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

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

Centrum Wiskunde & Informatica

# Motivation

- LWE, SIS, NTRU lattices: versatile, but poor decoding.

# Motivation

- LWE, SIS, NTRU lattices: versatile, but poor decoding.
- Many wonderful lattices exist with great geometric properties.

# Motivation

- LWE, SIS, NTRU lattices: versatile, but poor decoding.
- Many wonderful lattices exist with great geometric properties.
- Can we use these in cryptography?

- LWE, SIS, NTRU lattices: versatile, but poor decoding.
- Many wonderful lattices exist with great geometric properties.
- Can we use these in cryptography?

## Contributions

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

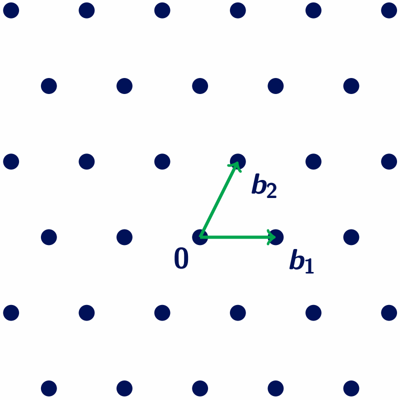
# Motivation

- LWE, SIS, NTRU lattices: versatile, but poor decoding.
- Many wonderful lattices exist with great geometric properties.
- Can we use these in cryptography?

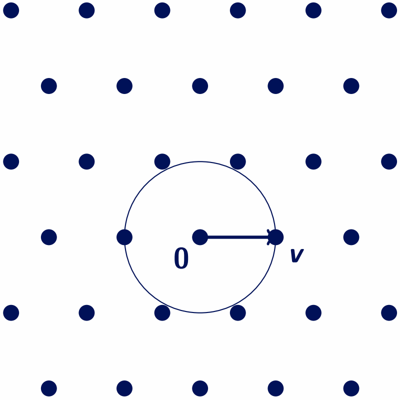
## Contributions

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

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



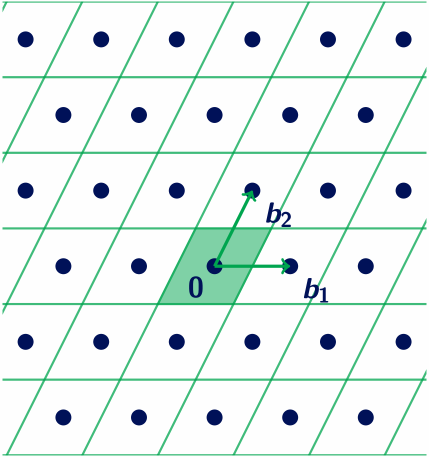
Lattice $\mathcal{L}(B) := \{\sum_i x_i b_i : x \in \mathbb{Z}^n\} \subset \mathbb{R}^n$




