On the Lattice Isomorphism Problem, Quadratic Forms, Remarkable Lattices, and Cryptography

Léo Ducas, Wessel van Woerden (CWI, Cryptology Group).

Centrum Wiskunde & Informatica

Motivation

- Most NIST PQC finalists (**5/7**) are based on hard lattice problems.

Motivation

- Most NIST PQC finalists (**5/7**) are based on hard lattice problems.
- LWE, SIS, NTRU lattices, while versatile, have poor decoding properties.

Motivation

- Most NIST PQC finalists (**5/7**) are based on hard lattice problems.
- LWE, SIS, NTRU lattices, while versatile, have poor decoding properties.
- Many wonderful lattices exist with great geometric properties.

Motivation

- Most NIST PQC finalists (**5/7**) are based on hard lattice problems.
- LWE, SIS, NTRU lattices, while versatile, have poor decoding properties.
- Many wonderful lattices exist with great geometric properties.
- Can we use these in cryptography?

Motivation

- Most NIST PQC finalists (**5/7**) are based on hard lattice problems.
- LWE, SIS, NTRU lattices, while versatile, have poor decoding properties.
- Many wonderful lattices exist with great geometric properties.
- Can we use these in cryptography?
- Many ad-hoc methods have been broken by ad-hoc attacks.

Motivation

- Most NIST PQC finalists (**5/7**) are based on hard lattice problems.
- LWE, SIS, NTRU lattices, while versatile, have poor decoding properties.
- Many wonderful lattices exist with great geometric properties.
- Can we use these in cryptography?
- Many ad-hoc methods have been broken by ad-hoc attacks.

Contributions

- General identification, encryption and signature scheme based on the Lattice Isomorphism Problem.

Motivation

- Most NIST PQC finalists (**5/7**) are based on hard lattice problems.
- LWE, SIS, NTRU lattices, while versatile, have poor decoding properties.
- Many wonderful lattices exist with great geometric properties.
- Can we use these in cryptography?
- Many ad-hoc methods have been broken by ad-hoc attacks.

Contributions

- General identification, encryption and signature scheme based on the Lattice Isomorphism Problem.
- Better lattices $\implies$ better efficiency and security.

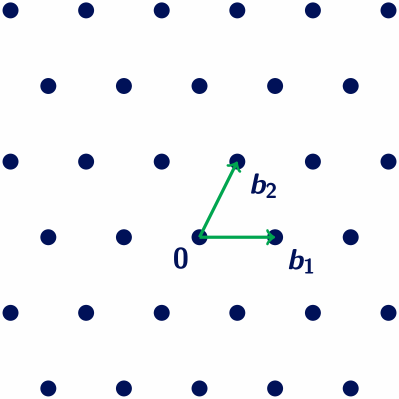
Motivation

- Most NIST PQC finalists (**5/7**) are based on hard lattice problems.
- LWE, SIS, NTRU lattices, while versatile, have poor decoding properties.
- Many wonderful lattices exist with great geometric properties.
- Can we use these in cryptography?
- Many ad-hoc methods have been broken by ad-hoc attacks.

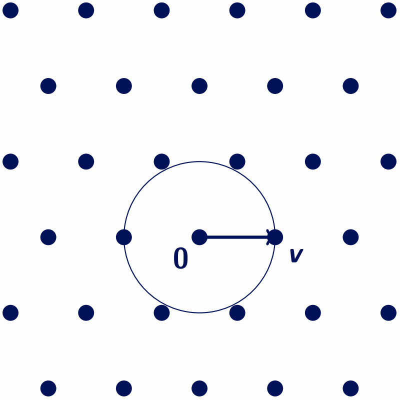
Contributions

- General identification, encryption and signature scheme based on the Lattice Isomorphism Problem.
- Better lattices $\implies$ better efficiency and security.
- Lots of open questions.

Lattice $\mathcal{L}(\boldsymbol{B}) := \{\sum_i x_i \boldsymbol{b}_i : \boldsymbol{x} \in \mathbb{Z}^n\} \subset \mathbb{R}^n$



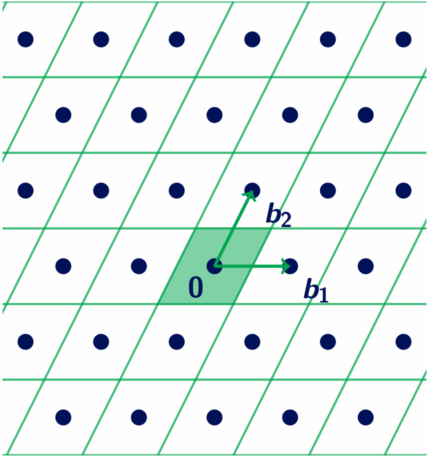
Lattice $\mathcal{L}(\boldsymbol{B}) := \{\sum_i x_i \boldsymbol{b}_i : \boldsymbol{x} \in \mathbb{Z}^n\} \subset \mathbb{R}^n$



First minimum

$$\lambda_1(\mathcal{L}) := \min_{x \in \mathcal{L} \setminus \{0\}} \|x\|_2$$

Lattice $\mathcal{L}(\boldsymbol{B}) := \{\sum_i x_i \boldsymbol{b}_i : \boldsymbol{x} \in \mathbb{Z}^n\} \subset \mathbb{R}^n$



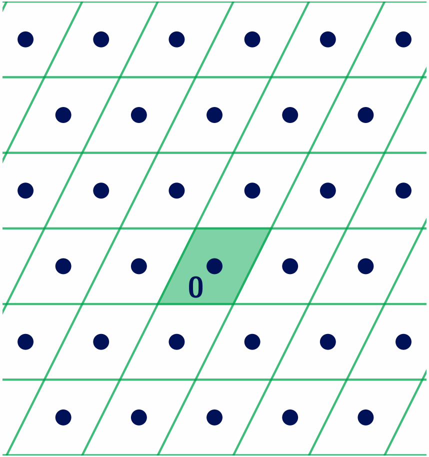
First minimum

$$\lambda_1(\mathcal{L}) := \min_{\boldsymbol{x} \in \mathcal{L} \setminus \{\boldsymbol{0}\}} \|\boldsymbol{x}\|_2$$

Determinant

$$\det(\mathcal{L}) := \mathrm{vol}(\mathbb{R}^n / \mathcal{L}) = |\det(\boldsymbol{B})|$$

Lattice $\mathcal{L}(\boldsymbol{B}) := \{\sum_i x_i \boldsymbol{b}_i : \boldsymbol{x} \in \mathbb{Z}^n\} \subset \mathbb{R}^n$



First minimum

$$\lambda_1(\mathcal{L}) := \min_{\boldsymbol{x} \in \mathcal{L} \setminus \{\boldsymbol{0}\}} \|\boldsymbol{x}\|_2$$

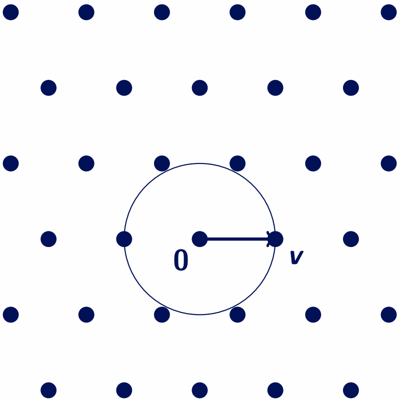
Determinant

$$\det(\mathcal{L}) := \mathrm{vol}(\mathbb{R}^n / \mathcal{L}) = |\det(\boldsymbol{B})|$$

