

# 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?

# 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.

# Motivation

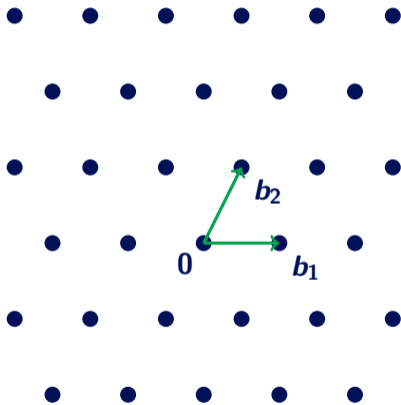
- LWE, SIS, NTRU lattices: `versatile`, but `poor decoding`.
- Many wonderful lattices exist with great geometric properties.
- Can we use these in cryptography?

## Contributions

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

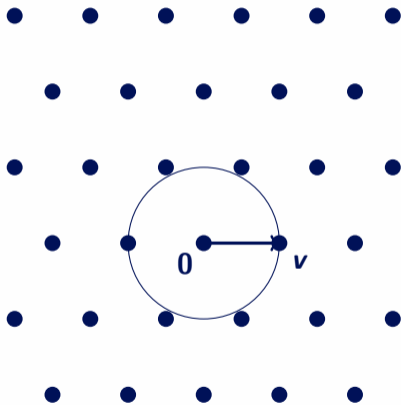
# Lattices

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



# Lattices

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

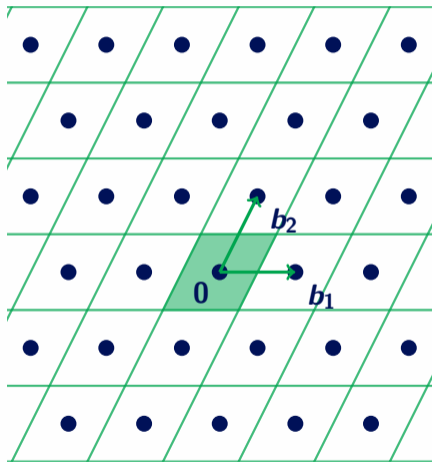


First minimum  
 $\lambda_1(\mathcal{L}) := \min_{x \in \mathcal{L} \setminus \{0\}} \|x\|_2$



# Lattices

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



First minimum

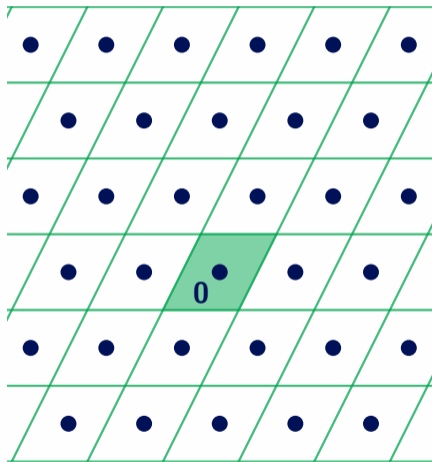
$$\lambda_1(\mathcal{L}) := \min_{x \in \mathcal{L} \setminus \{0\}} \|x\|_2$$

Determinant

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

# Lattices

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

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

Minkowski's Theorem

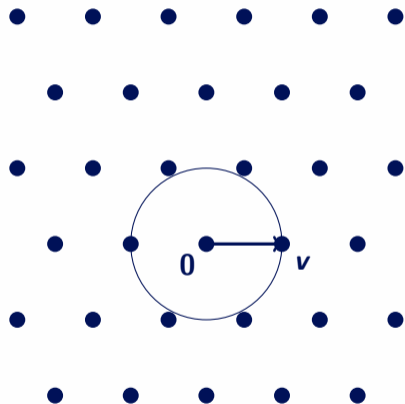
$$\lambda_1(\mathcal{L}) \leq 2 \underbrace{\frac{\det(\mathcal{L})^{1/n}}{\text{vol}(\mathcal{B}^n)^{1/n}}}_{\text{Mk}(\mathcal{L})} \leq \sqrt{n} \det(\mathcal{L})^{1/n}$$

# Hard Problems

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

SVP

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



# Hard Problems

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

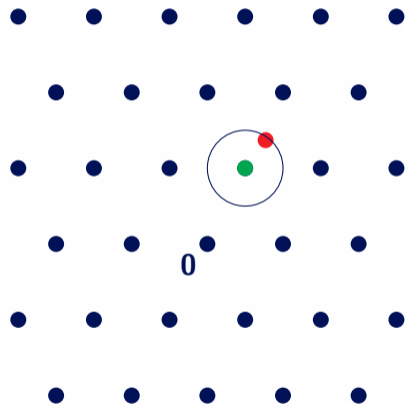
SVP

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

BDD

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

recover  $\mathbf{v} \in \mathcal{L}$ .