First minimum

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

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



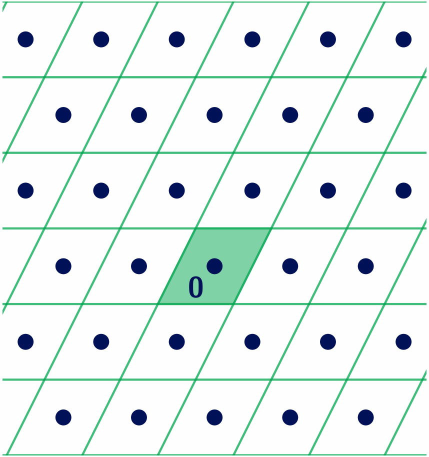

First minimum

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

Determinant

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

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




First minimum

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

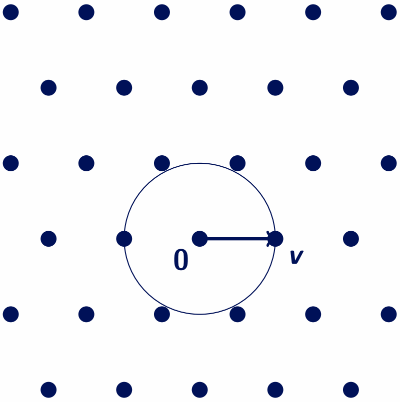
Determinant

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

Minkowski's Theorem

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

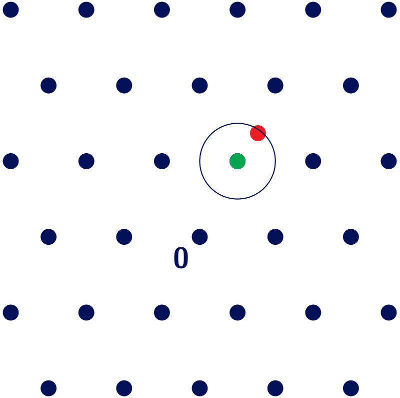
Lattice $\mathcal{L} \subset \mathbb{R}^n$




**SVP**

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

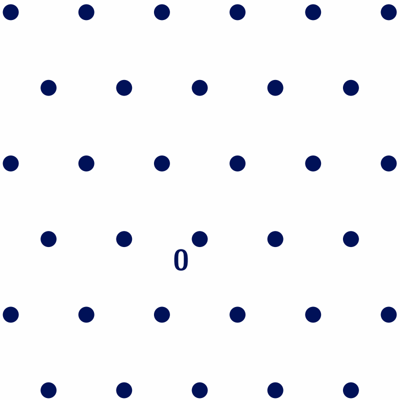
BDD

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 $\boldsymbol{v} \in \mathcal{L}$.

# Hard Problems

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




**SVP**

Find a *shortest* nonzero vector $v \in \mathcal{L}$ of length $\underbrace{\lambda_1(\mathcal{L}) \leq \mathrm{Mk}(\mathcal{L})}_{\mathrm{gap}(\mathcal{L})}$.

**BDD**

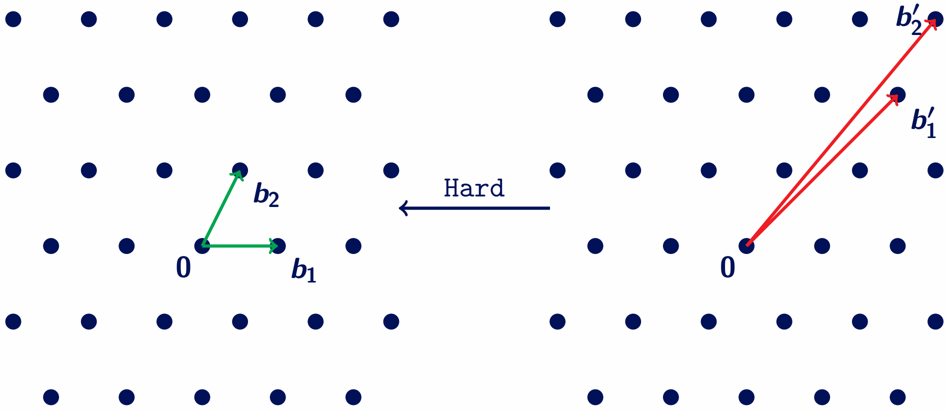
Given a target $t = v + e \in \mathbb{R}^n$ with $v \in \mathcal{L}$ and $\|e\| < \underbrace{\rho \leq \frac{1}{2}\lambda_1(\mathcal{L}) \leq \frac{1}{2}\mathrm{Mk}(\mathcal{L})}_{\mathrm{gap}(\mathcal{L},\rho)}$, recover $v \in \mathcal{L}$.

Hardness depends on the *gaps*!

