Don't Use It Twice: Reloaded! On the Lattice Isomorphism Group Action

Alessandro Budroni[1], Jesús-Javier Chi-Domínguez[1] and Ermes Franch[2]

[1] Cryptography Research Center, Technology Innovation Institute, Abu Dhabi, UAE
[2] University of Bergen, Bergen, Norway

Abstract. Group actions have emerged as a powerful framework in post-quantum cryptography, serving as the foundation for various cryptographic primitives. The Lattice Isomorphism Problem (LIP) has recently gained attention as a promising hardness assumption for designing quantum-resistant protocols. Its formulation as a group action has opened the door to new cryptographic applications, including a commitment scheme and a linkable ring signature.
In this work, we analyze the security properties of the LIP group action and present new findings. Specifically, we demonstrate that it fails to satisfy the weak unpredictability and weak pseudorandomness properties when the adversary has access to as few as three and two instances with the same secret, respectively. This significantly improves upon prior analysis by Benčina et al. (PQCrypto 2024).
As a direct consequence of our findings, we reveal a vulnerability in the linkable ring signature scheme proposed by Khuc et al. (SPACE 2024), demonstrating that the hardness assumption underlying the linkable anonymity property does not hold.

Keywords: Lattice Isomorphism · Group Action · Linkable Ring Signature · Cryptanalysis · Post-Quantum Cryptography

1 Introduction

Post-quantum cryptography is a rapidly evolving research field driven by the need to develop cryptographic schemes that remain secure against attacks by quantum computers. With NIST standardization processes for post-quantum key encapsulation mechanisms and digital signatures [Nat17] in their final stages, the research community is actively exploring the construction of post-quantum cryptographic primitives providing additional functionalities to support a broader range of applications.

Brassard and Yung introduced cryptographic group actions as a foundation to construct bit commitment schemes [BY91]. Currently, they are widely used as a framework for constructing advanced cryptographic primitives, including linkable ring signatures [BKP20], threshold signatures [BBMP24], blind signatures [DKQ+25], verifiable random functions [Lai24], commitment schemes [JWL+25], and updatable encryption [LR24]. This framework is particularly useful as it allows the definition of these cryptographic primitives at the abstraction level of group actions, which can then be instantiated using algebraic structures that underpin cryptographic assumptions. Examples include isogenies between elliptic curves [CLM+18], isomorphisms between lattices [BBCK24], and equivalence between linear codes [BMPS20], matrix codes [CNP+23], and trilinear forms [TDJ+22]. Given the presumed quantum resistance of the computationally hard problems underlying the above

E-mail: alessandro.budroni@tii.ae (Alessandro Budroni), jesus.dominguez@tii.ae (Jesús-Javier Chi-Domínguez), ermes.franch@uib.no (Ermes Franch)

This work is licensed under a "CC BY 4.0" license.
Date of this document: 2025-10-08.

algebraic structures, group actions have attracted significant interest in post-quantum cryptography.

The Lattice Isomorphism Problem (LIP) initially gathered attention thanks to the parallel works of Ducas and van Woerden [DvW22] and Bennett et al. [BGPS23], and subsequently because of the digital signature HAWK [DPPvW22, BBD+25] submitted to the ongoing NIST competition for additional signature schemes [Nat17]. [1] Recently, [BBCK24] showed how to model the LIP as a group action. Then, two group action-based schemes, a commitment scheme [JWL+25] and a linkable ring signature [KTS+24], have been instantiated with LIP.

In this work, we provide new results on the security properties of the LIP group action, considerably improving upon the work of Benčina et al. [BBCK24]. In particular, our study reveals a vulnerability in the linkable ring signature scheme proposed by Khuc et al. [KTS+24], demonstrating that such a linkable ring signature is not linkable anonymous. [2]

We emphasize that this contribution has no direct implications on the security of the digital signature HAWK [BBD+25] since our results break the 2-weakly pseudorandom and 3-weakly unpredictable properties of LIP group action.

1.1 Overview of the Contribution

Here, we give an informal overview of our contribution. Let us start with some background notation and definition.

Background. Informally, a *quadratic form* $\boldsymbol{Q}$ is a $n \times n$ symmetric and positive definite matrix. A matrix $\boldsymbol{U} \in \mathbb{Z}^{n\times n}$ is called *unimodular* if its determinant is ± 1 or, equivalently, if its invertible and its inverse lies in the ring $\mathbb{Z}^{n\times n}$. The Lattice Isomorphism Problem in the quadratic form version is as follows: Given two quadratic forms $\boldsymbol{Q}, \boldsymbol{Q}'$, find (if it exists) a unimodular $\boldsymbol{U}$ such that $\boldsymbol{Q}' = \boldsymbol{U}^\top \boldsymbol{Q}\boldsymbol{U}$. If such an unimodular exists, we say that $\boldsymbol{Q}$ and $\boldsymbol{Q}'$ belong to the same equivalence class $[\boldsymbol{Q}]$.

Let G denote the group of all invertible matrices with integer coefficients, and let us consider the set $X = [\boldsymbol{Q}]$. We define the Lattice Isomorphism Group Action (LIGA)

$$\star : \; G \times X \to X, \quad \boldsymbol{U} \star \boldsymbol{Q} \mapsto \boldsymbol{U}^\top \boldsymbol{Q}\boldsymbol{U}. \tag{1}$$

Cryptographic group actions must be *one-way*, that is, in our case, given $\boldsymbol{Q}$ and $\boldsymbol{U} \star \boldsymbol{Q}$, it is hard to compute $\boldsymbol{U}$. Two more properties must be satisfied for constructing certain cryptographic primitives, namely:

- *t-weakly unpredictable*: given a polynomial number t of pairs $(\boldsymbol{Q}_i, \boldsymbol{U} \star \boldsymbol{Q}_i)_{i=1}^t$ with the same secret group element $\boldsymbol{U}$, and given another input $\boldsymbol{Q}^* \neq \boldsymbol{Q}_i$, it is hard to predict the output $\boldsymbol{U} \star \boldsymbol{Q}^*$.

- *t-weakly pseudorandom*: given a polynomial number t of pairs $(\boldsymbol{Q}_i, \boldsymbol{U} \star \boldsymbol{Q}_i)_{i=1}^t$ with the same secret group element $\boldsymbol{U}$, it is hard to distinguish them from random pairs in the same set.

Previous this work, [BBCK24] proved that LIGA is not t-weakly unpredictable and t-weakly pseudorandom for $t = O(n^2)$ under certain assumptions on the distributions of the pairs.

[1] The HAWK signature bases its security on the module version of LIP.

[2] The title of this manuscript deliberately resembles the one of an analogous study on the Linear Code Equivalence group action [BCD+24], which inspired this work.

Contribution. In this manuscript, we greatly improve upon [BBCK24] and show that:

- LIGA is not 2-weakly pseudorandom, and
- LIGA is not 3-weakly unpredictable.

Our improvement relies on a new modeling for constructing a linear system determined by the t pairs of the form $(\boldsymbol{Q}_i, \boldsymbol{U} \star \boldsymbol{Q}_i)$. Specifically, the modeling introduced in [BBCK24] consists of considering the quadratic equations arising from the matrix equation $\boldsymbol{Q}_i' = \boldsymbol{U}^\top \boldsymbol{Q}_i \boldsymbol{U}$, where the entries of the matrix $\boldsymbol{U}$ are the unknowns, and then applying linearization techniques to retrieve the solution corresponding to $\boldsymbol{U}$. In particular, the approach from [BBCK24] yields a linear system with $O(n^4)$ variables. Instead, we exploit the fact that $\boldsymbol{U}$ is invertible over the integers and consider the linear equations deriving from $\boldsymbol{Q}_i' \boldsymbol{U}^{-1} = \boldsymbol{U}^\top \boldsymbol{Q}_i$, where each entry of $\boldsymbol{U}$ and $\boldsymbol{U}^{-1}$ determines an unknown variable. Consequently, the number of variables in this new modeling is $2n^2$, which is significantly fewer than the approach in [BBCK24].

We briefly summarize how we obtained the aforementioned results on the properties of LIGA: First, using our new modeling, we obtain a new linear system $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{0}$ whose solution space contains a vector corresponding to the secret unimodular $\boldsymbol{U}$. Then, by means of linear algebra, we study such a linear system and derive the following two results: i) for $t = 2$ pairs of quadratic forms, $\operatorname{rank}(\boldsymbol{A})$ takes different values depending on whether the input LIP pairs share the same secret unimodular, or not, ii) for $t = 3$ the linear system admits a unique solution with high probability that corresponds to the secret unimodular $\boldsymbol{U}$. These outcomes allow us to construct two probabilistic and polynomial-time algorithms that are provable under mild assumptions and that break the 2-weakly pseudorandomness and 3-weakly unpredictability properties, respectively. Our assumptions are supported both by theoretical linear algebra arguments and by experiments run on `SageMath` [The22]. The scripts to reproduce our experiments are available at [BCDF25].

