# A Short Survey of Lattice-Isomorphism-Based Cryptography

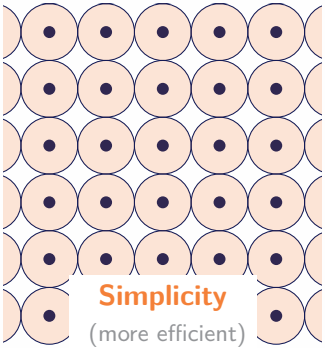
**Wessel van Woerden** (PQShield).

# Motivation

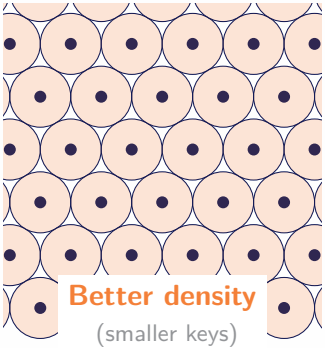
LWE, SIS, NTRU lattices: versatile, but poor geometry & algorithms.

# Motivation

LWE, SIS, NTRU lattices: versatile, but poor geometry & algorithms.
Many remarkable lattices exist with great geometric or algorithmic properties.



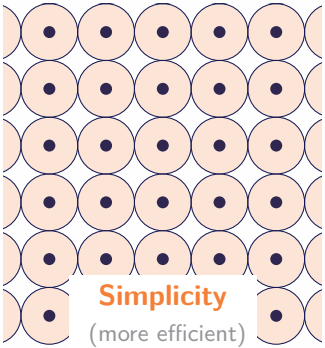
**Simplicity**
(more efficient)

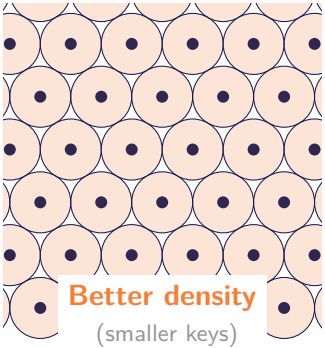


**Better density**
(smaller keys)

# Motivation

LWE, SIS, NTRU lattices: versatile, but poor geometry & algorithms.
Many remarkable lattices exist with great geometric or algorithmic properties.

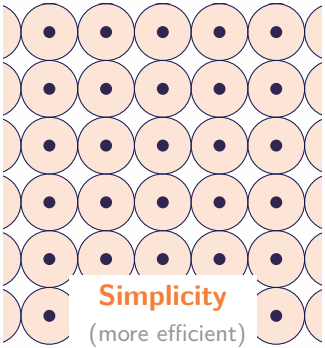


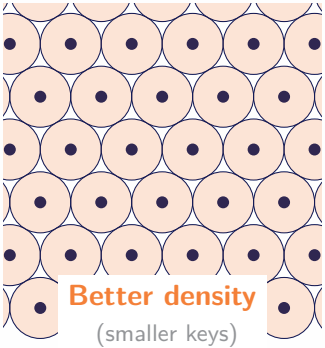




Can we use these in cryptography?

# Motivation

LWE, SIS, NTRU lattices: versatile, but poor geometry & algorithms.
Many remarkable lattices exist with great geometric or algorithmic properties.



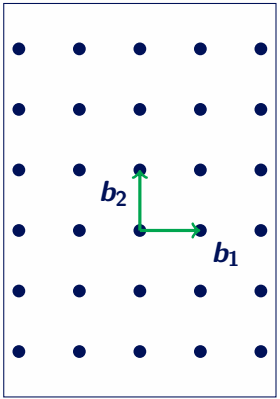




Can we use these in cryptography?

**Lattice Isomorphism Problem: yes, we can!**

# Lattices and decoding

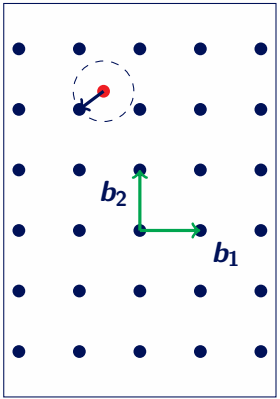
Lattice $\mathcal{L}(B) := \{\sum_i x_i b_i : x \in \mathbb{Z}^n\} \subset \mathbb{R}^n$




