Properties of Lattice Isomorphism as a Cryptographic Group Action

Benjamin Benčina, **Alessandro Budroni**, Jesús-Javier Chi-Domínguez, Mukul Kulkarni

Technology Innovation Institute

ROYAL HOLLOWAY UNIVERSITY OF LONDON

May 20th, 2024

Outline

Equivalence Problems in Cryptography

Several protocols have been proposed using hard problems as underlying assumption consisting of finding the *equivalence/isomorphism* between two algebraic/geometrical objects.

Equivalence Problems in Cryptography

Several protocols have been proposed using hard problems as underlying assumption consisting of finding the *equivalence/isomorphism* between two algebraic/geometrical objects.

In the NIST Standardization of Additional Digital Signature Schemes we find:

- LESS [1] $\leftarrow$ equivalence of linear codes
- MEDS [7] $\leftarrow$ equivalence of matrix codes
- ALTEQ [4] $\leftarrow$ equivalence of alternating trilinear forms
- HAWK [5] $\leftarrow$ isomorphism of lattices
- SQIsign [6] $\leftarrow$ isogenies between supersingular elliptic curves

Equivalence Problems in Cryptography

- Some equivalence problems have been modeled under the framework of **group actions**.

Equivalence Problems in Cryptography

- Some equivalence problems have been modeled under the framework of **group actions**.

This framework brings the following benefit. It allows us to

1. Define a cryptographic primitive in general for group actions,
2. Instantiate the primitive with a specific group action.

Examples: (Linkable) Ring Signatures [3], Updatable Encryption [10], Threshold signatures [2], MPCiTH [9].

Contributions

• In this work, we formalize Lattice Isomorphism as a group action, and study its cryptographic properties.

• Our study highlights that certain group actions-based primitives cannot be instantiated securely with Lattice Isomorphism.

• We introduce two new hard problems (and prove them to be) equivalent to LIP - one of which appeared already for isogenies [8].

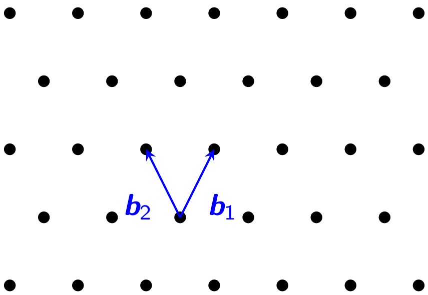
Outline

1. Introduction
2. **Preliminaries**
3. Lattice Isomorphism as a Group Action
4. Cryptographic Properties of LIGA
5. Two New Hard Problems
6. Discussion

Lattices

A lattice is the set of all **integer** linear combinations of a basis $B = \boldsymbol{b}_1, \cdots, \boldsymbol{b}_n, \in \mathbb{R}^n$

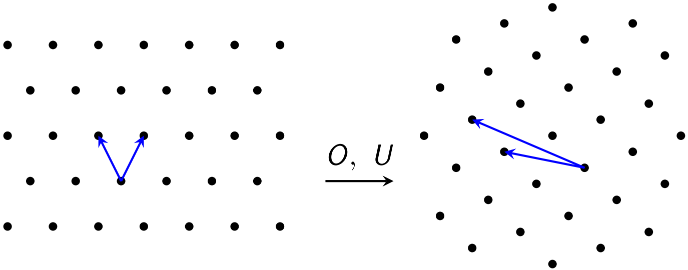
$$\mathcal{L}(B) = \left\{ \sum_{i=1}^{n} \alpha_i \boldsymbol{b}_i, \quad \alpha_i \in \mathbb{Z} \right\}.$$



Lattice Isomorphism

Two lattices $\mathcal{L}_1(B)$ and $\mathcal{L}_2(B')$ are *isomorphic* if there exist an ortonormal matrix O and an invertible integer matrix U such that

$$B' = OBU$$



Lattice Isomorphism Problem

Definition (LIP)

Given two basis B, B', find (if they exist) an orthonormal matrix $O \in \mathcal{O}_n(\mathbb{R})$ and an invertible integer matrix $U \in \mathsf{GL}_n(\mathbb{Z})$ such that

$$B' = OBU.$$

Lattice Isomorphism Problem

Definition (LIP)

