Commitment Schemes Based on Module-LIP

Hengyi Luo[1,2], Kaijie Jiang[3], Yanbin Pan[1,2(✉)], and Anyu Wang[3,4]

[1] State Key Laboratory of Mathematical Sciences, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, China
luohengyi23@mails.ucas.ac.cn, panyanbin@amss.ac.cn
[2] School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing, China
[3] Institute for Advanced Study, BNRist, Tsinghua University, Beijing, China
jkj21@mails.tsinghua.edu.cn, anyuwang@tsinghua.edu.cn
[4] Zhongguancun Laboratory, Beijing, China

Abstract. Recently, Jiang et al. (EUROCRYPT 2025) proposed a universal framework for constructing commitment schemes using group actions, and instantiated it with the Lattice Isomorphism Problem (LIP). This paper attempts to construct an instantiation based on module-LIP with this framework. More precisely, we first present a reduction from $\mathcal{O}_{\mathbb{L}}^2$-LIP to $\mathcal{O}_{\mathbb{L}}^2$-LAP. Then we develop a re-randomized algorithm based on the self-reduction framework of Module-LIP (Ducas et al. ASIACRYPT 2022), adapting it to the framework to construct commitment schemes.

Keywords: Lattice automorphism · module-LIP · Commitment

1 Introduction

Lattice-based cryptography has emerged as a leading candidate for post-quantum cryptography, offering robust security guarantees against quantum attacks. The hardness of problems such as the Shortest Vector Problem (SVP) and the Learning With Errors (LWE) problem forms the foundation for numerous cryptographic constructions, including encryption schemes and digital signatures. In recent years, the Lattice Isomorphism Problem (LIP) has gained significant attention due to its potential for developing efficient cryptographic protocols.

The Lattice Isomorphism Problem (LIP) asks whether two given lattices are isomorphic, i.e., whether there exists a bijective orthogonal transformation between them. This problem has been studied with a lot of advances in understanding its computational complexity and applications in cryptography. For example, Ducas and van Woerden [3] provided a worst-case to average-case reduction for LIP and proposed cryptographic schemes based on this problem, including a key encapsulation mechanism and a signature scheme. However, most existing works have focused on the application of LIP in signature and encryption schemes, leaving other cryptographic components relatively unexplored.

One notable application of LIP is the Hawk signature scheme, proposed by Ducas et al. [2]. Hawk is a concrete instantiation of proposals to use LIP as a

foundation for cryptography, focusing on simplicity and efficiency. By utilizing module lattices, Hawk achieves significant improvements in signing speed and signature size compared to existing lattice-based signature schemes. The security of Hawk is based on the hardness of the $\mathcal{O}_{\mathbb{L}}^2$-LIP problem, where $\mathcal{O}_{\mathbb{L}}^2$ denotes the module lattice structure over a cyclotomic number field $\mathbb{L}$.

Recently, Jiang et al. proposed a universal framework for constructing commitment schemes using group actions, and instantiated it with the LIP [5]. This marked the first application of LIP in cryptographic components beyond signatures and encryption, opening new avenues for leveraging the properties of LIP in diverse cryptographic contexts.

Our work builds on this foundation by providing a module lattice version of their framework. For this purpose, we firstly draw inspiration from the algorithmic framework presented in [10] to establish a reduction from $\mathcal{O}_{\mathbb{L}}^2$-LIP to $\mathcal{O}_{\mathbb{L}}^2$-LAP ($\mathcal{O}_{\mathbb{L}}^2$-Lattice Automorphism Problem). This reduction can be viewed as a structured analogue of the reduction from $\mathbb{Z}$-LIP to $\mathbb{Z}$-LAP presented in [6]. And then, we extend the self-reduction framework introduced in [2]. By adapting and extending this framework, we develop the necessary re-randomized algorithm required for the commitment scheme proposed in [5]. Our approach leverages the structured properties of module lattices to achieve improved efficiency and the security guarantee is based on $\mathcal{O}_{\mathbb{L}}^2$-LIP.

1.1 Our Contributions

The primary contributions of our work are as follows:

- We introduce a module lattice-structured reduction from $\mathcal{O}_{\mathbb{L}}^2$-LIP to $\mathcal{O}_{\mathbb{L}}^2$-LAP, extending the theoretical foundations of lattice isomorphism problems in the context of module lattices.
- We develop a re-randomized algorithm based on the self-reduction framework from [2], adapting it to the requirements of the commitment scheme proposed in [5].

Roadmap. The remainder of this paper is organized as follows. Section 2 provides the necessary background and preliminaries on lattice isomorphism problems, module lattices and group actions. Section 3 details our reduction from $\mathcal{O}_{\mathbb{L}}^2$-LIP to $\mathcal{O}_{\mathbb{L}}^2$-LAP. Section 4 presents the re-randomized algorithm needed in the construction framework.

2 Notations and preliminaries

2.1 Notations

- We use $x \leftarrow \mathcal{D}$ to denote that x is sampled from a distribution $\mathcal{D}$. In this paper, we focus solely on discrete distributions. For a finite set S, we write $s \leftarrow_{\$} S$ to indicate that s is drawn uniformly from S.

- The Euclidean norm of $a \in \mathbb{R}^n$ is denoted 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 rI_n to represent the matrix $\mathrm{diag}(r, r, \cdots, r)$, and sometimes use r to represent rI_n in matrix multiplications (such as $r\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} rx_1 \\ rx_2 \end{pmatrix}$). We will also emphasize this point from time to time in the proof.
- For a number field $\mathbb{K}$, the parameter $\mathbf{K}$ denotes degree of $\mathbb{K}$, $\log \Delta_{\mathbb{K}}$, and a basis of $\mathcal{O}_{\mathbb{K}}$.
- For x in a number field $\mathbb{K}$, we call x^* is the complex conjugation of x if $\sigma(x^*) = \overline{\sigma(x)}, \forall \sigma \in Hom_{\mathbb{Q}}(\mathbb{K}, \mathbb{C})$. For matrix $H = (h_{ij})$, let H^* denote $(h_{ij}^*)^T$ and $\overline{H}$ denote (h_{ij}^*) if all h_{ij}^* exist.
- For a ring A in a number field that are closed under complex conjugating, the unitary matrices over A is $\mathcal{U}_n(A) := \{T \in M_n(A) | T^*T = I_n\}$.
- For a number field $\mathbb{K}$, we use $\mu(\mathbb{K})$ to denote the roots of unity in $\mathbb{F}$. Note $\mu(\mathbb{K}) \subset \mathcal{O}_{\mathbb{K}}$ and $\mu(\mathbb{K}) = \mathcal{U}_1(\mathcal{O}_{\mathbb{K}})$

2.2 Lattices

A lattice is defined as a discrete additive subgroup of $\mathbb{R}^m$. Typically, one constructs a lattice by selecting n linearly independent vectors $b_1, b_2, \ldots, b_n$ in $\mathbb{R}^m$, so that every lattice element can be expressed as an integer linear combination of these basis vectors. In other words, if we denote the basis by $B = (b_1, \ldots, b_n)$, then the lattice $\mathcal{L}$ is given by $\{Bz : z \in \mathbb{Z}^n\}$, which defines a lattice of rank n in $\mathbb{R}^m$.