integer lattice $\mathbb{Z}^n$

# Lattices and decoding

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

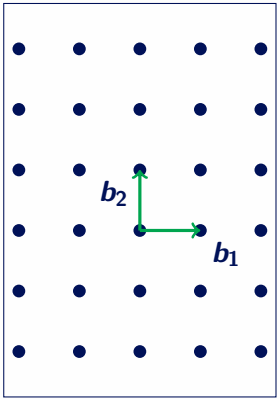



integer lattice $\mathbb{Z}^n$

decoding easy

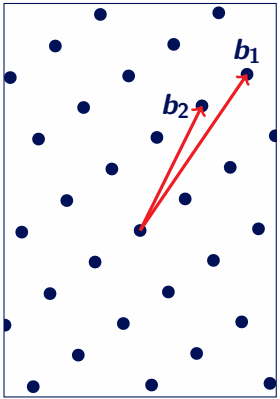
# Lattices and decoding

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




integer lattice $\mathbb{Z}^n$

decoding easy

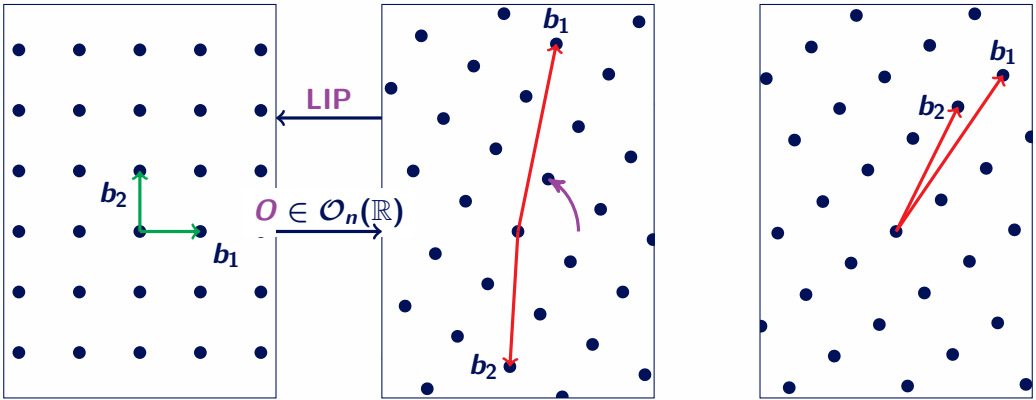



random lattice

decoding hard

# Lattices and decoding

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




integer lattice $\mathbb{Z}^n$

decoding easy

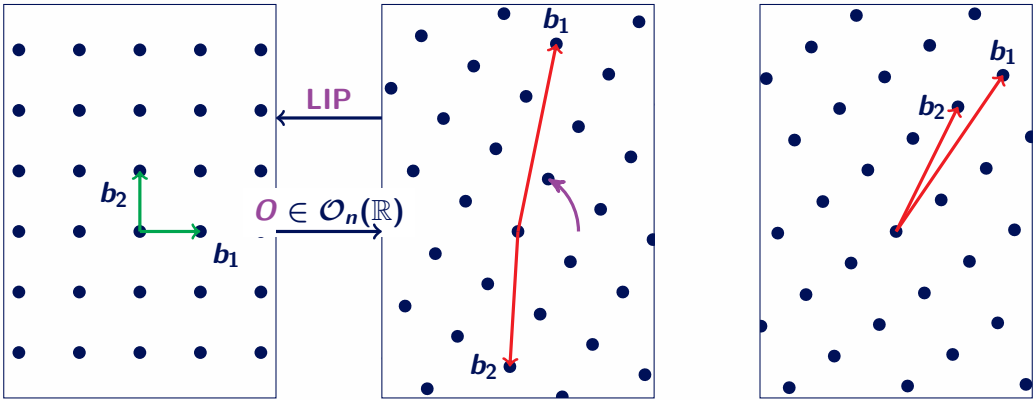
$\mathbb{Z}^n$ rotated

random lattice

decoding hard

# Lattices and decoding

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




integer lattice $\mathbb{Z}^n$

decoding easy

$\mathbb{Z}^n$ rotated

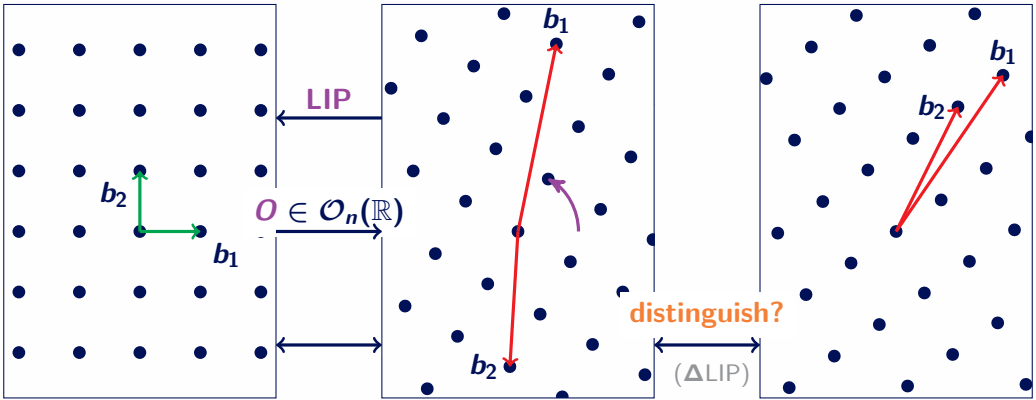
decoding hard?

random lattice

decoding hard

# Lattices and decoding

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




integer lattice $\mathbb{Z}^n$

decoding easy

$\mathbb{Z}^n$ rotated

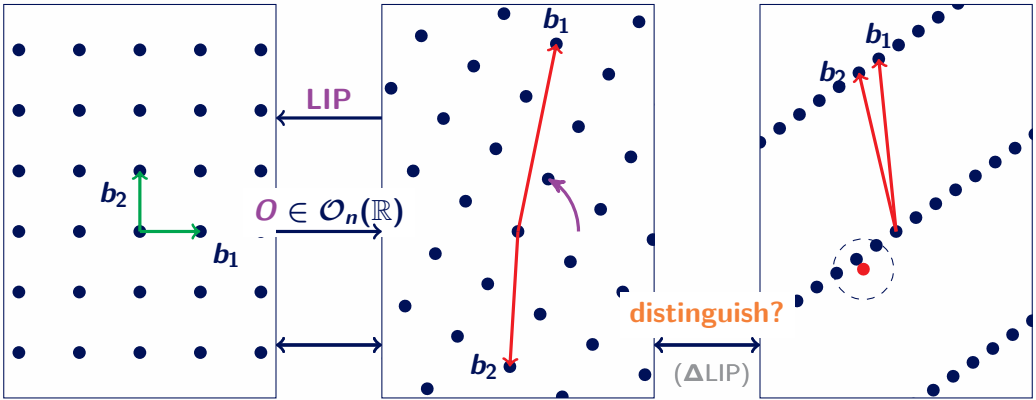
decoding hard?

random lattice

decoding hard

# Lattices and decoding

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




integer lattice $\mathbb{Z}^n$

decoding easy

$\mathbb{Z}^n$ rotated

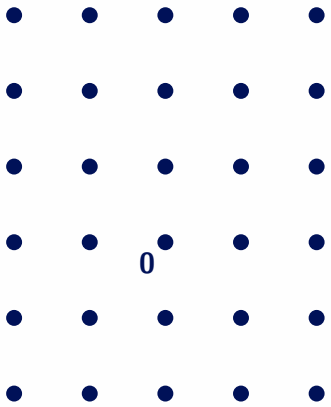
decoding hard?

dense sublattice

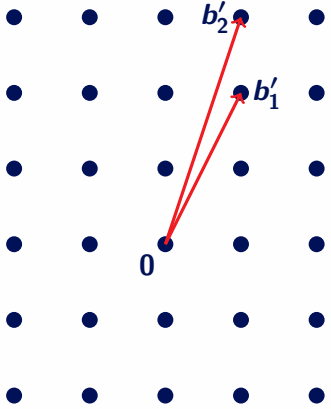
decoding hard

# Encryption scheme based on LIP

Decodable lattice

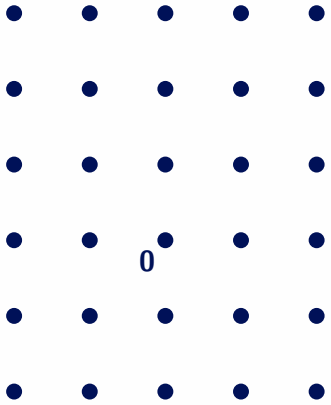



Bad basis of $\mathcal{L}$



# Encryption scheme based on LIP

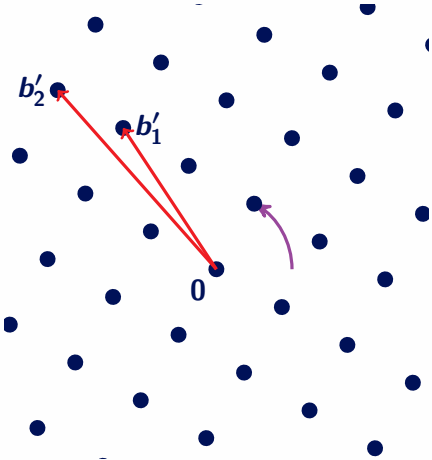
Decodable lattice




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

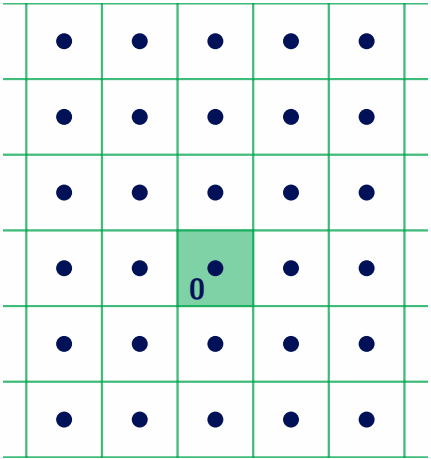
(Secret key)