# Encryption, legacy approach

Good basis (Secret key)

Bad basis (Public key)

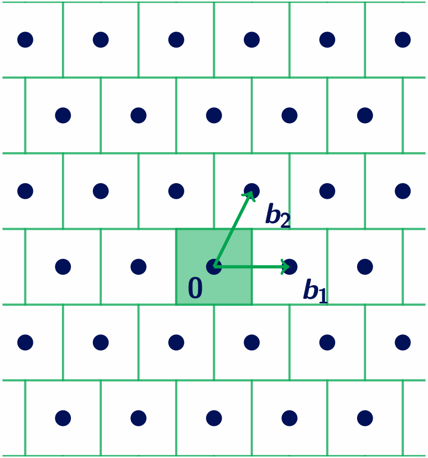



$B$

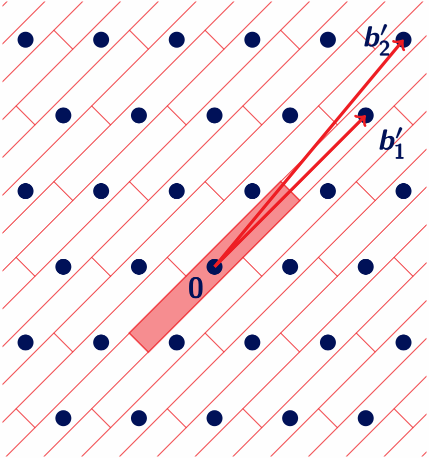
$B' = B \cdot U, \; U \in \mathrm{GL}_d(\mathbb{Z})$

# Encryption, legacy approach

Good basis (Secret key)

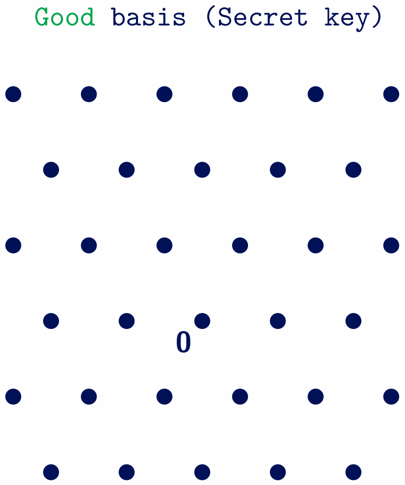


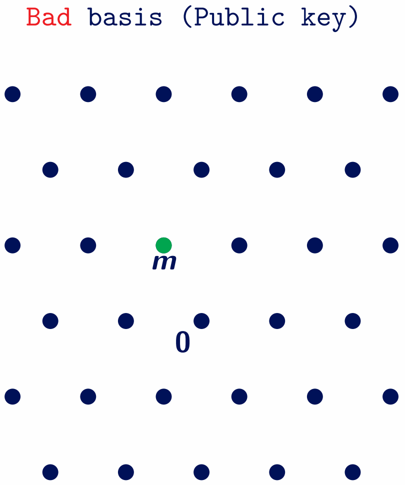

Bad basis (Public key)




Babai's nearest plane algorithm

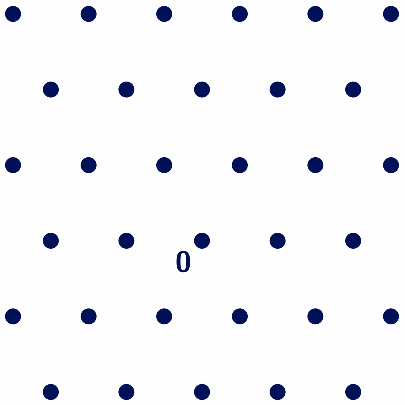
# Encryption, legacy approach



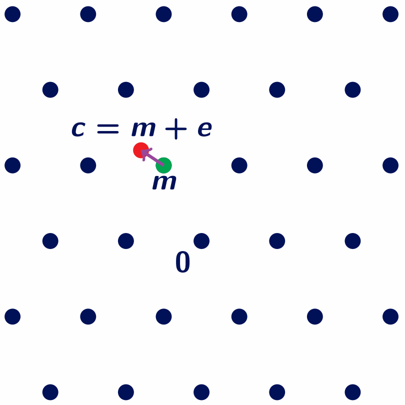



# Encryption, legacy approach

Good basis (Secret key)

