A Short Survey of Cryptography Based on the Lattice Isomorphism Problem

Wessel van Woerden (PQShield).

PQ SHIELD

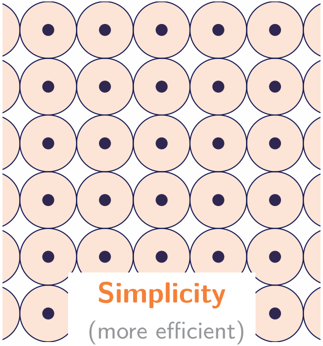
Motivation

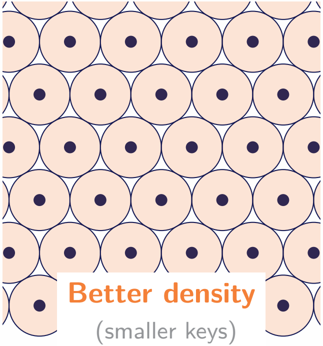
LWE, SIS, NTRU lattices: versatile, but poor geometry.

Motivation

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

Many remarkable lattices exist with great geometric properties.

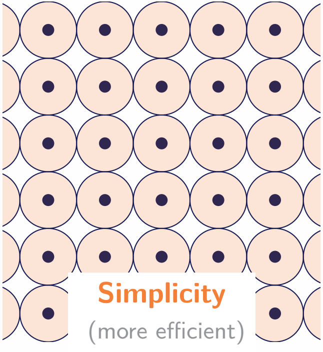


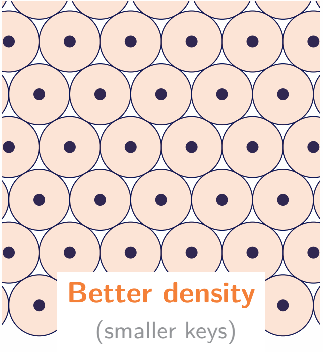


Motivation

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

Many remarkable lattices exist with great geometric properties.



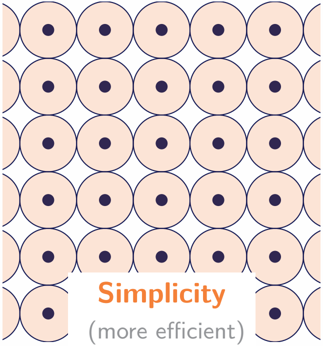


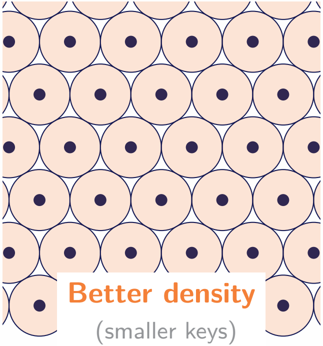
Can we use these in cryptography?

Motivation

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

Many remarkable lattices exist with great geometric properties.



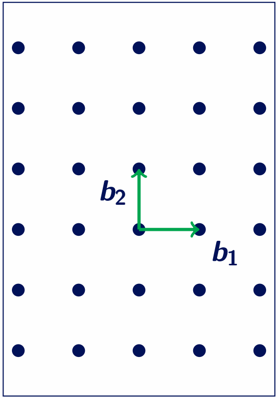


Can we use these in cryptography?

Lattice Isomorphism Problem: yes, we can!

Lattices and decoding

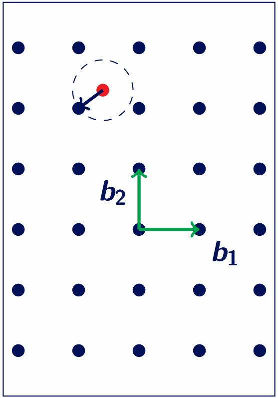
Lattice $\mathcal{L}(B) := \{\sum_i x_i b_i : x \in \mathbb{Z}^n\} \subset \mathbb{R}^n$



