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

4 April 2023

Context and Motivation

Definition (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

Definition (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

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

Computationally, the instance of the problem is with bases, not lattices.

Definition (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

$$OBU = B'.$$

Definition (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

$$OBU = B'.$$

Definition (Δ-Lattice Isomorphism Problem (Lattice Version))

Given two lattices L_1, L_2, and the promise that a third lattice L_3 is isomorphic to L_b where $b \in \{0, 1\}$, find b.

Definition (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

$$OBU = B'.$$

Definition (Δ-Lattice Isomorphism Problem (Lattice Version))

Given two lattices L_1, L_2, and the promise that a third lattice L_3 is isomorphic to L_b where $b \in \{0, 1\}$, find b.

[BGPSD21, DvW22] propose using ΔLIP for cryptography, while [DPPW22] propose LIP.

Using the Gap to Conjecture Hardness

All known attacks against ΔLIP solve SVP.

Using the Gap to Conjecture Hardness

All known attacks against ΔLIP solve SVP.
SVP can be solved by lattice reduction. BKZ reduction with blocksize β runs in time $2^{0.292\beta+o(\beta)}$ [BDGL16].

Using the Gap to Conjecture Hardness

All known attacks against ΔLIP solve SVP.
SVP can be solved by lattice reduction. BKZ reduction with blocksize β runs in time $2^{0.292\beta+o(\beta)}$ [BDGL16]. The parameter β required for solving SVP (heuristically) depends on the length of the shortest vector.

Using the Gap to Conjecture Hardness

All known attacks against ΔLIP solve SVP.
SVP can be solved by lattice reduction. BKZ reduction with blocksize β runs in time $2^{0.292\beta+o(\beta)}$ [BDGL16]. The parameter β required for solving SVP (heuristically) depends on the length of the 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 ΔLIP solve SVP.
SVP can be solved by lattice reduction. BKZ reduction with blocksize β runs in time $2^{0.292\beta+o(\beta)}$ [BDGL16]. The parameter β required for solving SVP (heuristically) depends on the length of the shortest vector.
In a random lattice L of dimension n, we expect $\lambda_1(L) \sim gh(n) \approx \det(L)^{1/n}\sqrt{\frac{n}{2\pi e}}$.

Definition (Gap)

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

Using the Gap to Conjecture Hardness

All known attacks against ΔLIP solve SVP.
SVP can be solved by lattice reduction. BKZ reduction with blocksize β runs in time $2^{0.292\beta+o(\beta)}$ [BDGL16]. The parameter β required for solving SVP (heuristically) depends on the length of the shortest vector.
In a random lattice L of dimension n, we expect $\lambda_1(L) \sim gh(n) \approx \det(L)^{1/n}\sqrt{\frac{n}{2\pi e}}$.

Definition (Gap)

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

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

Using the Gap to Conjecture Hardness

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

Using the Gap to Conjecture Hardness

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

Using the Gap to Conjecture Hardness

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

Conjecture ([DvW22] informal)

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

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

Using the Gap to Conjecture Hardness

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

Conjecture ([DvW22] informal)

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

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

Our result: a counterexample to this conjecture.

Using the Gap to Conjecture Hardness

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

Conjecture ([DvW22] informal)

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

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

Our result: a counterexample to this conjecture. We make the gap larger, by extracting the sublattice $\mathbb{Z}^n$, then solving $\mathbb{Z}$LIP.

Plan

- Construction A Lattices and their Hulls

Plan

- Construction A Lattices and their Hulls
- The Genus of the Hull.

Plan

- Construction A Lattices and their Hulls
- The Genus of the Hull.
- Solving LIP via $\mathbb{Z}$LIP and Code Equivalence

Plan

- Construction A Lattices and their Hulls
- The Genus of the Hull.
- Solving LIP via $\mathbb{Z}$LIP and Code Equivalence
- Solving instances of Code Equivalence via Graph Isomorphism

Hull of a Lattice

Hull of a Lattice

Definition

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

Definition

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

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

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

Definition

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

Hull of a Lattice

Definition

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

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

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

Definition

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

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

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

Which Values of s are Relevant?

Let L be a lattice with basis B. The s-hull can be written as

$$H_s = \left\{ Bx : x \in \mathbb{Z}^n, B^T Bx \in s\mathbb{Z}^n \right\}.$$

Which Values of s are Relevant?