2.3 Number Theory

A number field $\mathbb{K}$ is a finite extension of the rational numbers $\mathbb{Q}$. Equivalently, any such field may be expressed as $\mathbb{Q}[X]/(P)$, where P is a monic irreducible polynomial whose degree matches that of the extension. For a field $\mathbb{K}$ of degree d, there exist exactly d embeddings $\sigma_1, \ldots, \sigma_d$ into $\mathbb{C}$. Those mappings that send $\mathbb{K}$ into $\mathbb{R}$ are called real embeddings, while the others, which occur in complex conjugate pairs, are referred to as complex embeddings. If we denote by r_1 the number of real embeddings and by r_2 the number of pairs of complex embeddings, then $d = r_1 + 2r_2$. A field is said to be totally real if $r_1 = d$, and totally imaginary if $2r_2 = d$.

Canonical embedding The **canonical embedding** of a number field $\mathbb{K}$ is defined by the mapping $\sigma : x \mapsto (\sigma_1(x), \ldots, \sigma_d(x))^T$, which sends elements into $\mathbb{C}^d$. Often, one identifies $\mathbb{K}$ with its image under this mapping so that the ring of integers $\mathcal{O}_{\mathbb{K}}$ acquires a lattice structure in $\mathbb{C}^d$. It is important to note, we are not representing elements in $\mathbb{K}$ using the canonical embedding. The norm on $\mathbb{K}$ is defined as $\mathcal{N}_{\mathbb{K}}(z) = \prod_{i=1}^{d} \sigma_i(z)$ and the trace as $\mathrm{Tr}_{\mathbb{K}}(z) = \sum_{i=1}^{d} \sigma_i(z)$. By considering the $\mathbb{Q}$-linear map $m_z : x \mapsto zx$, one sees that $\mathcal{N}_{\mathbb{K}}(z)$ equals the determinant of m_z and $\mathrm{Tr}_{\mathbb{K}}(z)$ equals its trace; notably, both quantities belong

to $\mathbb{Q}$.
We also have the **coefficient embedding** $\text{vec} : \mathbb{Q}[X]/(P) \to \mathbb{Q}^n, \quad a_0 + a_1 X + \cdots + a_{n-1}X^{n-1} \mapsto (a_0, a_1, \ldots, a_{n-1})^T$, which is an additive group isomorphism. When P is a cyclotomic polynomial of 2-power order, i.e., when $\mathbb{Q}[X]/(P)$ is a cyclotomic field of 2-power order, the canonical embedding and the coefficient embedding differ only by a scaling factor geometrically.

CM number field A CM (number) field $\mathbb{L}$ is a number field if it's a quadratic extension $\mathbb{L}/\mathbb{K}$ where the base field $\mathbb{K}$ is totally real but $\mathbb{L}$ is totally imaginary. The extension $\mathbb{L}/\mathbb{K}$ is a Galois extension and we denote the Galois group by $Gal(\mathbb{L}/\mathbb{K})$. There is a complex conjugation in $Gal(\mathbb{L}/\mathbb{K})$, i.e $\exists \tau \in Gal(\mathbb{L}/\mathbb{K})$ s.t. $\forall x \in \mathbb{L}, \sigma_i(\tau(x)) = \overline{\sigma_i(x)}$. We usually denote $\tau(x)$ by x^*. As an important example, the cyclotomic number fields are all CM number fields.

Rings of integer Let $\mathcal{O}_\mathbb{L}$ denote the ring of integers of a number field $\mathbb{L}$. $\mathcal{O}_\mathbb{L}$ is a free $\mathbb{Z}$-module of rank d. The discriminant of $\mathbb{L}$, denoted $\Delta_\mathbb{L}$, is defined as $(\det(\sigma_i(\alpha_j))_{i,j})^2 \in \mathbb{Z}$, where $(\alpha_j)_{1 \le j \le d}$ is any basis of $\mathcal{O}_\mathbb{L}$. Specifically, there exists some absolute constant $c > 1$ such that $\Delta_\mathbb{L} \ge c^d$ for all number fields $\mathbb{K}$. In particular, we always have $d = \text{poly}(\log \Delta_\mathbb{L})$.

2.4 $\mathcal{O}_\mathbb{L}^2$-LIP and $\mathcal{O}_\mathbb{L}^2$-LAP

In this paper, we focus on a special instance of the module-LIP: the LIP corresponding to the module lattice $\mathcal{O}_\mathbb{L}^2$, which is also the module-LIP used in HAWK. For simplicity, let $\mathbb{L}$ be a CM number field in this subsection.

Definition 2.1 ($\mathcal{O}_\mathbb{L}^2$ Lattice isomorphism Problem, $\mathcal{O}_\mathbb{L}^2$-LIP) *Given a quadratic form $G = U^*U$ where $U \in GL_2(\mathcal{O}_\mathbb{L})$, the objective is to find an W such that $G = W^*W$.*

Another related problem can be interpreted as the automorphism problem on $\mathcal{O}_\mathbb{L}^2$, where the $\mathcal{O}_\mathbb{L}^2$-automorphisms are defined as follows.

Definition 2.2 *Assume $B \in GL_2(\mathcal{O}_\mathbb{L})$ and $G = B^*B$. Define the module lattice automorphism group of G as $Aut_\mathbb{L}(G) := B^{-1}(\mathcal{U}_2(\mathcal{O}_\mathbb{L}))B$. And we call a module lattice automorphism $P \in Aut_\mathbb{L}(G)$ is non-trivial if $P \notin \mu(\mathbb{L})I_2$.*

Remark 1. It is noted that $Aut_\mathbb{L}(G)$ has another equivalent definition: $\{X \in \text{GL}_2(\mathcal{O}_\mathbb{L}) | X^*GX = G\}$. From this definition, it is clear that the automorphism group depends only on G.

The following lemma guarantees that the automorphism group is not very large. Consequently, once an automorphism is obtained, we can guess its form.

Lemma 2.1 ([10, Lemma 3.1]) *Let $\mathbb{L}$ be a CM number field with degree $2d$. Then*

$$\mathcal{U}_2(\mathcal{O}_\mathbb{L}) = \{\begin{pmatrix}\xi_1 & 0\\ 0 & \xi_2\end{pmatrix} | \xi_1, \xi_2 \in \mu(\mathbb{L})\} \bigcup \{\begin{pmatrix}0 & \xi_1\\ \xi_2 & 0\end{pmatrix} | \xi_1, \xi_2 \in \mu(\mathbb{L})\}.$$

Furthermore, $\sharp(\mathcal{U}_2(\mathcal{O}_\mathbb{L})) \leq 2\sharp(\mu(\mathbb{L}))^2 \leq 128d^4$.

Definition 2.3 ($\mathcal{O}_\mathbb{L}^2$ Lattice Automorphism Problem, $\mathcal{O}_\mathbb{L}^2$-LAP) *Given a quadratic form $G = U^*U$ where $U \in GL_2(\mathcal{O}_\mathbb{L})$, the objective is to find an non-trivial module lattice automorphism automorphism $P \in Aut_\mathbb{L}(G)$.*

2.5 Algorithmic consideration

Representation of ideals and modules Assume $B_{\mathcal{O}_\mathbb{L}} = (\alpha_j)_{j=1,\ldots,d}$ is a basis of $\mathcal{O}_\mathbb{K}$. We represent elements in $\mathbb{L}$ by their coordinates in the basis $B_{\mathcal{O}_\mathbb{L}}$, which is a vector in $\mathbb{Q}^d$. For $x \in \mathbb{L}$ represented by the vector $(x_1, \ldots, x_d)^T \in \mathbb{Q}^d$, we define $\mathrm{size}(x) := \sum_i \mathrm{size}(x_i)$, where $\mathrm{size}(a/b) := \lceil \log_2 |a| \rceil + \lceil \log_2 |b| \rceil$ for $a, b \in \mathbb{Z}$ coprime. As is customary, we assume that in this paper the $B_{\mathcal{O}_\mathbb{L}}$ is always an LLL-reduced basis of $\mathcal{O}_\mathbb{L}$, i.e. $\sigma(B_{\mathcal{O}_\mathbb{K}})$ forms an LLL-reduced basis of $\mathcal{O}_\mathbb{K}$. This choice is made to ensure that the coefficients of $\alpha_i\alpha_j$ under $B_{\mathcal{O}_\mathbb{K}}$ representation do not blow up.