Bad basis of rotation



# Encryption scheme based on LIP

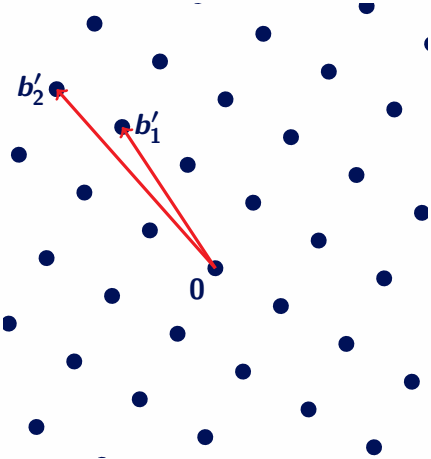
Decodable lattice




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

(Secret key)

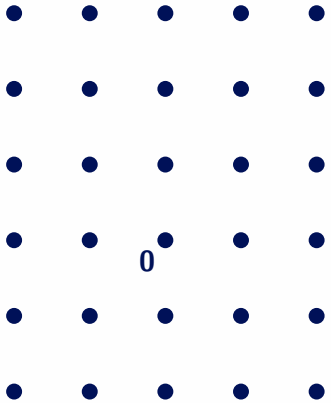
Bad basis of rotation




Hides (decoding) structure of $\mathcal{L}$

# Encryption scheme based on LIP

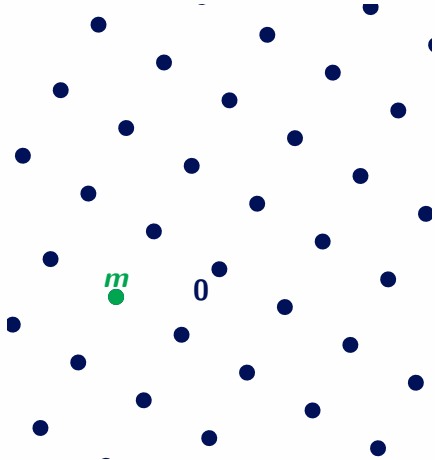
Decodable lattice



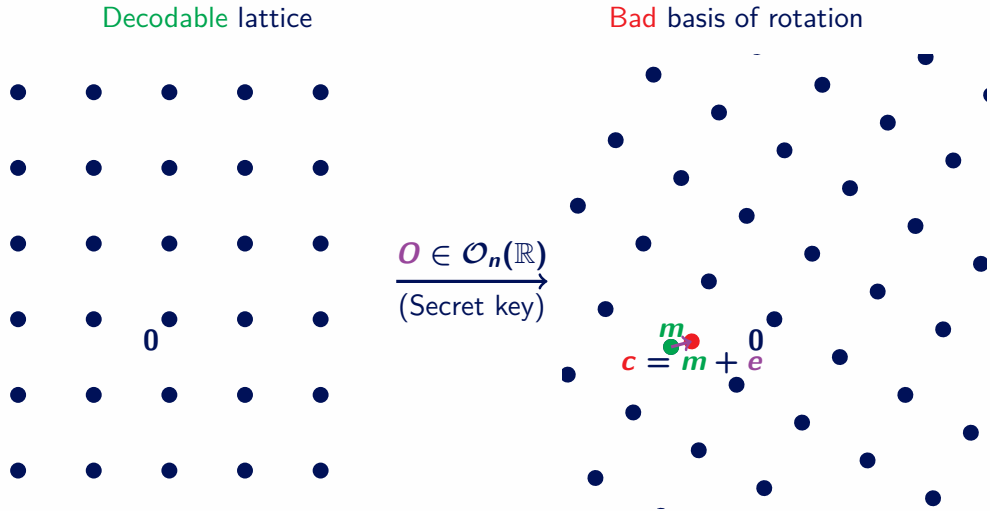

$O \in \mathcal{O}_n(\mathbb{R})$

(Secret key)

Bad basis of rotation



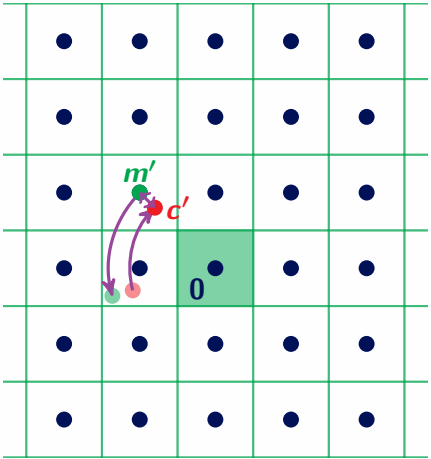
# Encryption scheme based on LIP




Encrypt by adding a small error

# Encryption scheme based on LIP

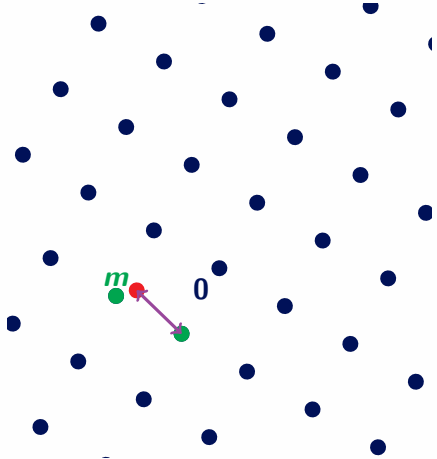
Decodable lattice




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

(Secret key)

Bad basis of rotation




Decrypt using decoding algorithm

# Lattice Isomorphism Problem

**Definition:** Lattice Isomorphism Problem (wc-sLIP)

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

# Lattice Isomorphism Problem

**Definition:** Lattice Isomorphism Problem (wc-sLIP)

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

- Best known attacks require to **solve SVP**.