# Hard Problems

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

SVP

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

BDD

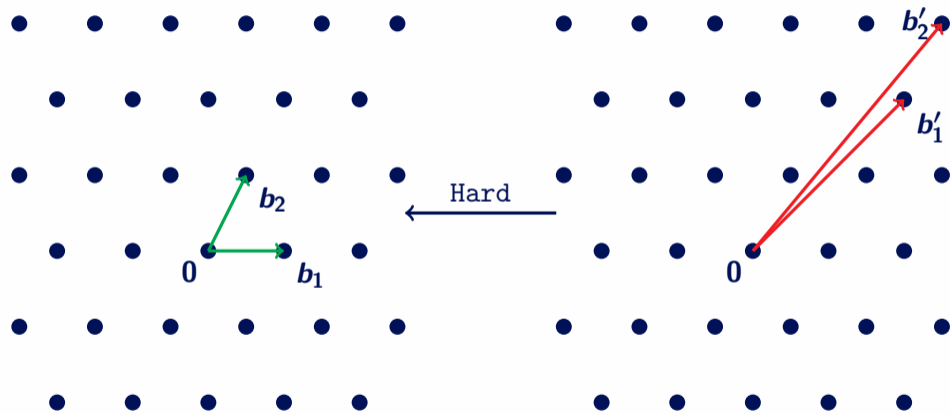
Given a target  $\mathbf{t} = \mathbf{v} + \mathbf{e} \in \mathbb{R}^n$  with  $\mathbf{v} \in \mathcal{L}$  and  $\|\mathbf{e}\| < \rho \leq \underbrace{\frac{1}{2}\lambda_1(\mathcal{L}) \leq \frac{1}{2}\text{Mk}(\mathcal{L})}_{\text{gap}(\mathcal{L}, \rho)}$ ,  
recover  $\mathbf{v} \in \mathcal{L}$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

Hardness depends on the *gaps*!

# Encryption, legacy approach

Good basis (Secret key)

Bad basis (Public key)

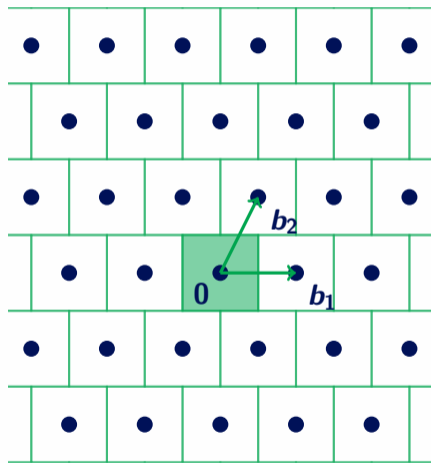


$B$

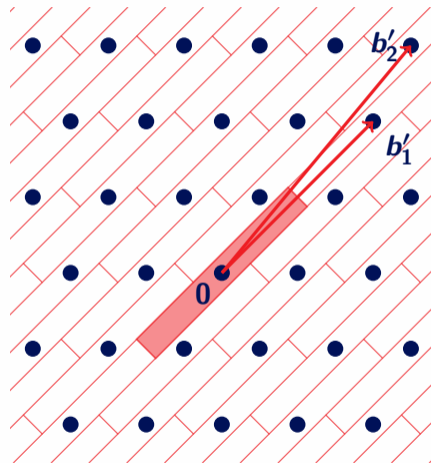
$$B' = B \cdot U, \quad U \in \text{GL}_d(\mathbb{Z})$$

# Encryption, legacy approach

Good basis (Secret key)



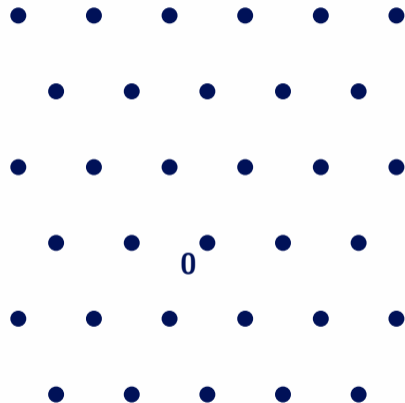
Bad basis (Public key)



