP and $\mathbb{Z}$SVP.

References

1. Aggarwal, D., Bennett, H., Golovnev, A., Stephens-Davidowitz, N.: Fine-grained hardness of CVP(P) - everything that we can prove (and nothing else). In: Marx, D. (ed.) Proceedings of the 2021 ACM-SIAM Symposium on Discrete Algorithms, SODA 2021, Virtual Conference, January 10 - 13, 2021. pp. 1816–1835. SIAM (2021). https://doi.org/10.1137/1.9781611976465.109, https://doi.org/10.1137/1.9781611976465.109
2. Aggarwal, D., Dadush, D., Regev, O., Stephens-Davidowitz, N.: Solving the shortest vector problem in 2^{n} time using discrete gaussian sampling: Extended abstract. In: Servedio, R.A., Rubinfeld, R. (eds.) Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing, STOC 2015, Portland, OR, USA, June 14-17, 2015. pp. 733–742. ACM (2015). https://doi.org/10.1145/2746539.2746606, https://doi.org/10.1145/2746539.2746606
3. Aggarwal, D., Li, J., Nguyen, P.Q., Stephens-Davidowitz, N.: Slide reduction, revisited—Filling the gaps in SVP approximation. In: CRYPTO (2020), http://arxiv.org/abs/1908.03724
4. Aggarwal, D., Li, Z., Stephens-Davidowitz, N.: A $2^{n/2}$-time algorithm for $\sqrt{n}$-SVP and $\sqrt{n}$-Hermite SVP, and an improved time-approximation tradeoff for (H)SVP. In: Eurocrypt (2021), http://arxiv.org/abs/2007.09556
5. Aggarwal, D., Stephens-Davidowitz, N.: Just take the average! an embarrassingly simple 2^n-time algorithm for SVP (and CVP). In: Seidel, R. (ed.) 1st Symposium on Simplicity in Algorithms, SOSA 2018, January 7-10, 2018, New Orleans, LA, USA. OASIcs, vol. 61, pp. 12:1–12:19. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2018). https://doi.org/10.4230/OASIcs.SOSA.2018.12, https://doi.org/10.4230/OASIcs.SOSA.2018.12
6. Aggarwal, D., Ursu, B., Vaudenay, S.: Faster sieving algorithm for approximate svp with constant approximation factors. Cryptology ePrint Archive (2019)
7. Babai, L.: Graph isomorphism in quasipolynomial time [extended abstract]. In: Wichs, D., Mansour, Y. (eds.) Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2016, Cambridge, MA, USA, June 18-21, 2016. pp. 684–697. ACM (2016). https://doi.org/10.1145/2897518.2897542, https://doi.org/10.1145/2897518.2897542
8. Bennett, H.: The complexity of the shortest vector problem. Electron. Colloquium Comput. Complex. **TR22-170** (2022), https://eccc.weizmann.ac.il/report/2022/170

9. Bennett, H., Ganju, A., Peetathawatchai, P., Stephens-Davidowitz, N.: Just how hard are rotations of F^{n}? algorithms and cryptography with the simplest lattice. IACR Cryptol. ePrint Arch. p. 1548 (2021), https://eprint.iacr.org/2021/1548
10. Bennett, H., Golovnev, A., Stephens-Davidowitz, N.: On the quantitative hardness of CVP. In: Umans, C. (ed.) 58th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2017, Berkeley, CA, USA, October 15-17, 2017. pp. 13–24. IEEE Computer Society (2017). https://doi.org/10.1109/FOCS.2017.11, https://doi.org/10.1109/FOCS.2017.11
11. Blanks, T.L., Miller, S.D.: Generating cryptographically-strong random lattice bases and recognizing rotations of z^ n z n. In: Post-Quantum Cryptography: 12th International Workshop, PQCrypto 2021, Daejeon, South Korea, July 20–22, 2021, Proceedings 12. pp. 319–338. Springer (2021)
12. Brakerski, Z., Langlois, A., Peikert, C., Regev, O., Stehlé, D.: Classical hardness of learning with errors. In: Boneh, D., Roughgarden, T., Feigenbaum, J. (eds.) Symposium on Theory of Computing Conference, STOC'13, Palo Alto, CA, USA, June 1-4, 2013. pp. 575–584. ACM (2013). https://doi.org/10.1145/2488608.2488680, https://doi.org/10.1145/2488608.2488680
13. Cai, J., Nerurkar, A.: An improved worst-case to average-case connection for lattice problems. In: 38th Annual Symposium on Foundations of Computer Science, FOCS '97, Miami Beach, Florida, USA, October 19-22, 1997. pp. 468–477. IEEE Computer Society (1997). https://doi.org/10.1109/SFCS.1997.646135, https://doi.org/10.1109/SFCS.1997.646135
14. Cash, D., Hofheinz, D., Kiltz, E., Peikert, C.: Bonsai trees, or how to delegate a lattice basis. In: Gilbert, H. (ed.) Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Monaco / French Riviera, May 30 - June 3, 2010. Proceedings. Lecture Notes in Computer Science, vol. 6110, pp. 523–552. Springer (2010). https://doi.org/10.1007/978-3-642-13190-5_27, https://doi.org/10.1007/978-3-642-13190-5_27
15. Collins, B., Śniady, P.: Integration with respect to the haar measure on unitary, orthogonal and symplectic group. Communications in Mathematical Physics **264**(3), 773–795 (2006)
16. Diaconis, P., Shahshahani, M.: The subgroup algorithm for generating uniform random variables. Probability in the engineering and informational sciences **1**(1), 15–32 (1987)
17. Ducas, L., Gibbons, S.: Hull attacks on the lattice isomorphism problem. IACR Cryptol. ePrint Arch. p. 194 (2023), https://eprint.iacr.org/2023/194
18. Ducas, L., Postlethwaite, E.W., Pulles, L.N., van Woerden, W.P.J.: Hawk: Module LIP makes lattice signatures fast, compact and simple. In: Agrawal, S., Lin, D. (eds.) Advances in Cryptology - ASIACRYPT 2022 - 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5-9, 2022, Proceedings, Part IV. Lecture Notes in Computer Science, vol. 13794, pp. 65–94. Springer (2022). https://doi.org/10.1007/978-3-031-22972-5_3, https://doi.org/10.1007/978-3-031-22972-5_3
19. Ducas, L., van Woerden, W.P.J.: On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography. In: Dunkelman, O., Dziembowski, S. (eds.) Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III. Lecture Notes in Computer Science, vol. 13277, pp. 643–673.

Springer (2022). https://doi.org/10.1007/978-3-031-07082-2_23, https://doi.org/10.1007/978-3-031-07082-2_23

20. Ducas, L.: Provable lattice reduction of F^n with blocksize $n/2$. Cryptology ePrint Archive, Paper 2023/447 (2023), https://eprint.iacr.org/2023/447, https://eprint.iacr.org/2023/447
21. Dutour Sikirić, M., Haensch, A., Voight, J., van Woerden, W.P.: A canonical form for positive definite matrices. Open Book Series **4**(1), 179–195 (2020)
22. Eisenträger, K., Hallgren, S., Kitaev, A.Y., Song, F.: A quantum algorithm for computing the unit group of an arbitrary degree number field. In: Shmoys, D.B. (ed.) Symposium on Theory of Computing, STOC 2014, New York, NY, USA, May 31 - June 03, 2014. pp. 293–302. ACM (2014). https://doi.org/10.1145/2591796.2591860, https://doi.org/10.1145/2591796.2591860
23. Geißler, K., Smart, N.P.: Computing the $\mathrm{M} = \mathrm{U}\ \mathrm{u}^{\mathrm{t}}$ integer matrix decomposition. In: Paterson, K.G. (ed.) Cryptography and Coding, 9th IMA International Conference, Cirencester, UK, December 16-18, 2003, Proceedings. Lecture Notes in Computer Science, vol. 2898, pp. 223–233. Springer (2003). https://doi.org/10.1007/978-3-540-40974-8_18, https://doi.org/10.1007/978-3-540-40974-8_18
24. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Dwork, C. (ed.) Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17-20, 2008. pp. 197–206. ACM (2008). https://doi.org/10.1145/1374376.1374407, https://doi.org/10.1145/1374376.1374407
25. Gentry, C., Szydlo, M.: Cryptanalysis of the revised NTRU signature scheme. In: Knudsen, L.R. (ed.) Advances in Cryptology - EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, April 28 - May 2, 2002, Proceedings. Lecture Notes in Computer Science, vol. 2332, pp. 299–320. Springer (2002). https://doi.org/10.1007/3-540-46035-7_20, https://doi.org/10.1007/3-540-46035-7_20
26. Goldreich, O., Goldwasser, S., Halevi, S.: Public-key cryptosystems from lattice reduction problems. In: Jr., B.S.K. (ed.) Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 1997, Proceedings. Lecture Notes in Computer Science, vol. 1294, pp. 112–131. Springer (1997). https://doi.org/10.1007/BFb0052231, https://doi.org/10.1007/BFb0052231
27. Haviv, I., Regev, O.: Hardness of the covering radius problem on lattices. Chic. J. Theor. Comput. Sci. **2012** (2012), http://cjtcs.cs.uchicago.edu/articles/2012/4/contents.html
28. Haviv, I., Regev, O.: On the lattice isomorphism problem. In: Chekuri, C. (ed.) Proceedings of the Twenty-Fifth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2014, Portland, Oregon, USA, January 5-7, 2014. pp. 391–404. SIAM (2014). https://doi.org/10.1137/1.9781611973402.29, https://doi.org/10.1137/1.9781611973402.29
29. Hoeffding, W.: Probability inequalities for sums of bounded random variables. The collected works of Wassily Hoeffding pp. 409–426 (1994)
30. Hoffstein, J., Howgrave-Graham, N., Pipher, J., Silverman, J.H., Whyte, W.: NTRUSIGN: digital signatures using the NTRU lattice. In: Joye, M. (ed.) Topics in Cryptology - CT-RSA 2003, The Cryptographers' Track at

the RSA Conference 2003, San Francisco, CA, USA, April 13-17, 2003, Proceedings. Lecture Notes in Computer Science, vol. 2612, pp. 122–140. Springer (2003). https://doi.org/10.1007/3-540-36563-X_9, https://doi.org/10.1007/3-540-36563-X_9