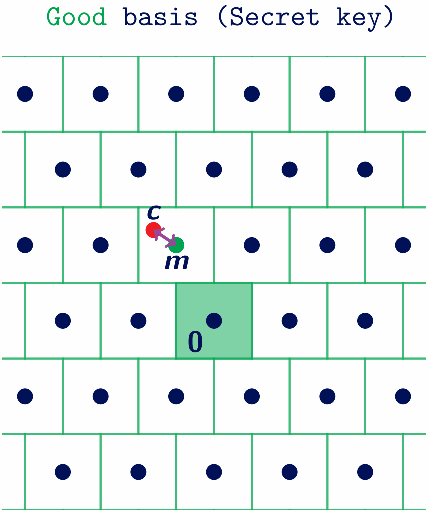


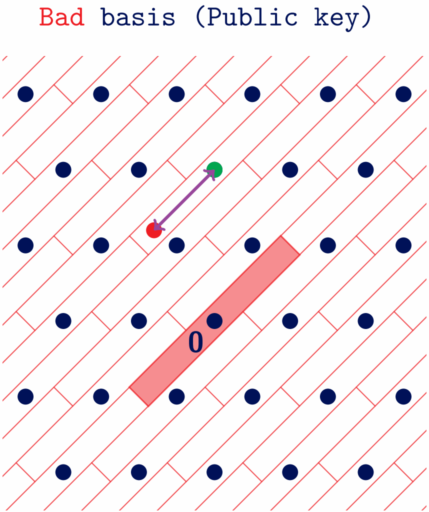

Bad basis (Public key)




Encrypt by adding a small error

# Encryption, legacy approach




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 $\beta \leq n/2 + o(n)$, e.g.
$n = 1024 \implies \beta \approx 450$.

## 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 $\beta \leq n/2 + o(n)$, e.g. $n = 1024 \implies \beta \approx 450$.

## An example: Prime Lattice [CR88]

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

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

### 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 $\beta \leq n/2 + o(n)$, e.g. $n = 1024 \implies \beta \approx 450$.

### 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 $\rho$ by trial division.

# Remarkable Lattices

### 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 $\beta \leq n/2 + o(n)$, e.g. $n = 1024 \implies \beta \approx 450$.

### An example: Prime Lattice [CR88]

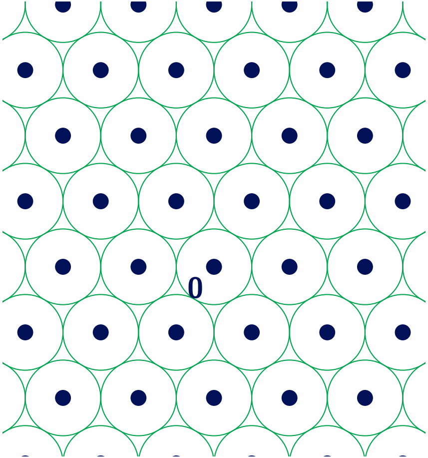
Let $p_1, \ldots, p_n$ be distinct small primes not dividing $m$, we define:

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

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

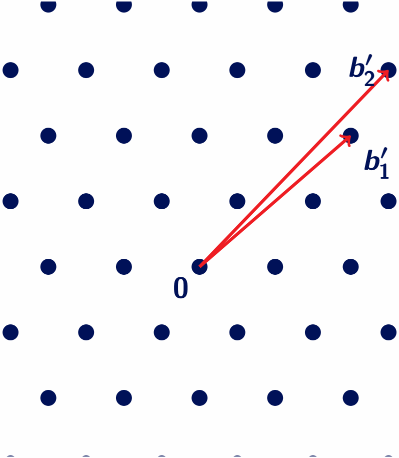
# How to hide the remarkable lattice?