# Lattice Isomorphism Problem

**Definition:** Lattice Isomorphism Problem (wc-sLIP)

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

- Best known attacks require to **solve SVP**.
- Can be rephrased with Gram matrices $\boldsymbol{Q} = \boldsymbol{B}^\top \boldsymbol{B}, \boldsymbol{Q}' = (\boldsymbol{B}')^\top \boldsymbol{B}'$:

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

# Lattice Isomorphism Problem

**Definition:** Lattice Isomorphism Problem (wc-sLIP)

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

- Best known attacks require to **solve SVP**.
- Can be rephrased with Gram matrices $\boldsymbol{Q} = \boldsymbol{B}^\top \boldsymbol{B}, \boldsymbol{Q}' = (\boldsymbol{B}')^\top \boldsymbol{B}'$:

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

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

# average-case LIP and ΔLIP

- $\exists$ average-case distribution $\mathcal{D}_\sigma([Q])$ + efficient sampler $(Q', U)$ (keygen!)

# average-case LIP and ΔLIP

- $\exists$ average-case distribution $\mathcal{D}_\sigma([Q])$ + efficient sampler $(Q', U)$ (keygen!)

Definition: **ac-sLIP**$^{Q}_{\sigma}$

Given $Q' \leftarrow \mathcal{D}_\sigma([Q])$, compute $U \in \mathrm{GL}_n(\mathbb{Z})$ s.t. $Q' = U^T Q U$.

# average-case LIP and ΔLIP

- $\exists$ average-case distribution $\mathcal{D}_\sigma([Q])$ + efficient sampler $(Q', U)$ (keygen!)

**Definition: ac-sLIP$^Q_\sigma$**

Given $Q' \leftarrow \mathcal{D}_\sigma([Q])$, compute $U \in \mathrm{GL}_n(\mathbb{Z})$ s.t. $Q' = U^T Q U$.

**Definition: ac-ΔLIP$^{Q_0,Q_1}_\sigma$**

Let $[Q_0] \neq [Q_1]$. Given $Q' \leftarrow \mathcal{D}_\sigma([Q_b])$, where $b \leftarrow \{0,1\}$ uniform, recover $b$ (with non-negligible advantage).

# average-case LIP and ΔLIP

- $\exists$ average-case distribution $\mathcal{D}_\sigma([Q])$ + efficient sampler $(Q', U)$ (keygen!)

**Definition: ac-sLIP$^Q_\sigma$**

Given $Q' \leftarrow \mathcal{D}_\sigma([Q])$, compute $U \in \mathrm{GL}_n(\mathbb{Z})$ s.t. $Q' = U^T Q U$.

**Definition: ac-ΔLIP$^{Q_0,Q_1}_\sigma$**

Let $[Q_0] \neq [Q_1]$. Given $Q' \leftarrow \mathcal{D}_\sigma([Q_b])$, where $b \leftarrow \{0,1\}$ uniform, recover $b$ (with non-negligible advantage).

- $\sigma > 0$ determines the **quality of the basis**.
- For $\sigma > 2^{\Omega(n)} \cdot \lambda_1([Q])$ we have ac-sLIP$^Q_\sigma \geq$ wc-sLIP$^Q$. **(WC-AC reduction)**

# average-case LIP and ΔLIP

- $\exists$ average-case distribution $\mathcal{D}_\sigma([Q])$ + efficient sampler $(Q', U)$ (keygen!)

**Definition: ac-sLIP$^Q_\sigma$**

Given $Q' \leftarrow \mathcal{D}_\sigma([Q])$, compute $U \in \mathrm{GL}_n(\mathbb{Z})$ s.t. $Q' = U^T Q U$.

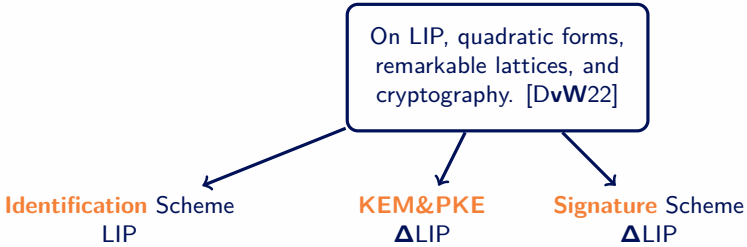
**Definition: ac-ΔLIP$^{Q_0,Q_1}_\sigma$**

Let $[Q_0] \neq [Q_1]$. Given $Q' \leftarrow \mathcal{D}_\sigma([Q_b])$, where $b \leftarrow \{0,1\}$ uniform, recover $b$ (with non-negligible advantage).

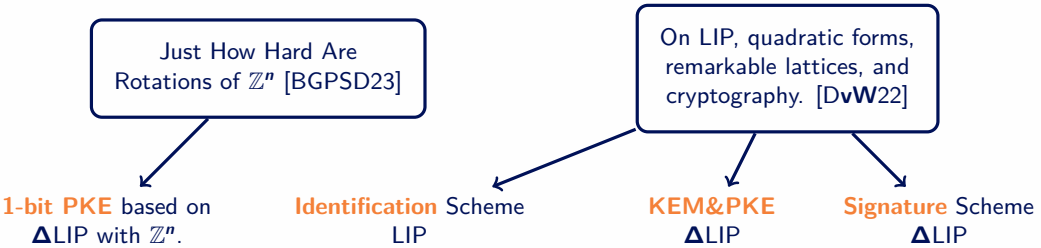
- $\sigma > 0$ determines the **quality of the basis**.
- For $\sigma > 2^{\Omega(n)} \cdot \lambda_1([Q])$ we have ac-sLIP$^Q_\sigma \geq$ wc-sLIP$^Q$. **(WC-AC reduction)**

LIP and ΔLIP problems **depend on fixed lattice(s)**.

