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.

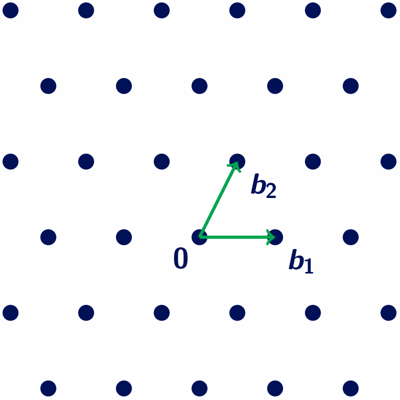
- LWE, SIS, NTRU lattices: versatile, but poor decoding.
- Many wonderful lattices exist with great geometric properties.
- Can we use these in cryptography?

Contributions

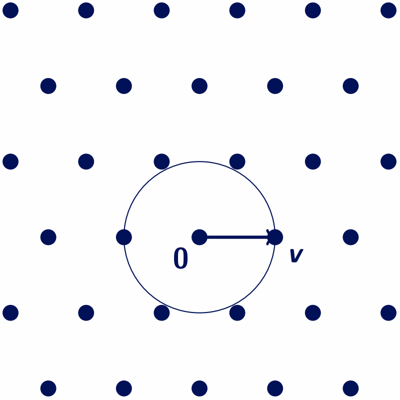
- General identification, encryption and signature scheme based on the Lattice Isomorphism Problem.
- Better lattice $\implies$ better efficiency and security.

Lattices

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



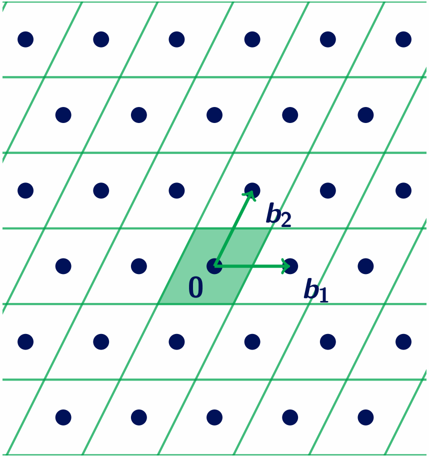
Lattice $\mathcal{L}(\boldsymbol{B}) := \{\sum_i x_i \boldsymbol{b}_i : \boldsymbol{x} \in \mathbb{Z}^n\} \subset \mathbb{R}^n$



First minimum

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

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



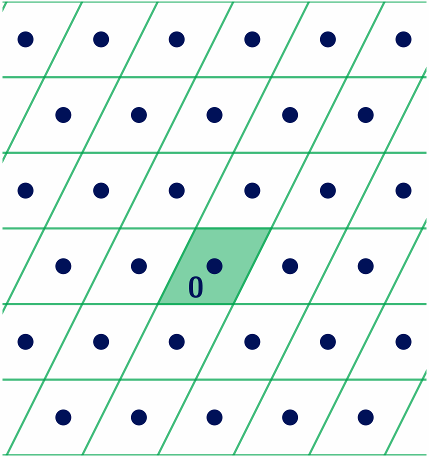
First minimum

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

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

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

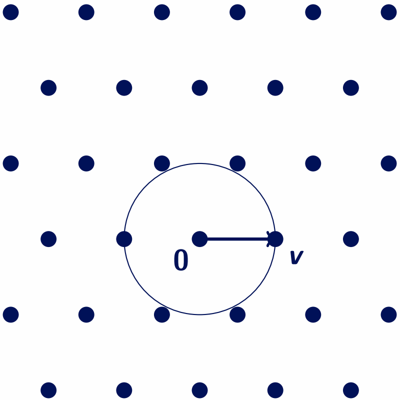
Determinant

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

Minkowski's Theorem

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

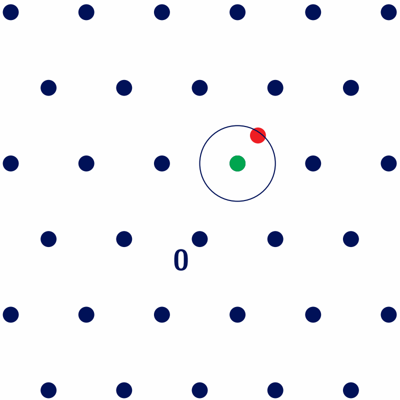
Lattice $\mathcal{L} \subset \mathbb{R}^n$