integer lattice $\mathbb{Z}^n$

Lattices and decoding

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

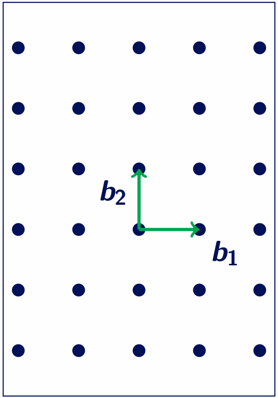


integer lattice $\mathbb{Z}^n$

decoding easy

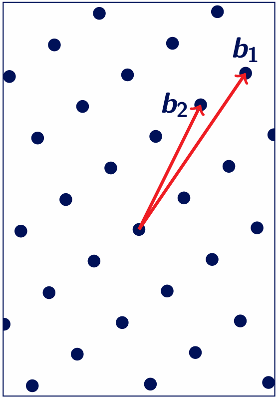
Lattices and decoding

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

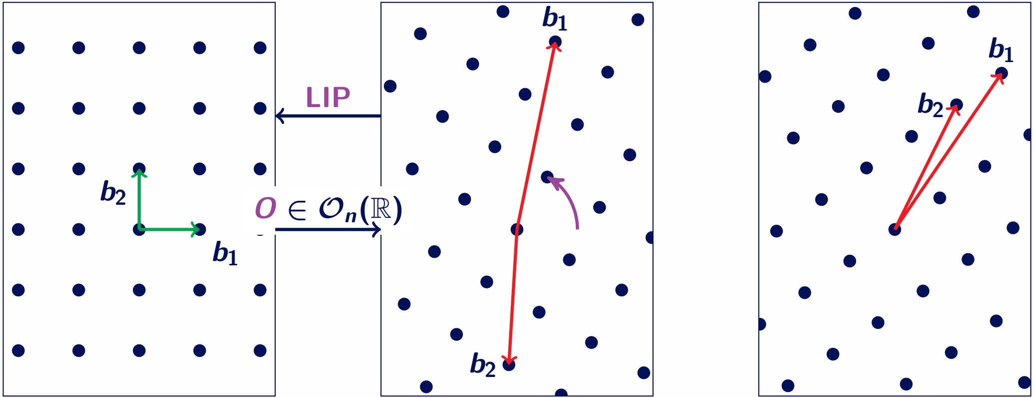


random lattice

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

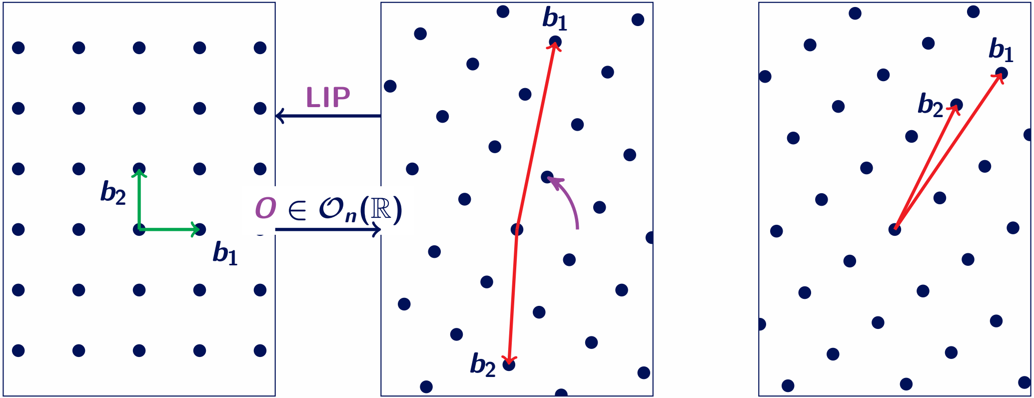
$\mathbb{Z}^n$ rotated

random lattice

decoding hard

Lattices and decoding

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



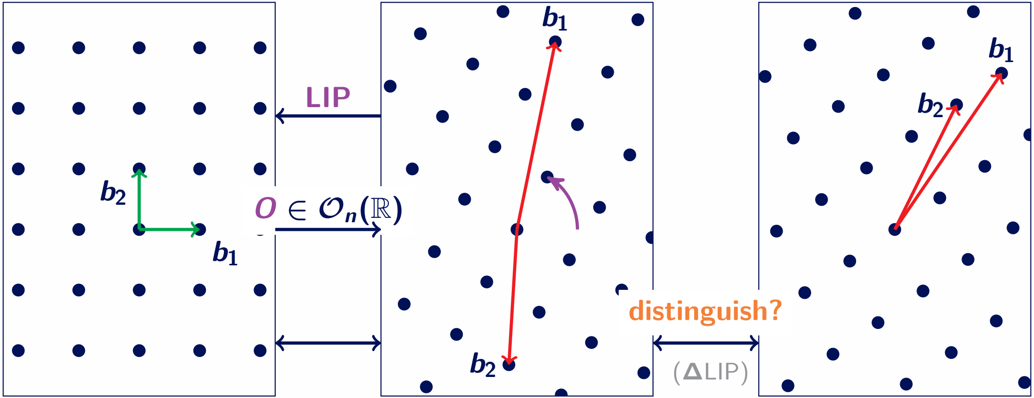
integer lattice $\mathbb{Z}^n$ — decoding easy