Minkowski's Theorem

$$\lambda_1(\mathcal{L}) \leq \underbrace{2 \frac{\det(\mathcal{L})^{1/n}}{\mathrm{vol}(\mathcal{B}^n)^{1/n}}}_{\mathrm{Mk}(\mathcal{L})} \leq \sqrt{n} \det(\mathcal{L})^{1/n}$$

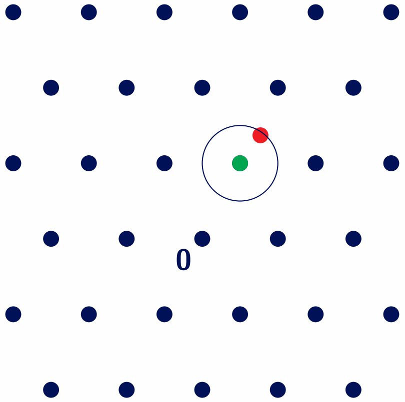
Lattice $\mathcal{L} \subset \mathbb{R}^n$



SVP

Find a *shortest* nonzero vector $\boldsymbol{v} \in \mathcal{L}$ of length $\lambda_1(\mathcal{L}) \leq \mathsf{Mk}(\mathcal{L})$.

Lattice $\mathcal{L} \subset \mathbb{R}^n$



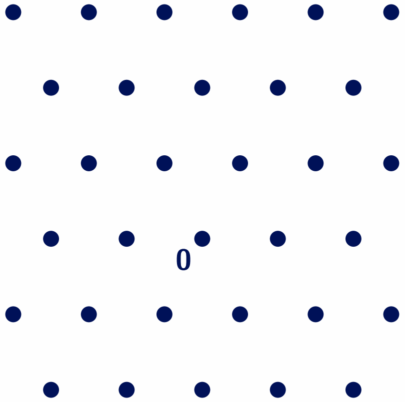
SVP

Find a *shortest* nonzero vector $\boldsymbol{v} \in \mathcal{L}$ of length $\lambda_1(\mathcal{L}) \leq \mathsf{Mk}(\mathcal{L})$.

BDD

Given a target $\boldsymbol{t} = \boldsymbol{v} + \boldsymbol{e} \in \mathbb{R}^n$ with $\boldsymbol{v} \in \mathcal{L}$ and $\|\boldsymbol{e}\| < \rho \leq \frac{1}{2}\lambda_1(\mathcal{L}) \leq \frac{1}{2}\mathsf{Mk}(\mathcal{L})$, recover the *closest* vector $\boldsymbol{v} \in \mathcal{L}$.

Lattice $\mathcal{L} \subset \mathbb{R}^n$



SVP

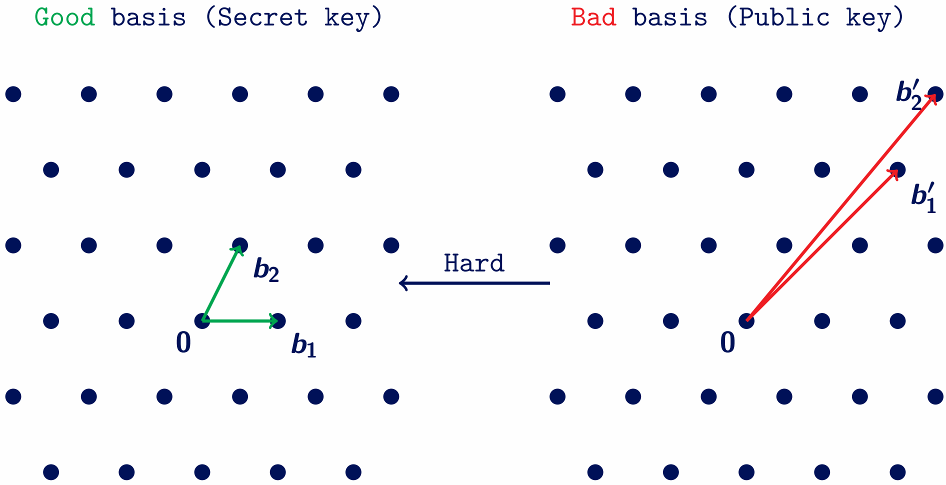
Find a *shortest* nonzero vector $\boldsymbol{v} \in \mathcal{L}$ of length $\lambda_1(\mathcal{L}) \leq \mathsf{Mk}(\mathcal{L})$.

BDD

Given a target $\boldsymbol{t} = \boldsymbol{v} + \boldsymbol{e} \in \mathbb{R}^n$ with $\boldsymbol{v} \in \mathcal{L}$ and $\|\boldsymbol{e}\| < \rho \leq \frac{1}{2}\lambda_1(\mathcal{L}) \leq \frac{1}{2}\mathsf{Mk}(\mathcal{L})$, recover the *closest* vector $\boldsymbol{v} \in \mathcal{L}$.

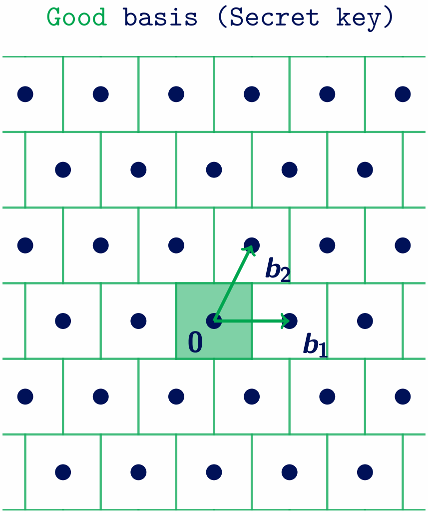
Hardness depends on the *gap*
$\mathsf{gap}(\mathcal{L}) := \frac{\mathsf{Mk}(\mathcal{L})}{\lambda_1(\mathcal{L})}$ or $\mathsf{gap}(\mathcal{L}, \rho) := \frac{\mathsf{Mk}(\mathcal{L})}{\rho}$.
(state-of-art heuristic algorithms)
[ADPS16], [AGVW17], [PV21]

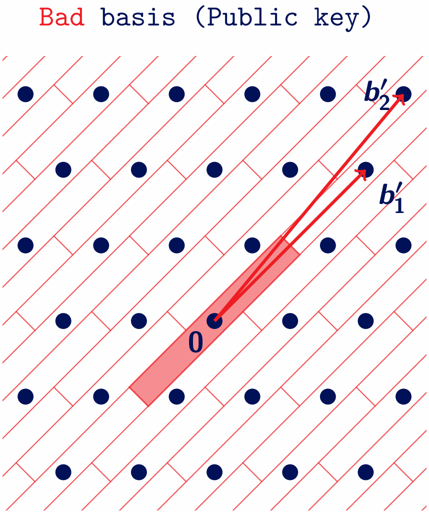
How to do encryption?