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

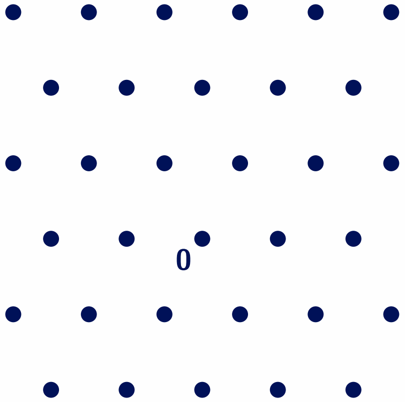
Find a *shortest* nonzero vector $\boldsymbol{v} \in \mathcal{L}$ of length $\lambda_1(\mathcal{L}) \leq \mathsf{Mk}(\mathcal{L})$.

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

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



SVP

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

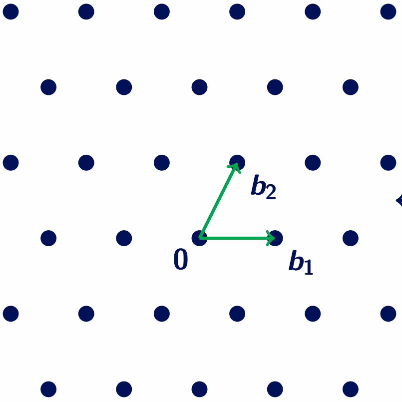
BDD

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

Hardness depends on the *gaps*!

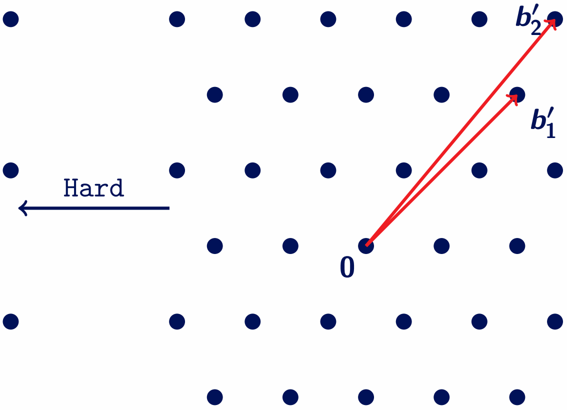
Encryption, legacy approach

Good basis (Secret key)



$\boldsymbol{B}$

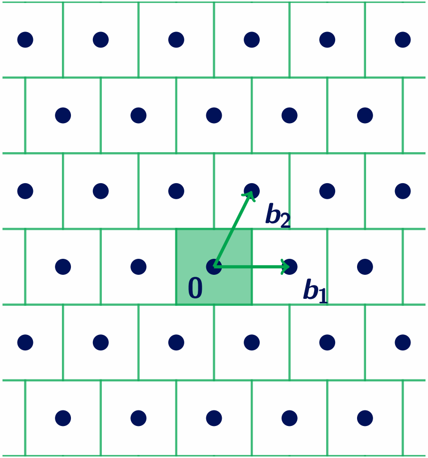
Bad basis (Public key)

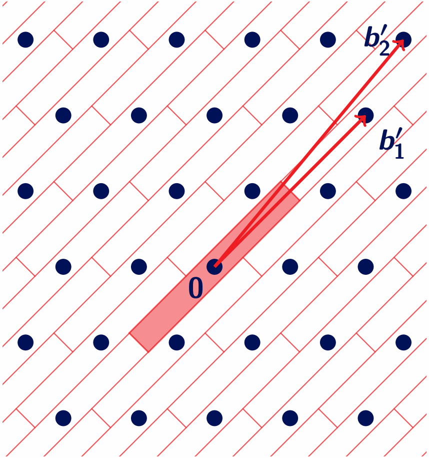


$\boldsymbol{B}' = \boldsymbol{B} \cdot \boldsymbol{U}, \ \boldsymbol{U} \in \mathrm{GL}_d(\mathbb{Z})$

Encryption, legacy approach

Good basis (Secret key) | Bad basis (Public key)