Given two basis B, B', find (if they exist) an orthonormal matrix $O \in \mathcal{O}_n(\mathbb{R})$ and an invertible integer matrix $U \in \mathrm{GL}_n(\mathbb{Z})$ such that

$$B' = OBU.$$

The orthonormal matrix O has, in general, entries in $\mathbb{R}$. For this reason, in practice, one uses quadratic forms as follows

$$Q = B^\top B \in \mathcal{S}_n^{>0}$$

$$Q' = B'^\top B' = U^\top B^\top O^\top OBU = U^\top QU \in \mathcal{S}_n^{>0}$$

Lattice Isomorphism Problem Reformulated

We can reformulate LIP in terms of Quadratic Forms

Definition (LIP - Quadratic Forms)

Given two quadratic forms Q, Q', find (if it exists) an invertible integer matrix $U \in \mathrm{GL}_n(\mathbb{Z})$ such that

$$Q' = U^\top Q U.$$

We denote with $[Q]$ the equivalence class of all quadratic forms Q' equivalent to Q.

Group Actions

Definition

Let $(G, \circ)$ be a group, and X be a set. G is said to *act* on X if there exists a map

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

satisfying the following properties:

- *identity:* $id \star x = x$, for every $x \in X$ and $id \in G$ identity,
- *compatibility:* $(g \circ h) \star x = g \star (h \star x)$, $\forall g, h \in G$, $x \in X$.

Group Actions

Definition

Let $(G, \circ)$ be a group, and X be a set. G is said to *act* on X if there exists a map

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

satisfying the following properties:

- *identity:* $id \star x = x$, for every $x \in X$ and $id \in G$ identity,
- *compatibility:* $(g \circ h) \star x = g \star (h \star x)$, $\forall g, h \in G$, $x \in X$.

Basic properties.

- *Transitive*, $\forall x_1, x_2 \in X$, $\exists g \in G \,:\, x_2 = g \star x_1$.
- *Faithful*, $x = g \star x, \forall x \in X \Rightarrow g = id$.
- *Free*, $x = g \star x$, for some $x \in X \Rightarrow g = id$.

Cryptographic Group Action

Properties for the use of group actions in Cryptography.

- **One-wayness**: Given $x, x' \in X$ such that

$$x' = g \star x, \qquad g \in G,$$

  it is hard to find g.

Cryptographic Group Action

Properties for the use of group actions in Cryptography.

- **One-wayness**: Given $x, x' \in X$ such that

$$x' = g \star x, \qquad g \in G,$$

  it is hard to find g.

- **Weak-unpredictability**: Given a polynomial number of pairs $(x_i, g \star x_i) \in X \times X$, and given $y \in X$, it is hard to compute $g \star y$.

Cryptographic Group Action

Properties for the use of group actions in Cryptography.

- **One-wayness**: Given $x, x' \in X$ such that

$$x' = g \star x, \qquad g \in G,$$

  it is hard to find g.

- **Weak-unpredictability**: Given a polynomial number of pairs $(x_i, g \star x_i) \in X \times X$, and given $y \in X$, it is hard to compute $g \star y$.

- **Weak-pseudorandomness**: It is hard to distinguish a polynomial number of pairs $(x_i, g \star x_i) \in X \times X$, from random pairs $(x_i, y_i) \in X \times X$.

Outline

Lattice Isomorphism Group Action (LIGA)

- Define as the base set $X = [Q]$, for a chosen quadratic form Q.
- Define the group as the quotient

$$G \;=\; \mathsf{GL}_n(\mathbb{Z})/\simeq_\pm \;=:\; \mathsf{GL}_n^\pm(\mathbb{Z})$$

  where

$$A \simeq_\pm B \iff A = \pm B,$$

  and operation $A \circ B = BA$, for $A, B \in \mathsf{GL}(\mathbb{Z})$.