31. Hunkenschröder, C.: Deciding whether a lattice has an orthonormal basis is in co-np. CoRR **abs/1910.03838** (2019), http://arxiv.org/abs/1910.03838
32. Jr., H.W.L., Silverberg, A.: Revisiting the gentry-szydlo algorithm. In: Garay, J.A., Gennaro, R. (eds.) Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part I. Lecture Notes in Computer Science, vol. 8616, pp. 280–296. Springer (2014). https://doi.org/10.1007/978-3-662-44371-2_16, https://doi.org/10.1007/978-3-662-44371-2_16
33. Jr., H.W.L., Silverberg, A.: Lattices with symmetry. J. Cryptol. **30**(3), 760–804 (2017). https://doi.org/10.1007/s00145-016-9235-7, https://doi.org/10.1007/s00145-016-9235-7
34. Khot, S.: Hardness of approximating the shortest vector problem in lattices. In: 45th Symposium on Foundations of Computer Science (FOCS 2004), 17-19 October 2004, Rome, Italy, Proceedings. pp. 126–135. IEEE Computer Society (2004). https://doi.org/10.1109/FOCS.2004.31, https://doi.org/10.1109/FOCS.2004.31
35. Köbler, J., Schöning, U., Torán, J.: The Graph Isomorphism Problem: Its Structural Complexity. Progress in Theoretical Computer Science, Birkhäuser/Springer (1993). https://doi.org/10.1007/978-1-4612-0333-9, https://doi.org/10.1007/978-1-4612-0333-9
36. Kuperberg, G.: The hidden subgroup problem for infinite groups (2020), https://simons.berkeley.edu/sites/default/files/docs/21261/berkeley.pdf
37. Kuperberg, G.: The hidden subgroup problem for $\mathbb{Z}^k$ for infinite-index subgroups (2022), https://simons.berkeley.edu/sites/default/files/docs/21261/berkeley.pdf
38. Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring polynomials with rational coefficients. Mathematische annalen **261**(ARTICLE), 515–534 (1982)
39. Liu, M., Wang, X., Xu, G., Zheng, X.: Shortest lattice vectors in the presence of gaps. Cryptology ePrint Archive (2011)
40. Luks, E.M.: Permutation groups and polynomial-time computation. In: Finkelstein, L., Kantor, W.M. (eds.) Groups And Computation, Proceedings of a DIMACS Workshop, New Brunswick, New Jersey, USA, October 7-10, 1991. DIMACS Series in Discrete Mathematics and Theoretical Computer Science, vol. 11, pp. 139–175. DIMACS/AMS (1991). https://doi.org/10.1090/dimacs/011/11, https://doi.org/10.1090/dimacs/011/11
41. Martinet, J.: Perfect lattices in Euclidean spaces, vol. 327. Springer Science & Business Media (2013)
42. Mezzadri, F.: How to generate random matrices from the classical compact groups. arXiv preprint math-ph/0609050 (2006)
43. Nguyen, P.Q., Regev, O.: Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures. In: Vaudenay, S. (ed.) Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings. Lecture Notes in Computer Science, vol. 4004, pp. 271–288. Springer (2006). https://doi.org/10.1007/11761679_17, https://doi.org/10.1007/11761679_17
44. Noam D. Elkies: Intro to SPLAG. https://people.math.harvard.edu/~elkies/M55a.02/lattice.html (2002)

45. Peikert, C.: A decade of lattice cryptography. Found. Trends Theor. Comput. Sci. **10**(4), 283–424 (2016). https://doi.org/10.1561/0400000074, https://doi.org/10.1561/0400000074
46. Plesken, W., Souvignier, B.: Computing isometries of lattices. Journal of Symbolic Computation **24**(3-4), 327–334 (1997)
47. Regev, O.: Quantum computation and lattice problems. In: 43rd Symposium on Foundations of Computer Science (FOCS 2002), 16-19 November 2002, Vancouver, BC, Canada, Proceedings. pp. 520–529. IEEE Computer Society (2002). https://doi.org/10.1109/SFCS.2002.1181976, https://doi.org/10.1109/SFCS.2002.1181976
48. Regev, O., Stephens-Davidowitz, N.: A reverse minkowski theorem. In: Hatami, H., McKenzie, P., King, V. (eds.) Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, Montreal, QC, Canada, June 19-23, 2017. pp. 941–953. ACM (2017). https://doi.org/10.1145/3055399.3055434, https://doi.org/10.1145/3055399.3055434
49. Shor, P.W.: Algorithms for quantum computation: Discrete logarithms and factoring. In: 35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, 20-22 November 1994. pp. 124–134. IEEE Computer Society (1994). https://doi.org/10.1109/SFCS.1994.365700, https://doi.org/10.1109/SFCS.1994.365700
50. Sikiric, M.D., Schürmann, A., Vallentin, F.: Complexity and algorithms for computing voronoi cells of lattices. Math. Comput. **78**(267), 1713–1731 (2009). https://doi.org/10.1090/S0025-5718-09-02224-8, https://doi.org/10.1090/S0025-5718-09-02224-8
51. Stephens-Davidowitz, N.: Search-to-decision reductions for lattice problems with approximation factors (slightly) greater than one. In: Jansen, K., Mathieu, C., Rolim, J.D.P., Umans, C. (eds.) Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, APPROX/RANDOM 2016, September 7-9, 2016, Paris, France. LIPIcs, vol. 60, pp. 19:1–19:18. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2016). https://doi.org/10.4230/LIPIcs.APPROX-RANDOM.2016.19, https://doi.org/10.4230/LIPIcs.APPROX-RANDOM.2016.19
52. Stewart, G.W.: The efficient generation of random orthogonal matrices with an application to condition estimators. SIAM Journal on Numerical Analysis **17**(3), 403–409 (1980)
53. Szydlo, M.: Hypercubic lattice reduction and analysis of GGH and NTRU signatures. In: Biham, E. (ed.) Advances in Cryptology - EUROCRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4-8, 2003, Proceedings. Lecture Notes in Computer Science, vol. 2656, pp. 433–448. Springer (2003). https://doi.org/10.1007/3-540-39200-9_27, https://doi.org/10.1007/3-540-39200-9_27
54. Wei, W., Liu, M., Wang, X.: Finding shortest lattice vectors in the presence of gaps. In: CT-RSA. vol. 9048, pp. 239–257. Springer (2015)

Appendix A Proof of the Toy Example

With respect to the oracle $\mathcal{O}$, the rotated square is determined by the angle θ between the line connecting its vertex on the first quadrant to the origin O and the positive direction of the x-axis. Denoted the rotated square by $\square_\theta, \theta \in [0, \frac{\pi}{2})$. Note we can regard θ as functional of ρ, and write $\theta[\rho] = \theta[\rho + \frac{\pi}{2}]$. We'll show that,

$$\Pr_{\rho \leftarrow G}[\rho^{-1}\mathcal{O}(\square_{\theta[\rho]}) = i] = \frac{1}{4}, \forall i \in \mathbb{Z}/4\mathbb{Z}.$$

Proof. For any $i \in \mathbb{Z}/4\mathbb{Z}$, $\Pr_{\rho \leftarrow G}[\rho^{-1}\mathcal{O}(\square_{\theta[\rho]}) = i]$ is a functional about ρ which is a distribution on $G = \mathbb{R}/2\pi\mathbb{Z}$. Then we have

$$\begin{aligned}
\Pr_{\rho \leftarrow G}[\rho^{-1}\mathcal{O}(\square_{\theta[\rho]}) = i] &= \Pr_{\rho \leftarrow G}[\mathcal{O}(\square_{\theta[\rho]}) = \rho(i)] \\
&= \Pr_{\rho + \frac{\pi}{2} \leftarrow G}[\mathcal{O}(\square_{\theta[\rho + \frac{\pi}{2}]}) = (\rho + \frac{\pi}{2})(i)] \\
&= \Pr_{\rho + \frac{\pi}{2} \leftarrow G}[\mathcal{O}(\square_{\theta[\rho]}) = \rho(i+1)] \\
&= \Pr_{\rho \leftarrow G}[\mathcal{O}(\square_{\theta[\rho]}) = \rho(i+1)].
\end{aligned}$$

This means $\forall i \in \mathbb{Z}/4\mathbb{Z}$, $\Pr_{\rho \leftarrow G}[\rho^{-1}\mathcal{O}(\square_{\theta[\rho]}) = i] = \frac{1}{4}$. □

Appendix B Proof of the Property of the Characteristic Vectors

Lemma 2.6 *Assume* $\mathbf{B} = (\mathbf{b}_1, ..., \mathbf{b}_n)$ *is a basis of* $\mathcal{L}$ *and* $\mathbf{B}^{-\top} = (\mathbf{d}_1, ..., \mathbf{d}_n)$*, then it has:*

1) $\mathbf{w} = \sum_{i=1}^n \|\mathbf{d}_i\|^2 \mathbf{b}_i$ *is a characteristic vector of* $\mathcal{L}$.
2) $\chi(\mathcal{L}) = \mathbf{w} + 2\mathcal{L}$ *for any characteristic vector* $\mathbf{w} \in \chi(\mathcal{L})$.
3) $\mathbf{w}$ *is a characteristic vector if and only if* $\langle \mathbf{w}, \mathbf{b}_i \rangle \equiv \langle \mathbf{b}_i, \mathbf{b}_i \rangle \mod 2$ *for* $i \in [n]$.