$\boldsymbol{B}$

$\boldsymbol{B}' = \boldsymbol{B} \cdot \boldsymbol{U},\ \ \boldsymbol{U} \in \mathrm{GL}_d(\mathbb{Z})$

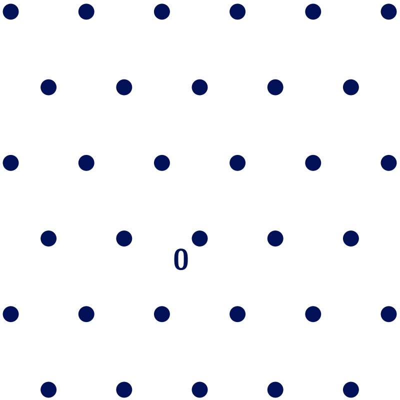




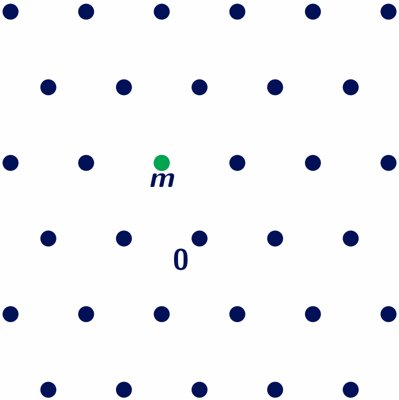
Babai's nearest plane algorithm

How to do encryption?

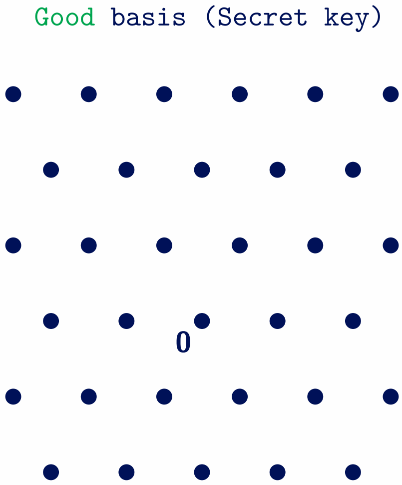
Good basis (Secret key)

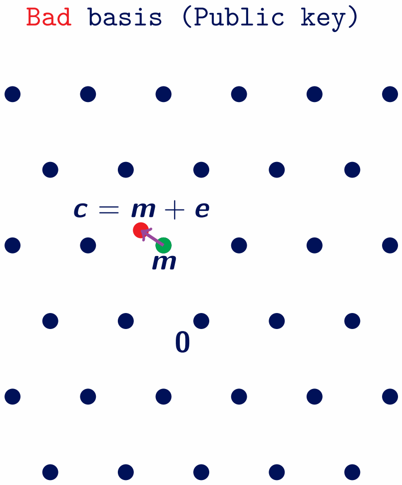


Bad basis (Public key)



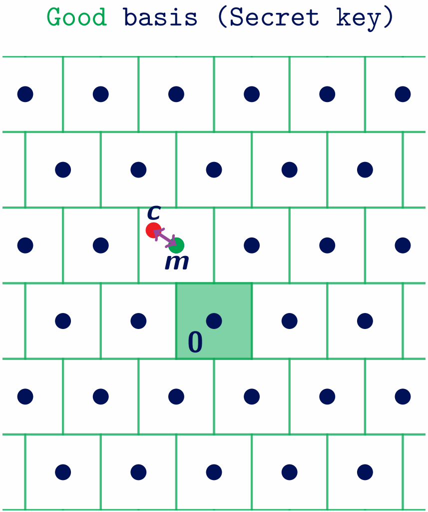
How to do encryption?

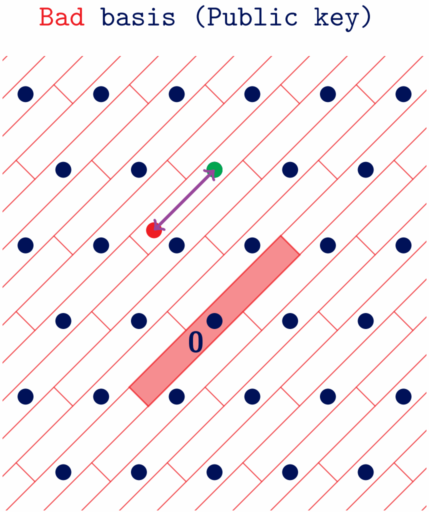




Encrypt by adding a small error

How to do encryption?





Decrypt using the good basis

Large gap

Current lattice based crypto relies on hardness of decoding with

$$\mathrm{gap}(\mathcal{L}, \rho) \geq \Omega(\sqrt{n}).$$

Broken by SVP in dimension $\beta \leq n/2 + o(n)$.

Large gap

Current lattice based crypto relies on hardness of decoding with

$$\mathrm{gap}(\mathcal{L}, \rho) \geq \Omega(\sqrt{n}).$$

Broken by SVP in dimension $\beta \leq n/2 + o(n)$.

An example: Prime Lattice [CR88]

Let $p_1, \ldots, p_n$ be distinct small primes not dividing m, we define:

$$\mathcal{L}_{\mathtt{prime}} := \{x = (x_1, \ldots, x_n) \in \mathbb{Z}^n : \prod_i p_i^{x_i} = 1 \bmod m\}.$$

Large gap

Current lattice based crypto relies on hardness of decoding with

$$\mathrm{gap}(\mathcal{L}, \rho) \geq \Omega(\sqrt{n}).$$

Broken by SVP in dimension $\beta \leq n/2 + o(n)$.

An example: Prime Lattice [CR88]

Let $p_1, \ldots, p_n$ be distinct small primes not dividing m, we define:

$$\mathcal{L}_{\texttt{prime}} := \{x = (x_1, \ldots, x_n) \in \mathbb{Z}^n : \prod_i p_i^{x_i} = 1 \bmod m\}.$$

- Efficiently decode up to large radius ρ by trial division.

Large gap

Current lattice based crypto relies on hardness of decoding with

$$\mathrm{gap}(\mathcal{L}, \rho) \geq \Omega(\sqrt{n}).$$

Broken by SVP in dimension $\beta \leq n/2 + o(n)$.

An example: Prime Lattice [CR88]

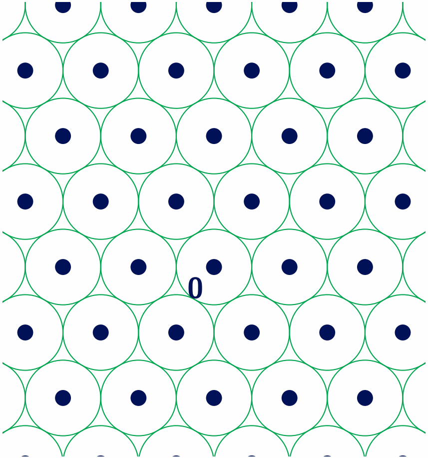
Let $p_1, \ldots, p_n$ be distinct small primes not dividing m, we define:

$$\mathcal{L}_{\mathtt{prime}} := \{x = (x_1, \ldots, x_n) \in \mathbb{Z}^n : \prod_i p_i^{x_i} = 1 \bmod m\}.$$

- Efficiently decode up to large radius ρ by trial division.
- With the right parameters $\mathrm{gap}(\mathcal{L}_{\mathtt{prime}}, \rho) = \Theta(\log(n))$ [DP19].

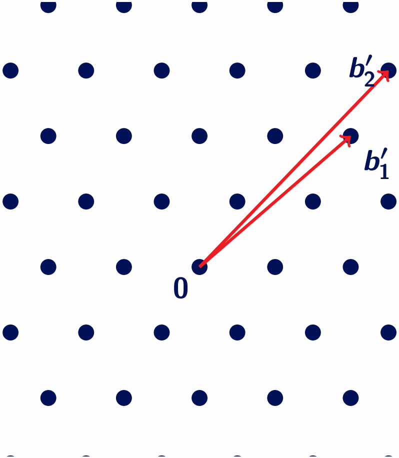
How to hide the remarkable lattice?