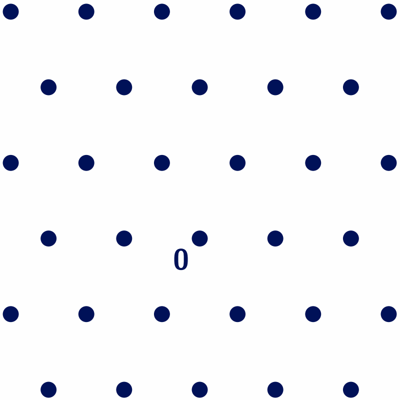




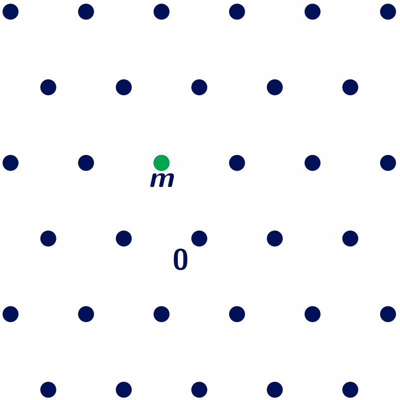
Babai's nearest plane algorithm

Encryption, legacy approach

Good basis (Secret key)

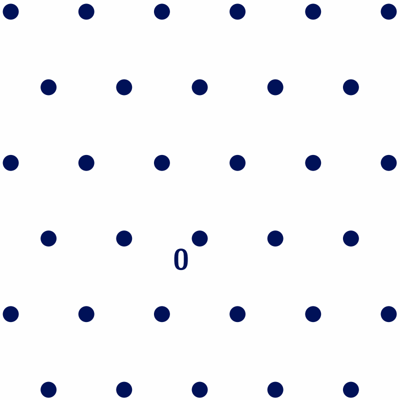


Bad basis (Public key)

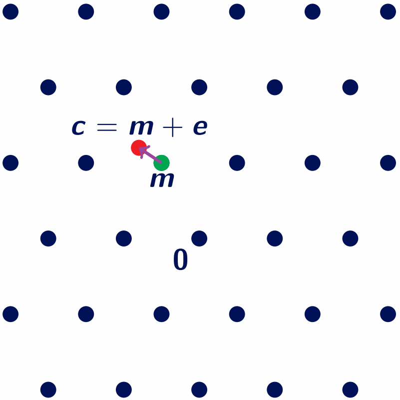


Encryption, legacy approach

Good basis (Secret key)



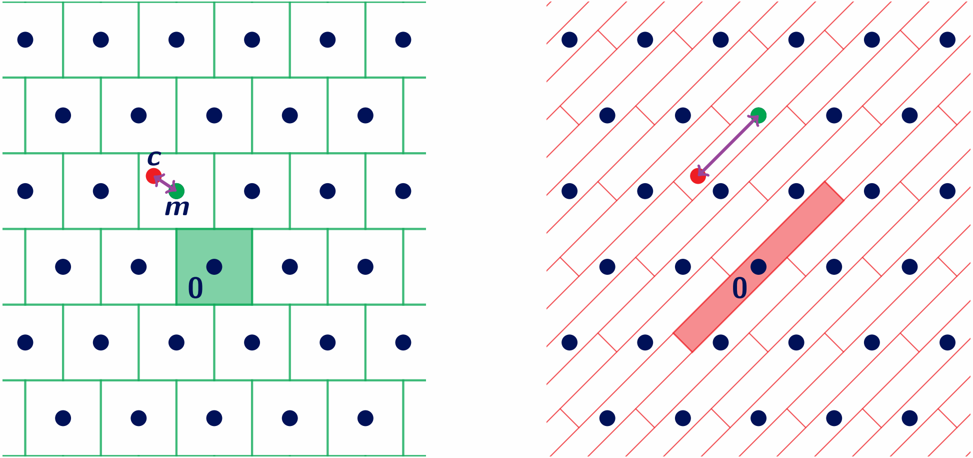
Bad basis (Public key)



Encrypt by adding a small error

Encryption, legacy approach

Good basis (Secret key) | Bad basis (Public key)



Decrypt using the good basis

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:

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

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 $\beta \leq n/2 + o(n)$, 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:

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

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

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]

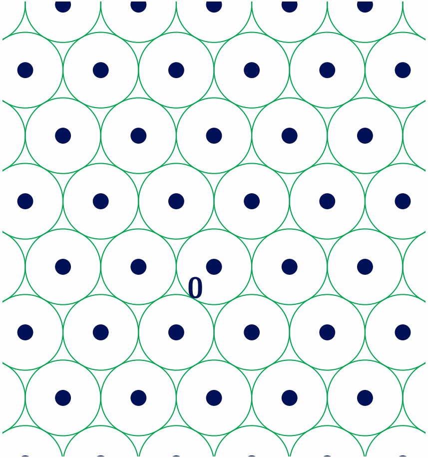
Let $p_1, \ldots, p_n$ be distinct small primes not dividing m, we define:

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

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

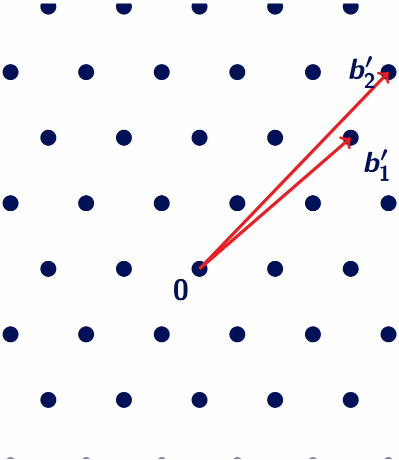
How to hide the remarkable lattice?

Good lattice (~~Secret key~~)



$\mathcal{L}$

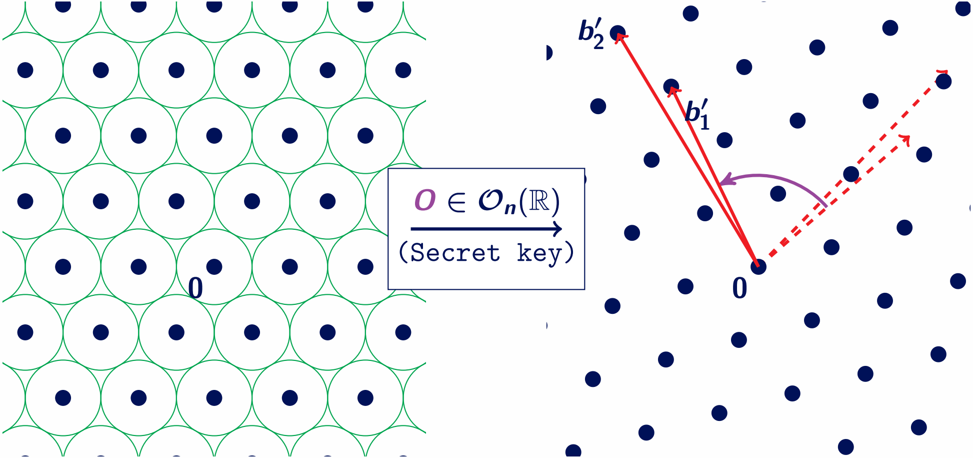
Bad basis (Public key)



$\mathcal{L}$

How to hide the remarkable lattice?

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

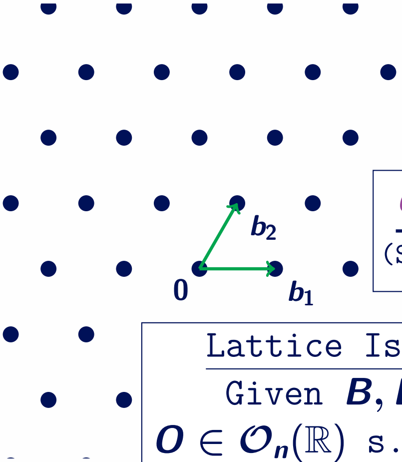


$\mathcal{L}$ $O \cdot \mathcal{L}$

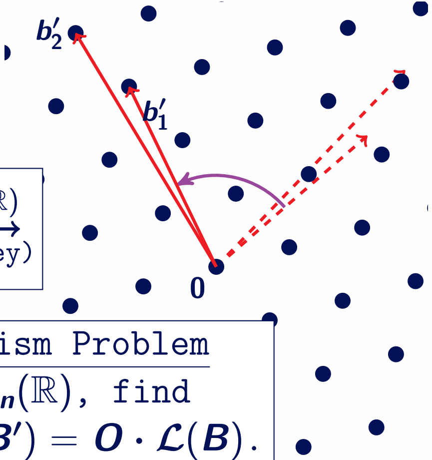
How to hide the remarkable lattice?