Basic algorithms The following lemma guarantees that the computation of roots of unity in a given field is efficient.

Lemma 2.2 ([11, Corollary 2.11]) *Let $\mathbb{K}$ be a degree d number field. Then, $\mathbb{K}$ has at most $2d^2$ roots of unity, and there exists a polynomial-time algorithm that, given a basis of the ring of integers $\mathcal{O}_\mathbb{K}$, computes the roots of unity in $\mathbb{K}$.*

The following lemma guarantees that we can compute the intersection of a module lattice and a $\mathbb{L}$-linear space.

Lemma 2.3 ([10, Lemma 4.4]) *Let $\mathbb{L}$ be a number field with degree n, and $B_{\mathcal{O}_\mathbb{L}}$ be a basis of $\mathcal{O}_\mathbb{L}$. Then for $A \in \mathbb{L}^{2\times 2}$ and a lattice $\mathcal{L} \subseteq \mathbb{L}^2$, there is a deterministic polynomial-time algorithm that, given $B_{\mathcal{O}_\mathbb{L}}$, A, and a basis $B_\mathcal{L}$ of $\mathcal{L}$, outputs $\ker(A) \cap \mathcal{L}$.*

Proposition 2.1 ([10, Proposition 3.2]) *Let $B \in GL_2(\mathbb{L})$, and $r \in \mathbb{L}$. Define $t_* : \begin{pmatrix}x\\ y\end{pmatrix} \in \mathbb{L}^2 \mapsto \begin{pmatrix}x^*\\ y^*\end{pmatrix} \in \mathbb{L}^2$. It's an $\mathbb{Q}$ linear map. Given as input a basis of $\mathcal{O}_\mathbb{L}$, $G = B^*B$, and $\det(B)$, we can compute $B^{-1}J_2t_*B$ and $m_r := B^{-1}(rI_2)B$ in the time of polynomial of the input size.*

Lenstra-Silverberg Algorithm Gentry and Szydlo initially proposed an algorithm in [4] to recover x from x^*x and xR (where R is a certain type of polynomial ring). Later, Lenstra and Silverberg extended this in [7,8,9]. Luo et al. used it to show an algorithm for which, in a certain sense, is a high-dimensional version of the rank 1 module-LIP.

Proposition 2.2 ([10, Proposition 4.1]) *Let $\mathbb{F}$ be a CM-field or a totally real number field with degree n. Let A be the ring of integers of $\mathbb{F}$. [9, Examples 3.7(i)(ii))] showed that A is a CM-order. The conjugate automorphsim is just the complex conjugation $x \mapsto x^*$, and the trace function is just $Tr_{\mathbb{F}}$.*

1. *For $\alpha \in \mathbb{F}$, there is a deterministic polynomial-time algorithm* LS1 *that, given A, αA and $\alpha^*\alpha$, then we can find $\alpha\mu(A)$ in polynomial time, where $\mu(A)$ means roots of unity in A.*
2. *For $v = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \in \mathbb{F}^2$ and $B \in GL_2(\mathbb{F})$, there is a deterministic polynomial-time algorithm* LS2 *that, given A, B^*B, $v^*v = v_1v_1^* + v_2v_2^*$, and $B^{-1}(A \cdot v)$, then we can find $B^{-1}(\mu(A) \cdot v)$ in polynomial time, where $\mu(A)$ means roots of unity in A.*

2.6 Commitments from Group actions

In this subsection, we introduce the basic definitions related to the group action that we will use. Given that the conclusion in [5] provides a good "encapsulation" for using these to construct a commitment scheme, we do not even need to provide the definition of the commitment scheme.

Definition 2.4 (Group Action) *Let G be a group with identity element e, and let X be a set. We say G acts on X if there is an operator $\star : G \times X \to X$ satisfying $e \star x = x$ and $g \star (h \star x) = (gh) \star x$ for all $g, h \in G$ and $x \in X$. The notation $(G, X, \star)$ will be used to denote such a group action.*

For a group action $(G, X, \star)$, the *orbit* of an element $x \in X$ is denoted by $\mathcal{O}(x) \coloneqq \{g \star x : g \in G\}$. The *stabilizer* of $x \in X$ is the subgroup of G defined as $\mathrm{Stab}(x) \coloneqq \{g \in G : g \star x = x\}$. Additionally, the set $\mathcal{I}(x, y) \coloneqq \{g \in G : g \star x = y\}$ is used to represent the elements of G mapping x to y. It is evident that $\mathcal{I}(x, y) = g \cdot \mathrm{Stab}(x)$ for any $g \in \mathcal{I}(x, y)$.

Additionally, we introduce the *search Group Action Stabilizer Problem* (s-GASP), which relates to finding a non-trivial element in a stabilizer. Specifically, given an $x \in X$ such that $\mathrm{Stab}(x) \neq \{e\}$, the goal is to find an $h \in G$ such that $x = h \star x$ and $h \neq e$. The formal definition is as follows.

Definition 2.5 (s-GASP) *Let $\mathcal{F}$ be a family of group actions such that for a security parameter λ, $\mathcal{F}(1^\lambda)$ returns a group action $(G, X, \star)$ with distribution $\mathcal{D}_{G,X}$ over $G \times X$. The s-GASP assumption requires that for all PPT adversaries $\mathcal{A}$, there is a negligible function $\mathsf{negl}(\lambda)$ such that*

$$\Pr[\mathcal{A}(y) \star y = y, \mathcal{A}(y) \neq e \mid y = h \star x, (h, x) \leftarrow \mathcal{D}_{G,X}, \mathit{Stab}(x) \neq \{e\}] \leq \mathsf{negl}(\lambda).$$

Definition 2.6 (Re-Randomized Algorithm) *For a group action $(G, X, \star)$, a re-randomized algorithm R takes as input $x \in X$ and outputs a pair $(g \star x, g) \in X \times G$ according to a distribution, denoted as $\mathsf{R}(x)$, such that:*

- *For any $x \in X$, $x' \in \mathcal{O}(x)$, and $(x'', g) \leftarrow \mathsf{R}(x)$, the marginal distributions of the first variable are identical for $\mathsf{R}(x)$ and $\mathsf{R}(x')$; g is uniformly distributed on $\mathcal{I}(x, x'')$.*

Definition 2.7 (Homomorphic Extractor) *For a group action $(G, X, \star)$ with a distribution $\mathcal{D}_{G,X}$ in $G \times X$, and M is an abelian group. A homomorphic extractor is a deterministic and efficient algorithm $\mathsf{E} : G \to M$ such that*

- *for $(h, x) \leftarrow \mathcal{D}_{G,X}$ and any $y', y'' \in \mathcal{O}(x)$, it holds that $\mathsf{E}(g)$ is uniformly distributed on M for $g \leftarrow_{\$} \mathcal{I}(y', y'')$.*
- *$\mathsf{E} : G \to M$ is a surjective group homomorphism, i.e, for any $g_0, g_1 \in G$, $\mathsf{E}(g_0) \cdot \mathsf{E}(g_1)^{-1} = \mathsf{E}(g_0 \cdot g_1^{-1})$*

Theorem 2.1 ([5, Theorem 4.2]) *Suppose that group action $(G, X, \star, \mathcal{D}_{G,X})$ satisfies the s-GASP assumption, R is a re-randomization algorithm, and E is a homomorphic extractor. Then there is an Enhanced Linkable Commitment.*

3 Reduction from $\mathcal{O}^2_{\mathbb{L}}$-LIP to $\mathcal{O}^2_{\mathbb{L}}$-LAP

In this section, we assume that $\mathbb{L}$ is a CM number field with degree n.

