Hull Attacks on the Lattice Isomorphism Problem

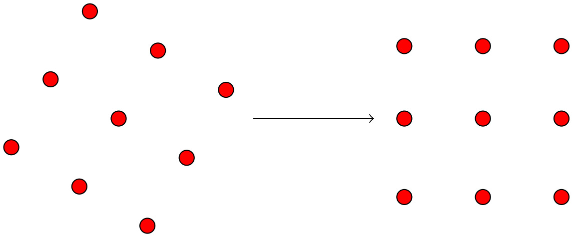
Léo Ducas [1,2] **Shane Gibbons** [1,2]

[1]Cryptology Group, CWI Amsterdam

[2]Mathematical Institute, Leiden University

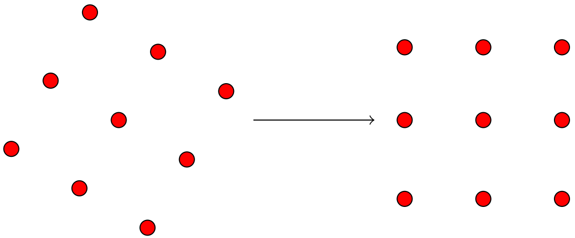
8 May 2023

Lattice Isomorphism



The Lattice Isomorphism Problem as a hardness assumption has gotten a lot of attention recently:

Lattice Isomorphism



The Lattice Isomorphism Problem as a hardness assumption has gotten a lot of attention recently:
ΔLIP proposed by [BGPSD23, DvW22] for cryptography, while [DPPW22] propose LIP.

Context and Motivation

Lattice Isomorphism

Let $L, L' \subseteq \mathbb{R}^n$ be lattices. Then L and L' are *isomorphic* if there exists an $O \in \mathcal{O}_n(\mathbb{R})$ such that

$$\{Ox : x \in L\} := O \cdot L = L'.$$

Context and Motivation

Lattice Isomorphism

Let $L, L' \subseteq \mathbb{R}^n$ be lattices. Then L and L' are *isomorphic* if there exists an $O \in \mathcal{O}_n(\mathbb{R})$ such that

$$\{Ox : x \in L\} := O \cdot L = L'.$$

Lattice Isomorphism Problem

Let $m \leq n$. Let $B, B' \in \mathbb{R}^{n \times m}$ be bases of lattices L, L' that are isomorphic. Find an invertible $U \in \mathrm{GL}_m(\mathbb{Z})$ and orthonormal $O \in \mathcal{O}_n(\mathbb{R})$ such that

$$OBU = B'.$$

Using the Gap to Conjecture Hardness

All known attacks against LIP require solving SVP, whose running time heuristically depends on length of a shortest vector.

Using the Gap to Conjecture Hardness

All known attacks against LIP require solving SVP, whose running time heuristically depends on length of a shortest vector.
In a random lattice L of dimension n, we expect

$$\lambda_1(L) \sim gh(n) \approx \det(L)^{1/n}\sqrt{\frac{n}{2\pi e}}.$$

Using the Gap to Conjecture Hardness

All known attacks against LIP require solving SVP, whose running time heuristically depends on length of a shortest vector.
In a random lattice L of dimension n, we expect

$$\lambda_1(L) \sim gh(n) \approx \det(L)^{1/n}\sqrt{\frac{n}{2\pi e}}.$$

Gap

The ratio between λ_1 and the Gaussian heuristic is called the gap:

Using the Gap to Conjecture Hardness

All known attacks against LIP require solving SVP, whose running time heuristically depends on length of a shortest vector.
In a random lattice L of dimension n, we expect

$$\lambda_1(L) \sim gh(n) \approx \det(L)^{1/n}\sqrt{\frac{n}{2\pi e}}.$$

Gap

The ratio between λ_1 and the Gaussian heuristic is called the gap:

$$\text{gap} := \max\left\{\frac{\text{gh}(L)}{\lambda_1(L)}, \frac{\text{gh}(L^*)}{\lambda_1(L^*)}\right\}.$$

Using the Gap to Conjecture Hardness

All known attacks against LIP require solving SVP, whose running time heuristically depends on length of a shortest vector.
In a random lattice L of dimension n, we expect

$$\lambda_1(L) \sim gh(n) \approx \det(L)^{1/n} \sqrt{\frac{n}{2\pi e}}.$$

Gap

The ratio between λ_1 and the Gaussian heuristic is called the gap:

$$\text{gap} := \max \left\{ \frac{\text{gh}(L)}{\lambda_1(L)}, \frac{\text{gh}(L^*)}{\lambda_1(L^*)} \right\}.$$

BKZ reduction with blocksize β runs in time $2^{0.292\beta + o(\beta)}$ [BDGL16].