Good lattice (~~Secret key~~)

Bad basis (Public key)



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



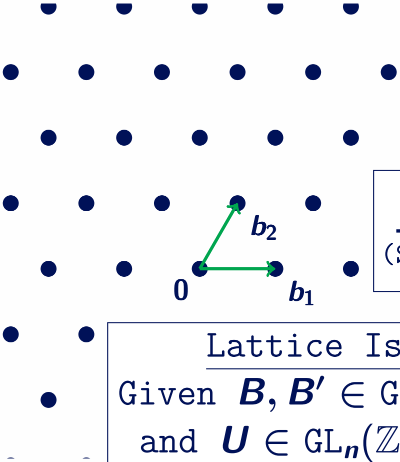
Lattice Isomorphism Problem

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

$\mathcal{L}$ $\qquad$ $O \cdot \mathcal{L}$

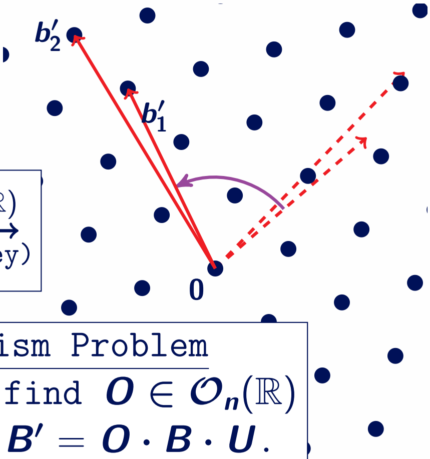
Good lattice (~~Secret key~~)

Bad basis (Public key)



B

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



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

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

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

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.

Algorithms

- $\mathrm{Min}(\mathcal{L}(B')) = O \cdot \mathrm{Min}(\mathcal{L}(B))$.
- 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).

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

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

Sidestep real values!

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

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

$$(\mathcal{L} \subset \mathbb{R}^n, \langle x, y \rangle) \Longrightarrow (\mathbb{Z}^n, \langle x, y \rangle_Q := x^t Q y)$$

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

$$(\mathcal{L} \subset \mathbb{R}^n, \langle x, y \rangle) \implies (\mathbb{Z}^n, \langle x, y \rangle_Q := x^t Q y)$$

Keep the geometry, forget the embedding.

LIP restated:

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

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

An average-case distribution

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

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

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

An average-case distribution

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

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

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

$$+ \quad \boxed{\begin{array}{c}\text{Efficient sampler } (\boldsymbol{Q}', \boldsymbol{U}) \leftarrow \mathrm{Sample}_\sigma(\boldsymbol{Q}) \\ \text{s.t. } \quad \boldsymbol{Q}' \sim \mathcal{D}_\sigma([\boldsymbol{Q}]) \text{ and } \boldsymbol{Q}' = \boldsymbol{U}^t \boldsymbol{Q} \boldsymbol{U}.\end{array}}$$

$\boldsymbol{Q}'$ only depends on the class $[\boldsymbol{Q}]$ and not on $\boldsymbol{Q}$ itself.

An average-case distribution

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

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

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

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

$\boldsymbol{Q}'$ only depends on the class $[\boldsymbol{Q}]$ and not on $\boldsymbol{Q}$ itself.

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

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

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

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

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

$\boldsymbol{Q}'$ *only depends on the class* $[\boldsymbol{Q}]$ *and not on* $\boldsymbol{Q}$ *itself.*

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

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

An average-case distribution

- ac-$\mathrm{LIP}_{\sigma}^{\boldsymbol{Q}}$: given $\boldsymbol{Q}$ and $\boldsymbol{Q}' \leftarrow \mathcal{D}_\sigma([\boldsymbol{Q}])$, recover $\boldsymbol{U} \in \mathrm{GL}_{\boldsymbol{n}}(\mathbb{Z})$.

An average-case distribution

- ac-LIP$^{\boldsymbol{Q}}_{\sigma}$: given $\boldsymbol{Q}$ and $\boldsymbol{Q}' \leftarrow \mathcal{D}_\sigma([\boldsymbol{Q}])$, recover $\boldsymbol{U} \in \mathrm{GL}_n(\mathbb{Z})$.
- ZKPoK: Given public $\boldsymbol{Q}_0, \boldsymbol{Q}_1 \in [\boldsymbol{Q}]$, prove knowledge of a $\boldsymbol{U}$ s.t. $\boldsymbol{Q}_1 = \boldsymbol{U}^t \boldsymbol{Q}_0 \boldsymbol{U}$, without revealing $\boldsymbol{U}$.

$$\begin{tikzcd}
\boldsymbol{Q}_0 \arrow[r, "\boldsymbol{U}"] \arrow[d, "\boldsymbol{V}"'] & \boldsymbol{Q}_1 \arrow[dl, dashed, "\boldsymbol{U}^{-1}\boldsymbol{V}"] \\
\boldsymbol{Q}' \sim \mathcal{D}_\sigma([\boldsymbol{Q}]) &
\end{tikzcd}$$

$$(\boldsymbol{Q}', \boldsymbol{V}) \leftarrow \mathtt{Sample}_\sigma(\boldsymbol{Q}_0)$$