Proof. 1) Let $\mathbf{v} = \sum_{i=1}^n v_i \mathbf{d}_i \in \mathcal{L}(\mathbf{B})$, then $\langle \mathbf{w}, \mathbf{v} \rangle = \langle \sum_{i=1}^n \|\mathbf{d}_i\|^2 \mathbf{b}_i, \sum_{i=1}^n v_i \mathbf{d}_i \rangle = \sum_{i=1}^n v_i \|\mathbf{d}_i\|^2 \equiv \sum_{i=1}^n v_i^2 \|\mathbf{d}_i\|^2 \equiv \langle \mathbf{v}, \mathbf{v} \rangle \mod 2$, we used $v_i \equiv v_i^2 \mod 2$. Thus $\mathbf{w}$ is a characteristic vector.

2) Assume $\mathbf{w}$ is a characteristic vector of $\mathcal{L}$, then for any $\mathbf{x} \in \mathcal{L}$, $\mathbf{w} + 2\mathbf{x}$ is also a characteristic vector of $\mathcal{L}$, because $\langle \mathbf{w} + 2\mathbf{x}, \mathbf{v} \rangle = \langle \mathbf{w}, \mathbf{v} \rangle + 2\langle \mathbf{x}, \mathbf{v} \rangle \equiv \langle \mathbf{w}, \mathbf{v} \rangle \equiv \langle \mathbf{v}, \mathbf{v} \rangle \mod 2$. On the other hand, if $\mathbf{w}' = \sum_{i=1}^n a_i \mathbf{b}_i \in \chi(\mathcal{L})$, then $a_i = \langle \mathbf{w}', \mathbf{d}_i \rangle \equiv \langle \mathbf{d}_i, \mathbf{d}_i \rangle = \|\mathbf{d}_i\|^2 \mod 2$, thus for any $i \in [n]$, $a_i \equiv \|\mathbf{d}_i\|^2 \mod 2$ and we know $\mathbf{w} = \sum_{i=1}^n \|\mathbf{d}_i\|^2 \mathbf{b}_i \in \chi(\mathcal{L})$, thus $\mathbf{w}' = \mathbf{w} + 2\mathcal{L}$. Thus $\chi(\mathcal{L})$ is a coset of $\mathbf{w} + 2\mathcal{L}$, where $\mathbf{w}$ is any element in $\chi(\mathcal{L})$.

3) Obviously, if $\mathbf{w} \in \chi(\mathcal{L})$, $\forall i \in [n]$, $\langle \mathbf{w}, \mathbf{b}_i \rangle \equiv \langle \mathbf{b}_i, \mathbf{b}_i \rangle \mod 2$. On the other hand, if $\mathbf{w} \in \mathcal{L}$ satisfying $\forall i \in [n]$, $\langle \mathbf{w}, \mathbf{b}_i \rangle \equiv \langle \mathbf{b}_i, \mathbf{b}_i \rangle \mod 2$. Then for any $\mathbf{v} = \sum_{i=1}^n v_i \mathbf{b}_i \in \mathcal{L}$, without loss of generality, assume $v_i \equiv 1 \mod 2$ for $1 \le i \le k$, and $v_i \equiv 0 \mod 2$ for $k+1 \le i \le n$. Thus we have $\langle \mathbf{w}, \mathbf{v} \rangle \equiv \langle \mathbf{w}, \mathbf{b}_1 + \ldots + \mathbf{b}_k \rangle \equiv \sum_{i=1}^k \langle \mathbf{w}, \mathbf{b}_i \rangle \equiv \sum_{i=1}^k \langle \mathbf{b}_i, \mathbf{b}_i \rangle \equiv \langle \mathbf{v}, \mathbf{v} \rangle \mod 2$.

□

Lemma 2.7 *Suppose* $\mathcal{L} \cong \mathbb{Z}^n$. *Assume* $\mathbf{B} = \mathbf{OU}$ *is a basis of* $\mathcal{L}$, *where* $\mathbf{O} \in O_n(\mathbb{R})$ *and* $\mathbf{U} \in GL_n(\mathbb{Z}^n)$. *Then it has:*

1) $\chi(\mathcal{L}) = \{\mathbf{Oz} : \mathbf{z} \in \mathbb{Z}^n$ *such that* $\mathbf{z}_i \equiv 1 \mod 2, \forall i \in [n]\}$.
2) *The shortest characteristic vectors are exactly* $\{\mathbf{Oz} : \mathbf{z}_i = \pm 1, \forall i \in [n]\}$.

Proof. 1) Let $\mathbf{O} = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ and $\mathbf{w} = \mathbf{B}(\mathbf{U}^{-1}\mathbf{z}) = \mathbf{Oz}$, where $\mathbf{z} \in \mathbb{Z}^n$ is the vector that $\forall i \in [n]$, $z_i = 1$. Note that $\mathcal{L} = \mathbf{O} \cdot \mathbb{Z}^n$. Thus assume $\mathbf{v} = \sum_{i=1}^n a_i \mathbf{v}_i$, then $\langle \mathbf{w}, \mathbf{v} \rangle = \sum_{i=1}^n a_i z_i \equiv \sum_{i=1}^n a_i^2 = \langle \mathbf{v}, \mathbf{v} \rangle \mod 2$, where we used $a_i^2 \equiv a_i \mod 2$ and $z_i \equiv 1 \mod 2$. Thus $\mathbf{w} \in \chi(\mathcal{L})$, so $\chi(\mathcal{L}) = \{\mathbf{Oz} : \mathbf{z} \in \mathbb{Z}^n$ such that $\mathbf{z}_i \equiv 1 \mod 2, \forall i \in [n]\}$.

2) Note that $\mathbf{O}$ is an orthogonal matrix, thus the shortest characteristic vectors are $\{\mathbf{Oz} : \mathbf{z}_i = \pm 1, \forall\, i \in [n]\}$ by 1).

□

Appendix C Proof of the Independence of Proposition 3.1

Proof. We demonstrate the proof of independence by considering the case where the number of trials is two. The general case follows in a similar approach. Specifically, our goal is to demonstrate that for any shortest characteristic vectors $\mathbf{w}_1, \mathbf{w}_2 \in \chi(\mathcal{L})$, it holds

$$\begin{aligned}
&\Pr_{\substack{\mathbf{O}_1 \leftarrow O_n(\mathbb{R}), \mathbf{B}_1 \leftarrow \mathcal{A}(\mathbf{O}_1\mathbf{B}) \\ \mathbf{O}_2 \leftarrow O_n(\mathbb{R}), \mathbf{B}_2 \leftarrow \mathcal{A}(\mathbf{O}_2\mathbf{B})}} [\mathbf{O}_1^{-1}\mathcal{O}(\mathbf{B}_1) = \mathbf{w}_1, \mathbf{O}_2^{-1}\mathcal{O}(\mathbf{B}_2) = \mathbf{w}_2] \\
&= \Pr_{\substack{\mathbf{O}_1 \leftarrow O_n(\mathbb{R}) \\ \mathbf{B}_1 \leftarrow \mathcal{A}(\mathbf{O}_1\mathbf{B})}} [\mathbf{O}_1^{-1}\mathcal{O}(\mathbf{B}_1) = \mathbf{w}_1] \cdot \Pr_{\substack{\mathbf{O}_2 \leftarrow O_n(\mathbb{R}) \\ \mathbf{B}_2 \leftarrow \mathcal{A}(\mathbf{O}_2\mathbf{B})}} [\mathbf{O}_2^{-1}\mathcal{O}(\mathbf{B}_2) = \mathbf{w}_2] \\
&= (\frac{1}{2^n})^2,
\end{aligned}$$

where the second equality follows from the uniformity as shown in Proposition 3.1. For any $\mathbf{M}_1, \mathbf{M}_2 \in \mathrm{Aut}(\mathcal{L})$, it has

$$\begin{aligned}
&\Pr_{\substack{\mathbf{O}_1 \leftarrow O_n(\mathbb{R}), \mathbf{B}_1 \leftarrow \mathcal{A}(\mathbf{O}_1\mathbf{B}) \\ \mathbf{O}_2 \leftarrow O_n(\mathbb{R}), \mathbf{B}_2 \leftarrow \mathcal{A}(\mathbf{O}_2\mathbf{B})}} [\mathbf{O}_1^{-1}\mathcal{O}(\mathbf{B}_1) = \mathbf{M}_1\mathbf{w}_1, \mathbf{O}_2^{-1}\mathcal{O}(\mathbf{B}_2) = \mathbf{M}_2\mathbf{w}_2] \\
&= \Pr_{\substack{\mathbf{O}_1 \leftarrow O_n(\mathbb{R}), \mathbf{B}_1 \leftarrow \mathcal{A}(\mathbf{O}_1\mathbf{B}) \\ \mathbf{O}_2 \leftarrow O_n(\mathbb{R}), \mathbf{B}_2 \leftarrow \mathcal{A}(\mathbf{O}_2\mathbf{B})}} [(\mathbf{O}_1\mathbf{M}_1)^{-1}\mathcal{O}(\mathbf{B}_1) = \mathbf{w}_1, (\mathbf{O}_2\mathbf{M}_2)^{-1}\mathcal{O}(\mathbf{B}_2) = \mathbf{w}_2] \\
&= \Pr_{\substack{\mathbf{O}_1\mathbf{M}_1 \leftarrow O_n(\mathbb{R}), \mathbf{B}_1 \leftarrow \mathcal{A}(\mathbf{O}_1\mathbf{B}) \\ \mathbf{O}_2\mathbf{M}_2 \leftarrow O_n(\mathbb{R}), \mathbf{B}_2 \leftarrow \mathcal{A}(\mathbf{O}_2\mathbf{B})}} [(\mathbf{O}_1\mathbf{M}_1)^{-1}\mathcal{O}(\mathbf{B}_1) = \mathbf{w}_1, (\mathbf{O}_2\mathbf{M}_2)^{-1}\mathcal{O}(\mathbf{B}_2) = \mathbf{w}_2] \\
&= \Pr_{\substack{\mathbf{O}_1\mathbf{M}_1 \leftarrow O_n(\mathbb{R}), \mathbf{B}_1 \leftarrow \mathcal{A}(\mathbf{O}_1\mathbf{M}_1\mathbf{B}) \\ \mathbf{O}_2\mathbf{M}_2 \leftarrow O_n(\mathbb{R}), \mathbf{B}_2 \leftarrow \mathcal{A}(\mathbf{O}_2\mathbf{M}_2\mathbf{B})}} [(\mathbf{O}_1\mathbf{M}_1)^{-1}\mathcal{O}(\mathbf{B}_1) = \mathbf{w}_1, (\mathbf{O}_2\mathbf{M}_2)^{-1}\mathcal{O}(\mathbf{B}_2) = \mathbf{w}_2] \\
&= \Pr_{\substack{\mathbf{O}_1 \leftarrow O_n(\mathbb{R}), \mathbf{B}_1 \leftarrow \mathcal{A}(\mathbf{O}_1\mathbf{B}) \\ \mathbf{O}_2 \leftarrow O_n(\mathbb{R}), \mathbf{B}_2 \leftarrow \mathcal{A}(\mathbf{O}_2\mathbf{B})}} [\mathbf{O}_1^{-1}\mathcal{O}(\mathbf{B}_1) = \mathbf{w}_1, \mathbf{O}_2^{-1}\mathcal{O}(\mathbf{B}_2) = \mathbf{w}_2],
\end{aligned}$$