Let L be a lattice with basis B. The s-hull can be written as

$$H_s = \left\{ Bx : x \in \mathbb{Z}^n, B^T Bx \in s\mathbb{Z}^n \right\}.$$

If L is integral, *i.e.* $B^T B \in \mathbb{Z}^{n \times n}$, then any s-hull is a scaling of one of a finite set of hulls.

- If $s \notin \mathbb{Q}$, then $H_s(L) = \{0\}$.

Which Values of s are Relevant?

Let L be a lattice with basis B. The s-hull can be written as

$$H_s = \left\{ Bx : x \in \mathbb{Z}^n, B^T Bx \in s\mathbb{Z}^n \right\}.$$

If L is integral, *i.e.* $B^T B \in \mathbb{Z}^{n \times n}$, then any s-hull is a scaling of one of a finite set of hulls.

- If $s \notin \mathbb{Q}$, then $H_s(L) = \{0\}$.
- If $s = a/b \in \mathbb{Q}$, then $H_s(L) = H_a(L)$.

Which Values of s are Relevant?

Let L be a lattice with basis B. The s-hull can be written as

$$H_s = \left\{ Bx : x \in \mathbb{Z}^n, B^T Bx \in s\mathbb{Z}^n \right\}.$$

If L is integral, *i.e.* $B^T B \in \mathbb{Z}^{n \times n}$, then any s-hull is a scaling of one of a finite set of hulls.

- If $s \notin \mathbb{Q}$, then $H_s(L) = \{0\}$.
- If $s = a/b \in \mathbb{Q}$, then $H_s(L) = H_a(L)$.
- If $s = s' s'' \in \mathbb{Z}$, where s'' is coprime to $\det(B^T B)$, then $H_s(L) = s'' H_{s'}(L)$.

Which Values of s are Relevant?

Let L be a lattice with basis B. The s-hull can be written as

$$H_s = \left\{ Bx : x \in \mathbb{Z}^n, B^T Bx \in s\mathbb{Z}^n \right\}.$$

If L is integral, *i.e.* $B^T B \in \mathbb{Z}^{n \times n}$, then any s-hull is a scaling of one of a finite set of hulls.

- If $s \notin \mathbb{Q}$, then $H_s(L) = \{0\}$.
- If $s = a/b \in \mathbb{Q}$, then $H_s(L) = H_a(L)$.
- If $s = s' s'' \in \mathbb{Z}$, where s'' is coprime to $\det(B^T B)$, then $H_s(L) = s'' H_{s'}(L)$.
- If $s = qp^{k+r}$, where p^k is the largest power of p dividing $\det(B^T B)$, then $H_s = p^r H_{qp^k}$.

Hull of Integral Lattices

The hull can be expressed as

Hull of Integral Lattices

The hull can be expressed as

$$H_s(L) = B \cdot \Lambda_s^{\perp}(B^T B) = B \cdot \left\{ x \in \mathbb{Z}^n : B^T B x = 0 \mod s \right\}.$$

Hull of Integral Lattices

The hull can be expressed as

$$H_s(L) = B \cdot \Lambda_s^{\perp}(B^T B) = B \cdot \left\{ x \in \mathbb{Z}^n : B^T B x = 0 \mod s \right\}.$$

Furthermore, only $s \mid \det(B^T B)$ can lead to unique hulls.

Construction A Lattices

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

$$L = C + p\mathbb{Z}^n = \pi^{-1}[C],$$

where $\pi : \mathbb{Z}^n \to \mathbb{F}_p^n$ is reduction modulo p.

Construction A Lattices

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

$$L = C + p\mathbb{Z}^n = \pi^{-1}[C],$$

where $\pi : \mathbb{Z}^n \to \mathbb{F}_p^n$ is reduction modulo p.

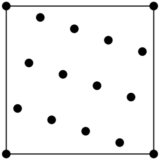

Figure: Construction A Lattice from a code over $\mathbb{F}_{13}$

Construction A Lattices

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

$$L = C + p\mathbb{Z}^n = \pi^{-1}[C],$$

where $\pi : \mathbb{Z}^n \to \mathbb{F}_p^n$ is reduction modulo p.