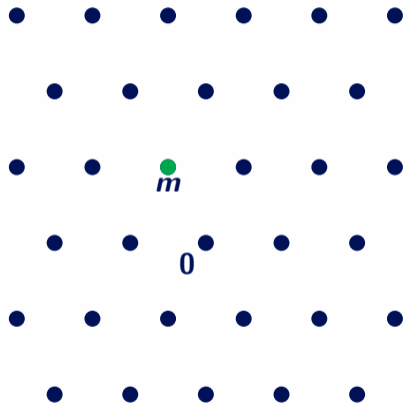
Babai's nearest plane algorithm

# Encryption, legacy approach

Good basis (Secret key)



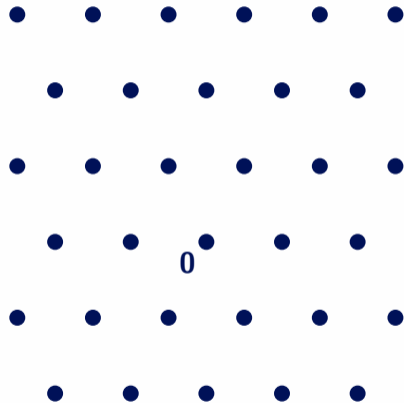
Bad basis (Public key)



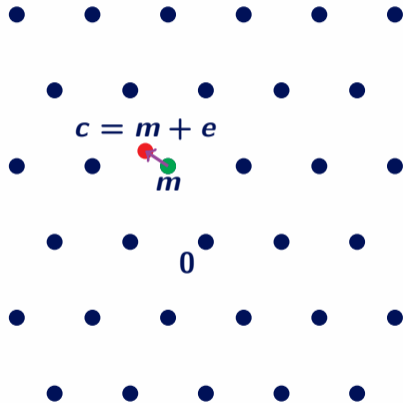


# Encryption, legacy approach

Good basis (Secret key)



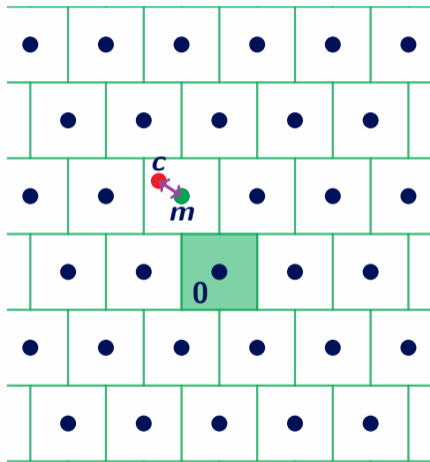
Bad basis (Public key)



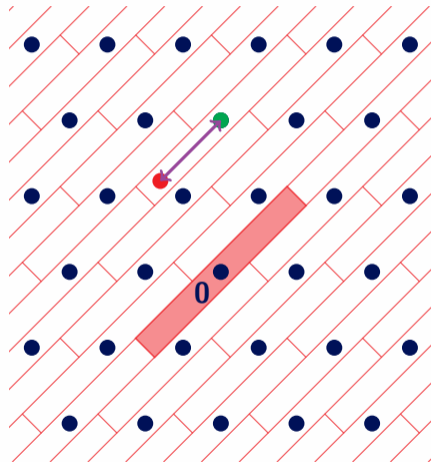
Encrypt by adding a small error

# Encryption, legacy approach

Good basis (Secret key)



Bad basis (Public key)



Decrypt using the good basis

# Remarkable Lattices

## Large gap

Current lattice based crypto relies on hardness of decoding with

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

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

$$n = 1024 \implies \beta \approx 450.$$

# Remarkable Lattices

## Large gap

Current lattice based crypto relies on hardness of decoding with

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

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

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

# Remarkable Lattices

## Large gap

Current lattice based crypto relies on hardness of decoding with

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

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

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

- Efficiently decode up to large radius  $\rho$  by trial division.

# Remarkable Lattices

## Large gap

Current lattice based crypto relies on hardness of decoding with

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

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

$$n = 1024 \implies \beta \approx 450.$$

## An example: Prime Lattice [CR88]

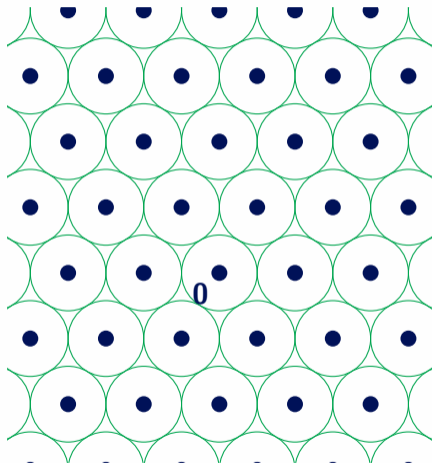
Let  $p_1, \dots, p_n$  be distinct small primes not dividing  $m$ , we define:

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

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

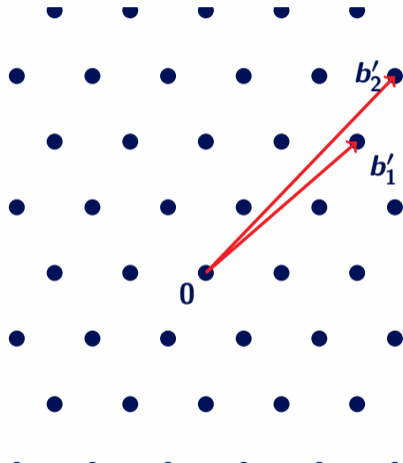
# How to hide the remarkable lattice?

Good lattice (~~Secret~~ key)



$\mathcal{L}$

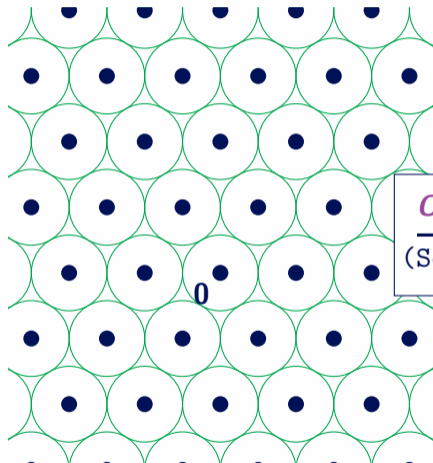
Bad basis (Public key)



$\mathcal{L}$

# How to hide the remarkable lattice?

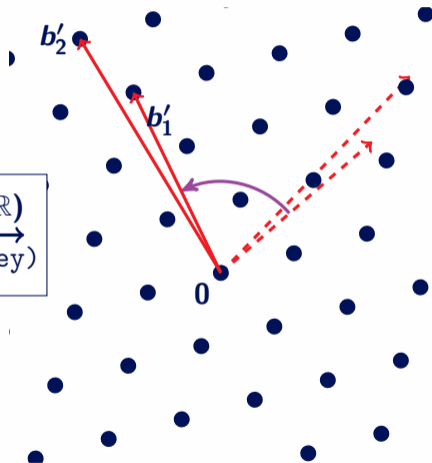
Good lattice (Secret key)



$\mathcal{L}$

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

Bad basis (Public key)



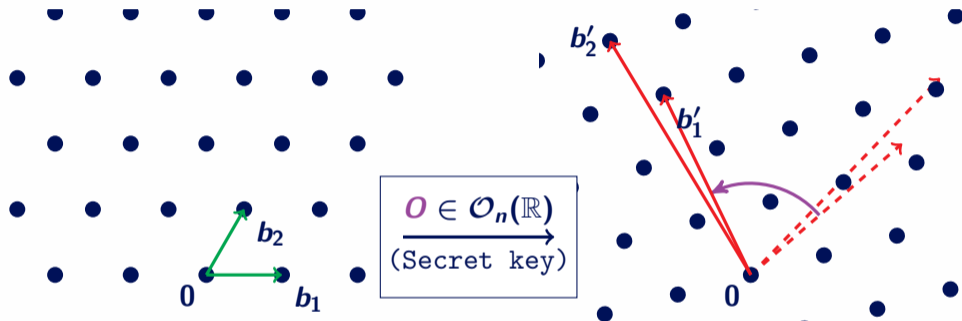
$O \cdot \mathcal{L}$



# How to hide the remarkable lattice?

Good lattice (Secret key)

Bad basis (Public key)



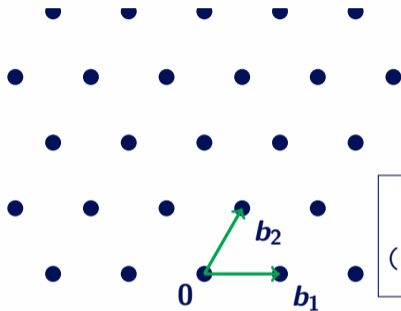
Lattice Isomorphism Problem  
Given  $B, B' \in GL_n(\mathbb{R})$ , find  
 $O \in \mathcal{O}_n(\mathbb{R})$  s.t.  $\mathcal{L}(B') = O \cdot \mathcal{L}(B)$ .