Good lattice (~~Secret key~~)



$\mathcal{L}$

Bad basis (Public key)

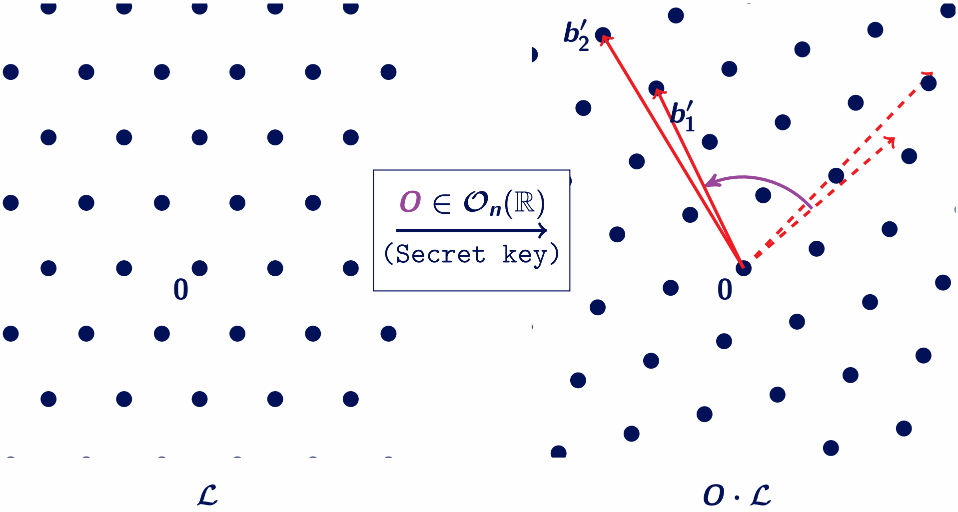


$\mathcal{L}$

How to hide the remarkable lattice?

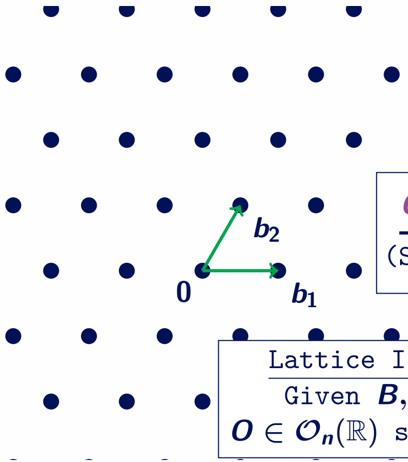
Good lattice (~~Secret key~~)

Bad basis (Public key)



How to hide the remarkable lattice?

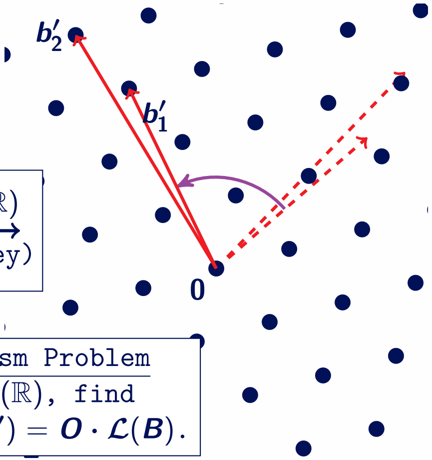
Good lattice (~~Secret key~~)



$\mathcal{L}$

$O \in \mathcal{O}_n(\mathbb{R})$ ⟶ (Secret key)

Bad basis (Public key)



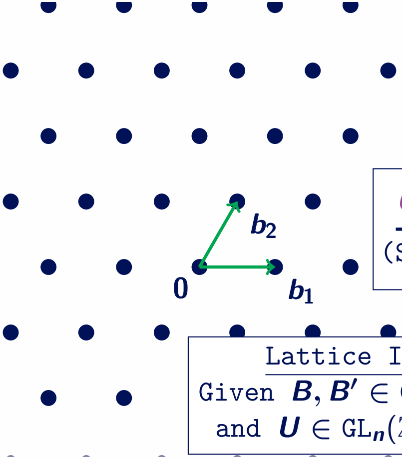
$O \cdot \mathcal{L}$

Lattice Isomorphism Problem

Given $B, B' \in \mathrm{GL}_n(\mathbb{R})$, find $O \in \mathcal{O}_n(\mathbb{R})$ s.t. $\mathcal{L}(B') = O \cdot \mathcal{L}(B)$.

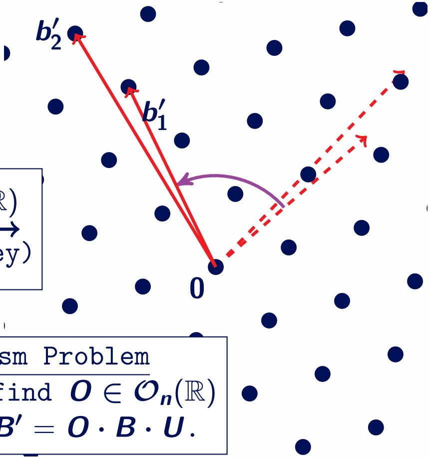
How to hide the remarkable lattice?

Good lattice (~~Secret key~~)



B

Bad basis (Public key)



$B' = O \cdot B \cdot U$

$\xrightarrow[\text{(Secret key)}]{O \in \mathcal{O}_n(\mathbb{R})}$

Lattice Isomorphism Problem

Given $B, B' \in \mathrm{GL}_n(\mathbb{R})$, find $O \in \mathcal{O}_n(\mathbb{R})$ and $U \in \mathrm{GL}_n(\mathbb{Z})$ s.t. $B' = O \cdot B \cdot U$.

LIP

Given isomorphic $\boldsymbol{B}, \boldsymbol{B}' \in \mathrm{GL}_{\boldsymbol{n}}(\mathbb{R})$, find $\boldsymbol{O} \in \mathcal{O}_{\boldsymbol{n}}(\mathbb{R})$ and $\boldsymbol{U} \in \mathrm{GL}_{\boldsymbol{n}}(\mathbb{Z})$ s.t. $\boldsymbol{B}' = \boldsymbol{O} \cdot \boldsymbol{B} \cdot \boldsymbol{U}$.

Lattice Isomorphism Problem

LIP

Given isomorphic $\boldsymbol{B}, \boldsymbol{B}' \in \mathrm{GL}_n(\mathbb{R})$, find $\boldsymbol{O} \in \mathcal{O}_n(\mathbb{R})$ and $\boldsymbol{U} \in \mathrm{GL}_n(\mathbb{Z})$ s.t. $\boldsymbol{B}' = \boldsymbol{O} \cdot \boldsymbol{B} \cdot \boldsymbol{U}$.

- The lattice analogue of 'vintage' McEliece $\boldsymbol{G}' = \boldsymbol{P} \cdot \boldsymbol{G} \cdot \boldsymbol{S}$.

Lattice Isomorphism Problem

LIP

Given isomorphic $\boldsymbol{B}, \boldsymbol{B}' \in \mathrm{GL}_{\boldsymbol{n}}(\mathbb{R})$, find $\boldsymbol{O} \in \mathcal{O}_{\boldsymbol{n}}(\mathbb{R})$ and $\boldsymbol{U} \in \mathrm{GL}_{\boldsymbol{n}}(\mathbb{Z})$ s.t. $\boldsymbol{B}' = \boldsymbol{O} \cdot \boldsymbol{B} \cdot \boldsymbol{U}$.