Theorem 3.1 *Let $\mathbb{L}$ be a CM number field. Given parameter $\mathbf{L}$, there is a reduction from $\mathcal{O}^2_{\mathbb{L}}$-LIP to $\mathcal{O}^2_{\mathbb{L}}$-LAP.*

For $P \in \mathcal{U}_2(\mathcal{O}_{\mathbb{L}})$, under the condition that the determinant is fixed, the possible candidates for P are polynomially many. Therefore, by enumeration, we can assume that given the input modular lattice automorphism $U^{-1}PU$, we have guessed P. (A more straightforward approach is to traverse the entire $\mathcal{U}_2(\mathcal{O}_{\mathbb{L}})$.)

By Lemma 2.1, the structure of P can be classified into two types: diagonal and anti-diagonal. We aim to replace (J_2, J_{BU}) with $(P, U^{-1}PU)$ to perform operations similar to the module lattice decomposition based on eigenspaces as described in the [10].

When P is a diagonal matrix, this operation can be easily accomplished. However, when P is an anti-diagonal matrix, in order to compute the eigenspaces, it is necessary to extend the field L by adjoining the square root of a root of unity in L. In this case, we must also prove that the extended field remains a CM field and that an integral basis of its ring of integers can still be efficiently computed.

Proposition 3.1 *Assume $U \in GL_2(\mathcal{O}_{\mathbb{L}})$. Given $\mathbf{L}$, U^*U, $\xi_1 \neq \xi_2 \in \mu(\mathbb{L})$, and $P_U := U^{-1}PU$ where $P := \begin{pmatrix} \xi_1 & 0 \\ 0 & \xi_2 \end{pmatrix}$, we can find U in polynomial time of the size of input.*

Proof. We first compute $\ker(P_U - \xi_1) \cap \mathcal{O}_{\mathbb{L}}^2$ by Lemma 2.3 in polynomial time, and it's just $U^{-1}e_1\mathcal{O}_{\mathbb{L}}$ where $e_1 = (1,0)^T$. Also we can compute $U^{-1}J_2t_*U$ by Proposition 2.1 using U^*U. Then using LS2 for input $\mathcal{O}_{\mathbb{L}}$, $U^{-1}e_1\mathcal{O}_{\mathbb{L}}$, we can find $\mu(\mathbb{L}) \cdot U^{-1}e_1$. Next, for every $w \in \mu(\mathbb{L}) \cdot U^{-1}e_1$, we compute $(e_1|J_2t_*e_1)(w|U^{-1}J_2t_*Uw)^{-1}$. Then we can find the all the U. □

Proposition 3.2 *Assume $U \in GL_2(\mathcal{O}_{\mathbb{L}})$. Given $\mathbf{L}$, U^*U, $\xi_1, \xi_2 \in \mu(\mathbb{L})$, and $U^{-1}PU$ where $P := \begin{pmatrix} 0 & \xi_1 \\ \xi_2 & 0 \end{pmatrix}$, we can find U in quantum polynomial time of the size of input.*

Lemma 3.1 *Assume $\xi \in \mathbb{L}$ is a root of unity and $X^2 - \xi$ doesn't have roots in $\mathbb{L}$. Let $\mathbb{F} := \mathbb{L}[X]/(X^2 - \xi)$. Then $\mathbb{F}$ is also a CM number field.*

Proof. Let $\mathbb{K}$ be the totally real number field such that of $\mathbb{L}|\mathbb{K}$ is a totally imaginary quadratic extension. If $\xi \neq -1$, consider $\mathbb{M} := \mathbb{K}(X + X^{-1}) \subseteq \mathbb{F}$. One can prove that $\mathbb{M}$ is totally real. And $M \neq \mathbb{K}$, otherwise $(\xi + 1)/X = (X^2 + 1)/X = X + X^{-1} \in \mathbb{K} \subseteq \mathbb{L} \Rightarrow X \in \mathbb{L}$, leading to a contradiction.

If $\xi = -1$, assume $\mathbb{L} = \mathbb{K}(\alpha)$ and consider $\mathbb{M} := \mathbb{K}(X \cdot \alpha) \subseteq \mathbb{F}$. One can prove that $\mathbb{M}$ is totally real. And $M \neq \mathbb{K}$, otherwise $X \cdot \alpha \in \mathbb{K} \subseteq \mathbb{L} \Rightarrow X \in \mathbb{L}$, leading to a contradiction. □

When $\mathbb{L}$ is a totally real number field and $\mathbb{F} = \mathbb{L}[X]/(X^2 + 1)$, Mureau et.al. showed $\log \Delta_{\mathbb{F}} = \text{poly}(\log \Delta_{\mathbb{L}})$ and we can compute $\mathcal{O}_{\mathbb{F}}$ from $\mathcal{O}_{\mathbb{L}}$ in [11, Section 2.2]. We generalize this conclusion as follows.

Lemma 3.2 ([1, Lemma 1.4]) *There are polynomial time algorithms that given an algebraic number field K and one of (a), (b), determine the other:*

(a) the ring of algebraic integers of K;
(b) the largest squarefree divisor of the discriminant of K.

Lemma 3.3 *Assume $\xi \in \mathbb{L}$ is a root of unity and $X^2 - \xi$ doesn't have roots in $\mathbb{L}$. Let $\mathbb{F} := \mathbb{L}[X]/(X^2 - \xi)$. There exists a polynomial time algorithm A that, given as input a $\mathbb{Z}$-basis $B_{\mathbb{L}}$ of $\mathcal{O}_{\mathbb{L}}$, computes a $\mathbb{Z}$-basis $B_{\mathbb{F}}$ of $\mathcal{O}_{\mathbb{F}}$.*

Proof. One can see $A := \mathcal{O}_{\mathbb{L}} + \mathcal{O}_{\mathbb{L}} \cdot X \subseteq \mathcal{O}_{\mathbb{F}}$ is an order of $\mathbb{F}$. Assume $B_{\mathbb{L}} = \{\beta_1, \ldots, \beta_n\}$, then A's discriminant over $\mathbb{Z}$ Δ_A is $\det\left(\begin{pmatrix} (\mathrm{Tr}_{\mathbb{F}}(\beta_i\beta_j)) & (\mathrm{Tr}_{\mathbb{F}}(X\beta_i\beta_j)) \\ (\mathrm{Tr}_{\mathbb{F}}(X\beta_j\beta_i)) & (\mathrm{Tr}_{\mathbb{F}}(\xi\beta_i\beta_j)) \end{pmatrix}\right)$.