Following our findings, we highlight one issue in the linkable ring signature based on LIP proposed by Khuc et al. [KTS+24]. Informally, the *linkable anonymity* property of this scheme relies on the assumption that, given a public quadratic form $\boldsymbol{Q}$, the following pair

$$\left(\boldsymbol{Q}' = \boldsymbol{U} \star \boldsymbol{Q}, \quad \boldsymbol{Q}'' = \boldsymbol{U}^{-1} \star \boldsymbol{Q}\right)$$

is indistinguishable from a random pair in the same set. However, given that $\boldsymbol{Q} = \boldsymbol{U}^\top \boldsymbol{Q}'' \boldsymbol{U}$, we derive that $(\boldsymbol{Q}, \boldsymbol{Q}')$ and $(\boldsymbol{Q}'', \boldsymbol{Q})$ are two pairs of quadratic forms coming from LIGA and with the same secret. Consequently, we can distinguish such pairs from random ones using one of the aforementioned algorithms. It follows that the linkable anonymity property is not satisfied.

Organization. Section 2 introduces the required notation, definitions, and background to understand the results presented in this manuscript. In Section 3, we present our new modeling approach to transforming LIP into a linear system, along with our findings on the properties of the associated group action. Section 4 discusses the cryptographic implications of our results. Finally, we give in Section 5 some final remarks and future research directions.

2 Preliminaries

Notation. Denote with $\mathbb{N}, \mathbb{Z}$ and $\mathbb{R}$ the set of natural, integer and real numbers, respectively. In the following, bold lowercase letters represent row vectors, e.g., $\boldsymbol{v}$, while bold uppercase letters represent matrices, e.g., $\boldsymbol{M}$. In this manuscript, we consider the following sets of $n \times n$ matrices:

- $\mathcal{O}_n(\mathbb{R})$ the set of all *orthonormal* matrices over $\mathbb{R}$,
- $\mathcal{S}_n^{>0}$ the set of all *symmetric positive definite* matrices over $\mathbb{R}$,
- $\mathcal{GL}_n(\mathbb{Z})$ the set of all *invertible* matrices over $\mathbb{Z}$,
- $\mathcal{C}(\boldsymbol{M}) := \{\boldsymbol{C} \in \mathbb{R}^{n\times n} \mid \boldsymbol{CM} = \boldsymbol{MC}\}$ the *centralizer* of $\boldsymbol{M} \in \mathbb{R}^{n\times n}$.

We denote by $\boldsymbol{I}_n$ the $n \times n$ identity matrix. If $\boldsymbol{M}$ is $m \times n$, then $\mathsf{vec}(\boldsymbol{M})$ denotes the column vector of length mn formed by appending the columns of the matrix $\boldsymbol{M}$ one after the other. We write the Gram-Schmidt orthogonalization of $\boldsymbol{M}$ as $\boldsymbol{M}^*$. Given two matrices $\boldsymbol{M}, \boldsymbol{N} \in \mathbb{R}^{n\times n}$, we denote by $\boldsymbol{M} \otimes \boldsymbol{N} \in \mathbb{R}^{n^2\times n^2}$ the matrix obtained by applying the Kronecker product. We recall the mixed Kronecker matrix-vector product property

$$(\boldsymbol{M} \otimes \boldsymbol{N}) \cdot \mathsf{vec}(\boldsymbol{X}) = \mathsf{vec}(\boldsymbol{MXN}^\top), \qquad \text{for } \boldsymbol{X} \in \mathbb{R}^{n\times n}.$$

For a finite set X, the notation $x \xleftarrow{\$} X$ signifies that x is sampled uniformly at random from X. If the set X is infinite, then $x \xleftarrow{\$} X$ means that x has been sampled according to a distribution that is public and efficient.

2.1 Lattice Isomorphism and Quadratic Forms

A full-rank n-dimensional lattice $\mathcal{L} = \mathcal{L}(\boldsymbol{B}) := \boldsymbol{B} \cdot \mathbb{Z}^n$ is generated by taking all of the possible integer combinations of the columns of a basis $\boldsymbol{B} \in \mathbb{R}^{n\times n}$. Two bases $\boldsymbol{B}$ and $\boldsymbol{B}'$ generate the same lattice if and only if there exists a unimodular matrix $\boldsymbol{U} \in \mathcal{GL}_n(\mathbb{Z})$ such that $\boldsymbol{B}' = \boldsymbol{BU}$. Two lattices $\mathcal{L}$, $\mathcal{L}'$ are *isomorphic* if there exists an orthonormal transformation $\boldsymbol{O} \in \mathcal{O}_n(\mathbb{R})$ such that $\mathcal{L}' = \boldsymbol{O} \cdot \mathcal{L}$.

Definition 1 (Lattice Isomorphism Problem (LIP))**.** Given two isomorphic lattices $\mathcal{L}$, $\mathcal{L}' \subset \mathbb{R}^n$ find an orthonormal transformation $\boldsymbol{O} \in \mathcal{O}_n(\mathbb{R})$ such that $\mathcal{L}' = \boldsymbol{O} \cdot \mathcal{L}$.

LIP can be rephrased in terms of lattice bases as follows. Given $\boldsymbol{B}$, $\boldsymbol{B}' \in \mathbb{R}^{n\times n}$ two bases for for $\mathcal{L}$ and $\mathcal{L}'$ respectively, find $\boldsymbol{O} \in \mathcal{O}_n(\mathbb{R})$ and $\boldsymbol{U} \in \mathcal{GL}_n(\mathbb{Z})$ such that $\boldsymbol{B}' = \boldsymbol{OBU}$. In a real-world scenario application, the real-valued entries of the orthonormal matrix can be inefficient to represent on a computer. Reformulating LIP in terms of quadratic forms allows to get around this problem. Let $\boldsymbol{Q}$ be the quadratic form associated to $\boldsymbol{B}$, i.e. the Gram matrix $\boldsymbol{Q} := \boldsymbol{B}^\mathsf{T}\boldsymbol{B}$. Note that, since $\boldsymbol{B}$ is a basis (and thus full-rank), $\boldsymbol{Q}$ is a *symmetric* and *positive definite* matrix. Then we have

$$\boldsymbol{Q}' := \boldsymbol{B}'^\mathsf{T}\boldsymbol{B}' = \boldsymbol{U}^\mathsf{T}\boldsymbol{B}^\mathsf{T}\boldsymbol{O}^\mathsf{T}\boldsymbol{OBU} = \boldsymbol{U}^\mathsf{T}\boldsymbol{B}^\mathsf{T}\boldsymbol{BU} = \boldsymbol{U}^\mathsf{T}\boldsymbol{QU}.$$

We call $\boldsymbol{Q}, \boldsymbol{Q}'$ equivalent if such $\boldsymbol{U} \in \mathcal{GL}_n(\mathbb{Z})$ exists. We define as $[\boldsymbol{Q}]$ the equivalence class of all quadratic forms $\boldsymbol{Q}'$ equivalent to $\boldsymbol{Q}$ under the group action described in Equation (1).

Definition 2 (LIP - Quadratic Form Version)**.** For a quadratic form $\boldsymbol{Q} \in \mathcal{S}_n^{>0}$, the problem LIP is as follows: Given any quadratic form $\boldsymbol{Q}' \in [\boldsymbol{Q}]$, find a unimodular matrix $\boldsymbol{U} \in \mathcal{GL}_n(\mathbb{Z})$ such that $\boldsymbol{Q}' = \boldsymbol{U}^\mathsf{T}\boldsymbol{QU}$.