Where the second equality is derived from the property of Haar measure and the independence of $\mathbf{O}_1$ and $\mathbf{O}_2$, the third equality follows from Lemma 3.1 and the independence of randomness used by $\mathcal{A}$ in each trial, and the last equality is simply a substitution of the variable. Thus, for any shortest characteristic vectors $\mathbf{w}_1, \mathbf{w}_2 \in \chi(\mathcal{L})$,

$$\Pr_{\substack{\mathbf{O}_1 \leftarrow O_n(\mathbb{R}), \mathbf{B}_1 \leftarrow \mathcal{A}(\mathbf{O}_1\mathbf{B}) \\ \mathbf{O}_2 \leftarrow O_n(\mathbb{R}), \mathbf{B}_2 \leftarrow \mathcal{A}(\mathbf{O}_2\mathbf{B})}}[\mathbf{O}_1^{-1}\mathcal{O}(\mathbf{B}_1) = \mathbf{w}_1, \mathbf{O}_2^{-1}\mathcal{O}(\mathbf{B}_2) = \mathbf{w}_2] = (\frac{1}{2^n})^2,$$

which completes the proof. □

Appendix D Reductions in the Gram Matrix Form

We demonstrate how the reductions in this paper can be expressed in the Gram matrix form (i.e., in a quadratic form setting as in [18,19,21]). In this appendix, we use the notation $\mathbf{G}_1 \cong \mathbf{G}_2$ to indicate that two positive definite matrices (quadratic forms) $\mathbf{G}_1, \mathbf{G}_2 \in \mathbb{Z}^{n \times n}$ are equivalent, i.e., there exists a unimodular matrix $\mathbf{U}$ such that $\mathbf{U}^\top \mathbf{G}_1 \mathbf{U} = \mathbf{G}_2$. Recall that a lattice $\mathcal{L}(\mathbf{B})$ is unimodular if and only if its Gram matrix $\mathbf{G} = \mathbf{B}^\top \mathbf{B}$ is a unimodular matrix. Then the characteristic vectors can be defined using the Gram matrix. Specifically, define $\chi(\mathbf{G}) = \{\mathbf{z} \in \mathbb{Z}^n : \mathbf{z}^\top \mathbf{G} \mathbf{e}_i \equiv \mathbf{e}_i^\top \mathbf{G} \mathbf{e}_i \bmod 2,\ i \in [n]\}$ to be the set of characteristic vectors of $\mathbf{G}$. Then $\mathbf{z} \in \chi(\mathbf{G})$ if and only if $\mathbf{B}\mathbf{z} \in \chi(\mathcal{L}(\mathbf{B}))$. The lattice problems involved in this paper can be reformulated using the Gram matrix as follows.

- LIP ($\mathbb{Z}$LIP): Given two matrices $\mathbf{G}_1 \cong \mathbf{G}_2$ $(= \mathbf{I}_n)$, find a unimodular matrix $\mathbf{U}$ such that $\mathbf{U}^\top \mathbf{G}_2 \mathbf{U} = \mathbf{G}_1$.
- $\mathbb{Z}$SVP: Given a matrix $\mathbf{G} \cong \mathbf{I}_n$, find a $\mathbf{z} \in \mathbb{Z}^n$ such that $\mathbf{z}^\top \mathbf{G} \mathbf{z} = 1$. We call such $\mathbf{z}$ a shortest vector of $\mathbf{G}$.
- γ-$\mathbb{Z}$SVP: Given a matrix $\mathbf{G} \cong \mathbf{I}_n$, find a $\mathbf{z} \in \mathbb{Z}^n$ such that $\mathbf{z}^\top \mathbf{G} \mathbf{z} \leq \gamma$.
- $\mathbb{Z}$SCVP: Given a matrix $\mathbf{G} \cong \mathbf{I}_n$, find a $\mathbf{z} \in \chi(\mathbf{G})$ such that $\mathbf{z}^\top \mathbf{G} \mathbf{z} = n$.
- LAP ($\mathbb{Z}$LAP): Given a matrix $\mathbf{G}$ $(\cong \mathbf{I}_n)$, find a unimodular matrix $\mathbf{U} \in \mathrm{Stab}(\mathbf{G})$ such that $\mathbf{U} \neq \pm \mathbf{I}_n$.

D.1 A Reduction from $\mathbb{Z}$LIP to $\mathbb{Z}$SCVP

To begin with, we provide a Gram matrix version of Lemma 3.1. Analogous results have also appeared in [9,14,28,19].

Lemma D.1 *There is an efficient algorithm that takes as input a Gram matrix* $\mathbf{G}$ *of a lattice* $\mathcal{L}$ *and outputs two matrices* $(\mathbf{G}_1, \mathbf{U}_1)$ *such that* $\mathbf{G}_1 = \mathbf{U}_1^\top \mathbf{G} \mathbf{U}_1$ *according to a distribution* $\mathcal{B}(\mathbf{G})$*, satisfying that*

$$\Pr[(\mathbf{G}_1, \mathbf{U}_1) \leftarrow \mathcal{B}(\mathbf{G})] = \Pr[(\mathbf{G}_1, \mathbf{V}\mathbf{U}_1) \leftarrow \mathcal{B}(\mathbf{G})] \tag{14}$$

for any $\mathbf{V} \in \mathit{Stab}(\mathbf{G})$*.*

Proof. To obtain $(\mathbf{G}_1, \mathbf{U}_1)$, we first apply the Cholesky decomposition to decompose $\mathbf{G}$ into $\mathbf{B}^\top \mathbf{B}$. Then, using Lemma 3.1, we obtain a basis $\mathbf{B}_1 \leftarrow \mathcal{A}(\mathbf{B})$ of the lattice $\mathcal{L}(\mathbf{B})$. Next, we compute a unimodular matrix $\mathbf{U}_1$ such that $\mathbf{B}_1 = \mathbf{B}\mathbf{U}_1$. Finally, we output the matrices $(\mathbf{G}_1 = \mathbf{B}_1^\top \mathbf{B}_1, \mathbf{U}_1)$.

It is clear that $\mathbf{G}_1 = \mathbf{U}_1^\top \mathbf{G}\mathbf{U}_1$. On the other hand, from Lemma 3.1, we know that $\Pr[\mathbf{B}_1 \leftarrow \mathcal{A}(\mathbf{B})] = \Pr[\mathbf{O}\mathbf{B}_1 \leftarrow \mathcal{A}(\mathbf{B})]$ for any $\mathbf{O} \in \mathrm{Aut}(\mathcal{L})$. According to Lemma 2.9, for any $\mathbf{O} \in \mathrm{Aut}(\mathcal{L})$, there exists a unique $\mathbf{V} \in \mathrm{Stab}(\mathbf{G})$ such that $\mathbf{O}\mathbf{B} = \mathbf{B}\mathbf{V}$. Therefore, we have $\Pr[\mathbf{B}_1 \leftarrow \mathcal{A}(\mathbf{B})] = \Pr[\mathbf{B}_1\mathbf{V} \leftarrow \mathcal{A}(\mathbf{B})]$, i.e. $\Pr[(\mathbf{G}_1, \mathbf{U}_1) \leftarrow \mathcal{B}(\mathbf{G})] = \Pr[(\mathbf{G}_1, \mathbf{V}\mathbf{U}_1) \leftarrow \mathcal{B}(\mathbf{G})]$ for any $\mathbf{V} \in \mathrm{Stab}(\mathbf{G})$. □

Remark 3. We note that the decomposition and basis operations are only performed to simplify the presentation of the above proof. A more effective approach to obtaining $(\mathbf{G}_1, \mathbf{U}_1)$ is to perform Gaussian sampling and LLL algorithms directly on the Gram matrix (as demonstrated in [19]), without decomposing $\mathbf{G}$. This method avoids any potential precision issues that may arise in Lemma D.1.

The proposition below can be viewed as a Gram matrix version of Proposition 3.1.

Proposition D.1 *Given a $\mathbb{Z}$SCVP oracle $\mathcal{O}$, which takes a Gram matrix $\mathbf{G}$ as input, subject to the condition that $\mathbf{G} \cong \mathbf{I}_n$, and returns a shortest vector in $\chi(\mathbf{G})$. Then we can sample uniformly and independently from the set of shortest characteristic vectors in $\chi(\mathbf{G})$.*

Proof. Given the Gram matrix $\mathbf{G}$, we first obtain $(\mathbf{G}_1, \mathbf{U}_1) \leftarrow \mathcal{B}(\mathbf{G})$ according to Lemma D.1. We then call the $\mathbb{Z}$SCVP oracle $\mathcal{O}$, taking $\mathbf{G}_1$ as input to obtain a shortest characteristic vector $\mathbf{z}_1 \in \chi(\mathbf{G}_1)$ satisfying $\mathbf{z}_1^\top \mathbf{G}_1 \mathbf{z}_1 = n$. Finally, we compute $\mathbf{U}_1\mathbf{z}_1$, which can be easily verified to be a shortest characteristic vector of $\mathbf{G}$.