On one hand, $A \subseteq \mathcal{O}_{\mathbb{F}}$ implies $\Delta_{\mathbb{F}} | \Delta_A$. On the other hand, we compute Δ_A to show it's just $2^{2n}\Delta_{\mathbb{L}}^2$. Thus $\Delta_{\mathbb{F}} | 2^{2n}\Delta_{\mathbb{L}}^2$. And we also know $\Delta_{\mathbb{L}} | \Delta_{\mathbb{F}}$. So the largest squarefree divisor of $\Delta_{\mathbb{F}}$ is the largest squarefree divisor of $\Delta_{\mathbb{L}}$ or the largest squarefree divisor of $\Delta_{\mathbb{L}}$ multiplied by 2. By Lemma 3.2, we can find the largest squarefree divisor of $\Delta_{\mathbb{L}}$ from $B_{\mathbb{L}}$. Then we can guess the largest squarefree divisor of $\Delta_{\mathbb{F}}$ and compute the $\mathbb{Z}$-basis of $\mathcal{O}_{\mathbb{F}}$ by Lemma 3.2.

The computation is as following. Note $\mathrm{Tr}_{\mathbb{F}}(X\beta_i\beta_j) = \mathrm{Tr}_{\mathbb{L}}(\mathrm{Tr}_{\mathbb{F}/\mathbb{L}}(X\beta_i\beta_j)) = \mathrm{Tr}_{\mathbb{L}}(0) = 0$, $\mathrm{Tr}_{\mathbb{F}}(\beta_i\beta_j) = \mathrm{Tr}_{\mathbb{L}}(\mathrm{Tr}_{\mathbb{F}/\mathbb{L}}(\beta_i\beta_j)) = 2\mathrm{Tr}_{\mathbb{L}}(\beta_i\beta_j)$ and $\mathrm{Tr}_{\mathbb{F}}(\xi\beta_i\beta_j) = \mathrm{Tr}_{\mathbb{L}}(\mathrm{Tr}_{\mathbb{F}/\mathbb{L}}(\xi\beta_i\beta_j)) = 2\mathrm{Tr}_{\mathbb{L}}(\xi\beta_i\beta_j)$. So $\Delta_A = \det((2\mathrm{Tr}_{\mathbb{L}}(\beta_i\beta_j))) \cdot \det((2\mathrm{Tr}_{\mathbb{L}}(\xi\beta_i\beta_j))) =$

$2^{2n}\Delta_{\mathbb{L}} \cdot \det((\mathrm{Tr}_{\mathbb{L}}(\xi\beta_i\beta_j)))$. For $(\mathrm{Tr}_{\mathbb{L}}(\xi\beta_i\beta_j))$, write it as $(\sigma_j(\xi\beta_i)) \cdot (\sigma_i(\beta_j))$, where $\{\sigma_i\}$ is $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{L}, \mathbb{C})$. Then $\det((\mathrm{Tr}_{\mathbb{L}}(\xi\beta_i\beta_j))) = \det((\sigma_j(\xi\beta_i))) \cdot \det((\sigma_i(\beta_j))) = \mathrm{Nm}_{\mathbb{L}}(\xi) \cdot \det((\sigma_j(\beta_i))) \cdot \det((\sigma_i(\beta_j))) = \det((\sigma_j(\beta_i))) \cdot \det((\sigma_i(\beta_j))) = \Delta_{\mathbb{L}}$. □

From the proof, we can see $\Delta_{\mathbb{F}} \leq 2^{2n}\Delta_{\mathbb{L}}^2$. Note $n = \mathrm{poly}(\log \Delta_{\mathbb{L}})$, so $\log \Delta_{\mathbb{F}} = \mathrm{poly}(\log \Delta_{\mathbb{L}})$.

Proof (of Proposition 3.2). Let $\xi := \xi_1 \cdot \xi_2$, and

$$\mathbb{F} := \begin{cases} \mathbb{L}[X]/(X^2 - \xi) \text{ if } X^2 - \xi \text{ doesn't have roots in } \mathbb{L}; \\ \mathbb{L} \text{ otherwise.} \end{cases}$$

By Lemma 3.3, we can compute the $\mathbb{Z}$-basis of $\mathcal{O}_{\mathbb{F}}$ in polynomial time.

We first compute $\ker(P_U - X) \cap \mathcal{O}_{\mathbb{F}}^2$ by Lemma 2.3 in polynomial time, and it's just $U^{-1}v\mathcal{O}_{\mathbb{L}}$ where $v = (\xi_1, X)^T$. Also we can compute $U^{-1}J_2t_*U$ by Proposition 2.1 using U^*U. Then using `LS2` for input $\mathcal{O}_{\mathbb{L}}$, $U^{-1}v\mathcal{O}_{\mathbb{L}}$, we can find $\mu(\mathbb{L}) \cdot U^{-1}e_1$. Next, for every $w \in \mu(\mathbb{L}) \cdot U^{-1}v$, we compute $(v|J_2t_*v)(w|U^{-1}J_2t_*Uw)^{-1}$. Then we can find the all the U. □

4 Commitment on $\mathcal{O}_{\mathbb{L}}^2$-LIP

In this section, as in HAWK, we set $\mathbb{L} = \mathbb{Q}[X]/(\Phi_{2^d}(X))$ to be a power of two cyclotomic number field and ζ_{2^d} to be a 2^d-th root of unity. Let $n = 2^{d-1} = \deg(\mathbb{L})$.

Group Action Based on Module Lattice A naive idea for constructing a structured version in A is to replace $\mathrm{GL}_n(\mathbb{Z})$ with $\mathrm{GL}_2(\mathcal{O}_{\mathbb{L}})$. However, when constructing the Re-randomize algorithm, obstacles arise because, unlike general lattices, which can use the LLL algorithm to find an integral basis, there is currently no efficient algorithm on classical computers for finding a $\mathcal{O}_{\mathbb{L}}$-basis for module lattices. This issue is also reflected in the self-reduction of the module lattice isomorphism problem. To bypass this difficulty, [2] considers $\mathrm{SL}_2(\mathcal{O}_{\mathbb{L}})$. If we adopt their strategy, we face another obstacle when constructing deterministic extractors (since we cannot still use det as an extractor as in A). To meet both requirements simultaneously, we consider such a subgroup.