An average-case distribution

- ac-LIP$^{\boldsymbol{Q}}_{\sigma}$: given $\boldsymbol{Q}$ and $\boldsymbol{Q}' \leftarrow \mathcal{D}_\sigma([\boldsymbol{Q}])$, recover $\boldsymbol{U} \in \mathrm{GL}_n(\mathbb{Z})$.
- ZKPoK: Given public $\boldsymbol{Q}_0, \boldsymbol{Q}_1 \in [\boldsymbol{Q}]$, prove knowledge of a $\boldsymbol{U}$ s.t. $\boldsymbol{Q}_1 = \boldsymbol{U}^t \boldsymbol{Q}_0 \boldsymbol{U}$, without revealing $\boldsymbol{U}$.

$$\begin{tikzcd} \boldsymbol{Q}_0 \arrow[r, "\boldsymbol{U}"] \arrow[dr, "\boldsymbol{V}"'] & \boldsymbol{Q}_1 \arrow[d, dashed, "\boldsymbol{U}^{-1}\boldsymbol{V}"] \\ & \boldsymbol{Q}' \sim \mathcal{D}_\sigma([\boldsymbol{Q}]) \end{tikzcd}$$

$$(\boldsymbol{Q}', \boldsymbol{V}) \leftarrow \mathrm{Sample}_\sigma(\boldsymbol{Q}_0)$$

- Worst-case to average-case reduction:

$$\begin{tikzcd} \boldsymbol{Q} \arrow[r, leftrightarrow, "\mathrm{WC}"] \arrow[dr, leftrightarrow, dashed, "\mathrm{AC}"'] & \boldsymbol{Q}' \arrow[d, "\boldsymbol{U}'"] \\ & \boldsymbol{Q}'' \end{tikzcd}$$

$$(\boldsymbol{Q}'', \boldsymbol{U}') \leftarrow \mathrm{Sample}_\sigma(\boldsymbol{Q}')$$

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: $\mathrm{gap}(\mathcal{L})$.

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

Best known: generic lattice reduction.

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

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

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

Best known: generic lattice reduction.

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

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

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

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	$\text{gap}(\mathcal{L})$	$\text{gap}(\mathcal{L}^*)$	$\text{gap}(\mathcal{L}, \rho)$
'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	$\Omega(1) \ldots O(\sqrt{n})$	$\Omega(1)$	$\Omega(\sqrt{n})$
Barnes-Wall	$\Theta(\sqrt[4]{n})$	$\Theta(\sqrt[4]{n})$	$\Theta(\sqrt[4]{n})$ [MN08]

Decodable Lattices

Lattice	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]

Interesting cases

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

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 $O(\sqrt[4]{n})$,

$$n = 1024 \implies \beta \approx 710.$$

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 $O(\sqrt[4]{n})$,

$$n = 1024 \implies \beta \approx 710.$$

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

$$\beta \approx n.$$

- Hash to target, Gaussian sample nearby lattice point.

HAWK - Signatures scheme from $\mathbb{Z}^n$

- Hash to target, Gaussian sample nearby lattice point.
- FALCON: Sample in NTRU lattice using good basis.

HAWK - Signatures scheme from $\mathbb{Z}^n$

- Hash to target, Gaussian sample nearby lattice point.
- Falcon: Sample in NTRU lattice using good basis.
  - Req. high-precision floating point arithmetic.

HAWK - Signatures scheme from $\mathbb{Z}^n$

- Hash to target, Gaussian sample nearby lattice point.
- FALCON: Sample in NTRU lattice using good basis.
  - Req. high-precision floating point arithmetic.
- Idea: Gaussian sampling in (cosets of) $\mathbb{Z}^n$ is (almost) trivial.

HAWK - Signatures scheme from $\mathbb{Z}^n$

- Hash to target, Gaussian sample nearby lattice point.
- FALCON: Sample in NTRU lattice using good basis.
  - Req. high-precision floating point arithmetic.
- Idea: Gaussian sampling in (cosets of) $\mathbb{Z}^n$ is (almost) trivial.
- Quality: FALCON : **1.17**, MITAKA : **2.04**, HAWK : **1.00**.