The squared norm of a vector $\mathbf{x}$ with respect to a quadratic form $\boldsymbol{Q}$ is defined as $\|\mathbf{x}\|_{\boldsymbol{Q}}^2 := \mathbf{x}^\mathsf{T}\boldsymbol{Q}\mathbf{x}$. Let $\boldsymbol{B}_{\boldsymbol{Q}}$ be the Cholesky decomposition of $\boldsymbol{Q}$, that is, an upper triangular matrix such that $\boldsymbol{Q} = \boldsymbol{B}_{\boldsymbol{Q}}{}^\mathsf{T}\boldsymbol{B}_{\boldsymbol{Q}}$. Ducas and van Woerden introduced the *Gaussian Form Distribution* $\mathcal{D}_s([\boldsymbol{Q}])$ over $[\boldsymbol{Q}]$ with a parameter $s > 0$ [DvW22, Def. 3.3], along with a polynomial-time algorithm to sample from it when $s \geq \max\{\lambda_n(\boldsymbol{Q}), \|\boldsymbol{B}_{\boldsymbol{Q}}^*\|\sqrt{\ln(2n+4)/\pi}\}$, [DvW22, Alg. 1] where $\lambda_n(\boldsymbol{Q})$ denotes the norm of the largest eigenvalues of $\boldsymbol{Q}$ and $\|\boldsymbol{B}_{\boldsymbol{Q}}^*\|$ is

the trace norm $\mathrm{Tr}(\boldsymbol{B_Q B_Q^*})^{1/2}$. This algorithm returns a quadratic form $\boldsymbol{Q'} \leftarrow \mathcal{D}_s([\boldsymbol{Q}])$ and a unimodular matrix $\boldsymbol{U}$ such that $\boldsymbol{Q'} = \boldsymbol{U}^\mathsf{T}\boldsymbol{Q}\boldsymbol{U}$ is independent from the input equivalence class representative $\boldsymbol{Q}$ [DvW22, Lemma 3.2]. More precisely, $\mathcal{D}_s([\boldsymbol{Q}])$ is described as below.

Definition 3 (Gaussian Form Distribution [DvW22, Def. 3.3])**.** Given a quadratic form equivalence class $[\boldsymbol{Q}] \subset \mathcal{S}_n^{>0}$, the Gaussian form distribution $\mathcal{D}_s([\boldsymbol{Q}])$ over $[\boldsymbol{Q}]$ with a parameter $s > 0$ is defined algorithmically as follows:

1. Fix a representative $\boldsymbol{Q} \in [\boldsymbol{Q}]$.
2. Sample n vectors $(\mathbf{y}_1, \mathbf{y}_2, \dots \mathbf{y}_n) \coloneqq Y$ from $\mathcal{D}_{\boldsymbol{Q},s}$. Repeat until linearly independent.
3. $(\boldsymbol{R}, \boldsymbol{U}) \leftarrow \mathbf{Extract}(\boldsymbol{Q}, \boldsymbol{Y})$.
4. Return $\boldsymbol{R}$.

where $\mathcal{D}_{\boldsymbol{Q},s}$ denotes the discrete Gaussian distribution with center at $\mathbf{0}$ as defined in [DvW22, Sec. 2.3], and the algorithm **Extract** includes a method to derive a unimodular matrix from a set of independent vectors employing the Hermite Normal Form reduction as done in the literature [BM21, MG02]. In particular, **Extract** returns a quadratic form $\boldsymbol{Q'}$ and a unimodular matrix $\boldsymbol{U}$ such that $\boldsymbol{Q'} = \boldsymbol{U}^\mathsf{T}\boldsymbol{Q}\boldsymbol{U}$.

2.2 Lattice Isomorphism as a Group Action

The Lattice Isomorphism Problem in the quadratic form version has been modeled as a group action problem in [BBCK24]. In this section, we briefly recall the necessary definitions for this manuscript. For a more detailed formalization of LIP as a group action, we refer the reader to [BBCK24].

Let $(G, \circ)$ be a group and X be a set. A *group action* is a map

$$\star : \ G \times X \to X$$

such that, for any $g_1, g_2 \in G$ and any $x \in X$, we have that $g_1 \star (g_2 \star x) = (g_1 \circ g_2) \star x$. A group action is called *cryptographic* when it satisfies certain properties that are interesting from a cryptographic point of view. Specifically, we are interested in the following properties.

Definition 4. A group action $\star : G \times X \to X$ is said to be:

- *one-way* if, given $x, x' \in X$, there is no probabilistic polynomial-time algorithm that outputs (if it exists) an element $g \in G$ such that $x' = g \star x$.
- *t-weakly unpredictable* if, given t pairs $(x_i, x_i') \in X \times X$ where $x_i' = g \star x_i$ for some unknown $g \in G$ (which remains the same across all pairs), and given an additional element $\bar{x} \in X$ different from each x_i, there is no probabilistic polynomial-time algorithm that outputs $\bar{x}' = g \star \bar{x}$.
- *t-weakly pseudorandom* if, given t pairs $(x_i, x_i') \in X \times X$, there is no probabilistic polynomial-time algorithm to decide whether each pair is of the form $(x_i, x_i' = g \star x_i)$ for some fixed secret $g \in G$, or $(x_i, x_i') \xleftarrow{\$} X \times X$ according to a public distribution.

Let $\mathcal{GL}_n^{\pm}(\mathbb{Z}) \coloneqq \mathcal{GL}_n(\mathbb{Z}) / \simeq_{\pm}$ be the quotient of $\mathcal{GL}_n(\mathbb{Z})$ with respect to the equivalence relation $\simeq_{\pm}$ such that $\boldsymbol{U} \simeq_{\pm} \boldsymbol{V} \iff \boldsymbol{U} = \pm\boldsymbol{V}$. Notice that $\mathcal{GL}_n^{\pm}(\mathbb{Z})$ forms a group with the multiplicative operation defined as follows. Let $[\boldsymbol{U}]_{\pm} = \{\boldsymbol{U}, -\boldsymbol{U}\}$ be the class of equivalence of the matrix $\boldsymbol{U} \in \mathcal{GL}_n(\mathbb{Z})$, then the multiplicative operation between elements of $\mathcal{GL}_n^{\pm}(\mathbb{Z})$ is defined as

$$[\boldsymbol{U}]_{\pm} \cdot [\boldsymbol{V}]_{\pm} \coloneqq [\boldsymbol{V}\boldsymbol{U}]_{\pm}, \quad \text{for} \quad [\boldsymbol{U}]_{\pm}, [\boldsymbol{V}]_{\pm} \in \mathcal{GL}_n^{\pm}(\mathbb{Z}).$$

In what follows, for simplicity, we drop the notation of the equivalence class $[\boldsymbol{U}]_{\pm}$ and simply use a representative $\boldsymbol{U}$. Given a quadratic form $\boldsymbol{Q} \in \mathcal{S}_n^{>0}$, the *Lattice Isomorphism Group Action* (LIGA) is defined as

$$\star \colon \mathcal{GL}_n^{\pm}(\mathbb{Z}) \times [\boldsymbol{Q}] \to [\boldsymbol{Q}], \qquad \star(\boldsymbol{U}, \boldsymbol{Q}_0) \mapsto \boldsymbol{U} \star \boldsymbol{Q}_0 \coloneqq \boldsymbol{U}^{\mathsf{T}} \boldsymbol{Q}_0 \boldsymbol{U},$$

Benčina et al. study the cryptographic properties of LIGA, and prove that it is not t-weakly unpredictable and t-weakly pseudorandom, for $t = O(n^2)$ [BBCK24].

3 New Results on the Properties of LIGA

This section introduces a new model for constructing a linear system from a set of LIP instances with $2n^2$ variables. This improves upon the formulation proposed in [BBCK24] by achieving a higher ratio of equations to variables. Leveraging this improved modeling, we design two probabilistic polynomial-time algorithms that establish new lower bounds on the necessary number of instances to break the weak unpredictability and pseudorandomness properties of LIGA.

Let

$$(\boldsymbol{Q}_i, \boldsymbol{Q}_i' = \boldsymbol{U}^{\top} \boldsymbol{Q}_i \boldsymbol{U}) \in \mathcal{S}_n^{>0} \times \mathcal{S}_n^{>0}, \quad i = 1, \ldots, t$$

be t LIP instances, where $\boldsymbol{Q}_i \leftarrow \mathcal{D}_s([\boldsymbol{Q}])$, for some $\boldsymbol{Q} \in \mathcal{S}_n^{>0}$, and $\boldsymbol{U} \in \mathcal{GL}_n(\mathbb{Z})$. Then, since $\boldsymbol{U}$ is invertible, we have that $\boldsymbol{Q}_i' \boldsymbol{U}^{-1} = \boldsymbol{U}^{\top} \boldsymbol{Q}_i$. Now, applying the mixed Kronecker matrix-vector product property on the matrix equation

$$\boldsymbol{Q}_i' \boldsymbol{U}^{-1} \boldsymbol{I}_n = \boldsymbol{I}_n \boldsymbol{U}^{\top} \boldsymbol{Q}_i,$$

we get that

$$\boldsymbol{Q}_i' \boldsymbol{U}^{-1} = \boldsymbol{U}^{\top} \boldsymbol{Q}_i \iff [\boldsymbol{Q}_i' \otimes \boldsymbol{I}_n] \cdot \mathsf{vec}(\boldsymbol{U}^{-1}) = [\boldsymbol{I}_n \otimes \boldsymbol{Q}_i] \cdot \mathsf{vec}(\boldsymbol{U}^{\top}),$$

for $i = 1, \ldots, t$. Thanks to this observation, we can write the following linear system with $2n^2$ variables and tn^2 equations.

$$\overbrace{\begin{bmatrix} \boldsymbol{Q}_1' \otimes \boldsymbol{I}_n & \mid & \boldsymbol{I}_n \otimes (-\boldsymbol{Q}_1) \\ \boldsymbol{Q}_2' \otimes \boldsymbol{I}_n & \mid & \boldsymbol{I}_n \otimes (-\boldsymbol{Q}_2) \\ \vdots & \vdots & \vdots \\ \boldsymbol{Q}_t' \otimes \boldsymbol{I}_n & \mid & \boldsymbol{I}_n \otimes (-\boldsymbol{Q}_t) \end{bmatrix}}^{\boldsymbol{A} \in \mathbb{R}^{tn^2 \times 2n^2}} \boldsymbol{x} = \boldsymbol{0} \in \mathbb{R}^{tn^2}. \tag{2}$$

By construction, the system $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{0}$ has at least one non-zero solution, namely the column vector $\boldsymbol{x} = \left[\mathsf{vec}(\boldsymbol{U}^{-1}) \mid \mathsf{vec}(\boldsymbol{U}^{\top})\right]$. Therefore, $\operatorname{rank}(\boldsymbol{A}) \leq 2n^2 - 1$ for any $t \geq 2$.