Definition 4.1 *We define the Generalized Special Linear group over $\mathcal{O}_{\mathbb{L}}$ as $GSL_2(\mathcal{O}_{\mathbb{L}}) := \{M \in GL_2(\mathcal{O}_{\mathbb{L}}) | \det(M) \in \mu(\mathbb{L})\}$ and the projective group of it is $PGSL_2(\mathcal{O}_{\mathbb{L}}) := GSL_2(\mathcal{O}_{\mathbb{L}})/\mu(\mathbb{L})I_2$.*

Let $\mathbf{Q} \in \mathcal{S}_n^{>0}(\mathcal{O}_{\mathbb{L}})$ be a positive definite quadratic form over $\mathcal{O}_{\mathbb{L}}$, and let $[\mathbf{Q}]$ denote the set of quadratic forms equivalent to $\mathbf{Q}$, i.e., $[\mathbf{Q}]_{\mathrm{sl}} := \{\mathbf{V}^*\mathbf{Q}\mathbf{V} : \mathbf{V} \in$

$\mathrm{SL}_n(\mathcal{O}_\mathbb{L})\}$, $[\mathbf{Q}]_{\mathrm{gsl}} \coloneqq \{\mathbf{V}^*\mathbf{Q}\mathbf{V} : \mathbf{V} \in \mathrm{GSL}_n(\mathcal{O}_\mathbb{L})\}$ [1]. A group action $(\mathrm{PGSL}_n(\mathcal{O}_\mathbb{L}), [\mathbf{Q}]_{\mathrm{gsl}}, \star)$ can then be defined as [2]:

$$\mathbf{Q}' \star \mathbf{V} = \mathbf{V}^*\mathbf{Q}'\mathbf{V} \quad \text{for any } \mathbf{V} \in \mathrm{PGSL}_n(\mathcal{O}_\mathbb{L}), \mathbf{Q}' \in [\mathbf{Q}]_{\mathrm{gsl}}. \tag{1}$$

This group action is closely related to free module lattice isomorphisms and automorphisms.

Here we focus on the case when n=2 and $\mathbf{Q} = I_2$. When $U \in \mathrm{GSL}_2(\mathcal{O}_\mathbb{L})$ and $Q := U^*U$, we have $[Q]_{\mathrm{gsl}} = [I_2]_{\mathrm{gsl}} = [I_2]_{\mathrm{sl}} \triangleq [I_2]$. And then the Stabilizer of Q under the group action is just $Aut_\mathbb{L}(Q)/\mu(\mathbb{L})I_n$ and its corresponding s-GASP i.e. finding a non-trivial element in $Stab(Q)$ is equivalent to finding a non-trivial module lattice automorphism of Q and is equivalent to finding U i.e. $\mathcal{O}_\mathbb{L}^2$-LIP by Theorem 3.1.

As mentioned earlier, the main difficulty in structuring the instantiation in [5] lies in constructing a suitable Re-randomize algorithm. We make adaptations to the construction in [2] for self-reduction to obtain the required Re-randomize algorithm.

We first provide a sufficient condition for a better use of the re-randomize algorithm.

Lemma 4.1 *For a group action $(G, X, \star)$, a algorithm R is a re-randomized algorithm if it takes as input $x \in X$ and outputs a pair $(g \star x, g) \in X \times G$ according to a distribution, denoted as $\mathsf{R}(x)$, such that:*

- *For any $x \in X$, $h \in G$, the distributions of $\mathsf{R}(h \star x)[2]$ and $\mathsf{R}(x)[2] \cdot h^{-1}$ are same.*

Proof. If R has the property: for any $x \in X$, $h, g \in G$, the distributions of $\mathsf{R}(h \star x)[2]$ and $\mathsf{R}(x)[2] \cdot h^{-1}$ are same. This means for any $x \in X$, $h, g \in G$, $\Pr[\mathsf{R}(h \star x)[2] = gh^{-1}] = \Pr[\mathsf{R}(x)[2] \cdot h^{-1} = gh^{-1}] = \Pr[\mathsf{R}(x)[2] = g]$.

For any $x \in X$, $x' \in \mathcal{O}(x)$, and $(x'', g) \leftarrow \mathsf{R}(x)$, assume $f \in \mathcal{I}(x, x')$. Firstly,

$$\begin{aligned}
&\Pr[\mathsf{R}(x)[1] = x''] = \Pr[\mathsf{R}(x)[2] \in \mathcal{I}(x, x'')] \\
=& \sum_{h \in \mathcal{I}(x,x'')} \Pr[\mathsf{R}(x)[2] = h] = \sum_{h \in \mathcal{I}(x,x'')} \Pr[\mathsf{R}(f \star x)[2] = h \cdot f^{-1}] \\
=& \sum_{t \in \mathcal{I}(x',x'')} \Pr[\mathsf{R}(x')[2] = t] = \Pr[\mathsf{R}(x)[1] = x'].
\end{aligned}$$

[1] Here, there is a subtle difference in notation compared to that in A. In A, to align with the conventional notation for left group actions, the left and right sides of the congruence transformation were swapped. However, in this context, to maintain consistency with the standard notation for module lattice isomorphisms, we do not perform the same swap as in A. This difference does not cause any substantive impact.

[2] The choice of representative in $\mathrm{GSL}_n(\mathcal{O}_\mathbb{L})/\mu(\mathbb{L})I_n$ does not matter for this group action since $\mathbf{V}^*\mathbf{Q}\mathbf{V} = (\xi\mathbf{V})^*\mathbf{Q}(\xi\mathbf{V})$ for any $\xi \in \mu(\mathbb{L})$.

The third equality uses the property, and the fourth equality uses $\mathcal{I}(x', x'') = \mathcal{I}(x, x'') \cdot f^{-1}$.
Secondly for any $g' \in \mathcal{I}(x, x'')$, we have $\Pr[\mathsf{R}(x)[2] = g'] = \Pr[\mathsf{R}((g^{-1} \cdot g') \star x)[2] = g' \cdot (g^{-1} \cdot g')^{-1}] = \Pr[\mathsf{R}(x)[2] = g]$. □

The following lemma, although not a direct consequence of the original lemma, can be directly derived by reviewing its proof and construction.

Lemma 4.2 ([2, Section 6 Lemma 4]) *There exists an heuristic efficient randomized algorithm* R_0 *that takes any* $\mathbf{Q} \in \mathcal{S}_2^{>0}(\mathcal{O}_\mathbb{L})$ *as input and outputs* $(\mathbf{R}, \mathbf{U})$ *such that* $(\mathbf{R} = \mathbf{U}^*\mathbf{Q}\mathbf{U}, \mathbf{U}) \in [\mathbf{Q}]_{sl} \times SL_2(\mathcal{O}_\mathbb{L})$. *The distribution of* $\mathsf{R}_0(\mathbf{Q})[2]$ *is given by:*

- *For any* $\mathbf{U} = (u_1 | u_2) \in SL_2(\mathcal{O}_\mathbb{L})$,

$$\Pr[\mathsf{R}_0(\mathbf{Q})[2] = \mathbf{U}] = \begin{cases} D_{\mathbf{Q},\sigma}(u_1), \text{ if } u_2 \text{ is reduced with respect to } u_1 \text{ and } \mathbf{Q}; \\ 0, \text{ otherwise,} \end{cases}$$

with the following property:

- *For any* $\mathbf{V} \in SL_2(\mathcal{O}_\mathbb{L})$, *the distribution of* $\mathbf{V}^{-1} \cdot \mathsf{R}_0(\mathbf{Q})[2]$ *is the same as that of* $\mathsf{R}_0(\mathbf{V}^*\mathbf{Q}\mathbf{V})[2]$.

Here, we say y *is reduced with respect to* x *and* $\mathbf{Q}$ *if* $\left\lceil \frac{x^* \cdot \mathbf{Q} \cdot y}{x^* \cdot \mathbf{Q} \cdot x} \right\rfloor$ *in which* $\lceil \cdot \rfloor : a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} \mapsto \lceil a_0 \rfloor + \lceil a_1 \rfloor X + \cdots + \lceil a_{n-1} \rfloor X^{n-1}$.

There are some observation about the randomized algorithm R_0.