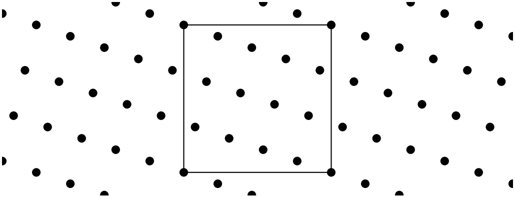

Figure: Construction A Lattice from a code over $\mathbb{F}_{13}$

The Genus as a Potential Attack on ΔLIP

An integral with basis $B \in \mathbb{R}^{n \times m}$ lattice satisfies $Q := B^T B \in \mathbb{Z}^{m \times m}$.

The Genus as a Potential Attack on ΔLIP

An integral with basis $B \in \mathbb{R}^{n \times m}$ lattice satisfies $Q := B^T B \in \mathbb{Z}^{m \times m}$.
The lattices generated by B, B' are isomorphic if there exists $U \in \mathrm{GL}_m(\mathbb{Z})$ with

$$U^T B^T B U = B'^T B'.$$

The Genus as a Potential Attack on ΔLIP

An integral with basis $B \in \mathbb{R}^{n \times m}$ lattice satisfies $Q := B^T B \in \mathbb{Z}^{m \times m}$.
The lattices generated by B, B' are isomorphic if there exists $U \in \mathrm{GL}_m(\mathbb{Z})$ with

$$U^T B^T B U = B'^T B'.$$

A more coarse equivalence class is the genus of a lattice/quadratic form.

The Genus as a Potential Attack on ΔLIP

An integral with basis $B \in \mathbb{R}^{n \times m}$ lattice satisfies $Q := B^T B \in \mathbb{Z}^{m \times m}$.
The lattices generated by B, B' are isomorphic if there exists $U \in \mathrm{GL}_m(\mathbb{Z})$ with

$$U^T B^T B U = B'^T B'.$$

A more coarse equivalence class is the genus of a lattice/quadratic form.

Definition (Genus)

Two Quadratic forms are in the same genus if they are equivalent over $\mathbb{R}$ and over the p-adic integers $\mathbb{Z}_p$ for all primes p.

Diagonalise over $\mathbb{Z}_p$ (Jordan Decomposition)

A (positive definite) quadratic form Q has a *Jordan decomposition*

$$Q \sim$$

Diagonalise over $\mathbb{Z}_p$ (Jordan Decomposition)

A (positive definite) quadratic form Q has a *Jordan decomposition*

$$Q \sim UQU^T =$$

Diagonalise over $\mathbb{Z}_p$ (Jordan Decomposition)

A (positive definite) quadratic form Q has a *Jordan decomposition*

$$Q \sim UQU^T = \begin{pmatrix} Q_1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & pQ_p & 0 & \cdots & 0 & 0 \\ 0 & 0 & p^2 Q_{p^2} & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & p^{e-1} Q_{p^{e-1}} & 0 \\ 0 & 0 & 0 & \cdots & 0 & p^e Q_{p^e} \end{pmatrix}$$

with each Q_i invertible over $\mathbb{Z}_p$, i.e. $\det(Q_i) \in \mathbb{Z}_p^*$

The Genus of the Hull

Proposition (Informal)

If L and L' admit quadratic forms $Q, Q' \in \mathbb{Z}^{m \times m}$ that are equivalent over $\mathbb{Z}_p$,

The Genus of the Hull

Proposition (Informal)

If L and L' admit quadratic forms $Q, Q' \in \mathbb{Z}^{m\times m}$ that are equivalent over $\mathbb{Z}_p$, then any quadratic forms admitted by the s-hulls of these lattices, Q_H and $Q_{H'}$, are also equivalent over $\mathbb{Z}_p$.

The Genus of the Hull

Proposition (Informal)

If L and L' admit quadratic forms $Q, Q' \in \mathbb{Z}^{m \times m}$ that are equivalent over $\mathbb{Z}_p$, then any quadratic forms admitted by the s-hulls of these lattices, Q_H and $Q_{H'}$, are also equivalent over $\mathbb{Z}_p$.

So the genus of the hull will not help solve ΔLIP, if the genus of the lattices cannot solve it.