- The lattice analogue of 'vintage' McEliece $\boldsymbol{G}' = \boldsymbol{P} \cdot \boldsymbol{G} \cdot \boldsymbol{S}$.
- At least as hard as Graph Isomorphism (doesn't say much..).

Lattice Isomorphism Problem

LIP

Given isomorphic $\mathbf{B}, \mathbf{B}' \in \mathrm{GL}_n(\mathbb{R})$, find $\mathbf{O} \in \mathcal{O}_n(\mathbb{R})$ and $\mathbf{U} \in \mathrm{GL}_n(\mathbb{Z})$ s.t. $\mathbf{B}' = \mathbf{O} \cdot \mathbf{B} \cdot \mathbf{U}$.

- The lattice analogue of 'vintage' McEliece $\mathbf{G}' = \mathbf{P} \cdot \mathbf{G} \cdot \mathbf{S}$.
- At least as hard as Graph Isomorphism (doesn't say much..).

Algorithms

- $\mathrm{Min}(\mathcal{L}(\mathbf{B}')) = \mathbf{O} \cdot \mathrm{Min}(\mathcal{L}(\mathbf{B}))$.
- Best practical algorithm: backtrack search all isometries between the sets of short vectors.
- Best proven algorithm uses short primal and dual vectors ($n^{O(n)}$ time and space).

$O \in \mathcal{O}_n(\mathbb{R})$

Computing with reals is a complex problem.

$O \in \mathcal{O}_n(\mathbb{R})$

Computing with reals is a complex problem.

- $B' = OBU \implies (B')^t B' = U^t B^t O^t O B U = U^t B^t B U.$

$O \in \mathcal{O}_n(\mathbb{R})$

Computing with reals is a complex problem.

- $B' = OBU \implies (B')^t B' = U^t B^t O^t O B U = U^t B^t B U.$
- $(B')^t B' = U^t B^t B U \implies \exists O \in \mathcal{O}_n(\mathbb{R}) : B' = OBU.$

$O \in \mathcal{O}_n(\mathbb{R})$

Computing with reals is a complex problem.

- $B' = OBU \implies (B')^t B' = U^t B^t O^t O B U = U^t B^t B U.$
- $(B')^t B' = U^t B^t B U \implies \exists O \in \mathcal{O}_n(\mathbb{R}) : B' = OBU.$
- $Q := B^t B \in \mathcal{S}_n^{>0}(\mathbb{R})$ induces a positive definite quadratic form.

$O \in \mathcal{O}_n(\mathbb{R})$

Computing with reals is a complex problem.

- $B' = OBU \implies (B')^t B' = U^t B^t O^t O B U = U^t B^t B U$.
- $(B')^t B' = U^t B^t B U \implies \exists O \in \mathcal{O}_n(\mathbb{R}) : B' = OBU$.
- $Q := B^t B \in \mathcal{S}_n^{>0}(\mathbb{R})$ induces a positive definite quadratic form.
- Lattice $\mathbb{Z}^n$ with i.p. $\langle x, y \rangle_Q = x^t Q y$ and norm $\|x\|_Q^2 := x^t Q x$.

$O \in \mathcal{O}_n(\mathbb{R})$

Computing with reals is a complex problem.

- $B' = OBU \implies (B')^t B' = U^t B^t O^t O B U = U^t B^t B U$.
- $(B')^t B' = U^t B^t B U \implies \exists O \in \mathcal{O}_n(\mathbb{R}) : B' = OBU$.
- $Q := B^t B \in \mathcal{S}_n^{>0}(\mathbb{R})$ induces a positive definite quadratic form.
- Lattice $\mathbb{Z}^n$ with i.p. $\langle x, y \rangle_Q = x^t Q y$ and norm $\|x\|_Q^2 := x^t Q x$.
- $\lambda_1(Q) := \min_{x \in \mathbb{Z}^n \setminus \{0\}} \|x\|_Q$.

$O \in \mathcal{O}_n(\mathbb{R})$

Computing with reals is a complex problem.

- $B' = OBU \implies (B')^t B' = U^t B^t O^t O B U = U^t B^t B U$.
- $(B')^t B' = U^t B^t B U \implies \exists O \in \mathcal{O}_n(\mathbb{R}) : B' = OBU$.
- $Q := B^t B \in \mathcal{S}_n^{>0}(\mathbb{R})$ induces a positive definite quadratic form.
- Lattice $\mathbb{Z}^n$ with i.p. $\langle x, y \rangle_Q = x^t Q y$ and norm $\|x\|_Q^2 := x^t Q x$.
- $\lambda_1(Q) := \min_{x \in \mathbb{Z}^n \setminus \{0\}} \|x\|_Q$.

LIP (restated)

Given equivalent $Q, Q' \in \mathcal{S}_n^{>0}(\mathbb{R})$, find $U \in \mathrm{GL}_n(\mathbb{Z})$ s.t. $Q' = U^t Q U$.

$O \in \mathcal{O}_n(\mathbb{R})$

Computing with reals is a complex problem.

- $B' = OBU \implies (B')^t B' = U^t B^t O^t O B U = U^t B^t B U$.
- $(B')^t B' = U^t B^t B U \implies \exists O \in \mathcal{O}_n(\mathbb{R}) : B' = OBU$.
- $Q := B^t B \in \mathcal{S}_n^{>0}(\mathbb{R})$ induces a positive definite quadratic form.
- Lattice $\mathbb{Z}^n$ with i.p. $\langle x, y \rangle_Q = x^t Q y$ and norm $\|x\|_Q^2 := x^t Q x$.
- $\lambda_1(Q) := \min_{x \in \mathbb{Z}^n \setminus \{0\}} \|x\|_Q$.

LIP (restated)

Given equivalent $Q, Q' \in \mathcal{S}_n^{>0}(\mathbb{R})$, find $U \in \mathrm{GL}_n(\mathbb{Z})$ s.t. $Q' = U^t Q U$.

- Only work with $Q \in \mathcal{S}_n^{>0}(\mathbb{Z})$.

Encryption [informal]

Prerequisite

Let S be a quadratic form with an efficient decoder up to some radius $\rho < \lambda_1(S)/2$.

Keygen :

Sample $(pk, sk) := (P, U) \leftarrow \mathcal{D}_\sigma([S])$, such that $P = U^t S U$.

Encrypt(P, m) :

$$c := m + e \text{ s.t. } \|e\|_P \leq \rho$$

Decrypt(U, c) :

$$m' := \mathrm{Decode}(S, Uc) \text{ s.t. } \|m' - Uc\|_S \leq \rho$$

$$m = U^{-1} m'$$

Average case instances

- Task: sample a 'random' public key $\boldsymbol{P} = \boldsymbol{U}^t \boldsymbol{S} \boldsymbol{U}$ together with $\boldsymbol{U}$?

Average case instances

- Task: sample a 'random' public key $P = U^t S U$ together with U?

$(R, U) \leftarrow \mathcal{D}_\sigma([Q])$, given $S \in [Q]$, σ large enough.

1. Sample n vectors $y_1, \ldots, y_n \in \mathbb{Z}^n$ from $\mathcal{D}_{S,\sigma}$ (discrete gaussian). Repeat if not linearly independent.
2. Let $Y = UT$ be the unique upper triangular HNF decomposition.
3. Return $(R = U^t S U, U)$.

Average case instances

- Task: sample a 'random' public key $\mathbf{P} = \mathbf{U}^t \mathbf{S} \mathbf{U}$ together with $\mathbf{U}$?