Using the Gap to Conjecture Hardness

- For a random lattice L, we expect $\text{gap}(L) = O(1)$. We solve with BKZ, $\beta = n$.

Using the Gap to Conjecture Hardness

- For a random lattice L, we expect $\text{gap}(L) = O(1)$. We solve with BKZ, $\beta = n$.
- For the lattice $\mathbb{Z}^n$, $\text{gap}(\mathbb{Z}^n) = O(n^{1/2})$, so we can solve with $\beta = n/2$.

Using the Gap to Conjecture Hardness

- For a random lattice L, we expect $\mathrm{gap}(L) = O(1)$. We solve with BKZ, $\beta = n$.
- For the lattice $\mathbb{Z}^n$, $\mathrm{gap}(\mathbb{Z}^n) = O(n^{1/2})$, so we can solve with $\beta = n/2$.
- In general, for a lattice with gap n^δ, we expect to be able to use $\beta = n/(1 + 2\delta)$. [AD21]

Using the Gap to Conjecture Hardness

- For a random lattice L, we expect $\text{gap}(L) = O(1)$. We solve with BKZ, $\beta = n$.
- For the lattice $\mathbb{Z}^n$, $\text{gap}(\mathbb{Z}^n) = O(n^{1/2})$, so we can solve with $\beta = n/2$.
- In general, for a lattice with gap n^δ, we expect to be able to use $\beta = n/(1 + 2\delta)$. [AD21]

Conjecture [DvW22] (informal)

The best attack against ΔLIP for lattices L, L' requires solving f-approx SVP in both lattices, where

$$f = \max\{\text{gap}(L), \text{gap}(L')\}$$

Using the Gap to Conjecture Hardness

- For a random lattice L, we expect $\text{gap}(L) = O(1)$. We solve with BKZ, $\beta = n$.
- For the lattice $\mathbb{Z}^n$, $\text{gap}(\mathbb{Z}^n) = O(n^{1/2})$, so we can solve with $\beta = n/2$.
- In general, for a lattice with gap n^δ, we expect to be able to use $\beta = n/(1 + 2\delta)$. [AD21]

Conjecture [DvW22] (informal)

The best attack against ΔLIP for lattices L, L' requires solving f-approx SVP in both lattices, where

$$f = \max\{\text{gap}(L), \text{gap}(L')\}$$

Our attack: We make the gap larger, by extracting the sublattice $\mathbb{Z}^n$, then solving $\mathbb{Z}$LIP.

Plan of Attack

- Lattice Hulls
- Construction A
- Solving LIP via $\mathbb{Z}$LIP and Code Equivalence

Hull of a Lattice

Hull of a Lattice

Code Hull

Given an $[n, k]_q$ linear code C over $\mathbb{F}_q$, the *hull of* C *is*

$$\mathcal{H} := C \cap C^{\perp},$$

where $C^{\perp} := \left\{ y \in \mathbb{F}_q^n : y \cdot x = 0 \quad \forall x \in C \right\}$.

Hull of a Lattice

Code Hull

Given an $[n, k]_q$ linear code C over $\mathbb{F}_q$, the *hull of C is*

$$\mathcal{H} := C \cap C^{\perp},$$

where $C^{\perp} := \left\{ y \in \mathbb{F}_q^n : y \cdot x = 0 \quad \forall x \in C \right\}.$

Lattice Hull

Let $s \in \mathbb{R}^{\times}$, and let $L \subseteq \mathbb{R}^n$ be a lattice.

Hull of a Lattice

Code Hull

Given an $[n, k]_q$ linear code C over $\mathbb{F}_q$, the *hull of C is*

$$\mathcal{H} := C \cap C^{\perp},$$

where $C^{\perp} := \left\{ y \in \mathbb{F}_q^n : y \cdot x = 0 \quad \forall x \in C \right\}.$

Lattice Hull

Let $s \in \mathbb{R}^{\times}$, and let $L \subseteq \mathbb{R}^n$ be a lattice. The s-hull of L is the sublattice

$$H_s(L) = L \cap sL^*,$$

where $L^* := \{x \in \mathrm{span}(L) : \langle x, L \rangle \subseteq \mathbb{Z}\}$.