Remark 1. In this section, we consider that $\boldsymbol{Q}_i \leftarrow \mathcal{D}_s([\boldsymbol{Q}])$, for $i = 1, \ldots, t$, in order to be consistent with the definition of group action where all elements $\boldsymbol{Q}_i$ belong to the same set $[\boldsymbol{Q}]$. However, the results presented in this section also hold for $\boldsymbol{Q}_i$ belonging to separate classes of equivalence.

3.1 LIGA is not 2-Weakly Pseudorandom

We show now that weak pseudorandomness is not guaranteed even for $t = 2$. First, let us consider the following result.

Lemma 1. *Given two* LIP *samples* $(\boldsymbol{Q}_i, \boldsymbol{Q}_i' = \boldsymbol{U}^{\top} \boldsymbol{Q}_i \boldsymbol{U})$*, for* $i = 1, 2$*, then the* $2n^2 \times 2n^2$ *matrix*

$$\boldsymbol{A} = \begin{bmatrix} \boldsymbol{Q}_1' \otimes \boldsymbol{I}_n & \mid & \boldsymbol{I}_n \otimes (-\boldsymbol{Q}_1) \\ \boldsymbol{Q}_2' \otimes \boldsymbol{I}_n & \mid & \boldsymbol{I}_n \otimes (-\boldsymbol{Q}_2) \end{bmatrix} \in \mathbb{R}^{2n^2 \times 2n^2} \tag{3}$$

has rank at most equal to $2n^2 - n$.

Proof. The linear system $\boldsymbol{Ax} = \boldsymbol{0}$ has at least one solution given by $[\mathsf{vec}(\boldsymbol{U}^{-1}) \mid \mathsf{vec}(\boldsymbol{U}^{\top})]$. To show it admits other solutions we rewrite it as matrix equations

$$\begin{aligned} \boldsymbol{Q}'_1\boldsymbol{X} &= \boldsymbol{Y}\boldsymbol{Q}_1 \\ \boldsymbol{Q}'_2\boldsymbol{X} &= \boldsymbol{Y}\boldsymbol{Q}_2 \end{aligned} \tag{4}$$

A solution to this second system is given by $\boldsymbol{X} = \boldsymbol{U}^{-1}$ and $\boldsymbol{Y} = \boldsymbol{U}^{\top}$. Assuming $\boldsymbol{Q}'_1$ to be full rank, we can express $\boldsymbol{X}$ in terms of $\boldsymbol{Y}$ as $\boldsymbol{X} = (\boldsymbol{Q}'_1)^{-1}\boldsymbol{Y}\boldsymbol{Q}_1$, where the inverse is defined over $\mathbb{R}$. Substituting in the second equation we get

$$\boldsymbol{Q}'_2(\boldsymbol{Q}'_1)^{-1}\boldsymbol{Y} = \boldsymbol{Y}\boldsymbol{Q}_2\boldsymbol{Q}_1^{-1}.$$

We rename $\boldsymbol{R} = \boldsymbol{Q}'_2(\boldsymbol{Q}'_1)^{-1}$ and $\boldsymbol{T} = \boldsymbol{Q}_2\boldsymbol{Q}_1^{-1}$ obtaining the equation

$$\boldsymbol{RY} = \boldsymbol{YT}. \tag{5}$$

Notice that it is still true that this equation is satisfied by $\boldsymbol{Y} = \boldsymbol{U}^{\top}$. Consider $\boldsymbol{Y}' = \boldsymbol{CY}$ where $\boldsymbol{C} \in \mathcal{C}(\boldsymbol{R}) := \{\boldsymbol{C} \in \mathbb{R}^{n\times n} \mid \boldsymbol{CR} = \boldsymbol{RC}\}$ is an element of the centralizer of $\boldsymbol{R}$, this is still a solution of Equation 5. In fact we have that

$$\boldsymbol{RY}' = \boldsymbol{RCY} = \boldsymbol{C}(\boldsymbol{RY}) = \boldsymbol{CYT} = \boldsymbol{Y}'\boldsymbol{T}.$$

Each element of the lateral $\mathcal{C}(\boldsymbol{R})\boldsymbol{U}^{\top} = \{\boldsymbol{CU}^{\top} \mid \boldsymbol{C} \in \mathcal{C}(\boldsymbol{R})\}$ is a solution of Equation 5 to which it corresponds a unique solution of Equation 4. Since $\mathcal{C}(\boldsymbol{R})$ is a vector space of dimension at least n [HJ94, Theorem 4.4.17] and $\boldsymbol{U}$ is an invertible matrix, then the lateral $\mathcal{C}(\boldsymbol{R})\boldsymbol{U}^{\top}$ is a vector space of the same dimension. It follows that the rank of the whole system is at most equal to $2n^2 - n$. □

Let us analyze the following scenario. Let $\boldsymbol{Q}_1, \boldsymbol{Q}'_1, \boldsymbol{Q}_2, \boldsymbol{Q}'_2 \leftarrow \mathcal{D}_s([\boldsymbol{Q}])$ be sampled independently, for some $\boldsymbol{Q} \in \mathcal{S}_n^{>0}$. Then, even if $(\boldsymbol{Q}'_0, \boldsymbol{Q}_0)$ and $(\boldsymbol{Q}'_1, \boldsymbol{Q}_1)$ are LIP instances, it is not guaranteed that the secret unimodular transformation is the same for both of them. We argue below that in this case, the linear system $\boldsymbol{Ax} = \boldsymbol{0}$ with $\boldsymbol{A}$ as in Equation 3 does not accept any solutions with high probability. Let us consider the following lemma.

Lemma 2. *Let $\boldsymbol{Q}_1, \boldsymbol{Q}'_1, \boldsymbol{Q}_2, \boldsymbol{Q}'_2 \leftarrow \mathcal{D}_s([\boldsymbol{Q}])$ be sampled independently and consider $\boldsymbol{U}, \boldsymbol{V} \in \mathcal{GL}(\mathbb{Z})$, with $\boldsymbol{U} \neq \boldsymbol{V}$, such that $\boldsymbol{Q}'_1 = \boldsymbol{U}^{\top}\boldsymbol{Q}_1\boldsymbol{U}$ and $\boldsymbol{Q}'_2 = \boldsymbol{V}^{\top}\boldsymbol{Q}_2\boldsymbol{V}$. If the matrices $\boldsymbol{R} = \boldsymbol{Q}'_2(\boldsymbol{Q}'_1)^{-1}$ and $\boldsymbol{T} = \boldsymbol{Q}_2(\boldsymbol{Q}_1)^{-1}$ do not share any eigenvalues, then the matrix*

$$\boldsymbol{A} = \left[\begin{array}{c|c} \boldsymbol{Q}'_1 \otimes \boldsymbol{I}_n & \boldsymbol{I}_n \otimes (-\boldsymbol{Q}_1) \\ \boldsymbol{Q}'_2 \otimes \boldsymbol{I}_n & \boldsymbol{I}_n \otimes (-\boldsymbol{Q}_2) \end{array}\right] \in \mathbb{R}^{2n^2\times 2n^2} \tag{6}$$

has rank $2n^2$.