$(\mathbf{R}, \mathbf{U}) \leftarrow \mathcal{D}_\sigma([\mathbf{Q}])$, given $\mathbf{S} \in [\mathbf{Q}]$, $\boldsymbol{\sigma}$ large enough.

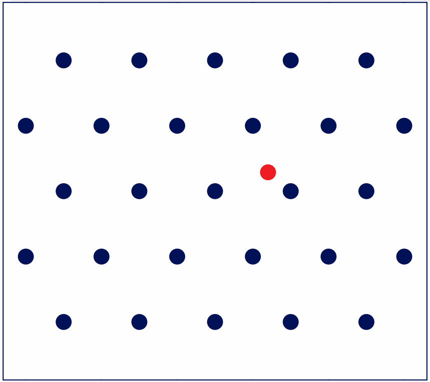
1. Sample n vectors $\mathbf{y}_1, \ldots, \mathbf{y}_n \in \mathbb{Z}^n$ from $\mathcal{D}_{\mathbf{S},\sigma}$ (discrete gaussian). Repeat if not linearly independent.
2. Let $\mathbf{Y} = \mathbf{U}\mathbf{T}$ be the unique upper triangular HNF decomposition.
3. Return $(\mathbf{R} = \mathbf{U}^t \mathbf{S} \mathbf{U}, \mathbf{U})$.

Properties

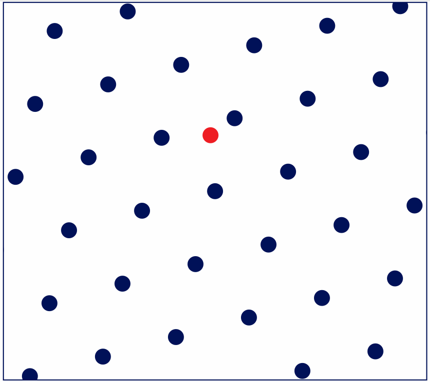
- $\mathbf{R}$ only depends on the class $[\mathbf{Q}]$ and σ (ZKPoK, identification).
- Defines an average-case LIP problem ac-$\mathrm{LIP}_\sigma^{\mathbf{S}}$.
- Given any representative we can sample at $\sigma \geq 2^{\Theta(n)} \cdot \lambda_n([\mathbf{S}])$ ($\implies$ worst-case to average-case reduction).

Actual hardness assumption

1. For a uniformly random $O \in \mathcal{O}_n(\mathbb{R})$, decoding in $O \cdot \mathcal{L}_0$ is hard.



$\mathcal{L}_0$

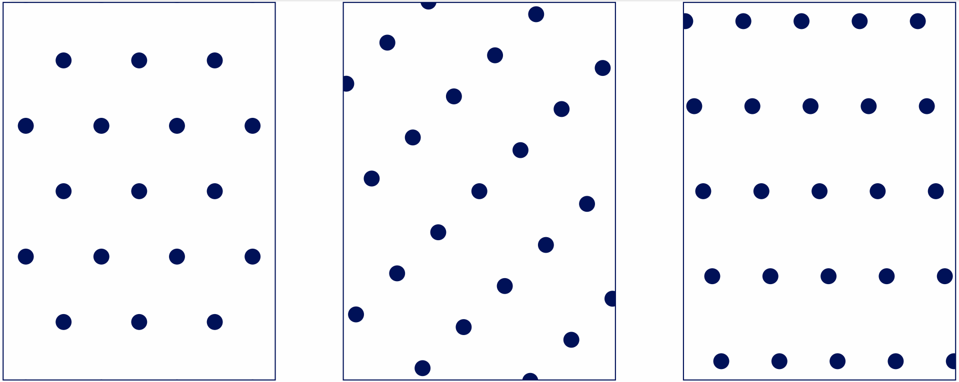


$\mathcal{L}_1 = O \cdot \mathcal{L}_0$

Distinguishing LIP

$\Delta\,\mathsf{LIP}_{\sigma}^{Q_0,Q_1}$

Given two quadratic forms $Q_0, Q_1 \in \mathcal{S}_n^{>0}$, and $Q \in \mathcal{D}_\sigma([Q_b])$ for a uniform random $b \in \{0,1\}$, find b.

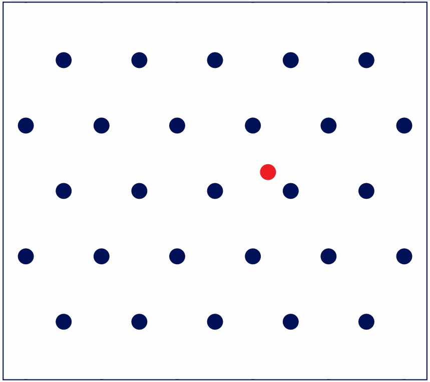


$\mathcal{L}_0$ $\qquad$ $O \cdot \mathcal{L}_b$ $\qquad$ $\mathcal{L}_1$

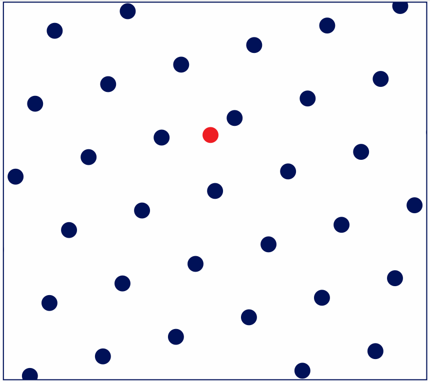
Security Proof

Security Assumption [informal]

1. $\mathcal{O} \cdot \mathcal{L}_0$ is *indistinguishable* from a *random* lattice.
2. Decoding in a *random* lattice is hard.



$\mathcal{L}_0$

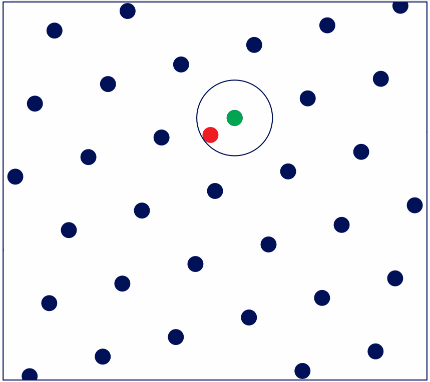


$\mathcal{L}_1 = \mathcal{O} \cdot \mathcal{L}_0$

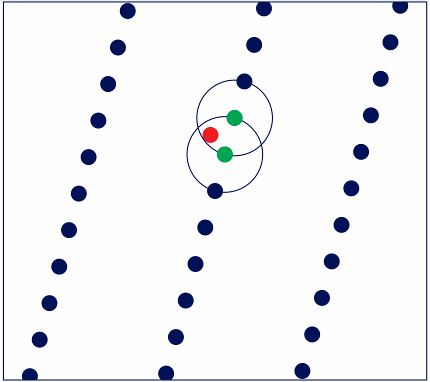
Security Assumption [informal]

1. ..*indistinguishable* from *some* lattice with a *dense* sublattice.