Good lattice (~~Secret key~~)




$\mathcal{L}$

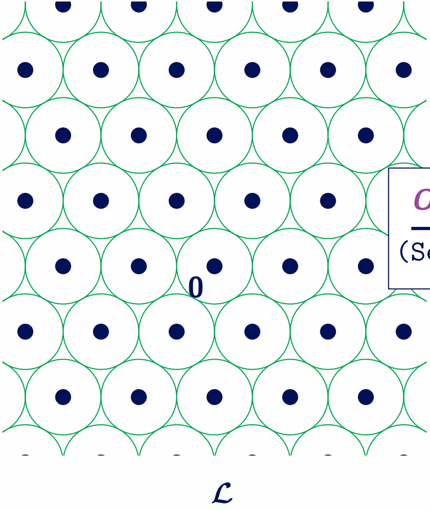
Bad basis (Public key)



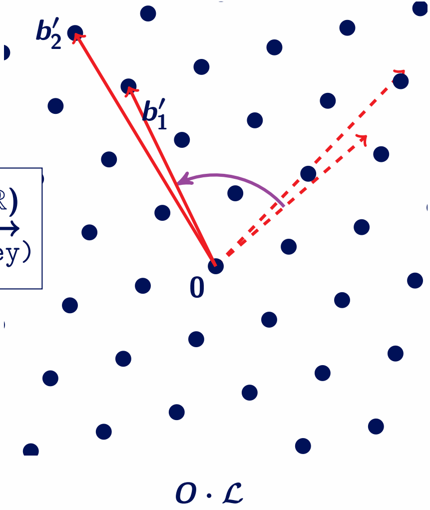

$\mathcal{L}$

# How to hide the remarkable lattice?

Good lattice (~~Secret key~~) Bad basis (Public key)

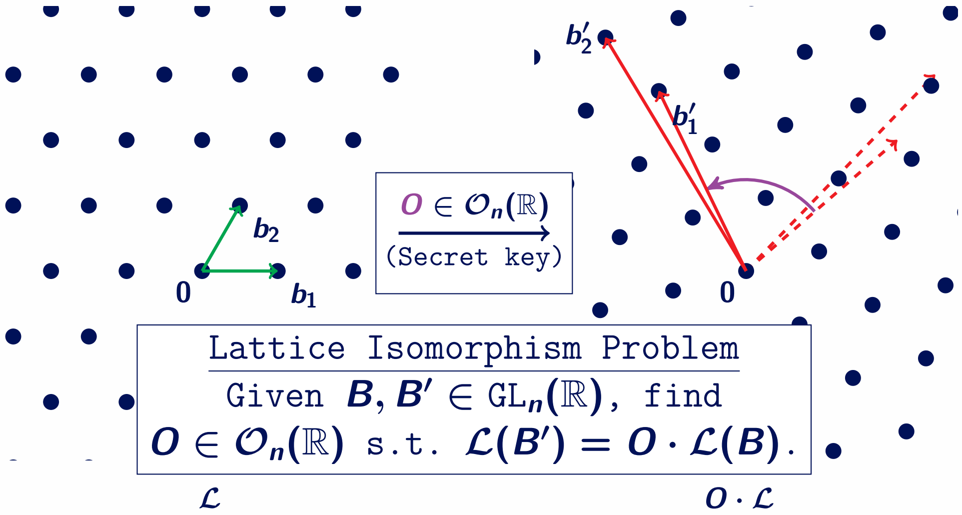






# How to hide the remarkable lattice?

Good lattice (~~Secret key~~) Bad basis (Public key)



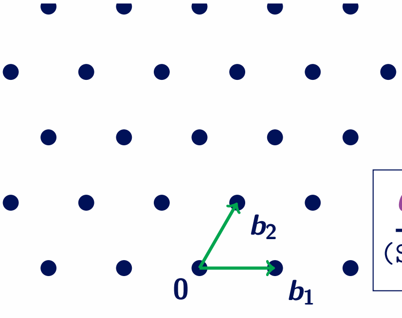

**Lattice Isomorphism Problem**

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

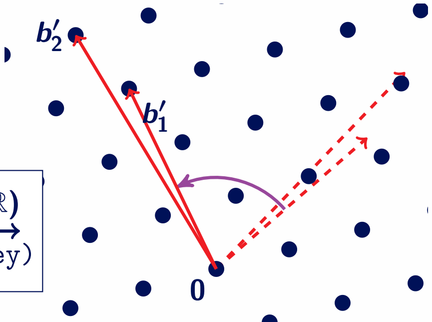
# How to hide the remarkable lattice?