Proof. The rank of $\boldsymbol{A}$ in Equation 3 is given by $2n^2 - t$, where t is the dimension of the solution space of $\boldsymbol{Ax} = \boldsymbol{0}$. Any solution is a column vector of the form $[\mathsf{vec}(\boldsymbol{X}) \mid \mathsf{vec}(\boldsymbol{Y})]$ where $\boldsymbol{X}$ and $\boldsymbol{Y}$ are two $n \times n$ matrices. In particular, $\boldsymbol{Y}$ fully determines the whole solution as $\boldsymbol{X} = (\boldsymbol{Q}'_1)^{-1}\boldsymbol{Y}\boldsymbol{Q}_1$, where the inverse is considered over $\mathbb{R}$. Moreover $\boldsymbol{Y}$ has to satisfy Equation 5 that can be rewritten as

$$\boldsymbol{R}^{-1}\boldsymbol{YT} = \boldsymbol{Y}, \tag{7}$$

where $\boldsymbol{R} = \boldsymbol{Q}'_2(\boldsymbol{Q}'_1)^{-1}$ and $\boldsymbol{T} = \boldsymbol{Q}_2(\boldsymbol{Q}_1)^{-1}$. In other words, the vector $\mathsf{vec}(\boldsymbol{Y})$ is an eigenvector of $\boldsymbol{R}^{-1} \otimes \boldsymbol{T}^{\top}$ of eigenvalue 1. If we show that the matrix $\boldsymbol{R}^{-1} \otimes \boldsymbol{T}^{\top}$ has no eigenvalue equal to 1, it means that there is no non-trivial solution $\boldsymbol{Y}$, which in turn implies that the matrix $\boldsymbol{A}$ is of full rank $2n^2$.

The eigenvalues of the Kronecker product of two matrices are the products of the eigenvalues of the two matrices [HJ94, Theorem 4.2.12]. Let $\mu_1, \ldots, \mu_{n_R}$ be the distinct

eigenvalues of $\boldsymbol{R}$ and $\lambda_1, \ldots, \lambda_{n_T}$ be the distinct eigenvalues of $\boldsymbol{T}$, the eigenvalues of $\boldsymbol{R}^{-1} \otimes \boldsymbol{T}^\top$ are all the values $\mu_1^{-1}\lambda_1, \ldots, \mu_{n_R}^{-1}\lambda_{n_T}$. Observe that the eigenvalue 1 is obtained if and only if $\boldsymbol{R}$ and $\boldsymbol{T}$ share at least one eigenvalue. In the hypothesis, we assumed that this is not the case. Hence, the eigenvalues of $\boldsymbol{R}^{-1} \otimes \boldsymbol{T}^\top$ are all different from 1; therefore, we cannot find a solution $\boldsymbol{Y}$ and the matrix $\boldsymbol{A}$ must have full rank $2n^2$.

□

Quantifying the probability that $\boldsymbol{R}$ and $\boldsymbol{T}$ in Lemma 2 share no eigenvalues, and so $\operatorname{rank}(\boldsymbol{A}) = 2n^2$, turned out to be an elusive task as it depends on the distribution of the eigenvalues of the quadratic forms sampled from $\mathcal{D}_s([\boldsymbol{Q}])$. Nevertheless, we heuristically expect this event to happen with high probability, which we formalize in the following assumption.

Assumption 1. *Let $\boldsymbol{Q}_1, \boldsymbol{Q}_1', \boldsymbol{Q}_2, \boldsymbol{Q}_2' \leftarrow \mathcal{D}_s([\boldsymbol{Q}])$ be sampled independently, then the matrix*

$$\boldsymbol{A} = \begin{bmatrix} \boldsymbol{Q}_1' \otimes \boldsymbol{I}_n & \mid & \boldsymbol{I}_n \otimes (-\boldsymbol{Q}_1) \\ \boldsymbol{Q}_2' \otimes \boldsymbol{I}_n & \mid & \boldsymbol{I}_n \otimes (-\boldsymbol{Q}_2) \end{bmatrix} \in \mathbb{R}^{2n^2 \times 2n^2} \tag{8}$$

has rank $2n^2$ with high probability.

Experimental validation. To support Assumption 1, we conducted extensive experiments in `SageMath` for $n \in \{10, 20, 30, 40, 50\}$ and different choices of the distribution parameter s ranging from 0.5 to $\max\{\lambda_n(\boldsymbol{Q}), \left\|\boldsymbol{B}_{\boldsymbol{Q}}^*\right\| \sqrt{\ln(2n+4)/\pi}\}$. For each setting, we ran 100 test trials in which we independently sampled four quadratic forms from $\mathcal{D}_s([\boldsymbol{Q}])$ and measured the rank of the relative matrix $\boldsymbol{A}$. We observed that $\operatorname{rank}(\boldsymbol{A}) = 2n^2$ in every trial. Additionally, we conducted a similar experiment to validate Lemma 1. This time, we sampled two LIP instances with the same unimodular matrix and quadratic forms belonging to the same class $[\boldsymbol{Q}]$. In this case, we consistently observed that $\operatorname{rank}(\boldsymbol{A}) = 2n^2 - n$ in every trial. We make the code to reproduce these experiments open source and available at [BCDF25].

We give now the following result regarding the properties of LIGA.

Theorem 1. *Under Assumption 1,* LIGA *is not 2-weakly pseudorandom.*

Proof. We prove this by introducing a probabilistic polynomial-time algorithm, formalized as Algorithm 1, that is able to decide whether, given $\boldsymbol{Q}_1, \boldsymbol{Q}_1', \boldsymbol{Q}_2, \boldsymbol{Q}_2' \in [\boldsymbol{Q}]$ for some $\boldsymbol{Q} \in \mathcal{S}_n^{>0}$, there exists a unimodular matrix $\boldsymbol{U} \in \mathcal{GL}_n(\mathbb{Z})$ such that $\boldsymbol{Q}_i' = \boldsymbol{U}^\top \boldsymbol{Q}_i \boldsymbol{U}$, for $i = 1, 2$, or not.

Algorithm 1 Distinguishing 2LIP

Input: $\boldsymbol{Q}_1, \boldsymbol{Q}_1', \boldsymbol{Q}_2, \boldsymbol{Q}_2' \in [\boldsymbol{Q}]$ for some $\boldsymbol{Q} \in \mathcal{S}_n^{>0}$
Output: *True* if there exists $\boldsymbol{U} \in \mathcal{GL}_n(\mathbb{Z})$ such that $\boldsymbol{Q}_i' = \boldsymbol{U}^\top \boldsymbol{Q}_i \boldsymbol{U}$ for $i = 1, 2$, and *False* otherwise.

1: Compute the matrix $\boldsymbol{A}$ as defined in Equation 3.
2: **if** $\operatorname{rank}(\boldsymbol{A}) \leq 2n^2 - n$ **then**
3: **Return** *True*
4: **else**
5: **Return** *False*
6: **end if**

Let us prove the correctness of Algorithm 1. If the pairs $(\boldsymbol{Q}_i, \boldsymbol{Q}_i')$ share the same secret unimodular transformation, Lemma 1 guarantees that $\operatorname{rank}(\boldsymbol{A}) \leq 2n^2 - n$, ensuring that Algorithm 1 returns *True*. Conversely, if $\boldsymbol{Q}_1, \boldsymbol{Q}_1', \boldsymbol{Q}_2, \boldsymbol{Q}_2' \leftarrow \mathcal{D}_s([\boldsymbol{Q}])$, then by Assumption 1, $\operatorname{rank}(\boldsymbol{A}) = 2n^2$ with high probability, leading Algorithm 1 to return *False*.

Finally, we analyze the algorithm's complexity. Computing the rank of $\boldsymbol{A}$ has a complexity in terms of integers operations of $O(n^6)$ in time and $O(n^4)$ in memory. Thus, Algorithm 1 runs in polynomial time in n. □

Theorem 1 represents an improvement over the work of [BBCK24] for which $O(n^2)$ LIP samples were necessary to break the weakly pseudorandomness property of LIGA.

3.2 LIGA is not 3-Weakly Unpredictable

Let us consider now the case of having three LIP instances with the same secret. In this case, the system in Equation 2 has $3n^2$ equations, and, as explained above, its rank is at most equal to $2n^2 - 1$. In this section, we argue that such an upper bound for the rank is reached with high probability, allowing an efficient recovery of the secret monomial $\boldsymbol{U}$ simply by running Gaussian elimination on such a linear system.