~~2. Decoding in a random lattice is hard.~~



$O \cdot \mathcal{L}_0$



$\mathcal{L}_1$

Arithmetic Invariants

- $\det(\boldsymbol{Q})$.
- $\gcd(\boldsymbol{Q}) := \gcd(\boldsymbol{Q}_{ij})_{i,j}$
- $\gcd\{\|\boldsymbol{x}\|_{\boldsymbol{Q}}^2 : \boldsymbol{x} \in \mathbb{Z}^n\}$
- Self dual? (up to scaling)

Arithmetic Invariants

- $\det(\boldsymbol{Q})$.
- $\gcd(\boldsymbol{Q}) := \gcd(\boldsymbol{Q}_{ij})_{i,j}$
- $\gcd\{\|\boldsymbol{x}\|_{\boldsymbol{Q}}^2 : \boldsymbol{x} \in \mathbb{Z}^n\}$
- Self dual? (up to scaling)
- Equivalence over $\boldsymbol{R} \supset \mathbb{Z}$, $\boldsymbol{U} \in \mathrm{GL}_n(\boldsymbol{R})$, $\boldsymbol{R} \in \{\mathbb{R}, \mathbb{Q}, \forall \boldsymbol{p}\ \mathbb{Q}_{\boldsymbol{p}}, \forall \boldsymbol{p}\ \mathbb{Z}_{\boldsymbol{p}}\}$

Arithmetic Invariants

- $\det(Q)$.
- $\gcd(Q) := \gcd(Q_{ij})_{i,j}$
- $\gcd\{\|x\|_Q^2 : x \in \mathbb{Z}^n\}$
- Self dual? (up to scaling)
- Equivalence over $R \supset \mathbb{Z}$, $U \in \mathrm{GL}_n(R)$, $R \in \{\mathbb{R}, \mathbb{Q}, \forall p\ \mathbb{Q}_p, \forall p\ \mathbb{Z}_p\}$

Definition (Conway Genus)

The Genus of $Q \in \mathcal{S}_n^{>0}(\mathbb{Z})$ represents the $\mathbb{Z}_p$-equivalence classes $[Q]_{\mathbb{Z}_p}$ for $p = 2$ and all primes $p | \det(Q)$.

Arithmetic Invariants

- $\det(Q)$.
- $\gcd(Q) := \gcd(Q_{ij})_{i,j}$
- $\gcd\{\|x\|_Q^2 : x \in \mathbb{Z}^n\}$
- Self dual? (up to scaling)
- Equivalence over $R \supset \mathbb{Z}$, $U \in \mathrm{GL}_n(R)$, $R \in \{\mathbb{R}, \mathbb{Q}, \forall p\ \mathbb{Q}_p, \forall p\ \mathbb{Z}_p\}$

Definition (Conway Genus)

The Genus of $Q \in \mathcal{S}_n^{>0}(\mathbb{Z})$ represents the $\mathbb{Z}_p$-equivalence classes $[Q]_{\mathbb{Z}_p}$ for $p = 2$ and all primes $p | \det(Q)$.

- Covers all above invariants, and is efficiently computable.

Arithmetic Invariants

- $\det(\boldsymbol{Q})$.
- $\gcd(\boldsymbol{Q}) := \gcd(\boldsymbol{Q}_{ij})_{i,j}$
- $\gcd\{\|\boldsymbol{x}\|_{\boldsymbol{Q}}^2 : \boldsymbol{x} \in \mathbb{Z}^n\}$
- Self dual? (up to scaling)
- Equivalence over $\boldsymbol{R} \supset \mathbb{Z}$, $\boldsymbol{U} \in \mathrm{GL}_n(\boldsymbol{R})$, $\boldsymbol{R} \in \{\mathbb{R}, \mathbb{Q}, \forall p\ \mathbb{Q}_p, \forall p\ \mathbb{Z}_p\}$

Definition (Conway Genus)

The Genus of $\boldsymbol{Q} \in \mathcal{S}_n^{>0}(\mathbb{Z})$ represents the $\mathbb{Z}_p$-equivalence classes $[\boldsymbol{Q}]_{\mathbb{Z}_p}$ for $p = 2$ and all primes $p | \det(\boldsymbol{Q})$.

- Covers all above invariants, and is efficiently computable.

Genus attack

If $\mathrm{genus}(\boldsymbol{Q}_0) \neq \mathrm{genus}(\boldsymbol{Q}_1)$, then $\Delta\,\mathrm{LIP}^{\boldsymbol{Q}_0,\boldsymbol{Q}_1}$ is easy.

- If the genera match, we have to distinguish by geometric invariants.

SVP Attack

If $\lambda_1(Q_0) \neq \lambda_1(Q_1)$, then $\Delta\,\mathsf{LIP}^{Q_0,Q_1} \leq \mathsf{SVP}$, with Minkowski Gap $\max\{\mathrm{gap}(Q_0), \mathrm{gap}(Q_1)\}$.

- If the genera match, we have to distinguish by geometric invariants.

SVP Attack

If $\lambda_1(Q_0) \neq \lambda_1(Q_1)$, then $\Delta\,\mathsf{LIP}^{Q_0,Q_1} \leq \mathsf{SVP}$, with Minkowski Gap $\max\{\mathrm{gap}(Q_0), \mathrm{gap}(Q_1)\}$.

- Dual LIP: $Q = U^t Q_b U \Leftrightarrow Q^{-1} = U^{-1} Q_b^{-1} U^{-t}$.

- If the genera match, we have to distinguish by geometric invariants.

SVP Attack

If $\lambda_1(Q_0) \neq \lambda_1(Q_1)$, then $\Delta\,\mathsf{LIP}^{Q_0,Q_1} \leq \mathsf{SVP}$, with Minkowski Gap $\max\{\mathrm{gap}(Q_0), \mathrm{gap}(Q_1)\}$.

- Dual LIP: $Q = U^t Q_b U \Leftrightarrow Q^{-1} = U^{-1} Q_b^{-1} U^{-t}$.

Dual SVP Attack

If $\lambda_1(Q_0^{-1}) \neq \lambda_1(Q_1^{-1})$, then $\Delta\,\mathsf{LIP}^{Q_0,Q_1} \leq \mathsf{SVP}$, with Minkowski Gap $\max\{\mathrm{gap}(Q_0^{-1}), \mathrm{gap}(Q_1^{-1})\}$.

- If the genera match, we have to distinguish by geometric invariants.

SVP Attack

If $\lambda_1(Q_0) \neq \lambda_1(Q_1)$, then $\Delta\,\mathsf{LIP}^{Q_0,Q_1} \leq \mathsf{SVP}$,
with Minkowski Gap $\max\{\mathrm{gap}(Q_0), \mathrm{gap}(Q_1)\}$.

- Dual LIP: $Q = U^t Q_b U \Leftrightarrow Q^{-1} = U^{-1} Q_b^{-1} U^{-t}$.

Dual SVP Attack

If $\lambda_1(Q_0^{-1}) \neq \lambda_1(Q_1^{-1})$, then $\Delta\,\mathsf{LIP}^{Q_0,Q_1} \leq \mathsf{SVP}$,
with Minkowski Gap $\max\{\mathrm{gap}(Q_0^{-1}), \mathrm{gap}(Q_1^{-1})\}$.

- Dense sublattice attack? (overstretched NTRU)

- If the genera match, we have to distinguish by geometric invariants.

SVP Attack

If $\lambda_1(Q_0) \neq \lambda_1(Q_1)$, then $\Delta\,\mathsf{LIP}^{Q_0,Q_1} \leq \mathsf{SVP}$, with Minkowski Gap $\max\{\mathrm{gap}(Q_0), \mathrm{gap}(Q_1)\}$.

- Dual LIP: $Q = U^t Q_b U \Leftrightarrow Q^{-1} = U^{-1} Q_b^{-1} U^{-t}$.