We claim that $\mathbf{U}_1\mathbf{z}_1$ is uniformly distributed in the set of shortest characteristic vectors of $\mathbf{G}$. In other words, the probability

$$\Pr_{(\mathbf{G}_1,\mathbf{U}_1)\leftarrow\mathcal{B}(\mathbf{G})}[\mathbf{U}_1\mathcal{O}(\mathbf{G}_1) = \mathbf{z}] \tag{15}$$

is identical for any shortest characteristic vector $\mathbf{z} \in \chi(\mathbf{G})$. Since the set of shortest characteristic vector of $\mathbf{G}$ can be written as $\{\mathbf{V}\mathbf{z} : \mathbf{V} \in \mathrm{Stab}(\mathbf{G})\}$, it suffices to show that $\Pr[\mathbf{U}_1\mathcal{O}(\mathbf{G}_1) = \mathbf{z}] = \Pr[\mathbf{U}_1\mathcal{O}(\mathbf{G}_1) = \mathbf{V}\mathbf{z}]$ for any $\mathbf{V}^{-1} \in \mathrm{Stab}(\mathbf{G})$. Note that

$$\begin{aligned}
&\Pr_{(\mathbf{G}_1,\mathbf{U}_1)\leftarrow\mathcal{B}(\mathbf{G})}[\mathbf{U}_1\mathcal{O}(\mathbf{G}_1) = \mathbf{z}] \\
&= \Pr_{(\mathbf{G}_1,\mathbf{V}^{-1}\mathbf{U}_1)\leftarrow\mathcal{B}(\mathbf{G})}[\mathbf{V}^{-1}\mathbf{U}_1\mathcal{O}(\mathbf{G}_1) = \mathbf{z}] \\
&= \Pr_{(\mathbf{G}_1,\mathbf{U}_1)\leftarrow\mathcal{B}(\mathbf{G})}[\mathbf{V}^{-1}\mathbf{U}_1\mathcal{O}(\mathbf{G}_1) = \mathbf{z}] \\
&= \Pr_{(\mathbf{G}_1,\mathbf{U}_1)\leftarrow\mathcal{B}(\mathbf{G})}[\mathbf{U}_1\mathcal{O}(\mathbf{G}_1) = \mathbf{V}\mathbf{z}].
\end{aligned}$$

The first equality results from a simple substitution of the variable, while the second equality is derived from Lemma D.1. As a result, the uniformity holds.

To demonstrate the independence of $\mathbf{U}_1\mathbf{z}_1$ for each trial, we can examine the joint distribution by utilizing the above method and taking into account that the randomness used in $\mathcal{B}(\mathbf{G})$ are independent. The proof is analogous to that of Proposition 3.1. □

Theorem D.1 *There is an efficient randomized reduction from* $\mathbb{Z}$*LIP to* $\mathbb{Z}$*SCVP in the same dimension.*

Proof. Given a matrix $\mathbf{G} \cong \mathbf{I}_n$ and suppose that we have access to a $\mathbb{Z}$SCVP oracle $\mathcal{O}$ as described in Proposition D.1. Our goal is to obtain a unimodular matrix $\mathbf{U}$ such that $\mathbf{G} = \mathbf{U}^\top \mathbf{U}$.

First, we apply the Cholesky decomposition to decompose $\mathbf{G} = \mathbf{B}^\top \mathbf{B}$, where $\mathcal{L}(\mathbf{B}) \cong \mathbb{Z}^n$. Note that $\mathbf{z} \in \chi(\mathbf{G})$ if and only if $\mathbf{Bz} \in \chi(\mathcal{L}(\mathbf{B}))$. Using Proposition D.1, we can uniformly and independently sample shortest characteristic vectors in $\chi(\mathbf{G})$ and transform them into $\chi(\mathcal{L}(\mathbf{B}))$. Finally, by Proposition 3.2, we can obtain an $\mathbf{O}$ such that $\mathcal{L}(\mathbf{B}) = \mathbf{O}\mathbb{Z}^n$ and then compute $\mathbf{U} = \mathbf{O}^{-1}\mathbf{B}$. It can be easily verified that $\mathbf{U}$ is unimodular and $\mathbf{G} = \mathbf{U}^\top \mathbf{U}$. □

Remark 4. In the proof, we transform the characteristic vectors into the basis form. We note that the precision issue in this step can be disregarded for two reasons: 1) An arbitrarily accurate approximation of a basis can be extracted from a Gram matrix using the Cholesky decomposition. 2) Given a sufficiently accurate approximation of a purported orthogonal transformation, it is possible to verify if it corresponds to a true lattice isomorphism by extracting the corresponding unimodular matrix $\mathbf{U}$ and checking the equality $\mathbf{G} = \mathbf{U}^\top \mathbf{U}$, which only involves exact arithmetic.

D.2 A Reduction from $\mathbb{Z}$LIP to $\mathbb{Z}$SVP

Theorem D.2 *There is an efficient randomized reduction from* $\mathbb{Z}$*LIP to* $\mathbb{Z}$*SVP in the same dimension.*

Proof. Given a matrix $\mathbf{G} \cong \mathbf{I}_n$ and suppose that we have access to a $\mathbb{Z}$SVP oracle $\mathcal{O}$, which takes a Gram matrix $\mathbf{G}'$ as input, subject to the condition that $\mathbf{G}' \cong \mathbf{I}_n$, and returns a shortest vector $\mathbf{z} \in \mathbb{Z}^n$ such that $\mathbf{z}^\top \mathbf{G}' \mathbf{z} = 1$.

From Lemma 2.9, we can deduce that $\mathrm{Stab}(\mathbf{G})$ acts transitively on the set of shortest vectors of $\mathbf{G}$, i.e., $\{\mathbf{z} \in \mathbb{Z}^n : \mathbf{z}^\top \mathbf{G} \mathbf{z} = 1\}$. By invoking the $\mathbb{Z}$SVP oracle with the randomization framework in the Gram matrix version, we can obtain vectors that are independently and uniformly distributed over the set of shortest vectors of $\mathbf{G}$. Then we can sample $O(n\mathrm{log}n)$ shortest vectors to get a set of linearly independent ones, e.g., $\{\mathbf{z}_1, \ldots, \mathbf{z}_n\}$. Define $\mathbf{V} = (\mathbf{z}_1, \ldots, \mathbf{z}_n)$. For any $\mathbf{B} \in \mathbb{R}^{n \times n}$ such that $\mathbf{G} = \mathbf{B}^\top \mathbf{B}$, it has $\{\mathbf{Bz}_1, \ldots, \mathbf{Bz}_n\}$ is a set of independent shortest vectors in $\mathcal{L}(\mathbf{B})$. It follows that $\mathbf{V}^\top \mathbf{G} \mathbf{V} = \mathbf{V}^\top \mathbf{B}^\top \mathbf{B} \mathbf{V} = \mathbf{I}_n$, which completes the proof. □

D.3 A Reduction from $\mathbb{Z}$SVP to γ-$\mathbb{Z}$SVP

Theorem D.3 *There is an efficient randomized reduction from* $\mathbb{Z}$*LIP to* γ-$\mathbb{Z}$*SVP for any constant* $\gamma = O(1)$ *in the same dimension.*

Proof. Given a matrix $\mathbf{G} \cong \mathbf{I}_n$ and suppose that we have access to a γ-$\mathbb{Z}$SVP oracle $\mathcal{O}$, which takes a Gram matrix $\mathbf{G}'$ as input, subject to the condition that $\mathbf{G}' \cong \mathbf{I}_n$, and returns a vector $\mathbf{z} \in \mathbb{Z}^n$ such that $\mathbf{z}^\top \mathbf{G}' \mathbf{z} \leq \gamma$.

Let $X_\gamma = \{\mathbf{z} \in \mathbb{Z}^n : \mathbf{z}^\top \mathbf{G} \mathbf{z} \leq \gamma\}$. By Lemma 2.1, we have $|X_\gamma| \leq n^c$ for some constant c. Also, it can be deduced from Lemma 2.9 that $\mathrm{Stab}(\mathbf{G})$ acts on X_γ by $(\mathbf{U} \in \mathrm{Stab}(\mathbf{G}), \mathbf{v} \in X_\gamma) \to \mathbf{U}\mathbf{v} \in X_\gamma$. Using the randomization framework, we can invoke the γ-$\mathbb{Z}$SVP oracle $m = \mathit{poly}(n)$ times, where $m > n^c$, to obtain a vector set $\{\mathbf{z}_1, \ldots, \mathbf{z}_m\}$. We then compute $\mathbf{z}_i - \mathbf{z}_j$ for all $i, j \in [m]$ and check if it is a multiple of a shortest vector. As shown in Theorem 3.2, the probability that $\mathbf{z}_i - \mathbf{z}_j$ is a multiple of a shortest vector of $\mathbf{G}$ is at least $1/n^c$. By repeating the whole process $O(n^{c+1})$ times, we can obtain a shortest vector in $\mathbf{G}$ with an overwhelming probability. □

D.4 A Reduction from ℤLIP to ℤLAP

Theorem D.4 *There is an efficient randomized reduction from* $\mathbb{Z}$*LIP to* $\mathbb{Z}$*LAP.*

Proof. Given a matrix $\mathbf{G} \cong \mathbf{I}_n$ and suppose that we have access to a $\mathbb{Z}$LAP oracle $\mathcal{O}$, which takes a Gram matrix $\mathbf{G}'$ as input, subject to the condition that $\mathbf{G}' \cong \mathbf{I}_n$, and returns a unimodular matrix $\mathbf{V}' \in \mathrm{Stab}(\mathbf{G}')$ and $\mathbf{V}' \neq \pm \mathbf{I}_n$.