Let $(\boldsymbol{Q}_i, \boldsymbol{Q}'_i = \boldsymbol{U}^\top \boldsymbol{Q}_i \boldsymbol{U})$ be three LIP instances, where $\boldsymbol{Q}_i \leftarrow \mathcal{D}_s([\boldsymbol{Q}])$ for $i = 1, 2, 3$. Let us consider the following $3n^2 \times 2n^2$ matrix

$$\boldsymbol{A} = \begin{bmatrix} \boldsymbol{Q}'_1 \otimes \boldsymbol{I}_n & | & \boldsymbol{I}_n \otimes (-\boldsymbol{Q}_1) \\ \boldsymbol{Q}'_2 \otimes \boldsymbol{I}_n & | & \boldsymbol{I}_n \otimes (-\boldsymbol{Q}_2) \\ \boldsymbol{Q}'_3 \otimes \boldsymbol{I}_n & | & \boldsymbol{I}_n \otimes (-\boldsymbol{Q}_3) \end{bmatrix} \in \mathbb{R}^{3n^2 \times 2n^2}. \tag{9}$$

We argue that $\operatorname{rank}(\boldsymbol{A}) = 2n^2 - 1$ with high probability. One solution to the system $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{0}$ is given by $[\mathsf{vec}(\boldsymbol{U}^{-1}) \mid \mathsf{vec}(\boldsymbol{U}^\top)]$, therefore the rank of $\boldsymbol{A}$ is less or equal than $2n^2 - 1$. We rewrite $\boldsymbol{A}$ in terms of matrix equations as

$$\begin{aligned} \boldsymbol{Q}'_1 \boldsymbol{X} &= \boldsymbol{Y} \boldsymbol{Q}_1 \\ \boldsymbol{Q}'_2 \boldsymbol{X} &= \boldsymbol{Y} \boldsymbol{Q}_2. \\ \boldsymbol{Q}'_3 \boldsymbol{X} &= \boldsymbol{Y} \boldsymbol{Q}_3 \end{aligned} \tag{10}$$

Let us consider only the first two equations. We have the same result as in Lemma 1, that is $\boldsymbol{Y} \in \mathcal{C}(\boldsymbol{R}_{12})\boldsymbol{U}^\top$, where $\mathcal{C}(\boldsymbol{R}_{12})$ is the centralizer of the matrix $\boldsymbol{R}_{12} = \boldsymbol{Q}'_2 \boldsymbol{Q}'^{-1}_1$. Since $\boldsymbol{Y}$ must satisfy the third equation, we get that

$$\boldsymbol{Y} \in \left(\mathcal{C}(\boldsymbol{R}_{12}) \cap \mathcal{C}(\boldsymbol{R}_{13}) \cap \mathcal{C}(\boldsymbol{R}_{23})\right) \boldsymbol{U}^\top$$

where $\boldsymbol{R}_{ij} = \boldsymbol{Q}'_j \boldsymbol{Q}'^{-1}_i$. Since the identity commutes with any matrix, each space $\mathcal{C}(\boldsymbol{R}_{ij})$ contains it, and so will their intersection. The three spaces $\mathcal{C}(\boldsymbol{R}_{ij})$ have in general dimension n and are all contained in the space $\mathbb{R}^{n \times n}$ of dimension n^2. Heuristically, we expect their intersection to be constituted by $\boldsymbol{I}_n$ and its scalar multiples only. Hence, all the possible solutions are in the form $\boldsymbol{Y} = \lambda \boldsymbol{U}^\top$ for some scalar λ and $\operatorname{rank}(\boldsymbol{A}) = 2n^2 - 1$. We formalize the above in the following.

Assumption 2. *Let $(\boldsymbol{Q}_i, \boldsymbol{Q}'_i = \boldsymbol{U}^\top \boldsymbol{Q}_i \boldsymbol{U})$ be three* LIP *instances, where $\boldsymbol{Q}_i \leftarrow \mathcal{D}_s([\boldsymbol{Q}])$ for $i = 1, 2, 3$. Then, the matrix $\boldsymbol{A}$ as in Equation 9 has rank $2n^2 - 1$ with high probability.*

The following theorem constitutes another improvement over the work of [BBCK24] which required $O(n^2)$ LIP instances with the same secret to recover the secret monomial.

Theorem 2. *Under Assumption 2,* LIGA *is not 3-weakly unpredictable.*

Proof. We prove that there exists a polynomial-time algorithm such that, given three LIP instances with the same secret, is able to recover such a secret and so predict any other outcome of the group action for that fixed group element. Under the setting of Assumption 2, applying Gaussian elimination on the linear system in Equation 9, one gets a solution vector $\boldsymbol{s} = [\mathsf{vec}(\lambda \boldsymbol{U}^{-1}) \mid \mathsf{vec}(\lambda \boldsymbol{U}^\top)] \in \mathbb{R}^{2n^2}$, for some $\lambda \in \mathbb{R}$, with high probability. The second half of the vector $\boldsymbol{s}$ corresponds to the concatenations of the rows of $\lambda \boldsymbol{U}^\top$. To retrieve $\boldsymbol{U}$ from $\lambda \boldsymbol{U}^\top$, observe that $\det(\lambda \boldsymbol{U}) = \pm \lambda^n$, then $\boldsymbol{U} = \pm |\det(\lambda \boldsymbol{U})|^{-\frac{1}{n}} \lambda \boldsymbol{U}$. The complexity of the whole procedure is ruled by running Gaussian elimination on $\boldsymbol{A}$, which has a polynomial-time cost of $O(n^6)$ integer operations and a memory cost of $O(n^4)$. □

Experimental validation. To support Assumption 2, we run extensive experiments in `SageMath` for dimensions $n \in \{10, 20, 30, 40, 50\}$, different values of the distribution parameter s. We run 100 trials for each parameter setting. We observe that $\operatorname{rank}(\boldsymbol{A}) = 2n^2 - 1$ for every run. Additionally, as a proof-of-concept, we tested Theorem 2 experimentally and successfully recovered the secret unimodular $\boldsymbol{U}$ for $n \in \{8, 16, 32, 64\}$. In this case, we focused on values of n that are powers of 2 as it allows efficient computation of $|\det(\lambda \boldsymbol{U})|^{-\frac{1}{n}}$ by recursively computing the square root. For other values of $n \geq 20$, the multi-precision integer arithmetic of `SageMath` fails to compute the n-th root when the integers are large. We make the code to reproduce these experiments open source and available at [BCDF25].

4 Cryptographic Implications

This section details the implications of the results reported in Section 3 from a cryptographic point of view. Specifically, we show that LIGA not being 2-weakly pseudorandom breaks the *linkable anonymity* property of the ring signature based on LIP proposed by Khuc et al. [KTS+24].

Background on linkable ring signatures. In a nutshell, a linkable ring signature consists of a 5-tuple of PPT algorithms ($\mathsf{LRS.Setup}$, $\mathsf{LRS.KeyGen}$, $\mathsf{LRS.Sign}$, $\mathsf{LRS.Verify}$, $\mathsf{LRS.Link}$) such that [3]

- $\mathsf{LRS.Setup}(\lambda) \to \mathsf{pp}$: On input of a security parameter λ, it returns the public parameters pp used by the scheme.
- $\mathsf{LRS.Keygen}(\mathsf{pp}) \to (\mathsf{sk}, \mathsf{vk})$: On input the public parameters pp, it outputs both secret and public keys $(\mathsf{sk}, \mathsf{vk})$.
- $\mathsf{LRS.Sign}(\mathsf{sk}, \mathsf{M}, \mathsf{R}) \to \sigma$: On input a secret key sk, a message M, and a list of public keys $\mathsf{R} = (\mathsf{vk}_1, \ldots, \mathsf{vk}_m)$ (called a ring), it outputs a signature σ.
- $\mathsf{LRS.Verify}(\mathsf{R}, \mathsf{M}, \sigma) \to b \in \{0, 1\}$: On input a ring $\mathsf{R} = (\mathsf{vk}_1, \ldots, \mathsf{vk}_m)$, a message M, and a signature σ, it outputs either 1 if the signature is accepted. Otherwise, it returns 0.
- $\mathsf{LRS.Link}(\sigma_0, \sigma_1) \to b \in \{0, 1\}$: On input two signatures σ_0 and σ_1, it outputs either 1 if the signatures are produced with the same secret key. Otherwise, it returns 0.

The linkable ring signature by Khuc et al. [KTS+24], which follows the framework from [BKP20], requires a pair of group actions and a function

$$\star : G \times X \to X, \qquad \bullet : G \times T \to T, \qquad \mathsf{LINK} : T \times T \to \{0, 1\},$$

that must satisfy the following properties:

- (*Correctness*) $\mathsf{LINK}(t, t) = 1$, for all $t \in T$.
- (*Linkability*) It is hard to find a secret key $g, g' \in G$ such that $g' \star x = g \star x$ but $\mathsf{LINK}(g' \bullet t, g \bullet t) = 0$.
- (*Linkable Anonymity*) Given $(x, t) \in X \times T$ and for a secret $g \in G$, the distributions $(g \star x, g \bullet t)$ and $(x', t') \xleftarrow{\$} X \times T$ are indistinguishable.
- (*Non-Frameability*) Given $x' = g \star x$ and $t' = g \bullet t$, it is hard to find $\mathsf{LINK}(s' \bullet t, t) = 1$.