Dual SVP Attack

If $\lambda_1(Q_0^{-1}) \neq \lambda_1(Q_1^{-1})$, then $\Delta\,\mathsf{LIP}^{Q_0,Q_1} \leq \mathsf{SVP}$, with Minkowski Gap $\max\{\mathrm{gap}(Q_0^{-1}), \mathrm{gap}(Q_1^{-1})\}$.

- Dense sublattice attack? (overstretched NTRU)

Open Question

Are there better attacks when the genera match?

Instantiating (simple)

Theorem [informal]

Let $\mathcal{L}_0$ be a decodable lattice, and let $\mathcal{L}_1$ be a lattice with a dense sublattice, then our scheme is CPA-secure if $\Delta\,\mathsf{LIP}^{Q_0,Q_1}$ is hard.

Instantiating (simple)

Theorem [informal]

Let $\mathcal{L}_0$ be a decodable lattice, and let $\mathcal{L}_1$ be a lattice with a dense sublattice, then our scheme is CPA-secure if $\Delta\,\mathsf{LIP}^{Q_0,Q_1}$ is hard.

- Let $\mathcal{L} \subset \mathbb{R}^{n/2}$ be a ρ-decodable lattice with integral gram matrix.
- For some $g \in \mathbb{Z}_{\geq 1}$ we define

$$\mathcal{L}_0 := g\mathcal{L} \oplus (g+1)\mathcal{L} \qquad \& \qquad \mathcal{L}_1 := \mathcal{L} \oplus g(g+1)\mathcal{L}.$$

Instantiating (simple)

Theorem [informal]

Let $\mathcal{L}_0$ be a decodable lattice, and let $\mathcal{L}_1$ be a lattice with a dense sublattice, then our scheme is CPA-secure if $\Delta\,\mathsf{LIP}^{Q_0,Q_1}$ is hard.

- Let $\mathcal{L} \subset \mathbb{R}^{n/2}$ be a ρ-decodable lattice with integral gram matrix.
- For some $g \in \mathbb{Z}_{\geq 1}$ we define

$$\mathcal{L}_0 := g\mathcal{L} \oplus (g+1)\mathcal{L} \qquad \& \qquad \mathcal{L}_1 := \mathcal{L} \oplus g(g+1)\mathcal{L}.$$

- Dense sublattice $\mathcal{L} \subset \mathcal{L}_1$ (set $g = \Theta\left(\mathsf{gap}(\mathcal{L}^*) \cdot \mathsf{gap}(\mathcal{L}, \rho)\right)$).

Theorem [informal]

Let $\mathcal{L}_0$ be a decodable lattice, and let $\mathcal{L}_1$ be a lattice with a dense sublattice, then our scheme is CPA-secure if $\Delta\,\mathsf{LIP}^{Q_0,Q_1}$ is hard.

- Let $\mathcal{L} \subset \mathbb{R}^{n/2}$ be a ρ-decodable lattice with integral gram matrix.
- For some $g \in \mathbb{Z}_{\geq 1}$ we define

$$\mathcal{L}_0 := g\mathcal{L} \oplus (g+1)\mathcal{L} \qquad \& \qquad \mathcal{L}_1 := \mathcal{L} \oplus g(g+1)\mathcal{L}.$$

- Dense sublattice $\mathcal{L} \subset \mathcal{L}_1$ (set $g = \Theta\left(\mathrm{gap}(\mathcal{L}^*) \cdot \mathrm{gap}(\mathcal{L}, \rho)\right)$).

Cryptanalysis

Invariants: $\mathrm{genus}(\mathcal{L}_0) = \mathrm{genus}(\mathcal{L}_1)$.

SVP: if $\mathrm{gap}(\mathcal{L}) \leq f$, $\mathrm{gap}(\mathcal{L}^*) \leq f^*$ and $\mathrm{gap}(\mathcal{L}, \rho) \leq f'$, then

$$\max\{\mathrm{gap}(\mathcal{L}_0), \mathrm{gap}(\mathcal{L}_0^*), \mathrm{gap}(\mathcal{L}_1), \mathrm{gap}(\mathcal{L}_1^*)\} \leq O(\max(f, f^*) \cdot f^* \cdot f')$$

Decodable Lattices

Lattice	$f := \mathrm{gap}(\mathcal{L})$	$f^* := \mathrm{gap}(\mathcal{L}^*)$	$f' := \mathrm{gap}(\mathcal{L}, \rho)$
$\mathbb{Z}^n$	$\Theta(\sqrt{n})$	$\Theta(\sqrt{n})$	$\Theta(\sqrt{n})$
'Random' Lattice	$\Theta(1)$	$\Theta(1)$	$2^{\Theta(n)}$
NTRU, LWE, ⋯	$\Theta(1)$	$\Theta(1)$	$\Omega(\sqrt{n})$
Prime Lattice	$\Theta(\log n)$	$\Omega(\sqrt{n})$	$\Theta(\log n)$ [CR88, DP19]
Barnes-Sloane	$\Theta(\sqrt{\log n})$	$\Omega(\sqrt{n})$	$\Theta(\sqrt{\log n})$ [MP20]
Reed-Solomon	$\Theta(\sqrt{\log n})$	$\Omega(\sqrt{n})$	$\Theta(\sqrt{\log n})$ [BP22]
Barnes-Wall	$\Theta(\sqrt[4]{n})$	$\Theta(\sqrt[4]{n})$	$\Theta(\sqrt[4]{n})$ [MN08]

Decodable Lattices

Lattice	$f := \mathrm{gap}(\mathcal{L})$	$f^* := \mathrm{gap}(\mathcal{L}^*)$	$f' := \mathrm{gap}(\mathcal{L}, \rho)$
$\mathbb{Z}^n$	$\Theta(\sqrt{n})$	$\Theta(\sqrt{n})$	$\Theta(\sqrt{n})$
'Random' Lattice	$\Theta(1)$	$\Theta(1)$	$2^{\Theta(n)}$
NTRU, LWE, ...	$\Theta(1)$	$\Theta(1)$	$\Omega(\sqrt{n})$
Prime Lattice	$\Theta(\log n)$	$\Omega(\sqrt{n})$	$\Theta(\log n)$ [CR88, DP19]
Barnes-Sloane	$\Theta(\sqrt{\log n})$	$\Omega(\sqrt{n})$	$\Theta(\sqrt{\log n})$ [MP20]
Reed-Solomon	$\Theta(\sqrt{\log n})$	$\Omega(\sqrt{n})$	$\Theta(\sqrt{\log n})$ [BP22]
Barnes-Wall	$\Theta(\sqrt[4]{n})$	$\Theta(\sqrt[4]{n})$	$\Theta(\sqrt[4]{n})$ [MN08]

Open Question

Can we construct a decodable lattice with $\max\{f, f^*, f'\} \leq \mathrm{polylog}(n)$?

Future work

Remarkable Lattices

Can we construct a decodable lattice with $\max\{f, f^*, f'\} \leq \text{polylog}(n)$?

LIP to Δ LIP?

Can we reduce the search version of LIP to the distinguishing version? (for $\mathbb{Z}^n$ we can [Szydlo03])

Genus Sampling

Can we sample 'random' $[Q']$ such that $\text{genus}(Q') = \text{genus}(Q)$. Is $[Q']$ expected to have a good geometry? Is decoding in $[Q']$ hard?

Module-LIP

LIP is easy for some Ideal lattices [Gentry-Szydlo, Lenstra-Silverberg]. Is rank $k \geq 2$ module-LIP secure?

Thank you! :)

Full paper at eprint.iacr.org/2021/1332