$\mathbb{Z}^n$ rotated — decoding hard?

random lattice — decoding hard

Lattices and decoding

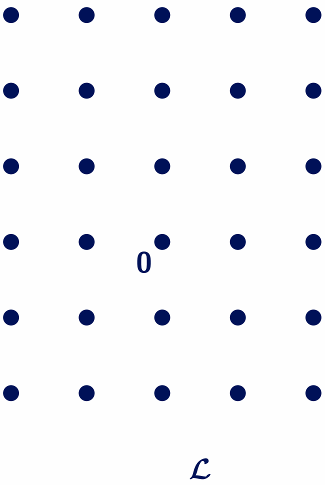
Lattice $\mathcal{L}(B) := \{\sum_i x_i b_i : x \in \mathbb{Z}^n\} \subset \mathbb{R}^n$



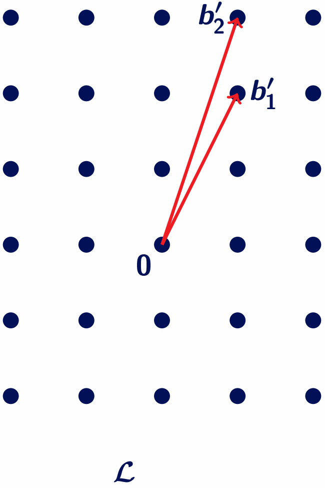
integer lattice $\mathbb{Z}^n$	$\mathbb{Z}^n$ rotated	random lattice
decoding easy	decoding hard?	decoding hard