To begin with, we show how to obtain random matrices in $\mathrm{Stab}(\mathbf{G})$ by invoking the $\mathbb{Z}$LAP oracle $\mathcal{O}$. As in Proposition D.1, we first generate $(\mathbf{G}', \mathbf{U}') \leftarrow \mathcal{B}(\mathbf{G})$ according to Lemma D.1. Then by invoking the $\mathbb{Z}$LAP oracle $\mathcal{O}$ and taking $\mathbf{G}'$ as input, we obtain a $\mathbf{V}' \in \mathrm{Stab}(\mathbf{G}')$ such that $\mathbf{V}' \neq \pm \mathbf{I}_n$. This allows us to obtain a $\mathbf{U}'\mathbf{V}'\mathbf{U}'^{-1} \in \mathrm{Stab}(\mathbf{G}')$.

Next, we use the Cholesky decomposition to decompose $\mathbf{G} = \mathbf{B}^\top \mathbf{B}$. Since $\mathrm{Stab}(\mathbf{G}) \cong \mathrm{Aut}(\mathcal{L}(\mathbf{B}))$, the operations in Section 4.1 can be transformed into the Gram matrix form. Specifically, finding the eigenspace X_1 of $\mathbf{B}\mathbf{V}\mathbf{B}^{-1} \in \mathrm{Aut}(\mathcal{L}(\mathbf{B}))$ is equivalent to finding the eigenspace X_2 of $\mathbf{V} \in \mathrm{Stab}(\mathbf{G})$ for the same eigenvalue such that $X_1 = \mathbf{B}X_2$, where $\mathbf{V}$ acts on $\mathbb{R}^n$ by $(\mathbf{V}, \mathbf{x} \in \mathbb{R}^n) \to \mathbf{V}\mathbf{x} \in \mathbb{R}^n$. Moreover, the corresponding induced sub-lattices are $V_1 \cap \mathcal{L}(\mathbf{B})$ and $V_2 \cap \mathbb{Z}^n$ respectively. Other operations in Section 4.1 can be directly converted to the Gram matrix form. Then, we can efficiently sample from a conjugacy class $\mathfrak{C}_{\mathbf{V}} = \{\mathbf{W}\mathbf{V}\mathbf{W}^{-1} : \mathbf{W} \in \mathrm{Stab}(\mathbf{G})\}$ of $\mathrm{Stab}(\mathbf{G})$, where $\mathbf{V} \in \mathrm{Stab}(\mathbf{G})$ corresponds to an automorphism $\phi \in \mathrm{Aut}(\mathcal{L}(\mathbf{B}))$ with $\phi \sim \mathbf{T}_{i,j,k}$. Next, we use Lemma 2.9 to transform these samples in $\mathfrak{C}_{\mathbf{V}}$ into automorphisms in $\mathrm{Aut}(\mathcal{L}(\mathbf{B}))$. Finally, we employ Proposition 4.2 to obtain an $\mathbf{O}$ such that $\mathcal{L}(\mathbf{B}) = \mathbf{O}\mathbb{Z}^n$ and compute $\mathbf{U} = \mathbf{O}^{-1}\mathbf{B}$. It can be easily verified that $\mathbf{U}$ is unimodular and $\mathbf{G} = \mathbf{U}^\top \mathbf{U}$. □

D.5 A Reduction from LAP to LIP

Theorem D.5 *There is an efficient randomized reduction from LAP to LIP in the same dimension.*

Proof. Given a Gram matrix $\mathbf{G}$ and suppose that we have access to an LIP oracle $\mathcal{O}$, which takes two Gram matrices $\mathbf{G}_1, \mathbf{G}_2$ as input, and returns a unimodular matrix $\mathbf{U}$ such that $\mathbf{U}^\top \mathbf{G}_2 \mathbf{U} = \mathbf{G}_1$.

To begin with, we obtain $(\mathbf{G}_1, \mathbf{U}_1) \leftarrow \mathcal{B}(\mathbf{G})$ according to Lemma D.1. Then we call the LIP oracle $\mathcal{O}$ with input $\mathbf{G}, \mathbf{G}_1$, and get a unimodular matrix $\mathbf{U}$ such that $\mathbf{U}^\top \mathbf{G}\mathbf{U} = \mathbf{G}_1$. For any $\mathbf{V}, \mathbf{V}_0 \in \mathrm{Stab}(\mathbf{G})$, it can be deduced that

$$\begin{aligned}
&\Pr_{(\mathbf{G}_1,\mathbf{U}_1)\leftarrow\mathcal{B}(\mathbf{G})}[\mathcal{O}(\mathbf{G}_1)\mathbf{U}_1^{-1} = \mathbf{V}] \\
=\ &\Pr_{(\mathbf{G}_1,\mathbf{V}_0\mathbf{U}_1)\leftarrow\mathcal{B}(\mathbf{G})}[\mathcal{O}(\mathbf{G}_1)(\mathbf{V}_0\mathbf{U}_1)^{-1} = \mathbf{V}] \\
=\ &\Pr_{(\mathbf{G}_1,\mathbf{U}_1)\leftarrow\mathcal{B}(\mathbf{G})}[\mathcal{O}(\mathbf{G}_1)(\mathbf{V}_0\mathbf{U}_1)^{-1} = \mathbf{V}] \\
=\ &\Pr_{(\mathbf{G}_1,\mathbf{U}_1)\leftarrow\mathcal{B}(\mathbf{G})}[\mathcal{O}(\mathbf{G}_1)\mathbf{U}_1^{-1} = \mathbf{V}\mathbf{V}_0].
\end{aligned}$$

Thus $\mathcal{O}(\mathbf{G}, \mathbf{G}_1)\mathbf{U}_1^{-1}$ is uniformly distributed in $\mathrm{Stab}(\mathbf{G})$. Thus if $\mathrm{Stab}(\mathbf{G}) \neq \{\pm\mathbf{I}_n\}$, we can efficiently obtain a nontrivial elements from $\mathrm{Stab}(\mathbf{G})$ with an overwhelming probability by repeating the above process $O(n)$ times. □

Appendix E Proof of Lemma 4.6

Proof. Let $\mathcal{D}$ be the set of $n \times n$ diagonal matrices whose diagonal entries are ± 1. Then $\mathcal{D}$ forms a subgroup of $\mathcal{S}_n^{\pm}$, and $\mathcal{S}_n^{\pm}$ is the semidirect product of $\mathcal{D}$ and $\mathcal{S}_n$.[6] For $\phi_0 \in \mathrm{Aut}(\mathcal{L})$ and $\phi_0 \sim \mathbf{T}_{k_1,k_2,l}$, let $\mathbf{O} \in \mathcal{O}_n(\mathbb{R})$ such that $\mathcal{L} = \mathbf{O}\mathbb{Z}^n$, then it has $\mathfrak{C}_{\phi_0} = \{\mathbf{O}\mathbf{T}\mathbf{T}_{k_1,k_2,l}\mathbf{T}^{-1}\mathbf{O}^{-1} : \mathbf{T} \in \mathcal{S}_n^{\pm}\}$. Denote $\mathbf{y} = \mathbf{O}^{-1}\mathbf{x} = (x_1, \cdots, x_n)$.[7]

For $k = 1$, it has

$$\begin{aligned}
g_1(\mathbf{x}) = \mathbb{E}[\langle \phi\mathbf{x}, \mathbf{x}\rangle] &= \frac{1}{|\mathcal{S}_n^{\pm}|} \sum_{\mathbf{T}\in\mathcal{S}_n^{\pm}} \langle \mathbf{O}\mathbf{T}\mathbf{T}_{k_1,k_2,l}\mathbf{T}^{-1}\mathbf{O}^{-1}\mathbf{x}, \mathbf{x}\rangle \\
&= \frac{1}{|\mathcal{S}_n^{\pm}|} \sum_{\mathbf{P}\in\mathcal{S}_n} \sum_{\mathbf{D}\in\mathcal{D}} \langle \mathbf{O}\mathbf{P}\mathbf{D}\mathbf{T}_{k_1,k_2,l}\mathbf{D}^{-1}\mathbf{P}^{-1}\mathbf{O}^{-1}\mathbf{x}, \mathbf{x}\rangle \\
&= \frac{1}{|\mathcal{S}_n^{\pm}|} \sum_{\mathbf{P}\in\mathcal{S}_n} \sum_{\mathbf{D}\in\mathcal{D}} \langle \mathbf{D}\mathbf{T}_{k_1,k_2,l}\mathbf{D}^{-1}\mathbf{P}^{-1}\mathbf{O}^{-1}\mathbf{x}, \mathbf{P}^{-1}\mathbf{O}^{-1}\mathbf{x}\rangle \\
&= \frac{1}{|\mathcal{S}_n^{\pm}|} \sum_{\mathbf{P}\in\mathcal{S}_n} \sum_{\mathbf{D}\in\mathcal{D}} \langle \mathbf{D}\mathbf{T}_{k_1,k_2,l}\mathbf{D}^{-1}\mathbf{P}^{-1}\mathbf{y}, \mathbf{P}^{-1}\mathbf{y}\rangle.
\end{aligned}$$

Denote $\mathbf{W}_{k_1,k_2,l} = \mathrm{diag}\{\mathbf{0}_{2l}, -\mathbf{I}_{k_1}, \mathbf{I}_{k_2}\}$, where $\mathbf{0}_{2l}$ is the $2l \times 2l$ zero matrix. Then it has $\sum_{D\in\mathcal{D}} \mathbf{D}\mathbf{T}_{k_1,k_2,l}\mathbf{D}^{-1} = |\mathcal{D}| \cdot \mathbf{W}_{k_1,k_2,l}$, and thus

$$\begin{aligned}
g_1(\mathbf{x}) &= \frac{|\mathcal{D}|}{|\mathcal{S}_n^{\pm}|} \sum_{\mathbf{P}\in\mathcal{S}_n} \langle \mathbf{W}_{k_1,k_2,l}\mathbf{P}^{-1}\mathbf{y}, \mathbf{P}^{-1}\mathbf{y}\rangle \\
&= \frac{1}{|\mathcal{S}_n|} \sum_{\mathbf{P}\in\mathcal{S}_n} (-(x_{\mathbf{P}(2l+1)}^2 + \cdots + x_{\mathbf{P}(2l+k_1)}^2) + (x_{\mathbf{P}(2l+k_1+1)}^2 + \cdots + x_{\mathbf{P}(n)}^2)) \\
&= \frac{-k_1 + k_2}{n}(x_1^2 + \cdots + x_n^2) = \frac{k_2 - k_1}{n} \|\mathbf{x}\|^2,
\end{aligned}$$

[6] 'Semidirect product' means that $\mathcal{S}_n^{\pm} = \mathcal{D}\mathcal{S}_n$, $\mathcal{D} \cap \mathcal{S}_n = \{\mathbf{I}_n\}$ and $\mathcal{D}$ is a normal subgroup of $\mathcal{S}_n^{\pm}$. This implies that for any $\mathbf{T} \in \mathcal{S}_n^{\pm}$, there exist unique $\mathbf{D} \in \mathcal{D}$ and $\mathbf{P} \in \mathcal{S}_n$ such that $\mathbf{T} = \mathbf{P}\mathbf{D}$.