Good lattice (~~Secret key~~)

Bad basis (Public key)




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




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

$B$

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

# Lattice Isomorphism Problem

**LIP**

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

**LIP**

Given $\boldsymbol{B}, \boldsymbol{B}' \in \mathrm{GL}_n(\mathbb{R})$ of isomorphic lattices, 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 $\boldsymbol{G}' = \boldsymbol{P} \cdot \boldsymbol{G} \cdot \boldsymbol{S}$,
- and Oil and Vinegar $\mathcal{P} = \mathcal{Q} \circ \mathcal{S}$.

# Lattice Isomorphism Problem

**LIP**

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

- The lattice analogue of 'vintage' McEliece $G' = P \cdot G \cdot S$,
- and Oil and Vinegar $\mathcal{P} = \mathcal{Q} \circ \mathcal{S}$.
- Best known attacks require to solve SVP.

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

$$\boldsymbol{B}' = \boldsymbol{O} \cdot \boldsymbol{B} \cdot \boldsymbol{U}.$$

Sidestep real values!

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

Sample $\boldsymbol{U} \in \mathrm{GL}_{\boldsymbol{n}}(\mathbb{Z})$ s.t.
$\boldsymbol{B}'$ is independent of $\boldsymbol{B}$.

$$\boldsymbol{B}' = \boldsymbol{O} \cdot \boldsymbol{B} \cdot \boldsymbol{U}.$$

Sidestep real values!
$\boldsymbol{O} \in \mathcal{O}_{\boldsymbol{n}}(\mathbb{R})$

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

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

$$(B')^t B' = U^t B^t O^t O B U = U^t B^t B U\,.$$

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

$$(B')^t B' = U^t B^t O^t O B U = U^t B^t B U.$$

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

Lattices $\Longrightarrow$ Quadratic Forms

*Keep the geometry, forget the embedding.*

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

$$(B')^t B' = U^t B^t O^t O B U = U^t B^t B U .$$

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

Lattices $\implies$ Quadratic Forms

*Keep the geometry, forget the embedding.*

LIP restated:

Find $U \in \mathrm{GL}_n(\mathbb{Z})$ s.t. $Q' = U^t Q U .$

# An average-case distribution

Unimodular $\boldsymbol{U} \in \mathrm{GL}_{\boldsymbol{n}}(\mathbb{Z})$

Unimodular $U \in \mathrm{GL}_n(\mathbb{Z})$

Equivalence class $[Q] := \{U^t Q U : U \in \mathrm{GL}_n(\mathbb{Z})\}$.

Def: Distribution $\mathcal{D}_\sigma([Q])$ over $[Q]$,

Unimodular $U \in \mathrm{GL}_n(\mathbb{Z})$

Equivalence class $[Q] := \{U^t Q U : U \in \mathrm{GL}_n(\mathbb{Z})\}$.

Def: Distribution $\mathcal{D}_\sigma([Q])$ over $[Q]$,

\+ Efficient sampler $(Q', U) \leftarrow \mathrm{Sample}_\sigma(Q)$
s.t. $Q' \sim \mathcal{D}_\sigma([Q])$ and $Q' = U^t Q U$.

*$Q'$ only depends on the class $[Q]$ and not on $Q$ itself.*

# An average-case distribution

Unimodular $U \in \mathrm{GL}_n(\mathbb{Z})$

Equivalence class $[Q] := \{U^t Q U : U \in \mathrm{GL}_n(\mathbb{Z})\}$.

Def: Distribution $\mathcal{D}_\sigma([Q])$ over $[Q]$,

+ Efficient sampler $(Q', U) \leftarrow \mathrm{Sample}_\sigma(Q)$ s.t. $Q' \sim \mathcal{D}_\sigma([Q])$ and $Q' = U^t Q U$.