- Define the action $\star$: $(\mathsf{GL}_n^\pm(\mathbb{Z}) \times [Q]) \to [Q]$

$$\star : (U, Q_0) \mapsto U \star Q_0 := U^\top Q_0 U,$$

Lattice Isomorphism Group Action (LIGA)

- Define as the base set $X = [Q]$, for a chosen quadratic form Q.
- Define the group as the quotient

$$G \; = \; \mathsf{GL}_n(\mathbb{Z})/{\simeq_\pm} \; =: \; \mathsf{GL}_n^{\pm}(\mathbb{Z})$$

where

$$A \simeq_\pm B \iff A = \pm B,$$

and operation $A \circ B = BA$, for $A, B \in \mathsf{GL}(\mathbb{Z})$.

- Define the action $\star$: $(\mathsf{GL}_n^{\pm}(\mathbb{Z}) \times [Q]) \to [Q]$

$$\star : (U, Q_0) \mapsto U \star Q_0 := U^\top Q_0 U,$$

$\to \star$ is compatible and the identity element $I_n \in \mathsf{GL}_n^{\pm}(\mathbb{Z})$ fixes any element of $[Q] \Rightarrow$ it is a group action

Basic Properties of LIGA

- **Transitivity.** ✓
- **Faithfulness.** ✓
- **Free.** $\iff$ Q has trivial automorphism group

Outline

Cryptographic Properties of LIGA

- **One-wayness.** ✓
(assuming LIP hard to solve $\Rightarrow$ LIGA is *one-way*)

- **Weak-unpredictability.** ?

- **Weak-pseudorandomness.** ?

Cryptographic Properties of LIGA

Theorem (informal)

Given $d = \frac{n(n-1)}{2} \in O(n^2)$ *independent LIP samples*[1]

$$Q_i' = U^\top Q_i U, \quad i = 1, \ldots, d,$$

then one can retrieve the secret U *in polynomial time* $O(n^{2\omega})$*, where* $\omega \in [2, 3]$*.*

[1] sampled according to a certain distribution.

Cryptographic Properties of LIGA

Theorem (informal)

Given $d = \frac{n(n-1)}{2} \in O(n^2)$ independent LIP samples[1]

$$Q_i' = U^\top Q_i U, \quad i = 1, \ldots, d,$$

then one can retrieve the secret U in polynomial time $O(n^{2\omega})$, where $\omega \in [2, 3]$.

- LIGA is not weakly-unpredictable
- LIGA is not weakly-pseudorandom

[1] sampled according to a certain distribution.

Cryptographic Properties of LIGA

proof.(informal)

• Given one sample $Q' = U^\top QU$, write the d-dimensional linear system of equation in d^2 variables

$$Q'_{i,j} = \sum_{k=1}^{n} \sum_{l=1}^{n} Q_{k,l} \cdot X_{(i,k),(j,l)}$$

where $X_{(i,k),(j,l)} = U_{i,k} \cdot U_{j,l}$ for each $i, j, k, l \in \{1, \ldots, n\}$.

Cryptographic Properties of LIGA

proof.(informal)

• Given one sample $Q' = U^\top Q U$, write the d-dimensional linear system of equation in d^2 variables

$$Q'_{i,j} = \sum_{k=1}^{n} \sum_{l=1}^{n} Q_{k,l} \cdot X_{(i,k),(j,l)}$$

where $X_{(i,k),(j,l)} = U_{i,k} \cdot U_{j,l}$ for each $i, j, k, l \in \{1, \ldots, n\}$.

• Given d samples, construct a determined linear system and solve it – Gaussian elimination.

Cryptographic Properties of LIGA

proof.(informal)

• Given one sample $Q' = U^\top Q U$, write the d-dimensional linear system of equation in d^2 variables

$$Q'_{i,j} = \sum_{k=1}^{n} \sum_{l=1}^{n} Q_{k,l} \cdot X_{(i,k),(j,l)}$$

where $X_{(i,k),(j,l)} = U_{i,k} \cdot U_{j,l}$ for each $i, j, k, l \in \{1, \ldots, n\}$.

• Given d samples, construct a determined linear system and solve it – Gaussian elimination.