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

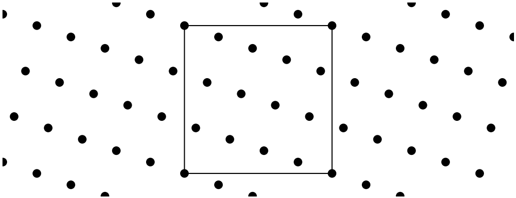

Figure: Hull of a Lattice

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

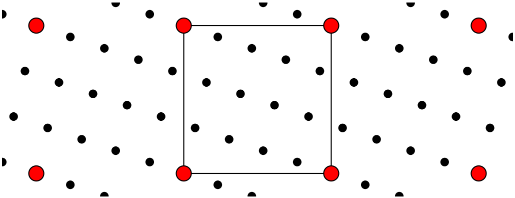

Figure: Hull of a Lattice

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

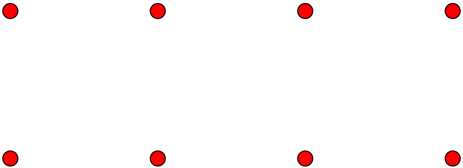

Figure: Hull of a Lattice

Rotation of the Hull

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

Rotation of the Hull

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

Rotation of the Hull

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

$$\begin{tikzcd}
L_1 \arrow[rr, "O"] & & L_2 \\
& C + p\mathbb{Z}^n \arrow[ul, "O_1"] \arrow[ur, "O_2"'] &
\end{tikzcd}$$

Figure: Isomorphism of Lattices

Rotation of the Hull

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

$$
\begin{tikzcd}
L_1 \arrow[rr, "O"] & & L_2 \\
& C + p\mathbb{Z}^n \arrow[ul, "O_1"] \arrow[ur, "O_2"'] &
\end{tikzcd}
$$

Figure: Isomorphism of Lattices

$$
\begin{tikzcd}
H_p(L_1) \arrow[rr, "O_2' {O_1'}^{-1}"] & & H_p(L_2) \\
& p\mathbb{Z}^n \arrow[ul, "O_1'"] \arrow[ur, "O_2'"'] &
\end{tikzcd}
$$

Figure: Isomorphism of Hulls

We now have two instances of $\mathbb{Z}$LIP.

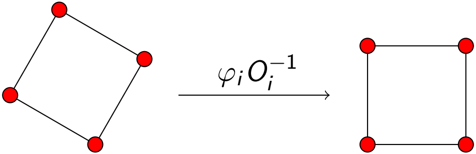

Figure: Rotation of the Hull

We now have two instances of $\mathbb{Z}$LIP.

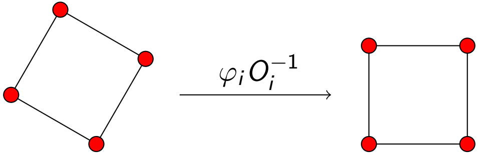

Figure: Rotation of the Hull

In each instance, we find O_i up to $\varphi_i \in \mathrm{Aut}(p\mathbb{Z}^n)$. An instance of $\mathbb{Z}$LIP takes $2^{0.292n/2+o(n)}$ [DPPW22].

Code Equivalence

We find this automorphism by solving a code equivalence problem between $\psi_1 O_1(L_1) \mod p$ and $\psi_2 O_2(L_2) \mod p$.

Code Equivalence

We find this automorphism by solving a code equivalence problem between $\psi_1 O_1(L_1) \mod p$ and $\psi_2 O_2(L_2) \mod p$.

Definition

(Linear Code Equivalence) Two linear $[n, k]_q$ codes $C,\ C' \subseteq \mathbb{F}_q^n$ are linearly equivalent if there exists a permutation matrix P and an $n \times n$ diagonal matrix D with non-zero diagonal entries such that

$$C' = DPC.$$

Code Equivalence

We find this automorphism by solving a code equivalence problem between $\psi_1 O_1(L_1) \mod p$ and $\psi_2 O_2(L_2) \mod p$.