HAWK - Signatures scheme from $\mathbb{Z}^n$

- Hash to target, Gaussian sample nearby lattice point.
- Falcon: Sample in NTRU lattice using good basis.
  - Req. high-precision floating point arithmetic.
- Idea: Gaussian sampling in (cosets of) $\mathbb{Z}^n$ is (almost) trivial.
- Quality: Falcon : **1.17**, Mitaka : **2.04**, Hawk : **1.00**.
- For efficiency & size:

HAWK - Signatures scheme from $\mathbb{Z}^n$

- Hash to target, Gaussian sample nearby lattice point.
- Falcon: Sample in NTRU lattice using good basis.
  - Req. high-precision floating point arithmetic.
- Idea: Gaussian sampling in (cosets of) $\mathbb{Z}^n$ is (almost) trivial.
- Quality: Falcon : **1.17**, Mitaka : **2.04**, Hawk : **1.00**.
- For efficiency & size:
  - Module-LIP: $R = \mathbb{Z}[X]/(X^m + 1)$ for $m = 2^k$, $R^2 \cong \mathbb{Z}^{2m}$.

HAWK - Signatures scheme from $\mathbb{Z}^n$

- Hash to target, Gaussian sample nearby lattice point.
- FALCON: Sample in NTRU lattice using good basis.
  - Req. high-precision floating point arithmetic.
- Idea: Gaussian sampling in (cosets of) $\mathbb{Z}^n$ is (almost) trivial.
- Quality: FALCON : $\mathbf{1.17}$, MITAKA : $\mathbf{2.04}$, HAWK : $\mathbf{1.00}$.
- For efficiency & size:
  - Module-LIP: $R = \mathbb{Z}[X]/(X^m + 1)$ for $m = 2^k$, $R^2 \cong \mathbb{Z}^{2m}$.
  - Sample basis similar to FALCON:

$$B = \begin{pmatrix} f & F \\ g & G \end{pmatrix},$$

sample f, g and complete with F, G such that $\det(B) = 1$.

HAWK - Signatures scheme from $\mathbb{Z}^n$

- Hash to target, Gaussian sample nearby lattice point.
- FALCON: Sample in NTRU lattice using good basis.
  - Req. high-precision floating point arithmetic.
- Idea: Gaussian sampling in (cosets of) $\mathbb{Z}^n$ is (almost) trivial.
- Quality: FALCON : **1.17**, MITAKA : **2.04**, HAWK : **1.00**.
- For efficiency & size:
  - Module-LIP: $\boldsymbol{R} = \mathbb{Z}[\boldsymbol{X}]/(\boldsymbol{X}^{\boldsymbol{m}} + 1)$ for $\boldsymbol{m} = 2^{\boldsymbol{k}}$, $\boldsymbol{R}^2 \cong \mathbb{Z}^{2\boldsymbol{m}}$.
  - Sample basis similar to FALCON:

$$\boldsymbol{B} = \begin{pmatrix} \boldsymbol{f} & \boldsymbol{F} \\ \boldsymbol{g} & \boldsymbol{G} \end{pmatrix},$$

    sample $\boldsymbol{f}, \boldsymbol{g}$ and complete with $\boldsymbol{F}, \boldsymbol{G}$ such that $\det(\boldsymbol{B}) = 1$.
  - $\boldsymbol{pk} = \boldsymbol{Q} = \boldsymbol{B}^t \boldsymbol{B}$, compress further.

HAWK - Signatures scheme from $\mathbb{Z}^n$

- Hash to target, Gaussian sample nearby lattice point.
- Falcon: Sample in NTRU lattice using good basis.
  - Req. high-precision floating point arithmetic.
- Idea: Gaussian sampling in (cosets of) $\mathbb{Z}^n$ is (almost) trivial.
- Quality: Falcon : $\mathbf{1.17}$, Mitaka : $\mathbf{2.04}$, Hawk : $\mathbf{1.00}$.
- For efficiency & size:
  - Module-LIP: $R = \mathbb{Z}[X]/(X^m + 1)$ for $m = 2^k$, $R^2 \cong \mathbb{Z}^{2m}$.
  - Sample basis similar to Falcon:

$$B = \begin{pmatrix} f & F \\ g & G \end{pmatrix},$$

    sample f, g and complete with F, G such that $\det(B) = 1$.
  - $pk = Q = B^t B$, compress further.
  - Hash to cosets $\{0, \frac{1}{2}\}^n + \mathbb{Z}^n$.