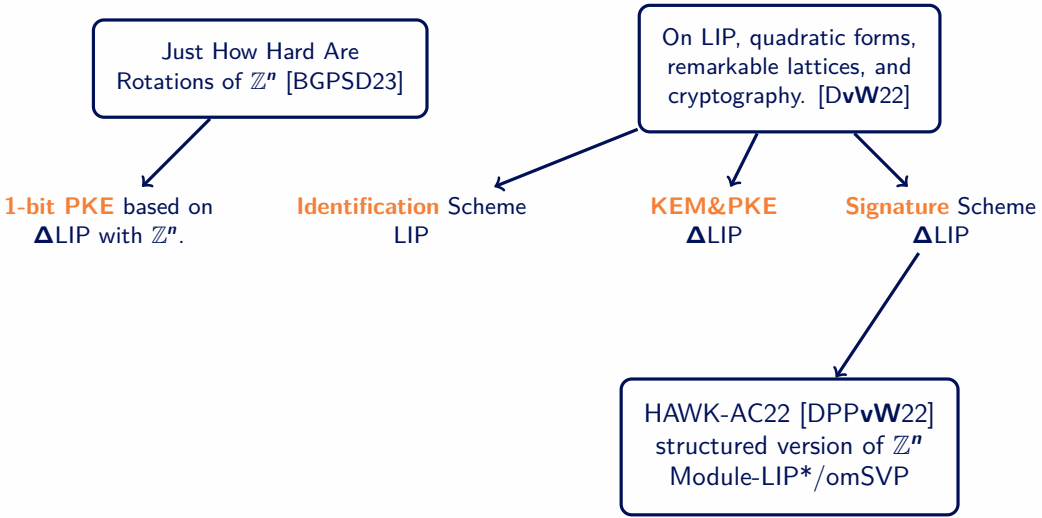
# The beginnings



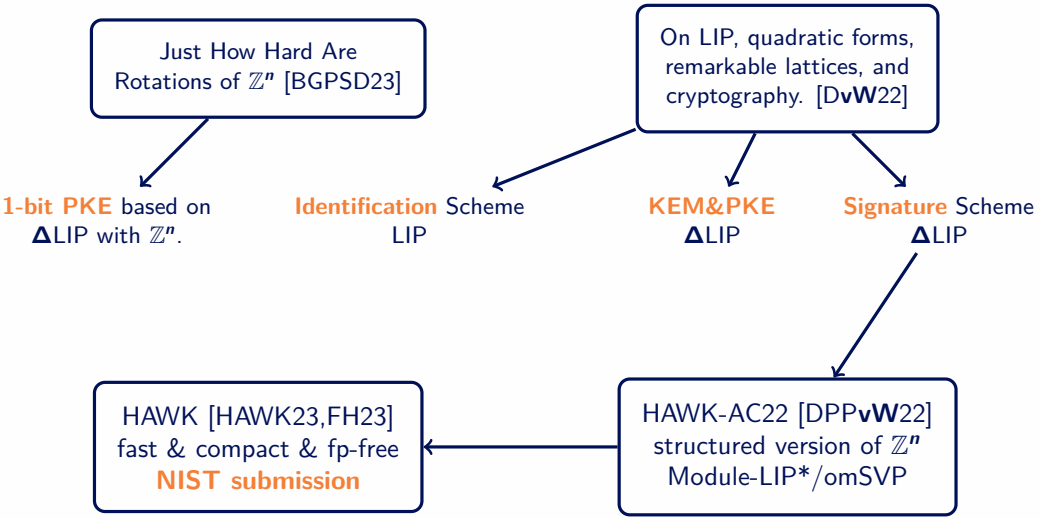
# The beginnings



# The beginnings



# The beginnings



# Constructions

**KEM&PKEs**
$\mathbb{Z}^n$ or $\mathrm{BW}_n$ + **Δ**LIP
[ARLW24,CBZIPC24]

**IBE**
**Δ**LIP
[BLSD26]

Various **Commitment Schemes**
LIP (group action)
[JWLLGPW25,LJPW25]

**∞-uPKE**
**Δ**PCE [ABL25]
or **Δ**LIP (WIP)

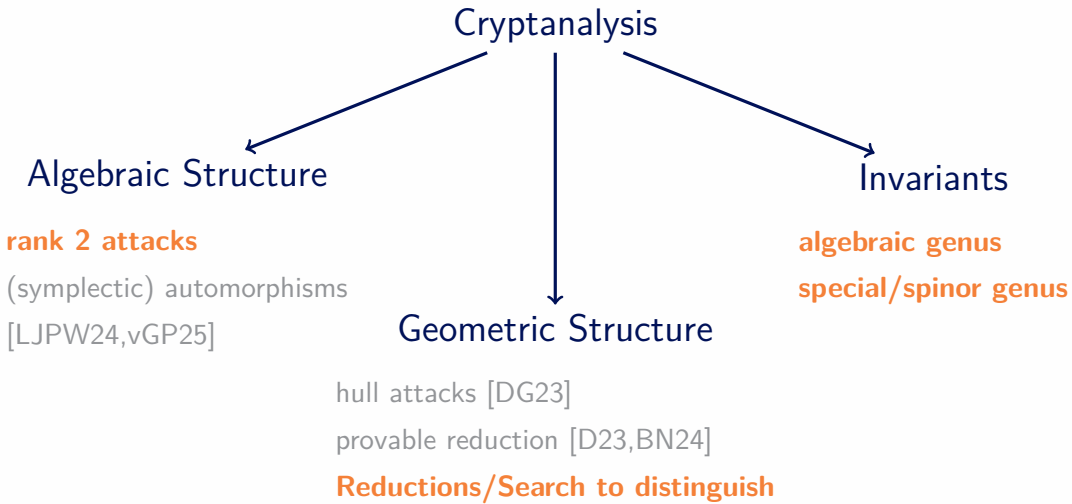
**Ring Signatures**
LIP + HAWK
[LGD26]

**Blind Signatures**
LIP (OR proofs)
[NP26]

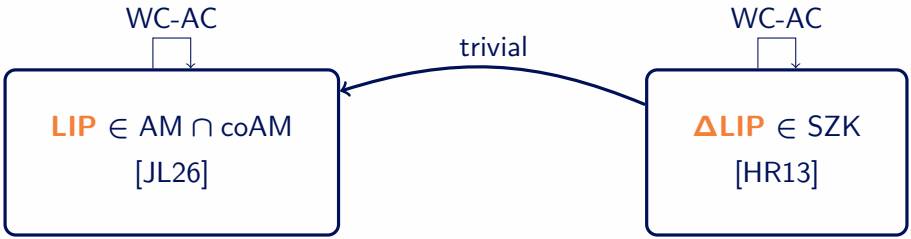
**(F)HE**
**Δ**LIP [BMM25,
LR**vW**25,BLSD26]