[3] For more details, we recommend to the readers [BKP20].

In the above, the function LINK is defined specifically for every group action, and the elements in T determine tags to check the link between signatures; for example, in the case of LIGA, we have that $\mathsf{LINK}(t, t') = 1 \iff t = t'$. On the other hand, each output of the algorithm $\mathsf{LRS.KeyGen}$ is of the form $(\mathsf{sk}, \mathsf{vk} = \mathsf{sk} \star x)$ for some public element $x \in X$, and each output of the algorithm $\mathsf{LRS.Sign}$ includes the tag $t = \mathsf{sk} \bullet x$. In addition, given two signatures σ_0 and σ_1, $\mathsf{LRS.Link}(\sigma_0, \sigma_1)$ is defined as $\mathsf{LINK}(t_0, t_1)$ where t_0 and t_1 are the tags in σ_0 and σ_1, respectively.

The linkable anonymity property asks that any adversary with multiple signatures from the same signer should be unable to determine which ring user produced a given signature. Formally speaking, linkable anonymity is defined in [BKP20] as follows.

Definition 5 (Linkable anonymity [BKP20])**.** A linkable ring signature is called linkable anonymous if, for all $\lambda \in \mathbb{N}$ and $m = \mathsf{poly}(\lambda)$, any PPT adversary $\mathcal{A}$ has a negligible advantage in the following game played against a challenger $\mathcal{C}$.

1. $\mathcal{C}$ starts by running $\mathsf{pp} \leftarrow \mathsf{LRS.Setup}(\lambda)$, generating $(\mathsf{sk}_i, \mathsf{vk}_i) \leftarrow \mathsf{LRS.KeyGen}(\mathsf{pp}; \mathsf{rr}_i)$ for each $i := 1, \ldots, m$ for some random coins rr_i, and sampling a random bit $b \xleftarrow{\$} \{0, 1\}$.
2. $\mathcal{C}$ shares pp and $\mathsf{vk} = \{\mathsf{vk}_1, \ldots, \mathsf{vk}_m\}$ with $\mathcal{A}$.
3. $\mathcal{A}$ sends two challenge verification keys $\mathsf{vk}_0^*, \mathsf{vk}_1^* \in \mathsf{vk}$ to $\mathcal{C}$.
4. $\mathcal{C}$ shares all rr_i of the corresponding $\mathsf{vk} \setminus \{\mathsf{vk}_0^*, \mathsf{vk}_1^*\}$ with $\mathcal{A}$.
5. $\mathcal{A}$ queries for signatures on input a verification key $\mathsf{vk}^* \in \{\mathsf{vk}_0^*, \mathsf{vk}_1^*\}$, a message M, and a ring $\mathsf{R} \supseteq \{\mathsf{vk}_0^*, \mathsf{vk}_1^*\}$. More precisely, if sk_i^* denotes the corresponding secret key such that $\mathsf{vk}_i^* = \mathsf{sk}_i^* \star x$ where $x \in \mathsf{pp}$ is fixed and public, then
   - If $\mathsf{vk}^* = \mathsf{vk}_0^*$, then $\mathcal{C}$ returns $\sigma^* \leftarrow \mathsf{LRS.Sign}(\mathsf{sk}_b^*, \mathsf{M}, \mathsf{R})$.
   - Otherwise, $\mathcal{C}$ returns $\sigma^* \leftarrow \mathsf{LRS.Sign}(\mathsf{sk}_{1-b}^*, \mathsf{M}, \mathsf{R})$.
6. $\mathcal{A}$ makes a guess $b^* \in \{0, 1\}$, and sends it to $\mathcal{C}$. If $b^* = b$, we say that the adversary $\mathcal{A}$ wins.

Vulnerability in the LIP-based proposal. Khuc et al. propose to instantiate the first group action $\star$ as LIGA, and the second group action $\bullet$ as

$$\bullet \colon \mathcal{GL}_n^{\pm}(\mathbb{Z}) \times [\boldsymbol{Q}] \to [\boldsymbol{Q}], \qquad \bullet(\boldsymbol{U}, \boldsymbol{Q}_0) \mapsto \boldsymbol{U} \bullet \boldsymbol{Q}_0 := \boldsymbol{U}^{-1} \star \boldsymbol{Q}_0.$$

In particular, Khuc et al. assume $X = T = [\boldsymbol{Q}]$ and the group actions are applied to the same element $\boldsymbol{Q}_0 \in [\boldsymbol{Q}]$. Now, given $\boldsymbol{Q}_0' = \boldsymbol{U} \star \boldsymbol{Q}_0$ and $\boldsymbol{Q}_0'' = \boldsymbol{U} \bullet \boldsymbol{Q}_0$ for some public $\boldsymbol{Q}_0$, observe that the linkability property requires that the following two pairs

$$(\boldsymbol{U} \star \boldsymbol{Q}_0, \boldsymbol{U} \bullet \boldsymbol{Q}_0) \quad \text{and} \quad (\bar{\boldsymbol{Q}} \leftarrow \mathcal{D}_s([\boldsymbol{Q}]), \hat{\boldsymbol{Q}} \leftarrow \mathcal{D}_s([\boldsymbol{Q}]))$$

are indistinguishable. Therefore, we want to show that this property is not satisfied for the above choices of group actions. First, notice that

$$\boldsymbol{Q}_0'' = \boldsymbol{U} \bullet \boldsymbol{Q}_0 = \boldsymbol{U}^{-\mathbf{1}} \star \boldsymbol{Q}_0 \Leftrightarrow \boldsymbol{U} \star \boldsymbol{Q}_0'' = \boldsymbol{Q}_0.$$

Then, the pairs $(\boldsymbol{Q}_0, \boldsymbol{Q}_0')$ and $(\boldsymbol{Q}_0'', \boldsymbol{Q}_0)$ are two LIP instances that share the same secret unimodular $\boldsymbol{U}$. However, as a consequence of Section 3.1, we can distinguish the pair $(\boldsymbol{Q}_0', \boldsymbol{Q}_0'',)$ from a random pair $(\bar{\boldsymbol{Q}}, \hat{\boldsymbol{Q}})$ using Algorithm 1 in polynomial time. Thus, the linkable anonymity property is not satisfied. In the following, we explain the impact of being able to distinguish $(\boldsymbol{Q}_0', \boldsymbol{Q}_0'',)$ from a random pair $(\bar{\boldsymbol{Q}}, \hat{\boldsymbol{Q}})$.

Observe that the adversary $\mathcal{A}$ in Definition 5 knows the verification key $\mathsf{vk}_i = \mathsf{sk}_i \star x$ for each $i := 1, \ldots, m$ (see step 2). Now, let us focus on step 5. By construction, we know that the signature σ^* includes either the tag t_0^* or t_1^*. More precisely,

- If $\mathsf{vk}^* = \mathsf{vk}_0^*$, then the adversary $\mathcal{A}$ knows $\mathsf{t}_b^* = \mathsf{sk}_b^* \bullet x$.
- Otherwise, the adversary $\mathcal{A}$ knows $\mathsf{t}_{1-b}^* = \mathsf{sk}_{1-b}^* \bullet x$.

Therefore, the adversary $\mathcal{A}$ can guess the value of $b^* = b$ by employing Algorithm 1 as follows. Let t^* be the tag in σ^*. Then $\mathcal{A}$ runs Algorithm 1 on input $(x, \mathsf{vk}^*, \mathsf{t}^*, x)$. If Algorithm 1 returns *True*, then $\mathcal{A}$ returns $b^* = 0$. If Algorithm 1 returns *False*, then $\mathcal{A}$ returns $b^* = 1$. Consequently, $\mathcal{A}$ correctly guesses the value of b used by the challenger $\mathcal{C}$. Hence, the linkable ring signature from [KTS+24] is not linkable anonymous.

5 Remarks and Future Directions

Remark on Module-LIP. Observe that our analysis from Section 3.1 does not exploit any additional structure on the pairs, and it is generic in the sense that we only need two pairs of the form $(\boldsymbol{Q}_i, \boldsymbol{U} \star \boldsymbol{Q}_i)$. Thus, our analysis also applies to the module variant of LIP.

Comparisons with Linear Code Equivalence. Analogous to the work of Budroni et al. [BCD+24] on the Linear Code Equivalence group action, we have demonstrated that using two instances of LIP with the same secret is insecure by introducing a heuristic polynomial-time algorithm that distinguishes them from random. However, our result is slightly weaker than that of [BCD+24] as they are able to compute the secret group element from only two instances, while we actually require three. Consequently, while Budroni et al. show that the *linkability* property in the linkable ring signature scheme based on the code equivalence group action is not secure, our result only breaks the *linkable anonymity* property. Even if we believe that our result is enough to discourage the use of multiple instances of LIP with the same secret in any cryptographic application, it would be of cryptanalytic interest to discover a polynomial-time algorithm that recovers the secret group element from only two instances. On the other hand, it remains an open question whether it is possible to construct secure linkable ring signatures from the lattice isomorphism and the code equivalence group actions.