HAWK - Signatures scheme from $\mathbb{Z}^n$

- Hash to target, Gaussian sample nearby lattice point.
- FALCON: Sample in NTRU lattice using good basis.
  - Req. high-precision floating point arithmetic.
- Idea: Gaussian sampling in (cosets of) $\mathbb{Z}^n$ is (almost) trivial.
- Quality: FALCON : **1.17**, MITAKA : **2.04**, HAWK : **1.00**.
- For efficiency & size:
  - Module-LIP: $R = \mathbb{Z}[X]/(X^m + 1)$ for $m = 2^k$, $R^2 \cong \mathbb{Z}^{2m}$.
  - Sample basis similar to FALCON:

$$B = \begin{pmatrix} f & F \\ g & G \end{pmatrix},$$

    sample f, g and complete with F, G such that $\det(B) = 1$.
  - $pk = Q = B^t B$, compress further.
  - Hash to cosets $\{0, \frac{1}{2}\}^n + \mathbb{Z}^n$.
  - Compression: drop half the signature and recover using public key.

HAWK - Signatures scheme from $\mathbb{Z}^n$

- Hash to target, Gaussian sample nearby lattice point.
- FALCON: Sample in NTRU lattice using good basis.
  - Req. high-precision floating point arithmetic.
- Idea: Gaussian sampling in (cosets of) $\mathbb{Z}^n$ is (almost) trivial.
- Quality: FALCON : $\mathbf{1.17}$, MITAKA : $\mathbf{2.04}$, HAWK : $\mathbf{1.00}$.
- For efficiency & size:
  - Module-LIP: $R = \mathbb{Z}[X]/(X^m + 1)$ for $m = 2^k$, $R^2 \cong \mathbb{Z}^{2m}$.
  - Sample basis similar to FALCON:

$$B = \begin{pmatrix} f & F \\ g & G \end{pmatrix},$$

    sample f, g and complete with F, G such that $\det(B) = 1$.
  - $pk = Q = B^t B$, compress further.
  - Hash to cosets $\{0, \frac{1}{2}\}^n + \mathbb{Z}^n$.
  - Compression: drop half the signature and recover using public key.
  - Tune parameters based on concrete cryptanalysis.

HAWK - Performance

	Falcon-512	Hawk-512	$\left(\frac{\text{Falcon}}{\text{Hawk}}\right)$
AVX2 KeyGen	**8.10** ms	**4.13** ms	$\times$**1.96**
Reference KeyGen	**18.76** ms	**13.78** ms	$\times$**1.36**
AVX2 Sign	**200** µs	**47** µs	$\times$**4.3**
Reference Sign	**2401** µs	**206** µs	$\times$**11.7**
AVX2 Verify	**51** µs	**20** µs	$\times$**2.6**
Reference Verify	**50** µs	**1043** µs	$\times$**0.048**
Secret key (bytes)	**1281**	**1153**	$\times$**1.11**
Public key (bytes)	**897**	**1006** $\pm$ **6**	$\times$**0.89**
Signature (bytes)	**652** $\pm$ **3**	**541** $\pm$ **4**	$\times$**1.21**

HAWK – Performance

	FALCON-512	HAWK-512	$\left(\frac{\text{FALCON}}{\text{HAWK}}\right)$
AVX2 KeyGen	**8.10** ms	**4.13** ms	$\times$**1.96**
Reference KeyGen	**18.76** ms	**13.78** ms	$\times$**1.36**
AVX2 Sign	**200** µs	**47** µs	$\times$**4.3**
Reference Sign	**2401** µs	**206** µs	$\times$**11.7**
AVX2 Verify	**51** µs	**20** µs	$\times$**2.6**
Reference Verify	**50** µs	**1043** µs	$\times$**0.048**
Secret key (bytes)	**1281**	**1153**	$\times$**1.11**
Public key (bytes)	**897**	**1006** $\pm$ **6**	$\times$**0.89**
Signature (bytes)	**652** $\pm$ **3**	**541** $\pm$ **4**	$\times$**1.21**

	Uncompressed HAWK-512
Reference Sign	**185** µs
Reference Verify	**238** µs
Signature (bytes)	**1223** $\pm$ **7**

Conclusion

Any lattice $\Longrightarrow$ Identification scheme.

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

Gaussian sampleable lattice $\mathcal{L}$ $\Longrightarrow$ 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 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 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 LWE and NTRU.

End goal: do even better.

Thanks! :)