Lemma 4.3 *For any* $\xi \in \mu(\mathbb{L})$, *let* $\mathbf{X} = \begin{pmatrix} 1 & 0 \\ 0 & \xi \end{pmatrix}$ *and* $\mathbf{Y} = \begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix}$. *Then for any* $\mathbf{U} \in SL_2(\mathcal{O}_\mathbb{L})$, *we have* $\Pr[\mathsf{R}_0(\mathbf{I_2})[2] = \mathbf{X^{-1}UX}] = \Pr[\mathsf{R}_0(\mathbf{I_2})[2] = \mathbf{U}] = \Pr[\mathsf{R}_0(\mathbf{I_2})[2] = \mathbf{UY}]$

Proof. Write $\mathbf{U}$ as $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then $\mathbf{X^{-1}UX} = \begin{pmatrix} a & \xi b \\ \xi^{-1} c & d \end{pmatrix}$ and $\mathbf{UY} = \begin{pmatrix} \xi a & \xi^{-1} b \\ \xi c & \xi^{-1} d \end{pmatrix}$.

Note $D_\sigma(\begin{pmatrix} a \\ c \end{pmatrix}) = D_\sigma(\begin{pmatrix} a \\ \xi^{-1} c \end{pmatrix}) = D_\sigma(\begin{pmatrix} \xi a \\ \xi c \end{pmatrix})$ and $\begin{pmatrix} \xi b \\ d \end{pmatrix}$ is reduced with respect to $\begin{pmatrix} a \\ \xi^{-1} c \end{pmatrix}$ and $\mathbf{I_2}$ iff $\begin{pmatrix} b \\ d \end{pmatrix}$ is reduced with respect to $\begin{pmatrix} a \\ c \end{pmatrix}$ and $\mathbf{I_2}$ iff $\begin{pmatrix} \xi^{-1} b \\ \xi^{-1} d \end{pmatrix}$ is reduced with respect to $\begin{pmatrix} \xi a \\ \xi c \end{pmatrix}$ and $\mathbf{I_2}$. These are all because the action of multiplying by ξ can be viewed as a sign permutation on the coefficients.

Thus, by Lemma 4.2, we obtain the desired conclusion. □

Note that the matrices in $\mathrm{GSL}_2(\mathcal{O}_\mathbb{L})$ can always be uniquely represented as a product of a matrix in $\mathrm{SL}_2(\mathcal{O}_\mathbb{L})$ and a matrix of the form $\mathrm{diag}(1, \xi)$. A natural construction for a re-randomized algorithm on $(\mathrm{GSL}_2(\mathcal{O}_\mathbb{L}), [I_2])$ is to sample

the part of $\mathrm{SL}_2(\mathcal{O}_\mathbb{L})$ using R_0 and uniformly randomly sample the part of the form $\mathrm{diag}(1, \xi)$. Here, we consider the equivalence class $[I_2]$, so it can be directly used as the input for R_0. We next prove that such a construction is indeed a re-randomized algorithm that satisfies the requirement.

Lemma 4.4 (Re-randomize algorithm) *If R_0 is efficient, there exists an efficient randomized algorithm R that takes any $\mathbf{Q} \in [I_2]$ as input and outputs $(\mathbf{R}, \mathbf{U})$ such that $(\mathbf{R} = \mathbf{U}^*\mathbf{Q}\mathbf{U}, \mathbf{U}) \in [I_2] \times GSL_2(\mathcal{O}_\mathbb{L})$, with the following property:*

- *For any $\mathbf{V} \in GSL_2(\mathcal{O}_\mathbb{L})$, the distribution of $\mathbf{V}^{-1} \cdot \mathsf{R}(\mathbf{Q})[2]$ is the same as that of $\mathsf{R}(\mathbf{V}^*\mathbf{Q}\mathbf{V})[2]$*

  And so does also if we consider the induced group action for $PGSL_2(\mathcal{O}_\mathbb{L})$.

Proof. It's easy to see its efficiency if R_0 is efficient. We only need to prove the properties.

For the first claim, we want to show that for any $\mathbf{U} \in \mathrm{GSL}_2(\mathcal{O}_\mathbb{L})$, $\Pr[\mathsf{R}(\mathbf{V}^*\mathbf{Q}\mathbf{V})[2] = \mathbf{U}] = \Pr[\mathbf{V}^{-1}\mathsf{R}(\mathbf{Q})[2] = \mathbf{U}]$.

Firstly, we write them as $\mathbf{Q} = \mathbf{B}^*\mathbf{B}$, $\mathbf{V} = \mathbf{V_0}\mathbf{V_1}$, $\mathbf{U} = \mathbf{U_0}\mathbf{U_1}$ where $\mathbf{B}, \mathbf{V_0}, \mathbf{U_0} \in \mathrm{SL}_2(\mathcal{O}_\mathbb{L})$ and $\mathbf{V_1}(\text{resp. } \mathbf{U_1}) = \begin{pmatrix} 1 & 0 \\ 0 & \det(\mathbf{V}) \end{pmatrix}(\text{resp. } \begin{pmatrix} 1 & 0 \\ 0 & \det(\mathbf{U}) \end{pmatrix})$. And so we can write $\mathbf{V}^*\mathbf{Q}\mathbf{V} = (\mathbf{V_1^{-1}}\mathbf{B}\mathbf{V_0}\mathbf{V_1})^*(\mathbf{V_1^{-1}}\mathbf{B}\mathbf{V_0}\mathbf{V_1})$. Note that $\mathbf{V_1^{-1}}\mathbf{B}\mathbf{V_0}\mathbf{V_1} \in \mathrm{SL}_2(\mathcal{O}_\mathbb{L})$

From the construction of R, we can see

$$\begin{aligned} &\Pr[\mathsf{R}(\mathbf{V}^*\mathbf{Q}\mathbf{V})[2] = \mathbf{U}] \\ =&\frac{1}{n} \cdot \Pr[\mathsf{R}_0(\mathbf{V}^*\mathbf{Q}\mathbf{V})[2] = \mathbf{U_0}] \\ =&\frac{1}{n} \cdot \Pr[\mathsf{R}_0(I_2)[2] = (\mathbf{V_1^{-1}}\mathbf{B}\mathbf{V_0}\mathbf{V_1})\mathbf{U_0}]. \end{aligned}$$

The last equality holds by Lemma 4.2. Similarly, we have

$$\begin{aligned} &\Pr[\mathbf{V}^{-1}\mathsf{R}(\mathbf{Q})[2] = \mathbf{U}] \\ =&\Pr[\mathsf{R}(\mathbf{Q})[2] = \mathbf{V}\mathbf{U}] \\ =&\frac{1}{n} \cdot \Pr[\mathsf{R}_0(\mathbf{Q})[2] = \mathbf{V_0}\mathbf{V_1}\mathbf{U_0}\mathbf{V_1^{-1}}] \\ =&\frac{1}{n} \cdot \Pr[\mathsf{R}_0(I_2)[2] = \mathbf{B}(\mathbf{V_0}\mathbf{V_1}\mathbf{U_0}\mathbf{V_1^{-1}})]. \end{aligned}$$

Denote $\mathbf{B}(\mathbf{V_0}\mathbf{V_1}\mathbf{U_0}\mathbf{V_1^{-1}})$ by $\mathbf{M} \in \mathrm{SL}_2(\mathcal{O}_\mathbb{L})$, then $(\mathbf{V_1^{-1}}\mathbf{B}\mathbf{V_0}\mathbf{V_1})\mathbf{U_0} = \mathbf{V_1^{-1}}\mathbf{M}\mathbf{V_1}$. By Lemma 4.3, $\Pr[\mathsf{R}_0(I_2)[2] = \mathbf{M}] = \Pr[\mathsf{R}_0(I_2)[2] = \mathbf{V_1^{-1}}\mathbf{M}\mathbf{V_1}]$, so $\Pr[\mathsf{R}(\mathbf{V}^*\mathbf{Q}\mathbf{V})[2] = \mathbf{U}] = \Pr[\mathbf{V}^{-1}\mathsf{R}(\mathbf{Q})[2] = \mathbf{U}]$.