*$Q'$ only depends on the class $[Q]$ and not on $Q$ itself.*

$\implies$ average-case LIP, ZKPoK and identification scheme.

Unimodular $U \in \mathrm{GL}_n(\mathbb{Z})$

Equivalence class $[Q] := \{U^t Q U : U \in \mathrm{GL}_n(\mathbb{Z})\}$.

Def: Distribution $\mathcal{D}_\sigma([Q])$ over $[Q]$,

\+ Efficient sampler $(Q', U) \leftarrow \mathrm{Sample}_\sigma(Q)$
s.t. $Q' \sim \mathcal{D}_\sigma([Q])$ and $Q' = U^t Q U$.

*$Q'$ only depends on the class $[Q]$ and not on $Q$ itself.*

$\Longrightarrow$ average-case LIP, ZKPoK and identification scheme.

$\Longrightarrow$ Worst-case to average-case reduction over $[Q]$.

Decodable lattice $\mathcal{L}$ $\Longrightarrow$ Encryption scheme.

Best known: generic lattice reduction.

Decodable lattice $\mathcal{L} \implies$ Encryption scheme.

Best known: generic lattice reduction.

SVP attack: $\mathbf{gap}(\mathcal{L})$.

Decodable lattice $\mathcal{L}$ $\implies$ Encryption scheme.

Best known: generic lattice reduction.

SVP attack: $\mathbf{gap}(\mathcal{L})$.

Dual SVP attack: $\mathbf{gap}(\mathcal{L}^*)$.

Decodable lattice $\mathcal{L}$ $\implies$ Encryption scheme.

Best known: generic lattice reduction.

SVP attack: $\mathbf{gap}(\mathcal{L})$.

Dual SVP attack: $\mathbf{gap}(\mathcal{L}^*)$.

Decoding attack (BDD): $\mathbf{gap}(\mathcal{L}, \rho)$.

# Decodable Lattices

| Lattice | gap($\mathcal{L}$) | gap($\mathcal{L}^*$) | gap($\mathcal{L}, \rho$) |
|---|---|---|---|
| 'Random' Lattice | $\Theta(1)$ | $\Theta(1)$ | $2^{\Theta(n)}$ |
| 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] |
| $\mathbb{Z}^n$ | $\Theta(\sqrt{n})$ | $\Theta(\sqrt{n})$ | $\Theta(\sqrt{n})$ |
| NTRU, LWE | $\Omega(1)\ldots O(\sqrt{n})$ | $\Omega(1)$ | $\Omega(\sqrt{n})$ |
| Barnes-Wall | $\Theta(\sqrt[4]{n})$ | $\Theta(\sqrt[4]{n})$ | $\Theta(\sqrt[4]{n})$ [MN08] |

# Decodable Lattices

| Lattice | $\mathrm{gap}(\mathcal{L})$ | $\mathrm{gap}(\mathcal{L}^*)$ | $\mathrm{gap}(\mathcal{L}, \rho)$ |
|---|---|---|---|
| 'Random' Lattice | $\Theta(1)$ | $\Theta(1)$ | $2^{\Theta(n)}$ |
| 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] |
| $\mathbb{Z}^n$ | $\Theta(\sqrt{n})$ | $\Theta(\sqrt{n})$ | $\Theta(\sqrt{n})$ |
| NTRU, LWE | $\Omega(1) \ldots O(\sqrt{n})$ | $\Omega(1)$ | $\Omega(\sqrt{n})$ |
| Barnes-Wall | $\Theta(\sqrt[4]{n})$ | $\Theta(\sqrt[4]{n})$ | $\Theta(\sqrt[4]{n})$ [MN08] |