Construction A Lattices

Given a linear code C over $\mathbb{F}_p$, the *Construction A lattice* is

$$L = C + p\mathbb{Z}^n$$

Construction A Lattices

Given a linear code C over $\mathbb{F}_p$, the *Construction A lattice* is

$$L = C + p\mathbb{Z}^n$$

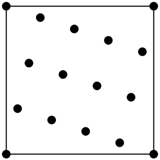


Figure: Construction A Lattice from a code over $\mathbb{F}_{13}$

Construction A Lattices

Given a linear code C over $\mathbb{F}_p$, the *Construction A lattice* is

$$L = C + p\mathbb{Z}^n$$

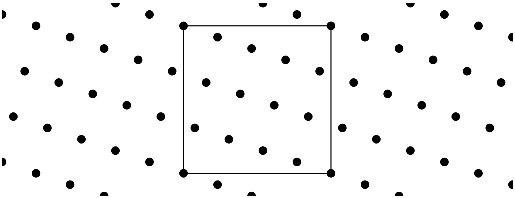


Figure: Construction A Lattice from a code over $\mathbb{F}_{13}$

Solve LIP via the Hull

Given a linear code C over $\mathbb{F}_p$ with hull $\mathcal{H}$,

$$H_p(C + p\mathbb{Z}^n) = \mathcal{H} + p\mathbb{Z}^n.$$

Solve LIP via the Hull

Given a linear code C over $\mathbb{F}_p$ with hull $\mathcal{H}$,

$$H_p(C + p\mathbb{Z}^n) = \mathcal{H} + p\mathbb{Z}^n.$$

If $\mathcal{H} = \{0\}$:

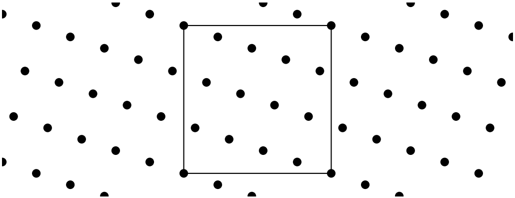


Figure: Hull of a Lattice

Solve LIP via the Hull

Given a linear code C over $\mathbb{F}_p$ with hull $\mathcal{H}$,

$$H_p(C + p\mathbb{Z}^n) = \mathcal{H} + p\mathbb{Z}^n.$$

If $\mathcal{H} = \{0\}$:

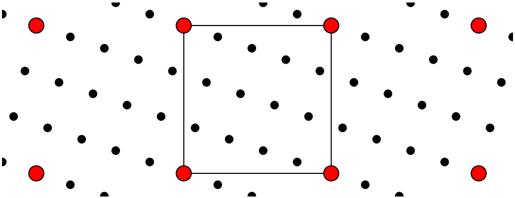


Figure: Hull of a Lattice

Solve LIP via the Hull

Given a linear code C over $\mathbb{F}_p$ with hull $\mathcal{H}$,

$$H_p(C + p\mathbb{Z}^n) = \mathcal{H} + p\mathbb{Z}^n.$$

If $\mathcal{H} = \{0\}$:

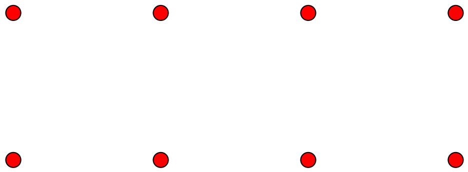


Figure: Hull of a Lattice

Isomorphism of the Hull

Fix a rate 1/2 code C with trivial hull $\mathcal{H} = \{0\}$.

Isomorphism of the Hull

Fix a rate $1/2$ code C with trivial hull $\mathcal{H} = \{0\}$. For $O_1, O_2 \in \mathcal{O}_n(\mathbb{R})$, consider LIP for lattices of the form $L_i = O_i(C + p\mathbb{Z}^n)$ that have hull $H_p(L_i) = O_i(p\mathbb{Z}^n)$.

Isomorphism of the Hull

Fix a rate $1/2$ code C with trivial hull $\mathcal{H} = \{0\}$. For $O_1, O_2 \in \mathcal{O}_n(\mathbb{R})$, consider LIP for lattices of the form $L_i = O_i(C + p\mathbb{Z}^n)$ that have hull $H_p(L_i) = O_i(p\mathbb{Z}^n)$.

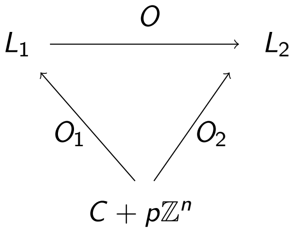


Figure: Isomorphism of Lattices

Isomorphism of the Hull

Fix a rate $1/2$ code C with trivial hull $\mathcal{H} = \{0\}$. For $O_1, O_2 \in \mathcal{O}_n(\mathbb{R})$, consider LIP for lattices of the form $L_i = O_i(C + p\mathbb{Z}^n)$ that have hull $H_p(L_i) = O_i(p\mathbb{Z}^n)$.