• Retrieve U from the values $X_{(i,k),(j,l)}$.

Time/Samples Trade-off using Gröbner basis

In the system $Q' = U^\top Q U$

$$Q' = \begin{bmatrix} u_{1,1} & \cdots & u_{n,1} \\ \vdots & \ddots & \vdots \\ u_{1,n} & \cdots & u_{n,n} \end{bmatrix} \cdot Q \cdot \begin{bmatrix} u_{1,1} & \cdots & u_{1,n} \\ \vdots & \ddots & \vdots \\ u_{n,1} & \cdots & u_{n,n} \end{bmatrix}$$

we consider only *norm equations*, that is, equations in n variables of the form

$$U_i^\top Q U_i = Q'_{i,i}, \quad \text{for } i = 1, \ldots, n.$$

Time/Samples Trade-off using Gröbner basis

In the system $Q' = U^\top Q U$

$$Q' = \begin{bmatrix} u_{1,1} & \cdots & u_{n,1} \\ \vdots & \ddots & \vdots \\ u_{1,n} & \cdots & u_{n,n} \end{bmatrix} \cdot Q \cdot \begin{bmatrix} u_{1,1} & \cdots & u_{1,n} \\ \vdots & \ddots & \vdots \\ u_{n,1} & \cdots & u_{n,n} \end{bmatrix}$$

we consider only *norm equations*, that is, equations in n variables of the form

$$U_i^\top Q U_i = Q'_{i,i}, \quad \text{for } i = 1, \ldots, n.$$

Proposition (informal)

For an index of regularity $i \geq 2$ and at least $m = O(\frac{n^2}{i^2})$ LIP samples, one can retrieve the secret U in time $O(n^{2+i\omega})$, where $\omega \in [2, 3]$.

Comparison

n	16	32	64	128	256	512	1024
LIN.	22.5	28.1	33.7	39.3	44.9	50.5	56.2
GB - $i_{\text{reg}} = 2$	30.5	38.1	45.7	53.3	60.9	68.5	76.2
GB - $i_{\text{reg}} = 3$	41.7	52.1	62.5	73.0	83.4	93.8	104.2
GB - $i_{\text{reg}} = 4$	52.9	66.2	79.4	92.6	105.8	119.1	132.3
GB - $i_{\text{reg}} = 5$	64.2	80.2	96.2	112.3	128.3	144.3	160.4

Estimated bit complexity comparison - Linearization vs. Gröbner basis approaches.

Experiments

n	16	20	24	28	32	36	40
LIN.	0.34	1.00	1.98	3.36	5.51	10.57	17.31
GB	2.04	5.64	13.40	31.59	67.72	130.52	252.16

Time in seconds for breaking weak-unpredictability - both with $m = \frac{n(n-1)}{2}$ samples. In the case of Gröbner basis, we considered the case of $i_{\text{reg}} = 2$.

Outline

Two New Hard Problems

We use our result to derive the following two new hard problems.

Definition (Transpose Quadratic Form Problem (TQFP))

Given Q and $Q' = U^\top QU$, find $\tilde{Q} = UQU^\top$.

Definition (Inverse Quadratic Form Problem (IQFP))

Given Q and $Q' = U^\top QU$, find $\tilde{Q} = (U^{-1})^\top Q(U^{-1})$.

We show that with $O(n^2)$ calls to an oracle that solves TQFP (or IQFP), one can solve LIP.

Two New Hard Problems

Sketch of the reduction. (LIP $\rightarrow$ TQFP).

Given an LIP instance $(Q, Q' = U^{\top} Q U)$, we give it as input to the TQFP oracle and get $(Q, \tilde{Q} = U Q U^{\top})$

Two New Hard Problems

Sketch of the reduction. (LIP $\to$ TQFP).

Given an LIP instance $(Q, Q' = U^\top QU)$, we give it as input to the TQFP oracle and get $(Q, \tilde{Q} = UQU^\top)$

- Sample a quadratic form $\bar{Q} = W^\top QW$ along with $W \in \mathrm{GL}_n(\mathbb{Z})$.
- Compute $Q'' = W\tilde{Q}W^\top = WUQU^\top W^\top$ and send (Q, Q'') to the TQFP oracle. Record its response as

$$\hat{Q} = U^\top W^\top QWU = U^\top \bar{Q} U.$$

This is a a new LIP sample with U as unknown unimodular matrix.