Allows for **Advanced Cryptographic Constructions**

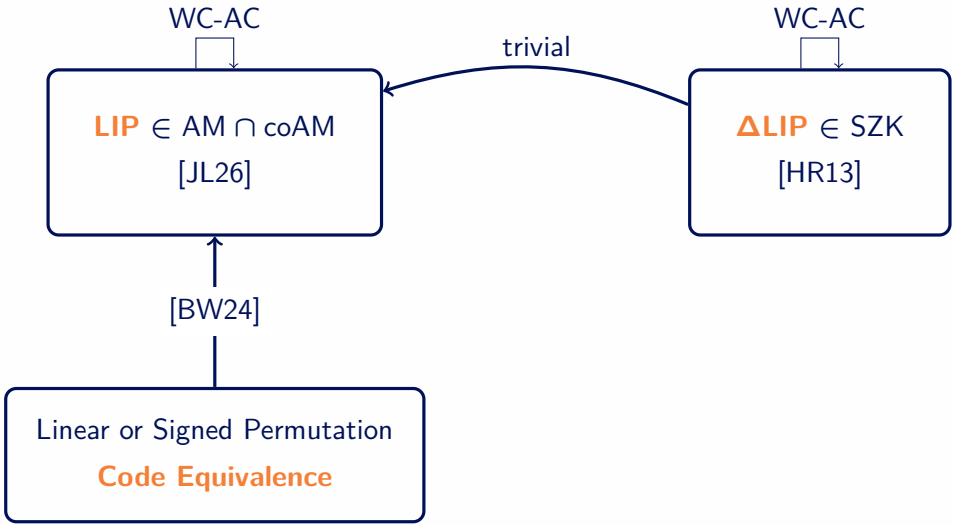
# Cryptanalysis



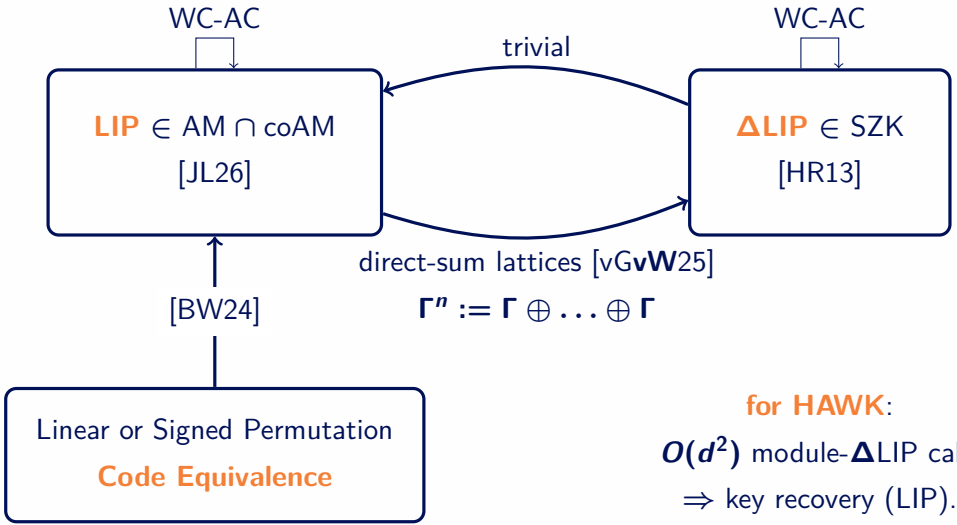
# Reductions



# Reductions


WC-AC
trivial
WC-AC
LIP ∈ AM ∩ coAM
[JL26]
ΔLIP ∈ SZK
[HR13]
[BW24]
Linear or Signed Permutation
Code Equivalence

# Reductions




**for HAWK**:

$O(d^2)$ module-$\Delta$LIP calls

$\Rightarrow$ key recovery (LIP).

# Algebraic Structure

How much **structure** is allowed?

# Algebraic Structure

How much **structure** is allowed?

Module-LIP: replace $\mathcal{L} = B \cdot \mathbb{Z}^n$ by $\mathcal{L} = B \cdot O_K^r$ for ring of integers $O_K$.

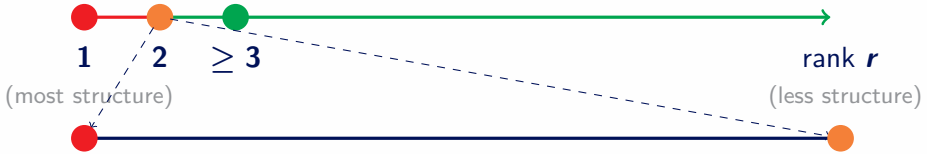
# Algebraic Structure

How much **structure** is allowed?

Module-LIP: replace $\mathcal{L} = B \cdot \mathbb{Z}^n$ by $\mathcal{L} = B \cdot O_K^r$ for ring of integers $O_K$.

How much **structure** is allowed?

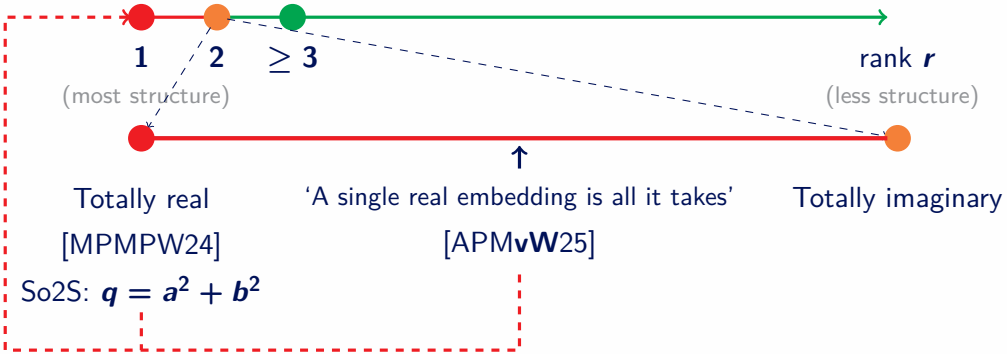
Module-LIP: replace $\mathcal{L} = B \cdot \mathbb{Z}^n$ by $\mathcal{L} = B \cdot O_K^r$ for ring of integers $O_K$.



# Algebraic Structure

How much **structure** is allowed?

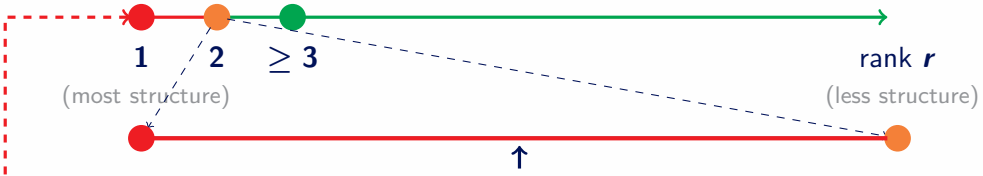
Module-LIP: replace $\mathcal{L} = B \cdot \mathbb{Z}^n$ by $\mathcal{L} = B \cdot O_K^r$ for ring of integers $O_K$.



# Algebraic Structure

How much **structure** is allowed?

Module-LIP: replace $\mathcal{L} = B \cdot \mathbb{Z}^n$ by $\mathcal{L} = B \cdot O_K^r$ for ring of integers $O_K$.