$\mathcal{L}$

$O \cdot \mathcal{L}$

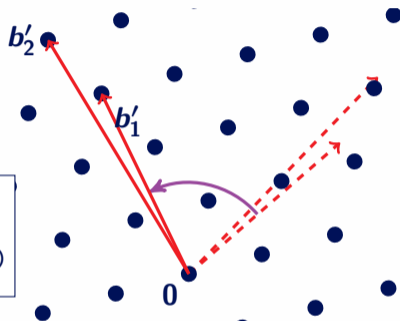
# How to hide the remarkable lattice?

Good lattice (Secret key)



$$\begin{array}{c} \mathcal{O} \in \mathcal{O}_n(\mathbb{R}) \\ \xrightarrow{\text{(Secret key)}} \end{array}$$

Bad basis (Public key)



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

$B$

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

# Lattice Isomorphism Problem

## LIP

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

# Lattice Isomorphism Problem

## LIP

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

- The lattice analogue of 'vintage' McEliece  $G' = P \cdot G \cdot S$ ,
- and Oil and Vinegar  $\mathcal{P} = Q \circ S$ .

# Lattice Isomorphism Problem

## LIP

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

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

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

## Two Challenges

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

Sidestep real values!

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

## Two Challenges

Sample  $U \in \text{GL}_n(\mathbb{Z})$  s.t.  
 $B'$  is independent of  $B$ .

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

Sidestep real values!

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



## Quadratic Forms

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

## Quadratic Forms

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

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

## Quadratic Forms

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.*

## Quadratic Forms

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

# An average-case distribution

Unimodular  $U \in GL_n(\mathbb{Z})$

## An average-case distribution

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

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

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

## An average-case distribution

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

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

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

+ Efficient sampler  $(Q', U) \leftarrow \text{Sample}_\sigma(Q)$   
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  $U \in \text{GL}_n(\mathbb{Z})$

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

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

+  $\text{Efficient sampler } (Q', U) \leftarrow \text{Sample}_\sigma(Q)$   
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.



## An average-case distribution

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

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

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

+ Efficient sampler  $(Q', U) \leftarrow \text{Sample}_\sigma(Q)$   
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.

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

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

Best known: generic lattice reduction.

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

Best known: generic lattice reduction.

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

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

Best known: generic lattice reduction.

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

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

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

Best known: generic lattice reduction.

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

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

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

# Decodable Lattices

Lattice	$\text{gap}(\mathcal{L})$	$\text{gap}(\mathcal{L}^*)$	$\text{gap}(\mathcal{L}, \rho)$
'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	$\text{gap}(\mathcal{L})$	$\text{gap}(\mathcal{L}^*)$	$\text{gap}(\mathcal{L}, \rho)$
'Random' Lattice	$\Theta(1)$	$\Theta(1)$	$2^{\Theta(n)}$
<u>Prime Lattice</u>	$\Theta(\log n)$	$\Omega(\sqrt{n})$	$\Theta(\log n)$ [CR88, DP19]
<u>Barnes-Sloane</u>	$\Theta(\sqrt{\log n})$	$\Omega(\sqrt{n})$	$\Theta(\sqrt{\log n})$ [MP20]
<u>Reed-Solomon</u>	$\Theta(\sqrt{\log n})$	$\Omega(\sqrt{n})$	$\Theta(\sqrt{\log n})$ [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	$\text{gap}(\mathcal{L})$	$\text{gap}(\mathcal{L}^*)$	$\text{gap}(\mathcal{L}, \rho)$
'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]
$\mathbb{Z}^n$	$\Theta(\sqrt{n})$	$\Theta(\sqrt{n})$	$\Theta(\sqrt{n})$
<u>NTRU</u> , <u>LWE</u>	$\Omega(1) \dots O(\sqrt{n})$	$\Omega(1)$	$\Omega(\sqrt{n})$
Barnes-Wall	$\Theta(\sqrt[4]{n})$	$\Theta(\sqrt[4]{n})$	$\Theta(\sqrt[4]{n})$ [MN08]



# Decodable Lattices

Lattice	$\text{gap}(\mathcal{L})$	$\text{gap}(\mathcal{L}^*)$	$\text{gap}(\mathcal{L}, \rho)$
'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	$\Omega(1) \dots O(\sqrt{n})$	$\Omega(1)$	$\Omega(\sqrt{n})$
<u>Barnes-Wall</u>	$\Theta(\sqrt[4]{n})$	$\Theta(\sqrt[4]{n})$	$\Theta(\sqrt[4]{n})$ [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.

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

## Interesting cases

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

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

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

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

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

## Interesting cases

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

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

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

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

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

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

$$\beta \approx n.$$

## 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! :)