Definition

(Linear Code Equivalence) Two linear $[n, k]_q$ codes C, $C' \subseteq \mathbb{F}_q^n$ are linearly equivalent if there exists a permutation matrix P and an $n \times n$ diagonal matrix D with non-zero diagonal entries such that

$$C' = DPC.$$

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

Signed Permutation Equivalence

Definition

Let $C \subseteq \mathbb{F}_q^n$ be a linear code of dimension k. The *signed closure* $C^{\pm}$ of the code C is the linear code of length $2n$ and dimension k over $\mathbb{F}_q$ given by:

$$C^{\pm} := \left\{(x_1, -x_1, x_2, -x_2, \ldots, x_n, -x_n) : (x_i)_{i\in[n]} \in C\right\}.$$

Signed Permutation Equivalence

Definition

Let $C \subseteq \mathbb{F}_q^n$ be a linear code of dimension k. The *signed closure* $C^{\pm}$ of the code C is the linear code of length $2n$ and dimension k over $\mathbb{F}_q$ given by:

$$C^{\pm} := \left\{ (x_1, -x_1, x_2, -x_2, \ldots, x_n, -x_n) : (x_i)_{i \in [n]} \in C \right\}.$$

Lemma (Adapted from [SS13a])

Let C, $C' \subseteq \mathbb{F}_q^n$ be linear codes. Then C and C' are signed permutation equivalent if and only if $C^{\pm}$ and $C'^{\pm}$ are permutation equivalent.

Signed Permutation Equivalence

Definition

Let $C \subseteq \mathbb{F}_q^n$ be a linear code of dimension k. The *signed closure* $C^{\pm}$ of the code C is the linear code of length $2n$ and dimension k over $\mathbb{F}_q$ given by:

$$C^{\pm} := \left\{(x_1, -x_1, x_2, -x_2, \ldots, x_n, -x_n) : (x_i)_{i\in[n]} \in C\right\}.$$

Lemma (Adapted from [SS13a])

Let C, $C' \subseteq \mathbb{F}_q^n$ be linear codes. Then C and C' are signed permutation equivalent if and only if $C^{\pm}$ and $C'^{\pm}$ are permutation equivalent.

Any permutation from $C^{\pm}$ to $C'^{\pm}$ can be lifted to a signed permutation from C to C'

PEP to Graph Isomorphism

- Key difference from [SS13b]: if $\mathrm{char}(\mathbb{F}_q) \neq 2$, then $\mathcal{H}(C^{\pm}) = (\mathcal{H}(C))^{\pm}$.

PEP to Graph Isomorphism

- Key difference from [SS13b]: if $\mathrm{char}(\mathbb{F}_q) \neq 2$, then $\mathcal{H}(C^{\pm}) = (\mathcal{H}(C))^{\pm}$.
- If $\dim(\mathcal{H}(C)) = 0$, then $\dim(\mathcal{H}(C^{\pm})) = 0$: an easy instance of permutation equivalence, via graph isomorphism.[BOST19]

PEP to Graph Isomorphism

- Key difference from [SS13b]: if $\mathrm{char}(\mathbb{F}_q) \neq 2$, then $\mathcal{H}(C^{\pm}) = (\mathcal{H}(C))^{\pm}$.
- If $\dim(\mathcal{H}(C)) = 0$, then $\dim(\mathcal{H}(C^{\pm})) = 0$: an easy instance of permutation equivalence, via graph isomorphism.[BOST19]
- Graph isomorphism can be solved in time $2^{O((\log n)^c)}$ for some constant c [Bab15].

Summary of the Attack

Given an $[n, k]_p$ code C with hull of dimension 0, the Construction A lattice generated by this code $C + p\mathbb{Z}^n$ has p-hull given by $p\mathbb{Z}^n$.

Summary of the Attack

Given an $[n, k]_p$ code C with hull of dimension 0, the Construction A lattice generated by this code $C + p\mathbb{Z}^n$ has p-hull given by $p\mathbb{Z}^n$. Given two orthonormal transformations of this Construction A lattice $O_1, O_2 \in \mathcal{O}_n(\mathbb{R})$, ΔLIP can be solved in time $2^{0.292n/2+o(n)}$.

- Take the p-hull of L_1 and L_2.

Summary of the Attack

Given an $[n, k]_p$ code C with hull of dimension 0, the Construction A lattice generated by this code $C + p\mathbb{Z}^n$ has p-hull given by $p\mathbb{Z}^n$. Given two orthonormal transformations of this Construction A lattice $O_1, O_2 \in \mathcal{O}_n(\mathbb{R})$, ΔLIP can be solved in time $2^{0.292n/2+o(n)}$.

- 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 ψO_1, φO_2 for some $\psi, \varphi \in \mathrm{Aut}(\mathbb{Z}^n)$.