Other future directions. We believe that Equation 2 for $t = 1$ offers a model that can be useful for studying the complexity of LIP from an algebraic point of view. For example, one could incorporate the non-linear constraints $\boldsymbol{U}^{-1} \cdot \boldsymbol{U} = \boldsymbol{U} \cdot \boldsymbol{U}^{-1} = \boldsymbol{I}_n$, which are not inherently captured by the linear equations, and analyze the resulting system using Gröbner basis theory.

Acknowledgments. This work was supported by RCN (Research Council of Norway) in the Crypto AI project.

References

[BBCK24] Benjamin Benčina, Alessandro Budroni, Jesús-Javier Chi-Domínguez, and Mukul Kulkarni. Properties of lattice isomorphism as a cryptographic group action. In Markku-Juhani Saarinen and Daniel Smith-Tone, editors, *Post-Quantum Cryptography - 15th International Workshop, PQCrypto 2024, Part I*, pages 170–201, Oxford, UK, June 12–14, 2024. Springer, Cham, Switzerland. doi:10.1007/978-3-031-62743-9_6.

[BBD+25] Joppe W. Bos, Olivier Bronchain, Léo Ducas, Serge Fehr, Yu-Hsuan Huang, Thomas Pornin, Eamonn W. Postlethwaite, Thomas Prest, Ludo N. Pulles,

and Wessel van Woerden. Hawk version 2.0 (march 2025). Tech. rep., National Institute of Standards and Technology, 2025. URL: https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-2/spec-files/hawk-spec-round2-web.pdf.

[BBMP24] Michele Battagliola, Giacomo Borin, Alessio Meneghetti, and Edoardo Persichetti. Cutting the GRASS: Threshold GRoup action signature schemes. In Elisabeth Oswald, editor, *CT-RSA 2024*, volume 14643 of *LNCS*, pages 460–489, San Francisco, CA, USA, May 6–9, 2024. Springer, Cham, Switzerland. doi:10.1007/978-3-031-58868-6_18.

[BCD+24] Alessandro Budroni, Jesús-Javier Chi-Domínguez, Giuseppe D'Alconzo, Antonio J. Di Scala, and Mukul Kulkarni. Don't use it twice! Solving relaxed linear equivalence problems. In Kai-Min Chung and Yu Sasaki, editors, *ASIACRYPT 2024, Part VIII*, volume 15491 of *LNCS*, pages 35–65, Kolkata, India, December 9–13, 2024. Springer, Singapore, Singapore. doi:10.1007/978-981-96-0944-4_2.

[BCDF25] Alessandro Budroni, Jesús-Javier Chi-Domínguez, and Ermes Franch, 2025. Available at https://github.com/Crypto-TII/pqc-duit-reloaded.

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

[BKP20] Ward Beullens, Shuichi Katsumata, and Federico Pintore. Calamari and Falafl: Logarithmic (linkable) ring signatures from isogenies and lattices. In Shiho Moriai and Huaxiong Wang, editors, *ASIACRYPT 2020, Part II*, volume 12492 of *LNCS*, pages 464–492, Daejeon, South Korea, December 7–11, 2020. Springer, Cham, Switzerland. doi:10.1007/978-3-030-64834-3_16.

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

[BMPS20] Jean-François Biasse, Giacomo Micheli, Edoardo Persichetti, and Paolo Santini. LESS is more: Code-based signatures without syndromes. In Abderrahmane Nitaj and Amr M. Youssef, editors, *AFRICACRYPT 20*, volume 12174 of *LNCS*, pages 45–65, Cairo, Egypt, July 20–22, 2020. Springer, Cham, Switzerland. doi:10.1007/978-3-030-51938-4_3.

[BY91] Gilles Brassard and Moti Yung. One-way group actions. In Alfred J. Menezes and Scott A. Vanstone, editors, *CRYPTO'90*, volume 537 of *LNCS*, pages 94–107, Santa Barbara, CA, USA, August 11–15, 1991. Springer Berlin Heidelberg, Germany. doi:10.1007/3-540-38424-3_7.

[CLM+18] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part III*, volume 11274 of *LNCS*, pages 395–427, Brisbane, Queensland, Australia,

December 2–6, 2018. Springer, Cham, Switzerland. doi:10.1007/978-3-030-03332-3_15.

[CNP+23] Tung Chou, Ruben Niederhagen, Edoardo Persichetti, Tovohery Hajatiana Randrianarisoa, Krijn Reijnders, Simona Samardjiska, and Monika Trimoska. Take your MEDS: Digital signatures from matrix code equivalence. In Nadia El Mrabet, Luca De Feo, and Sylvain Duquesne, editors, *AFRICACRYPT 23*, volume 14064 of *LNCS*, pages 28–52, Sousse, Tunisia, July 19–21, 2023. Springer, Cham, Switzerland. doi:10.1007/978-3-031-37679-5_2.

[DKQ+25] Dung Hoang Duong, Xuan Thanh Khuc, Youming Qiao, Willy Susilo, and Chuanqi Zhang. Blind signatures from cryptographic group actions. Cryptology ePrint Archive, Paper 2025/397, 2025. URL: https://eprint.iacr.org/2025/397.

[DPPvW22] Léo Ducas, Eamonn W. Postlethwaite, Ludo N. Pulles, and Wessel P. J. van Woerden. Hawk: Module LIP makes lattice signatures fast, compact and simple. In Shweta Agrawal and Dongdai Lin, editors, *ASIACRYPT 2022, Part IV*, volume 13794 of *LNCS*, pages 65–94, Taipei, Taiwan, December 5–9, 2022. Springer, Cham, Switzerland. doi:10.1007/978-3-031-22972-5_3.

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

[HJ94] Roger A. Horn and Charles R. Johnson. *Topics in Matrix Analysis*. Cambridge University Press, Cambridge; New York, 1994.

[JWL+25] Kaijie Jiang, Anyu Wang, Hengyi Luo, Guoxiao Liu, Gang Tang, Yanbin Pan, and Xiaoyun Wang. Re-randomize and extract: A novel commitment construction framework based on group actions. In *Advances in Cryptology - EUROCRYPT 2025: 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Madrid, Spain, May 4-8, 2025, Proceedings, Part VII*, pages 124–153, Cham, 2025. Springer Nature Switzerland. doi:10.1007/978-3-031-91124-8_5.

[KTS+24] Xuan Thanh Khuc, Anh The Ta, Willy Susilo, Dung Hoang Duong, Fuchun Guo, Kazuhide Fukushima, and Shinsaku Kiyomoto. Logarithmic-size (linkable) ring signatures from lattice isomorphism problems. In Francesco Regazzoni, Bodhisatwa Mazumdar, and Sri Parameswaran, editors, *Security, Privacy, and Applied Cryptography Engineering*, pages 214–241, Cham, 2024. Springer Nature Switzerland.

[Lai24] Yi-Fu Lai. Capybara and tsubaki: Verifiable random functions from group actions and isogenies. *IACR Communications in Cryptology*, 1(3), 2024. doi:10.62056/avr-11zn4.

[LR24] Antonin Leroux and Maxime Roméas. Updatable encryption from group actions. In Markku-Juhani Saarinen and Daniel Smith-Tone, editors, *Post-Quantum Cryptography - 15th International Workshop, PQCrypto 2024, Part II*, pages 20–53, Oxford, UK, June 12–14, 2024. Springer, Cham, Switzerland. doi:10.1007/978-3-031-62746-0_2.

[MG02] Daniele Micciancio and Shafi Goldwasser. *Complexity of Lattice Problems: A Cryptographic Perspective*, volume 671. Springer Science+Business Media, LLC, 01 2002. doi:10.1007/978-1-4615-0897-7.

[Nat17] National Institute of Standards and Technology. Post-Quantum Cryptography Standardization. https://csrc.nist.gov/projects/post-quantum-cryptography, 2017.

[TDJ+22] Gang Tang, Dung Hoang Duong, Antoine Joux, Thomas Plantard, Youming Qiao, and Willy Susilo. Practical post-quantum signature schemes from isomorphism problems of trilinear forms. In *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*, page 582–612, Berlin, Heidelberg, 2022. Springer-Verlag. doi:10.1007/978-3-031-07082-2_21.

[The22] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.5)*, 2022. URL: https://www.sagemath.org.