Encryption scheme based on LIP

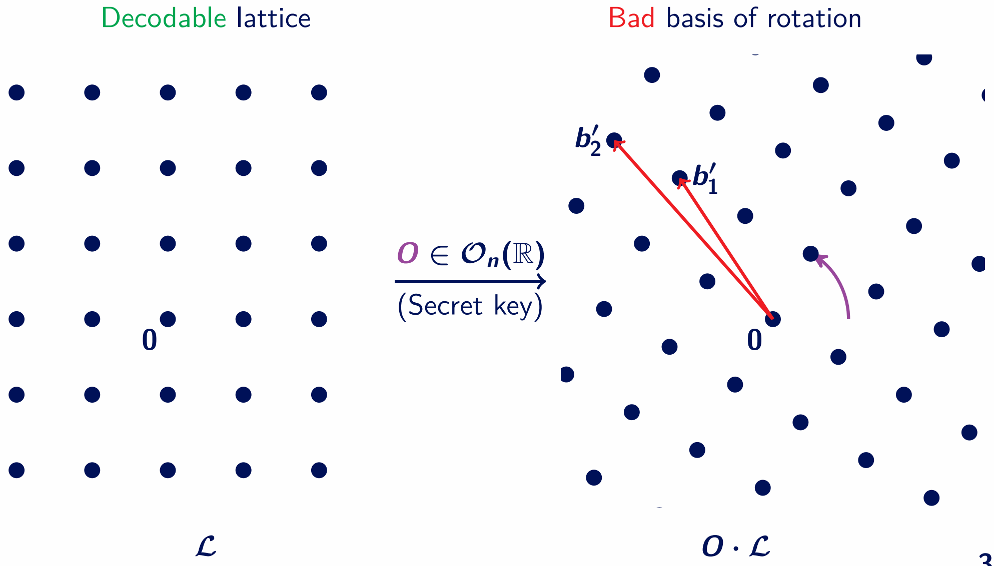
Decodable lattice



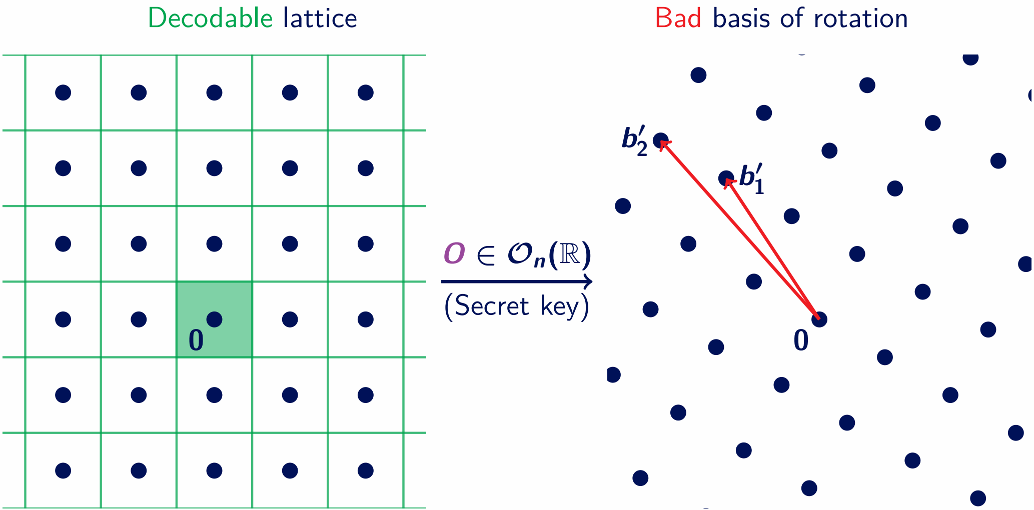
Bad basis of $\mathcal{L}$



Encryption scheme based on LIP



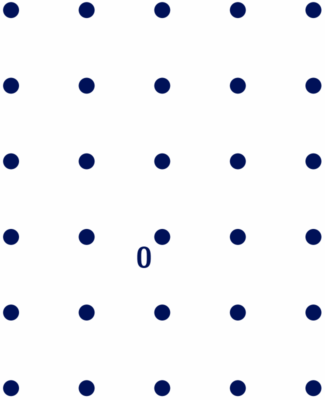
Encryption scheme based on LIP



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

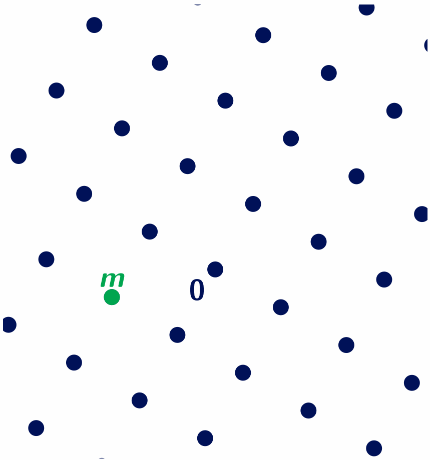
Encryption scheme based on LIP

Decodable lattice

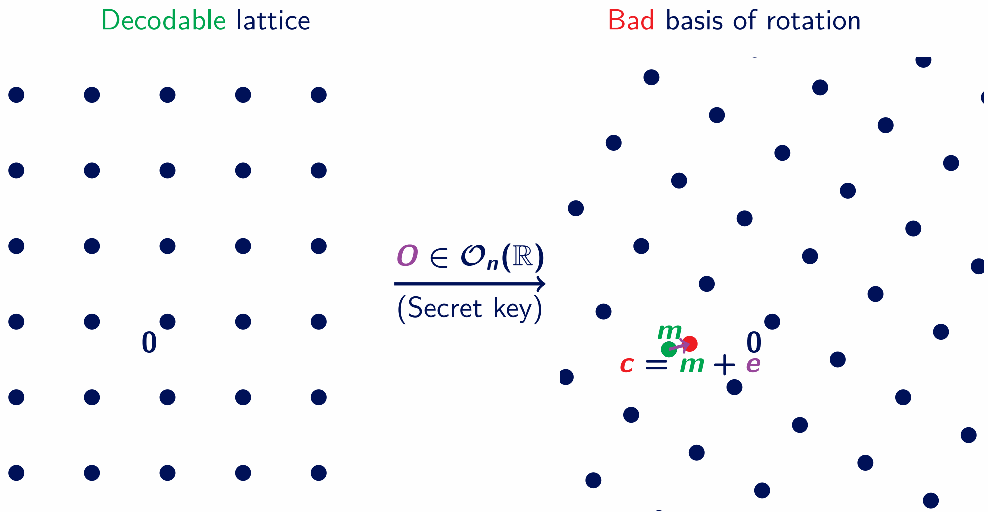


$$\xrightarrow[\text{(Secret key)}]{O \in \mathcal{O}_n(\mathbb{R})}$$

Bad basis of rotation

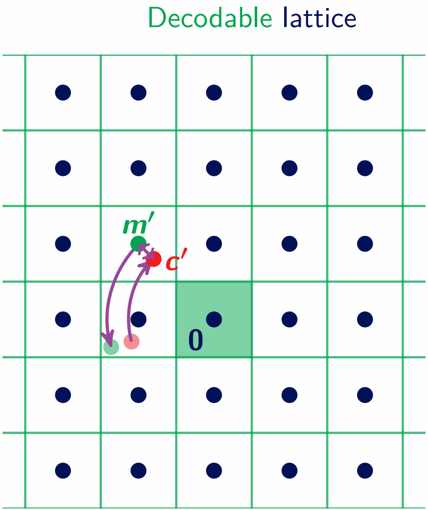


Encryption scheme based on LIP

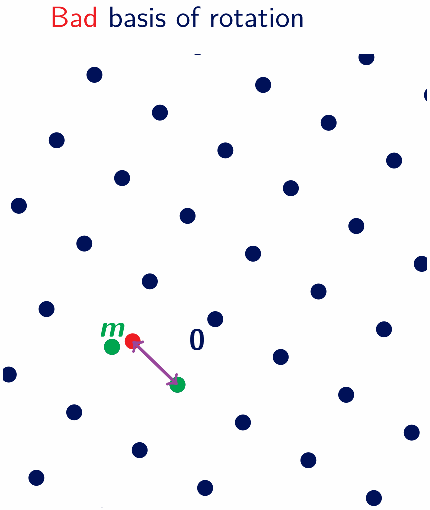


Encrypt by adding a small error

Encryption scheme based on LIP



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