Two New Hard Problems

Sketch of the reduction. (LIP $\to$ TQFP).

Given an LIP instance $(Q, Q' = U^\top QU)$, we give it as input to the TQFP oracle and get $(Q, \tilde{Q} = UQU^\top)$

- Sample a quadratic form $\bar{Q} = W^\top QW$ along with $W \in \mathrm{GL}_n(\mathbb{Z})$.
- Compute $Q'' = W\tilde{Q}W^\top = WUQU^\top W^\top$ and send (Q, Q'') to the TQFP oracle. Record its response as

$$\hat{Q} = U^\top W^\top QWU = U^\top \bar{Q} U.$$

  This is a a new LIP sample with U as unknown unimodular matrix.

Repeating the above two steps for $O(n^2)$ times, one obtains enough samples to retrieve the secret. (Same procedure for IQFP).

Outline

Implications of our work

What can/can't you do with LIP
(what can/can't you do with one-wayness only)

ID scheme/ signature	commitment	PRF	updatable encryption
✓	✓	✗	✗

Thanks for listening!

Bibliography

[1] M. Baldi, A. B. L. Beckwith, J.-F. Biasse, A. Esser, K. Gaj, K. Mohajerani, G. Pelosi, E. Persichetti, M.-J. O. Saarinen, P. Santini, and R. Wallace. LESS (version 1.1). Tech. rep., National Institute of Standards and Technology, 2023.

[2] M. Battagliola, G. Borin, A. Meneghetti, and E. Persichetti. Cutting the grass: Threshold group action signature schemes. In E. Oswald, editor, *Topics in Cryptology – CT-RSA 2024*, pages 460–489, Cham, 2024. Springer Nature Switzerland.

[3] W. Beullens, S. Katsumata, and F. Pintore. Calamari and falafl: Logarithmic (linkable) ring signatures from isogenies and lattices. In S. Moriai and H. Wang, editors, *Advances in Cryptology – ASIACRYPT 2020*, pages 464–492, Cham, 2020. Springer International Publishing.

[4] M. Bläser, D. H. Duong, A. K. Narayanan, T. Plantard, Y. Qiao, A. Sipasseuth, and G. Tang. Alteq version 1.0 (june 1, 2023). Tech. rep., National Institute of Standards and Technology, 2023.

[5] J. W. Bos, O. Bronchain, L. Ducas, S. Fehr, Y.-H. Huang, T. Pornin, E. W. Postlethwaite, T. Prest, L. N. Pulles, and W. van Woerden. Hawk version 1.0 (june 1, 2023). Tech. rep., National Institute of Standards and Technology, 2023.

[6] J. Chavez-Saab, M. C.-R. Santos, L. D. Feo, J. K. Eriksen, B. Hess, D. Kohel, A. Leroux, P. Longa, M. Meyer, L. Panny, S. Patranabis, C. Petit, F. R. Henríquez, S. Schaeffler, and B. Wesolowski. Sqisign version 1.0 (june 1, 2023). Tech. rep., National Institute of Standards and Technology, 2023.

[7] T. Chou, R. Niederhagen, E. Persichetti, L. Ran, T. Hajatiana, K. Reijnders, S. Samardjiska, and M. Trimoska. MEDS (version 1.1). Tech. rep., National Institute of Standards and Technology, 2023.

[8] J. Felderhoff. Hard Homogenous Spaces and Commutative Supersingular Isogeny based Diffie–Hellman. 2019.

[9] A. Joux. Mpc in the head for isomorphisms and group actions. Cryptology ePrint Archive, Paper 2023/664, 2023. https://eprint.iacr.org/2023/664.

[10] A. Leroux and M. Roméas. Updatable encryption from group actions. Cryptology ePrint Archive, Paper 2022/739, 2022. https://eprint.iacr.org/2022/739.