# Decodable Lattices

| Lattice | $\mathrm{gap}(\mathcal{L})$ | $\mathrm{gap}(\mathcal{L}^*)$ | $\mathrm{gap}(\mathcal{L}, \rho)$ |
|---|---|---|---|
| 'Random' Lattice | $\Theta(1)$ | $\Theta(1)$ | $2^{\Theta(n)}$ |
| 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] |
| $\mathbb{Z}^n$ | $\Theta(\sqrt{n})$ | $\Theta(\sqrt{n})$ | $\Theta(\sqrt{n})$ |
| NTRU, LWE | $\Omega(1) \dots O(\sqrt{n})$ | $\Omega(1)$ | $\Omega(\sqrt{n})$ |
| Barnes-Wall | $\Theta(\sqrt[4]{n})$ | $\Theta(\sqrt[4]{n})$ | $\Theta(\sqrt[4]{n})$ [MN08] |

# Decodable Lattices

| Lattice | $\mathsf{gap}(\mathcal{L})$ | $\mathsf{gap}(\mathcal{L}^*)$ | $\mathsf{gap}(\mathcal{L}, \rho)$ |
|---|---|---|---|
| 'Random' Lattice | $\Theta(1)$ | $\Theta(1)$ | $2^{\Theta(n)}$ |
| 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] |
| $\mathbb{Z}^n$ | $\Theta(\sqrt{n})$ | $\Theta(\sqrt{n})$ | $\Theta(\sqrt{n})$ |
| NTRU, LWE | $\Omega(1) \ldots O(\sqrt{n})$ | $\Omega(1)$ | $\Omega(\sqrt{n})$ |
| Barnes-Wall | $\Theta(\sqrt[4]{n})$ | $\Theta(\sqrt[4]{n})$ | $\Theta(\sqrt[4]{n})$ [MN08] |

# Interesting cases

Decodable lattice $\mathcal{L} \implies$ Encryption scheme.

# Interesting cases

Decodable lattice $\mathcal{L}$ $\implies$ Encryption scheme.

$\mathbb{Z}^n$: similar geometry to NTRU, LWE,
but extremely simple and efficient.

$$n = 1024 \implies \beta \approx 440$$

Decodable lattice $\mathcal{L} \implies$ Encryption scheme.

$\mathbb{Z}^n$: similar geometry to NTRU, LWE,
but extremely simple and efficient.

$$n = 1024 \implies \beta \approx 440$$

$BW^n$: better geometry and decoding $O(\sqrt[4]{n})$,

$$n = 1024 \implies \beta \approx 780.$$

Decodable lattice $\mathcal{L} \implies$ Encryption scheme.

$\mathbb{Z}^n$: similar geometry to NTRU, LWE,
but extremely simple and efficient.

$$n = 1024 \implies \beta \approx 440$$

$BW^n$: better geometry and decoding $O(\sqrt[4]{n})$,

$$n = 1024 \implies \beta \approx 780.$$

?: gaps $\leq$ poly-log$(n)$,

$$\beta \approx n.$$

# Conclusion

Any lattice $\implies$ Identification scheme.

Decodable lattice $\mathcal{L}$ $\implies$ Encryption scheme.

Gaussian sampleable lattice $\mathcal{L}$ $\implies$ Signature scheme.

# Conclusion

Any lattice $\implies$ Identification scheme.

Decodable lattice $\mathcal{L}$ $\implies$ Encryption scheme.

Gaussian sampleable lattice $\mathcal{L}$ $\implies$ Signature scheme.

$\mathbb{Z}^n$ seems enough to match security of LWE and NTRU.

# Conclusion

Any lattice $\implies$ Identification scheme.

Decodable lattice $\mathcal{L}$ $\implies$ Encryption scheme.

Gaussian sampleable lattice $\mathcal{L}$ $\implies$ Signature scheme.

$\mathbb{Z}^n$ seems enough to match security of LWE and NTRU.

End goal: do even better.

# Conclusion

Any lattice $\implies$ Identification scheme.

Decodable lattice $\mathcal{L}$ $\implies$ Encryption scheme.

Gaussian sampleable lattice $\mathcal{L}$ $\implies$ Signature scheme.

$\mathbb{Z}^n$ seems enough to match
security of LWE and NTRU.

End goal: do even better.

Thanks! :)