Decrypt using decoding algorithm

The beginnings

On LIP, quadratic forms, remarkable lattices, and cryptography. [D**vW**22]

Identification Scheme
LIP

KEM&PKE
ΔLIP

Signature Scheme
ΔLIP

The beginnings

Just How Hard Are Rotations of $\mathbb{Z}^n$ [BGPSD23]

$\mathbf{1}$-bit PKE based on $\mathbf{\Delta}$LIP with $\mathbb{Z}^n$.

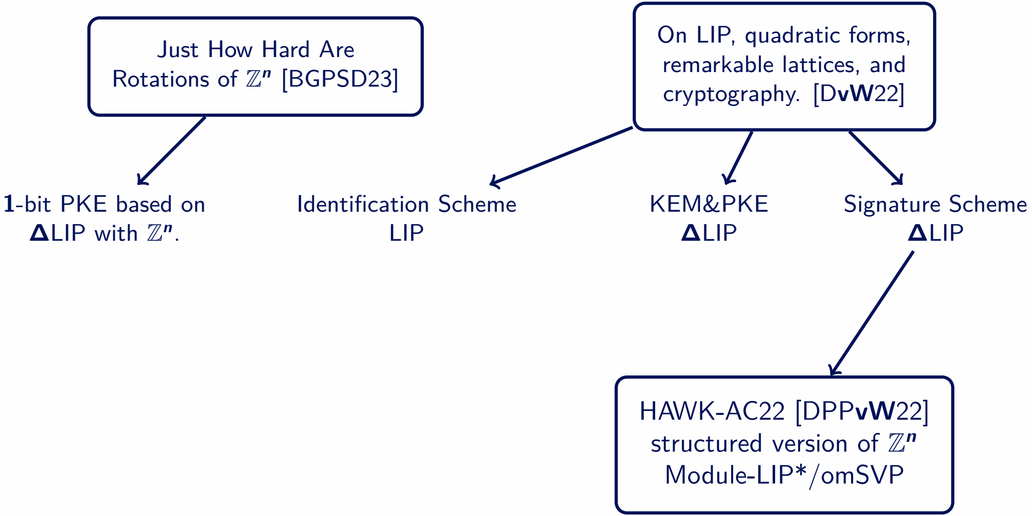
On LIP, quadratic forms, remarkable lattices, and cryptography. [D**vW**22]

Identification Scheme
LIP

KEM&PKE
$\mathbf{\Delta}$LIP

Signature Scheme
$\mathbf{\Delta}$LIP

The beginnings



The beginnings

Just How Hard Are Rotations of $\mathbb{Z}^n$ [BGPSD23]

On LIP, quadratic forms, remarkable lattices, and cryptography. [D**vW**22]

1-bit PKE based on **Δ**LIP with $\mathbb{Z}^n$.