[7] This is consistent with the notation $x_i = \langle \mathbf{x}, \mathbf{v}_i\rangle$ in Section 4.2.

where $\mathbf{P}(i)$ represents the row number of the '1' in $\mathbf{P}$'s i-th column.

For $k = 2$, it has

$$\begin{aligned} g_2(\mathbf{x}) &= \frac{1}{|\mathcal{S}_n^{\pm}|} \sum_{\mathbf{T} \in \mathcal{S}_n^{\pm}} \langle \mathbf{O}\mathbf{T}\mathbf{T}_{k_1,k_2,l}\mathbf{T}^{-1}\mathbf{O}^{-1}\mathbf{x}, \mathbf{x} \rangle^2 \\ &= \frac{1}{|\mathcal{S}_n^{\pm}|} \sum_{\mathbf{P} \in \mathcal{S}_n} \sum_{\mathbf{D} \in \mathcal{D}} \langle \mathbf{D}\mathbf{T}_{k_1,k_2,l}\mathbf{D}^{-1}\mathbf{P}^{-1}\mathbf{O}^{-1}\mathbf{x}, \mathbf{P}^{-1}\mathbf{O}^{-1}\mathbf{x} \rangle^2 \\ &= \frac{1}{|\mathcal{S}_n^{\pm}|} \sum_{\mathbf{P} \in \mathcal{S}_n} \sum_{\mathbf{D} \in \mathcal{D}} \langle \mathbf{D}\mathbf{T}_{k_1,k_2,l}\mathbf{D}^{-1}\mathbf{P}^{-1}\mathbf{y}, \mathbf{P}^{-1}\mathbf{y} \rangle^2. \end{aligned}$$

For fixed $\mathbf{P} \in \mathcal{S}_n$ and $\mathbf{D} \in \mathcal{D}$, denote $\mathbf{z} = \mathbf{P}^{-1}y = (z_1, \cdots, z_n)$ and $\mathbf{D} = \mathbf{D}^{-1} = \mathrm{diag}\{d_1, \cdots, d_n\}$, where $d_i = \pm 1$. Then it has

$$\begin{aligned} \mathbf{D}\mathbf{T}_{k_1,k_2,l}\mathbf{D}^{-1}\mathbf{z} = (&d_1 d_2 z_2, d_1 d_2 z_1, \ldots, d_{2l-1}d_{2l}z_{2l}, d_{2l-1}d_{2l}z_{2l-1}, \\ &- z_{2l+1}, \ldots, -z_{2l+k_1}, z_{2l+k_1+1}, \ldots, z_n), \end{aligned}$$

and $\langle \mathbf{D}\mathbf{T}_{k_1,k_2,l}\mathbf{D}^{-1}\mathbf{z}, \mathbf{z} \rangle = \sum_{i=1}^{l} 2d_{2i-1}d_{2i}z_{2i-1}z_{2i} - \sum_{i=2l+1}^{2l+k_1} z_i^2 + \sum_{i=2l+k_1+1}^{n} z_i^2$. It follows that

$$\begin{aligned} \sum_{\mathbf{D} \in \mathcal{D}} \langle \mathbf{D}\mathbf{T}_{k_1,k_2,l}\mathbf{D}^{-1}\mathbf{z}, \mathbf{z} \rangle^2 = |\mathcal{D}| \Bigg(&4\sum_{i=1}^{l} z_{2i-1}^2 z_{2i}^2 + \sum_{i=2l+1}^{n} z_i^4 + \sum_{2l+1 \le i,j \le 2l+k_1} z_i^2 z_j^2 \\ &-2 \sum_{\substack{2l+1 \le i \le 2l+k_1 \\ 2l+k_1+1 \le j \le n}} z_i^2 z_j^2 + \sum_{2l+k_1+1 \le i,j \le n} z_i^2 z_j^2 \Bigg). \end{aligned}$$

Observe that $z_i = x_{\mathbf{P}(i)}$ for $1 \le i \le n$, then it can be deduced that

$$\begin{aligned} g_2(\mathbf{x}) &= \frac{1}{|\mathcal{S}_n^{\pm}|} \sum_{\mathbf{P} \in \mathcal{S}_n} \sum_{\mathbf{D} \in \mathcal{D}} \langle \mathbf{D}\mathbf{T}_{k_1,k_2,l}\mathbf{D}^{-1}\mathbf{z}, \mathbf{z} \rangle^2 \\ &= \frac{4l + k_1(k_1-1) - 2k_1k_2 + k_2(k_2-1)}{n(n-1)} \sum_{1 \le i,j \le n} x_i^2 x_j^2 + \frac{(n-2l)}{n} \sum_{1 \le i \le n} x_i^4 \\ &= \frac{6l + (k_1-k_2)^2 - n}{n(n-1)} \sum_{1 \le i,j \le n} x_i^2 x_j^2 + \frac{(n-2l)}{n} \sum_{1 \le i \le n} x_i^4 \\ &= \frac{n^2 - 2nl - (k_1-k_2)^2 - 4l}{n(n-1)} \sum_{i=1}^{n} {x_i}^4 + \frac{6l + (k_1-k_2)^2 - n}{n(n-1)} (\sum_{i=1}^{n} {x_i}^2)^2. \end{aligned}$$

□

Appendix F Recover the Exact Shortest Vectors in Proposition 4.2

In this appendix, we demonstrate how to recover the exact shortest vectors by using good enough approximations of the shortest vectors of $\mathcal{L}$ and automorphisms of $\mathrm{Aut}(\mathcal{L})$, thereby completing Proposition 4.2. In fact, this can be reduced to the following problem.

Problem F.1 *Suppose n is odd. Given a basis $\mathbf{B}$ of a lattice $\mathcal{L} \cong \mathbb{Z}^n$, a polynomial number of automorphisms $\phi_1, \phi_2, \ldots, \phi_{p(n)} \in \mathrm{Aut}(\mathcal{L})$ that are drawn uniformly and independently from a conjugacy class $\mathfrak{C}_{\phi_0}$, where $\phi_0 \sim \mathbf{T}_{k_1,k_2,l}$ and k_1, k_2, l are fixed, and an approximation of a set of independent shortest vectors $\mathbf{v}_i$, i.e., $\{\tilde{\mathbf{v}}_1, \ldots, \tilde{\mathbf{v}}_n\}$ such that $\tilde{\mathbf{v}}_i = \mathbf{v}_i + \boldsymbol{\epsilon}_i$ and $\|\boldsymbol{\epsilon}_i\| \leq n^{-c}$. The goal is to find the shortest vectors of $\mathcal{L}$, i.e., $\mathbf{V} = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$.*

Note that for any $\phi \in \mathfrak{C}_{\phi_0}$, it has $\phi = \mathbf{VSV}^{-1}$, where $\mathbf{S} \in \mathcal{S}_n^{\pm}$ and $\mathbf{S} \sim \mathbf{T}_{k_1,k_2,l}$ (i.e., $\exists \mathbf{T} \in \mathcal{S}_n^{\pm}$ such that $\mathbf{S} = \mathbf{T}\mathbf{T}_{k_1,k_2,l}\mathbf{T}^{-1}$), and ϕ acts on the set of shortest vectors $\{\pm\mathbf{v}_1, \ldots, \pm\mathbf{v}_n\}$. Then for $1 \leq i, j \leq n$, it has $\|\phi\mathbf{v}_i \pm \mathbf{v}_j\| = 0$ or 2 and

$$\left|\|\phi\tilde{\mathbf{v}}_i \pm \tilde{\mathbf{v}}_j\| - \|\phi\mathbf{v}_i \pm \mathbf{v}_j\|\right| \leq \|\phi\boldsymbol{\epsilon}_i \pm \boldsymbol{\epsilon}_j\| \leq 2n^{-c}. \tag{16}$$

Thus, for any given $\phi \in \mathfrak{C}_{\phi_0}$, we can decide whether $\|\phi\mathbf{v}_i \pm \mathbf{v}_j\| = 0$, and thus exactly recover the corresponding matrix $\mathbf{S} \in \mathcal{S}_n^{\pm}$.