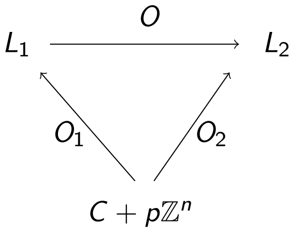


Figure: Isomorphism of Lattices

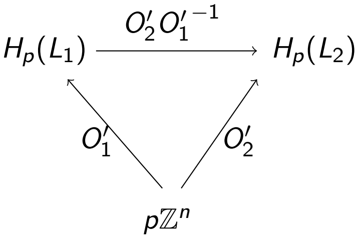


Figure: Isomorphism of Hulls

Code Equivalence

We find this automorphism by solving a code equivalence problem between $(O_1')^{-1}L_1 \mod p$ and $(O_2')^{-1}L_2 \mod p$.

Code Equivalence

We find this automorphism by solving a code equivalence problem between $(O_1')^{-1}L_1 \mod p$ and $(O_2')^{-1}L_2 \mod p$.

- Signed permutation equivalence (SPEP)
- Permutation equivalence (PEP)

Summary of the Attack

Let C be an $[n, k]_p$ code with trivial hull.

Summary of the Attack

Let C be an $[n, k]_p$ code with trivial hull. Given two orthonormal transformations of $C + p\mathbb{Z}^n$ via $O_1, O_2 \in \mathcal{O}_n(\mathbb{R})$, LIP can be solved with blocksize $\beta = n/2$.

- Take the p-hull of L_1 and L_2.

Summary of the Attack

Let C be an $[n, k]_p$ code with trivial hull. Given two orthonormal transformations of $C + p\mathbb{Z}^n$ via $O_1, O_2 \in \mathcal{O}_n(\mathbb{R})$, LIP can be solved with blocksize $\beta = n/2$.

- Take the p-hull of L_1 and L_2.
- Solve $\mathbb{Z}$LIP from both lattices hulls to $p\mathbb{Z}^n$ to find $O_1\psi$, $O_2\varphi$ for some $\psi, \varphi \in \mathrm{Aut}(\mathbb{Z}^n)$.

Summary of the Attack

Let C be an $[n,k]_p$ code with trivial hull. Given two orthonormal transformations of $C + p\mathbb{Z}^n$ via $O_1, O_2 \in \mathcal{O}_n(\mathbb{R})$, LIP can be solved with blocksize $\beta = n/2$.

- Take the p-hull of L_1 and L_2.
- Solve $\mathbb{Z}$LIP from both lattices hulls to $p\mathbb{Z}^n$ to find $O_1\psi$, $O_2\varphi$ for some $\psi, \varphi \in \mathrm{Aut}(\mathbb{Z}^n)$.
- Solve the easy instance of code equivalence between $(O_1')^{-1}L_1 \mod p$ and $(O_2')^{-1}L_2 \mod p$

Conclusion

We restate the conjecture from [DvW22]

Updated conjecture (Informal)

The best attack against ΔLIP for lattices L, L' requires solving f-approx SVP in both lattices, where

$$f = \max\{\text{hullgap}(L), \text{hullgap}(L')\}$$

where

$$\text{hullgap}(L) := \max_{s \mid \det(B^T B)} \{\text{gap}(H_s)\}.$$

Conclusion

We restate the conjecture from [DvW22]

Updated conjecture (Informal)

The best attack against ΔLIP for lattices L, L' requires solving f-approx SVP in both lattices, where

$$f = \max\{\mathrm{hullgap}(L), \mathrm{hullgap}(L')\}$$

where

$$\mathrm{hullgap}(L) := \max_{s \mid \det(B^T B)} \{\mathrm{gap}(H_s)\}.$$

Thank you!

References I

Martin Albrecht and Léo Ducas, *Lattice attacks on ntru and lwe: A history of refinements*, London Mathematical Society Lecture Note Series, p. 15–40, Cambridge University Press, 2021.

Anja Becker, Leo Ducas, Nicolas Gama, and Thijs Laarhoven, *New directions in nearest neighbor searching with applications to lattice sieving*, Proceedings of the Annual ACM-SIAM Symposium on Discrete Algorithms, vol. 1, 2016, p. 10 – 24.

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*, Advances in Cryptology – EUROCRYPT 2023 (Cham) (Carmit Hazay and Martijn Stam, eds.), Springer Nature Switzerland, 2023, pp. 252–281.

References II

Léo Ducas, Eamonn W. Postlethwaite, Ludo N. Pulles, and Wessel van Woerden, *Hawk: Module LIP makes lattice signatures fast, compact and simple*, Advances in Cryptology – ASIACRYPT 2022 (Cham) (Shweta Agrawal and Dongdai Lin, eds.), Springer Nature Switzerland, 2022, pp. 65–94.

Léo Ducas and Wessel van Woerden, *On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography*, Advances in Cryptology – EUROCRYPT 2022 (Cham) (Orr Dunkelman and Stefan Dziembowski, eds.), Springer International Publishing, 2022, pp. 643–673.