Totally real

[MPMPW24]

So2S: $q = a^2 + b^2$

'A single real embedding is all it takes'

[APM**vW**25]

Totally imaginary

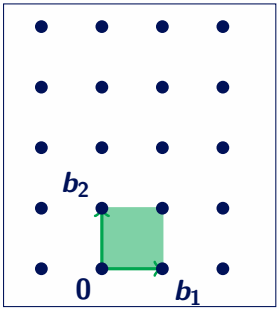
HAWK (CM field)

[CMEPMPW25,CM25]:

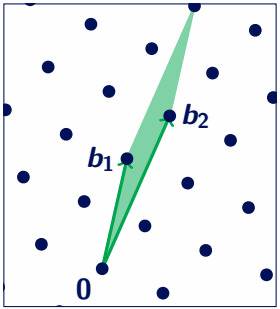
So4S: $q = a^2 + b^2 + c^2 + d^2$

**attack does not apply**

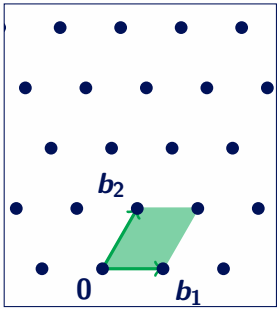
# Invariants




$\det(\mathcal{L}_1)$ $\overset{?}{=}$

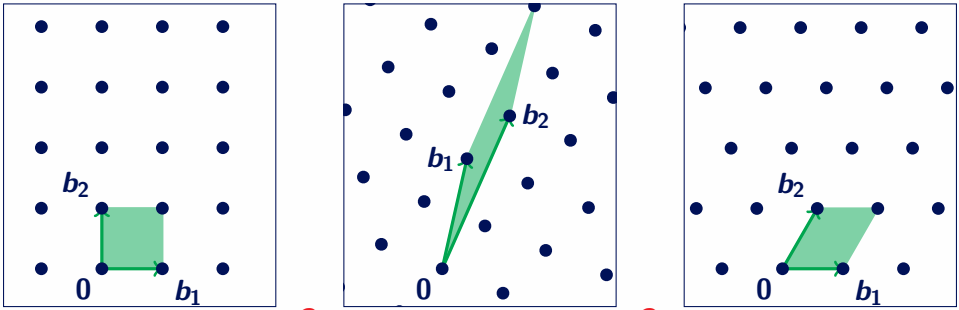



$\det(O \cdot \mathcal{L}_b)$ $\overset{?}{=}$




$\det(\mathcal{L}_2)$

# Invariants

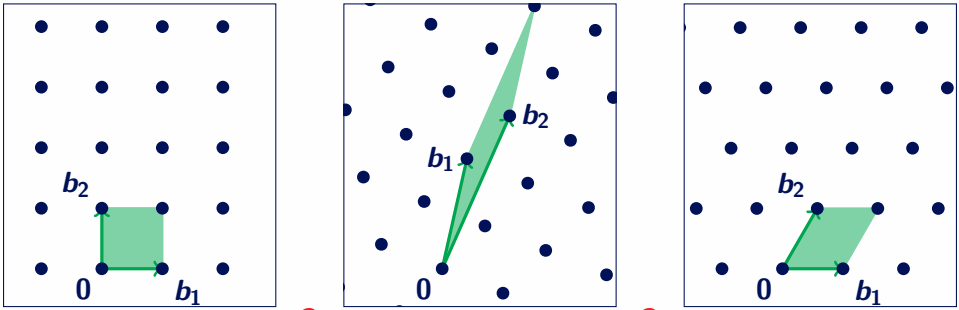



$\det(\mathcal{L}_1) \stackrel{?}{=} \det(O \cdot \mathcal{L}_b) \stackrel{?}{=} \det(\mathcal{L}_2)$

Lemma:

If $\det(\mathcal{L}_1) \neq \det(\mathcal{L}_2)$, then $\Delta$LIP can be solved efficiently.

# Invariants




Lemma:

If $\det(\mathcal{L}_1) \neq \det(\mathcal{L}_2)$, then $\Delta$LIP can be solved efficiently.

Conjecture [DvW22]: **Genus is the strongest** efficiently computable invariant.

# Alternative LIP Assumptions

- Genus contains **finite #equivalence classes** and has a **natural distribution**.

# Alternative LIP Assumptions

- Genus contains **finite #equivalence classes** and has a **natural distribution**.

[**vW**24] Random lattices in a genus behave like general random lattices.

$\Rightarrow$ any genus contains dense and smooth lattices $\Rightarrow$ tighter security proofs

# Alternative LIP Assumptions

- Genus contains **finite #equivalence classes** and has a **natural distribution**.

[**vW**24] Random lattices in a genus behave like general random lattices.

$\Rightarrow$ any genus contains dense and smooth lattices $\Rightarrow$ tighter security proofs

Security Assumption: (informal) [LR**vW**25]

Let $\mathcal{L}$ be a lattice. For a random lattice $\mathcal{L}' \leftarrow \text{Genus}(\mathcal{L})$,
solving $\boldsymbol{\Delta}$BDD in $\mathcal{L}'$ is hard.

- Direct analogue of dLWE in family of random $q$-ary lattices.

# Alternative LIP Assumptions

- Genus contains **finite #equivalence classes** and has a **natural distribution**.

[**vW**24] Random lattices in a genus behave like general random lattices.

$\Rightarrow$ any genus contains dense and smooth lattices $\Rightarrow$ tighter security proofs

Security Assumption: (informal) [LR**vW**25]

Let $\mathcal{L}$ be a lattice. For a random lattice $\mathcal{L}' \leftarrow \text{Genus}(\mathcal{L})$,
solving $\mathbf{\Delta}$BDD in $\mathcal{L}'$ is hard.

- Direct analogue of dLWE in family of random $q$-ary lattices.
- 'vintage' McEliece: **distinguish assumption** + **random lattice problem**.

# Alternative LIP Assumptions

- Genus contains **finite #equivalence classes** and has a **natural distribution**.

[**vW**24] Random lattices in a genus behave like general random lattices.

$\Rightarrow$ any genus contains dense and smooth lattices $\Rightarrow$ tighter security proofs

Security Assumption: (informal) [LR**vW**25]

Let $\mathcal{L}$ be a lattice. For a random lattice $\mathcal{L}' \leftarrow \text{Genus}(\mathcal{L})$,
solving $\boldsymbol{\Delta}$BDD in $\mathcal{L}'$ is hard.

- Direct analogue of dLWE in family of random $q$-ary lattices.
- 'vintage' McEliece: **distinguish assumption** + **random lattice problem**.
- (WIP) **WC-AC reduction** within a fixed genus for BDD, CVP, DGS, ...

# LIP as a group action

- (Right) **group action** on equivalence class $[Q := B^T B]$ by $U \in \mathrm{GL}_d(\mathbb{Z})$:

$$U \circ Q \mapsto U^T Q U$$

# LIP as a group action

- (Right) **group action** on equivalence class $[Q := B^T B]$ by $U \in \mathrm{GL}_d(\mathbb{Z})$:

$$U \circ Q \mapsto U^T Q U$$

- Group is **infinite** (not even compact!) and **non-commutative**.

  $\Rightarrow$ Can't sample 'uniformly' from $G = \mathrm{GL}_d(\mathbb{Z})$.

# LIP as a group action

- (Right) **group action** on equivalence class $[Q := B^T B]$ by $U \in \mathrm{GL}_d(\mathbb{Z})$:

$$U \circ Q \mapsto U^T Q U$$

- Group is **infinite** (not even compact!) and **non-commutative**.

  $\Rightarrow$ Can't sample 'uniformly' from $G = \mathrm{GL}_d(\mathbb{Z})$.
- Instead: sample image $Q' \leftarrow \mathcal{D}_\sigma([Q])$ **along with** uniform $U \in \mathrm{Isom}(Q, Q')$.