For the second claim, we just need to show that for any $\mathbf{U} \in \mathrm{GSL}_2(\mathcal{O}_\mathbb{L})$, $\sum_{\xi \in \mu(\mathbb{L})} \Pr[\mathsf{R}(\mathbf{V}^*\mathbf{Q}\mathbf{V})[2] = \xi I_2 \cdot \mathbf{U}] = \sum_{\xi \in \mu(\mathbb{L})} \Pr[\mathbf{V}^{-1}\mathsf{R}(\mathbf{Q})[2] = \xi I_2 \cdot \mathbf{U}]$ which is which can be directly derived from the previous conclusion. □

Algorithm 1: R: Re-randomization for $(\mathrm{GSL}_2(\mathcal{O}_\mathbb{L}), [I_2])$

Require: Conductor $m = 2^\kappa$ cyclotomic $\mathbb{L}$, $Q \in [I_2]$
Ensure: $\mathbf{R} \in [I_2]$ and $\mathbf{U} \in \mathrm{GSL}_2(\mathcal{O}_K)$ such that $\mathbf{R} = \mathbf{U}^* \cdot \mathbf{Q} \cdot \mathbf{U}$
1: Let $(\mathbf{R_0}, \mathbf{U_0}) \leftarrow \mathsf{R}_0(Q)$
2: Parse $\xi \leftarrow_\$ \mu(\mathbb{L})$
3: Let $Y = \begin{pmatrix} 1 & 0 \\ 0 & \xi \end{pmatrix}$, $\mathbf{U} = \mathbf{U_0}Y$, and $\mathbf{R} = \mathbf{U}^*\mathbf{Q}\mathbf{U}$
4: **return** $(\mathbf{R}, \mathbf{U})$

Remark 2. We can prove $\Pr[\mathsf{R}(\mathbf{V}^*\mathbf{Q}\mathbf{V})[2] = \mathbf{U}] = \Pr[\mathsf{R}(\mathbf{V}^*\mathbf{Q}\mathbf{V})[2] = \xi I_2 \cdot \mathbf{U}]$ for any $\xi \in \mu(\mathbb{L})$ by the other equality in Lemma 4.3.

We define $\mathcal{D}_{\mathrm{PGSL}_2(\mathcal{O}_\mathbb{L}),[I_2]} := \mathsf{R}(\mathsf{R}(I_2)[1])$.

Lemma 4.5 *For the group action $(PGSL_2(\mathcal{O}_\mathbb{L}), [I_2], \star)$ with distribution $\mathcal{D}_{PGSL_2(\mathcal{O}_\mathbb{L}),[\mathbf{Q}]}$ on $PGSL_2(\mathcal{O}_\mathbb{L}) \times [\mathbf{Q}]$ and the group $M = (\langle\zeta_{2^d}\rangle / \langle\zeta_{2^{d-1}}\rangle, \times) \simeq (\{\pm 1\}, \times)$, define $\mathsf{E} : PGSL_2(\mathcal{O}_\mathbb{L}) \to M$ such that $\mathsf{E}(\mathbf{U}) \mapsto \det(\mathbf{U})/\langle\zeta_{2^{d-1}}\rangle$. Then, E is a Homomorphic extractor as in Definition 2.7.*

Proof. It's easy to see E is a well-defined group homomorphism. For any $\mathbf{Q} \in [I_2]$, $\mathsf{E}(\mathrm{Stab}(\mathbf{Q})) = \det(Aut_\mathbb{L}(\mathbf{Q}))/\langle\zeta_{2^{d-1}}\rangle = \det(\mathcal{U}_2(\mathcal{O}_\mathbb{L}))/\langle\zeta_{2^{d-1}}\rangle = M$. Thus, E is surjective even when restricted to the subgroup $\mathrm{Stab}(\mathbf{Q})$. Furthermore, $\mathsf{E}(U(\mathrm{Stab}(\mathbf{Q}))) = U(M)$ from the invariance of the $U(\mathrm{Stab}(\mathbf{Q}))$ to shifts by elements from that same group.

Then for any $\mathbf{Q}, \mathbf{Q}' \in [I_2]$, assume $\mathbf{Y} \in \mathcal{I}(\mathbf{Q}, \mathbf{Q}')$. We have $\mathsf{E}(U(\mathcal{I}(\mathbf{Q}, \mathbf{Q}'))) = \mathsf{E}(\mathbf{Y} \cdot U(\mathrm{Stab}(\mathbf{Q}))) = \mathsf{E}(\mathbf{Y}) \cdot U(M) = U(M)$. □

Finally, by Lemma 4.4, Lemma 4.5 and Theorem 2.1, under a heuristic assumption, there is an Enhanced Linkable Commitment based on the $\mathcal{O}^2_\mathbb{L}$-LIP assumption.

5 Conclusion

The paper introduces a reduction from $\mathcal{O}^2_\mathbb{L}$-LIP to $\mathcal{O}^2_\mathbb{L}$-LAP, building on the framework proposed in [10]. Then we use the theorem given in [5] to construct a commitment scheme based on $\mathcal{O}^2_\mathbb{L}$-LAP. Our work highlights the potential of module lattice structures for enhancing cryptographic protocols.

References

1. Buchmann, J.A., Lenstra, H.W.: Approximatting rings of integers in number fields. Journal de théorie des nombres de Bordeaux **6**(2), 221–260 (1994), https://jtnb.centre-mersenne.org/item/JTNB_1994__6_2_221_0/
2. 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
3. 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
4. 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
5. Jiang, K., Wang, A., Luo, H., Liu, G., Tang, G., Pan, Y., Wang, X.: Re-randomize and extract: A novel commitment construction framework based on group actions. Springer-Verlag (2025), https://eprint.iacr.org/2025/400
6. Jiang, K., Wang, A., Luo, H., Liu, G., Yu, Y., Wang, X.: Exploiting the symmetry of $\mathbb{Z}^n$: Randomization and the automorphism problem. In: Guo, J., Steinfeld, R. (eds.) Advances in Cryptology – ASIACRYPT 2023. pp. 167–200. Springer Nature Singapore, Singapore (2023)
7. 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
8. 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
9. Lenstra Jr, H.W., Silverberg, A.: Testing isomorphism of lattices over cm-orders. SIAM Journal on Computing **48**(4), 1300–1334 (2019)
10. Luo, H., Jiang, K., Pan, Y., Wang, A.: Cryptanalysis of rank-2 module-lip with symplectic automorphisms. In: Chung, K.M., Sasaki, Y. (eds.) Advances in Cryptology – ASIACRYPT 2024. pp. 359–385. Springer Nature Singapore, Singapore (2025)
11. Mureau, G., Pellet-Mary, A., Pliatsok, G., Wallet, A.: Cryptanalysis of rank-2 module-lip in totally real number fields. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 226–255. Springer (2024)