Summary of the Attack

Given an $[n,k]_p$ code C with hull of dimension 0, the Construction A lattice generated by this code $C + p\mathbb{Z}^n$ has p-hull given by $p\mathbb{Z}^n$. Given two orthonormal transformations of this Construction A lattice $O_1, O_2 \in \mathcal{O}_n(\mathbb{R})$, ΔLIP can be solved in time $2^{0.292n/2+o(n)}$.

- 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 ψO_1, φO_2 for some $\psi, \varphi \in \mathrm{Aut}(\mathbb{Z}^n)$.
- Apply O_1^{-1} and O_2^{-1} to L_1 and L_2, respectively, and then reduce modulo p.

Summary of the Attack

Given an $[n, k]_p$ code C with hull of dimension 0, the Construction A lattice generated by this code $C + p\mathbb{Z}^n$ has p-hull given by $p\mathbb{Z}^n$. Given two orthonormal transformations of this Construction A lattice $O_1, O_2 \in \mathcal{O}_n(\mathbb{R})$, ΔLIP can be solved in time $2^{0.292n/2+o(n)}$.

- 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 ψO_1, φO_2 for some $\psi, \varphi \in \mathrm{Aut}(\mathbb{Z}^n)$.
- Apply O_1^{-1} and O_2^{-1} to L_1 and L_2, respectively, and then reduce modulo p.
- Reduce from solving SPEP on the resulting codes to solving PEP on their closures.

Summary of the Attack

Given an $[n, k]_p$ code C with hull of dimension 0, the Construction A lattice generated by this code $C + p\mathbb{Z}^n$ has p-hull given by $p\mathbb{Z}^n$. Given two orthonormal transformations of this Construction A lattice $O_1, O_2 \in \mathcal{O}_n(\mathbb{R})$, ΔLIP can be solved in time $2^{0.292n/2+o(n)}$.

- 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 ψO_1, φO_2 for some $\psi, \varphi \in \mathrm{Aut}(\mathbb{Z}^n)$.
- Apply O_1^{-1} and O_2^{-1} to L_1 and L_2, respectively, and then reduce modulo p.
- Reduce from solving SPEP on the resulting codes to solving PEP on their closures.
- Solve PEP on their closures via graph isomorphism.

Conclusion

We restate the conjecture from [DvW22]

Conjecture (informal)

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

$$f = \mathrm{hullgap}(L)$$

where

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

Conclusion

- Recommendaton:

Conclusion

- Recommendaton: Use unimodular (i.e. self-dual) lattices for LIP, to avoid this or similar attacks.

Conclusion

- Recommendaton: Use unimodular (i.e. self-dual) lattices for LIP, to avoid this or similar attacks.
- Coincidentally, the lattices used in [DPPW22, BGPSD21] (rotations of $\mathbb{Z}^n$) are unimodular.

Conclusion

- Recommendaton: Use unimodular (i.e. self-dual) lattices for LIP, to avoid this or similar attacks.
- Coincidentally, the lattices used in [DPPW22, BGPSD21] (rotations of $\mathbb{Z}^n$) are unimodular.

https://eprint.iacr.org/2023/194.pdf

References I

László Babai, *Graph isomorphism in quasipolynomial time*, 2015, `https://arxiv.org/abs/1512.03547`.

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*, Cryptology ePrint Archive, Paper 2021/1548, 2021.

References II

Magali Bardet, Ayoub Otmani, and Mohamed Saeed-Taha, *Permutation code equivalence is not harder than graph isomorphism when hulls are trivial*, 2019 IEEE International Symposium on Information Theory (ISIT), IEEE, jul 2019.

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.

References III

- 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.
- Nicolas Sendrier and Dimitris Simos, *How easy is code equivalence over fq*, International Workshop on Coding and Cryptography - WCC 2013, Apr 2013, Bergen, Norway, 2013, `https://hal.inria.fr/hal-00790861v2`.

References IV

Nicolas Sendrier and Dimitris E. Simos, *The hardness of code equivalence over $\mathbb{F}_q$ and its application to code-based cryptography*, Post-Quantum Cryptography (Berlin, Heidelberg) (Philippe Gaborit, ed.), Springer Berlin Heidelberg, 2013, pp. 203–216.