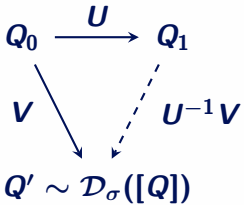
# LIP as a group action

- (Right) **group action** on equivalence class $[Q := B^T B]$ by $U \in \mathrm{GL}_d(\mathbb{Z})$:

$$U \circ Q \mapsto U^T Q U$$

- Group is **infinite** (not even compact!) and **non-commutative**.

  $\Rightarrow$ Can't sample 'uniformly' from $G = \mathrm{GL}_d(\mathbb{Z})$.
- Instead: sample image $Q' \leftarrow \mathcal{D}_\sigma([Q])$ **along with** uniform $U \in \mathrm{Isom}(Q, Q')$.
- ZKPoK [D**vW**21]:




$$(Q', V) \leftarrow \mathrm{Sample}_\sigma(Q_0)$$
$$\text{for } \sigma^2 \geq \tilde{\Omega}(\max\{\|\tilde{Q}_0\|, \|\tilde{Q}_1\|\})$$

# Mistakes to avoid

LIP does not give a standard cryptographic group action.

# Mistakes to avoid

LIP does not give a standard cryptographic group action.

- Alternatives to $(Q_1, U) \leftarrow \mathrm{Sample}_\sigma(Q_0)$ are typically **insecure**.

# Mistakes to avoid

LIP does not give a standard cryptographic group action.

- Alternatives to $(Q_1, U) \leftarrow \mathrm{Sample}_\sigma(Q_0)$ are typically **insecure**.

[BM21] **Never sample $U \in \mathrm{GL}_d(\mathbb{Z})$ first** (independent of $Q_0$).

# Mistakes to avoid

⚠ LIP does not give a standard cryptographic group action.

- Alternatives to $(Q_1, U) \leftarrow \mathrm{Sample}_\sigma(Q_0)$ are typically **insecure**.

[BM21] **Never sample $U \in \mathrm{GL}_d(\mathbb{Z})$ first** (independent of $Q_0$).

[BBCK24,BCDF25] **Never (re)use $U \in \mathrm{GL}_d(\mathbb{Z})$** on another $Q_2$. (~~WP~~)

# Mistakes to avoid

⚠ LIP does not give a standard cryptographic group action.

- Alternatives to $(Q_1, U) \leftarrow \mathrm{Sample}_\sigma(Q_0)$ are typically **insecure**.

[BM21] **Never sample $U \in \mathrm{GL}_d(\mathbb{Z})$ first** (independent of $Q_0$).

[BBCK24,BCDF25] **Never (re)use $U \in \mathrm{GL}_d(\mathbb{Z})$** on another $Q_2$. (~~WP~~)

Led to several **broken** constructions in group-action-based frameworks.

- See [NP26] for a more careful treaty of LIP as a group action.

# The Future of LIP?

# The Future of LIP?

Better lattices $\Rightarrow$ smaller keys and ciphertexts

# The Future of LIP?

Better lattices $\Rightarrow$ smaller keys and ciphertexts

Lattices with unique algorithmic properties?

# The Future of LIP?

Better lattices $\Rightarrow$ smaller keys and ciphertexts

Lattices with unique algorithmic properties?

Reductions: WC $\longrightarrow$ AC within any genus? (WIP)
LIP $\leftrightarrow$ $\boldsymbol{\Delta}$LIP?

# The Future of LIP?

Better lattices $\Rightarrow$ smaller keys and ciphertexts

Lattices with unique algorithmic properties?

Reductions: WC $\longrightarrow$ AC within any genus? (WIP)
LIP $\leftrightarrow$ $\mathbf{\Delta}$LIP?

Cryptanalysis: module-LIP,
stronger invariants & remarkable lattices

# The Future of LIP?

Better lattices $\Rightarrow$ smaller keys and ciphertexts

Lattices with unique algorithmic properties?

Reductions: WC $\longrightarrow$ AC within any genus? (WIP)
LIP $\leftrightarrow$ $\mathbf{\Delta}$LIP?

Cryptanalysis: module-LIP,
stronger invariants & remarkable lattices

Thank you!

# Bibliography (1/3)


[ABL25] Hollow LWE: A New Spin: Unbounded Updatable Encryption from LWE and PCE

[APMvW25] cryptanalysis of rank-2 module-LIP: a single real embedding is all it takes

[ARLW24] Public-key encryption from the lattice isomorphism problem

[HAWK23] HAWK https://hawk-sign.info/

[BDG23] Genus distribution of random q-ary lattices

[BGPSD23] Just How Hard Are Rotations of $\mathbb{Z}^n$? Algorithms and Cryptography with the Simplest Lattice

[BMM25] Fully-Homomorphic Encryption from Lattice Isomorphism

[BN24] Improved provable reduction of NTRU and hypercubic lattices

[BW25] Relating code equivalence to other isomorphism problems

[CBZIPC24] A concrete LIP-based KEM with simple lattices

[BLSD26] Advanced cryptography from lattice isomorphism—new constructions of IBE and FHE

# Bibliography (2/3)


[CM25] Ideally HAWKward: How Not to Break Module-LIP

[CMEPMPW25] A reduction from Hawk to the principal ideal problem in a quaternion algebra

[D23] Provable lattice reduction of with blocksize n/2

[DG23] Hull attacks on the lattice isomorphism problem

[DPPvW22] Hawk: Module LIP Makes Lattice Signatures Fast, Compact and Simple

[DvW22] On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography

[FH23] On the Quantum Security of HAWK

[JWLLGPW25] Re-randomize and extract: A novel commitment construction framework based on group actions

[LJPW24] Cryptanalysis of rank-2 module-LIP with symplectic automorphisms

[LGD26] RingSLIP: Ring Signatures from the Lattice Isomorphism Problem

[JL26] Exploiting the complexity of Lattice Isomorphism Problem via Irreducible Decomposition

# Bibliography (3/3)


[LJPW25] Commitment Schemes Based on Module-LIP

[LLM24] On the spinor genus and the distinguishing lattice isomorphism problem

[LRvW25] Beyond LWE: a Lattice Framework for Homomorphic Encryption

[M25] Special Genera of Hermitian Lattices and Applications to HAWK

[MPMPW24] Cryptanalysis of rank-2 module-lip in totally real number fields

[vG25] A note on the genus of the HAWK lattice

[vGP25] HAWK: Having Automorphisms Weakens Key

[vGvW25] A search to distinguish reduction for the isomorphism problem on direct sum lattices

[vW24] Dense and smooth lattices in any genus

[KS26] (Mis)using the Lattice Isomorphism Problem Cryptanalysis of the double-LIP and Construction of LIP-Based Blind Signatures

[NP26] Post-Quantum Anonymous Signatures from the Lattice Isomorphism Group Action