Next, we demonstrate that, for the given automorphisms $\phi_1, \phi_2, \ldots, \phi_{p(n)} \in \mathfrak{C}_{\phi_0}$ and the corresponding matrices $\mathbf{S}_i \in \mathcal{S}_n^{\pm}, 1 \leq i \leq p(n)$, such that $\phi_i = \mathbf{V}\mathbf{S}_i\mathbf{V}^{-1}$, we can efficiently recover $\mathbf{V}$. For $\phi, \mathbf{S} \in \mathbb{R}^{n\times n}$, define $K(\phi, \mathbf{S}) := \{\mathbf{X} \in \mathbb{R}^{n\times n} : \mathbf{XSX}^{-1} = \phi\}$. Then clearly, $K(\phi, \mathbf{S})$ is an $\mathbb{R}$-linear space, and $\mathbf{V} \in K(\phi_i, \mathbf{S}_i)$. Moreover,

$$\begin{aligned} K(\phi_i, \mathbf{S}_i) &= \{\mathbf{X} : \mathbf{X}\mathbf{S}_i\mathbf{X}^{-1} = \mathbf{V}\mathbf{S}_i\mathbf{V}^{-1}\} \\ &= \{\mathbf{X} : (\mathbf{V}^{-1}\mathbf{X})\mathbf{S}_i(\mathbf{V}^{-1}\mathbf{X})^{-1} = \mathbf{S}_i\} \\ &= \{\mathbf{VX} : \mathbf{X}\mathbf{S}_i\mathbf{X}^{-1} = \mathbf{S}_i\} \\ &= \mathbf{V} \cdot \{\mathbf{X} : \mathbf{X}\mathbf{S}_i\mathbf{X}^{-1} = \mathbf{S}_i\} \\ &= \mathbf{V} \cdot K(\mathbf{S}_i, \mathbf{S}_i). \end{aligned}$$

Therefore, $\mathbf{V} \in \mathbf{V} \cdot \bigcap_{i=1}^{p(n)} K(\mathbf{S}_i, \mathbf{S}_i)$. Note that $K(\mathbf{S}_i, \mathbf{S}_i)$ is a subgroup of $\mathcal{S}_n^{\pm}$. Let $\mathbf{T}_i \in \mathcal{S}_n^{\pm}$ such that $\mathbf{S}_i = \mathbf{T}_i\mathbf{T}_{k_1,k_2,l}\mathbf{T}_i^{-1}$. Then it has

$$\begin{aligned} K(\mathbf{S}_i, \mathbf{S}_i) &= \{\mathbf{X} : \mathbf{X}\mathbf{S}_i\mathbf{X}^{-1} = \mathbf{S}_i\} \\ &= \{\mathbf{X} : \mathbf{X}\mathbf{T}_i\mathbf{T}_{k_1,k_2,l}\mathbf{T}_i^{-1}\mathbf{X}^{-1} = \mathbf{T}_i\mathbf{T}_{k_1,k_2,l}\mathbf{T}_i^{-1}\} \\ &= \{\mathbf{X} : (\mathbf{T}_i^{-1}\mathbf{X}\mathbf{T}_i)\mathbf{T}_{k_1,k_2,l}(\mathbf{T}_i^{-1}\mathbf{X}\mathbf{T}_i)^{-1} = \mathbf{T}_{k_1,k_2,l}\} \\ &= \mathbf{T}_i K(\mathbf{T}_{k_1,k_2,l}, \mathbf{T}_{k_1,k_2,l})\mathbf{T}_i^{-1}. \end{aligned}$$

Since ϕ_i is drawn uniformly from the conjugacy class $\mathfrak{C}_{\phi_0}$, then $\mathbf{S}_i$ is distributed uniformly in the conjugacy class $\mathfrak{C}_{\mathbf{T}_{k_1,k_2,l}}$. Then from the group action perspective, the coset $\mathbf{T}_i K(\mathbf{T}_{k_1,k_2,l}, \mathbf{T}_{k_1,k_2,l})$ is distributed uniformly in the left cosets of $\mathbf{T}_{k_1,k_2,l}$ in $\mathcal{S}_n^{\pm}$. Equivalently, $K(\mathbf{S}_i, \mathbf{S}_i) = \mathbf{T}_i K(\mathbf{T}_{k_1,k_2,l}, \mathbf{T}_{k_1,k_2,l})\mathbf{T}_i^{-1}$ can be viewed as a random subgroup of $\mathcal{S}_n^{\pm}$ such that $\mathbf{T}_i$ is drawn uniformly at random from $\mathcal{S}_n^{\pm}$. There are two cases for $\mathbf{T}_{k_1,k_2,l}$.

Case 1. $l = 0$. In this case, it has $k_1, k_2 > 0$, and thus there exists $1 \leq a \neq b \leq n$ such that $\mathbf{T}_{k_1,k_2,l}\mathbf{e}_a = \mathbf{e}_a$ and $\mathbf{T}_{k_1,k_2,l}\mathbf{e}_b = -\mathbf{e}_b$ (we recall that $\{\mathbf{e}_a\}_{a\in[n]}$ is the standard basis). Thus, for an $\mathbf{X} \in K(\mathbf{T}_{k_1,k_2,l}, \mathbf{T}_{k_1,k_2,l})$, we have $\mathbf{e}_a^\top \mathbf{X}\mathbf{e}_b = -\mathbf{e}_a^\top \mathbf{X}\mathbf{T}_{k_1,k_2,l}\mathbf{e}_b = -\mathbf{e}_a^\top \mathbf{T}_{k_1,k_2,l}\mathbf{X}\mathbf{e}_b = -\mathbf{e}_a^\top \mathbf{X}\mathbf{e}_b$, i.e., $\mathbf{e}_a^\top \mathbf{X}\mathbf{e}_b = 0$. Similarly, it can be deduced that $\mathbf{e}_b^\top \mathbf{X}\mathbf{e}_a = 0$.

Therefore, for any $\mathbf{Y} \in K(\mathbf{S}_i, \mathbf{S}_i)$, we have $\mathbf{T}_i^\top \mathbf{Y}\mathbf{T}_i \in K(\mathbf{T}_{k_1,k_2,l}, \mathbf{T}_{k_1,k_2,l})$. It follows that $(\mathbf{T}_i\mathbf{e}_a)^\top \mathbf{Y}(\mathbf{T}_i\mathbf{e}_b) = (\mathbf{T}_i\mathbf{e}_b)^\top \mathbf{Y}(\mathbf{T}_i\mathbf{e}_a) = 0$. Note that $\mathbf{T}_i$ can be viewed as drawn uniformly at random from $\mathcal{S}_n^{\pm}$, and $\mathcal{S}_n^{\pm}$ acts transitively on all the pairs $\{(\pm\mathbf{e}_a, \pm\mathbf{e}_b) : 1 \leq a \neq b \leq n\}$. Thus, for a sufficiently large polynomial $p(n)$, it has $\mathbf{e}_a^\top \mathbf{Y}\mathbf{e}_b = \mathbf{e}_b^\top \mathbf{Y}\mathbf{e}_a = 0$ for all $1 \leq a \neq b \leq n$ and $\mathbf{Y} \in \bigcap_{i=1}^{p(n)} K(\mathbf{S}_i, \mathbf{S}_i)$. In other words, $\bigcap_{i=1}^{p(n)} K(\mathbf{S}_i, \mathbf{S}_i)$ consists of all diagonal matrices in $\mathbb{R}^{n\times n}$, i.e., $\bigcap_{i=1}^{p(n)} K(\phi_i, \mathbf{S}_i) = \{\mathbf{V}\cdot \mathrm{diag}\{d_1, \ldots, d_n\} : d_i \in \mathbb{R}\}$. Then $\mathbf{V}$ can be reconstructed by first computing an $\mathbb{R}$-linear basis of the space $\bigcap_{i=1}^{p(n)} K(\phi_i, \mathbf{S}_i)$ and then recovering each $\pm\mathbf{v}_i$ via vector normalization.

Case 2: $l \neq 0$. In this case, it has $k_1 \neq 0$ (or $k_2 \neq 0$). Thus we have $\mathbf{T}_{k_1,k_2,l}\mathbf{e}_1 = \mathbf{e}_2, \mathbf{T}_{k_1,k_2,l}\mathbf{e}_2 = \mathbf{e}_1$, and there exists $3 \leq j \leq n$ such that $\mathbf{T}_{k_1,k_2,l}\mathbf{e}_j = -\mathbf{e}_j$ (or $\mathbf{T}_{k_1,k_2,l}\mathbf{e}_j = \mathbf{e}_j$ if $k_2 \neq 0$). Then, by a similar deduction as in Case 1, we have $\mathbf{e}_1^\top \mathbf{X}\mathbf{e}_1 = \mathbf{e}_2^\top \mathbf{X}\mathbf{e}_2$, $\mathbf{e}_1^\top \mathbf{X}\mathbf{e}_2 = \mathbf{e}_2^\top \mathbf{X}\mathbf{e}_1$, and $\mathbf{e}_1^\top \mathbf{X}\mathbf{e}_j = -\mathbf{e}_2^\top \mathbf{X}\mathbf{e}_j$ (or $\mathbf{e}_1^\top \mathbf{X}\mathbf{e}_j = \mathbf{e}_2^\top \mathbf{X}\mathbf{e}_j$ if $k_2 \neq 0$) for all $j \in [n]$ and $\mathbf{X} \in K(\mathbf{T}_{k_1,k_2,l}, \mathbf{T}_{k_1,k_2,l})$.

Again, due to the transitivity of the action of $\mathcal{S}_n^{\pm}$ on $\{(\pm\mathbf{e}_a, \pm\mathbf{e}_b, \pm\mathbf{e}_c)\}$, we can deduce that for a large enough polynomial $p(n)$, it has $\mathbf{e}_a^\top \mathbf{Y}\mathbf{e}_a = \mathbf{e}_b^\top \mathbf{Y}\mathbf{e}_b$, $\mathbf{e}_a^\top \mathbf{Y}\mathbf{e}_b = \mathbf{e}_b^\top \mathbf{Y}\mathbf{e}_a$, and $\mathbf{e}_a^\top \mathbf{Y}\mathbf{e}_c = -\mathbf{e}_b^\top \mathbf{Y}\mathbf{e}_c$, $\mathbf{e}_a^\top \mathbf{Y}\mathbf{e}_c = \mathbf{e}_b^\top \mathbf{Y}\mathbf{e}_c$ for all $1 \leq a \neq b \neq c \leq n$ and $\mathbf{Y} \in \bigcap_{i=1}^{p(n)} K(\mathbf{S}_i, \mathbf{S}_i)$. In other words, $\bigcap_{i=1}^{p(n)} K(\mathbf{S}_i, \mathbf{S}_i) = \{h\mathbf{I}_n : h \in \mathbb{R}\}$. Then $\mathbf{V}$ can be reconstructed by first computing a nonzero matrix in $\bigcap_{i=1}^{p(n)} K(\phi_i, \mathbf{S}_i)$ and then performing normalization.