Identification Scheme
LIP

KEM&PKE
ΔLIP

Signature Scheme
ΔLIP

HAWK-AC22 [DPP**vW**22]
structured version of $\mathbb{Z}^n$
Module-LIP*/omSVP

HAWK [HAWK23,FH23]
fast & compact & fp-free
NIST submission

Simplicity of $\mathbb{Z}^n$ + module-LIP*

$\Downarrow$

competitive signature scheme (vs FN-DSA!)

[1] On Ludo's Laptop

Simplicity of $\mathbb{Z}^n$ + module-LIP*

$\Downarrow$

competitive signature scheme (vs FN-DSA!)

Fast:	KeyGen: **3.5** ms[1]	Sign/Verify: $<$ **0.1** ms
Compact:	$\|$🔑$_{\text{pub}}\| =$ **1024** bytes	$\|\text{sig}\| =$ **555** bytes
Hardware friendly:	$\leq$ **12**KiB RAM	no *float*/*double*

[1]On Ludo's Laptop

Simplicity of $\mathbb{Z}^n$ + module-LIP*

$\Downarrow$

competitive signature scheme (vs FN-DSA!)

Fast:	KeyGen: **3.5** ms[1]	Sign/Verify: $<$ **0.1** ms
Compact:	|🔑$_{\text{pub}}$| = **1024** bytes	|sig| = **555** bytes
Hardware friendly:	$\leq$ **12**KiB RAM	no *float*/*double*

Team from academia and industry: Joppe W. Bos, Olivier Bronchain, Léo Ducas, Serge Fehr, Yu-Hsuan Huang, Thomas Pornin, Eamonn W. Postlethwaite, Thomas Prest, Ludo N. Pulles, **vW**

Only lattice scheme in round **2** of NIST call for additional signature schemes.

[1] On Ludo's Laptop

HAWK - a Signature Scheme from $\mathbb{Z}^n$

Simplicity of $\mathbb{Z}^n$ + module-LIP*

$\Downarrow$

competitive signature scheme (vs FN-DSA!)

Fast:	KeyGen: **3.5** ms[1]	Sign/Verify: $<$ **0.1** ms
Compact:	$\lvert$ 🔑$_{\text{pub}}\rvert$ = **1024** bytes	$\lvert\text{sig}\rvert$ = **555** bytes
Hardware friendly:	$\leq$ **12**KiB RAM	no *float*/*double*

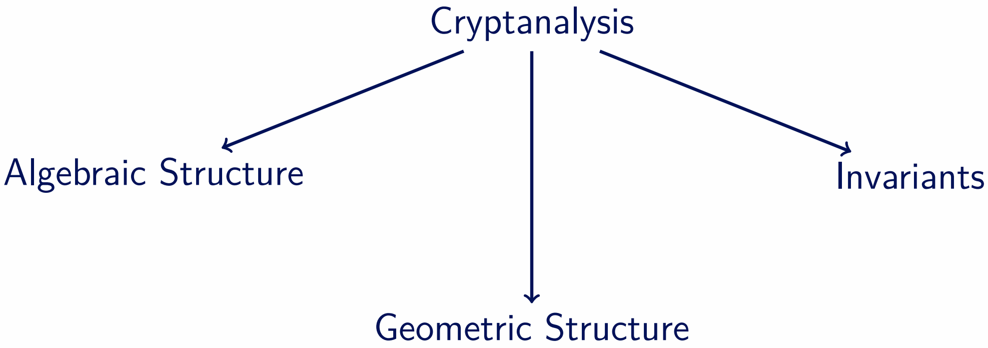
Team from academia and industry: Joppe W. Bos, Olivier Bronchain, Léo Ducas, Serge Fehr, Yu-Hsuan Huang, Thomas Pornin, Eamonn W. Postlethwaite, Thomas Prest, Ludo N. Pulles, **vW**

Only lattice scheme in round **2** of NIST call for additional signature schemes.

[1] On Ludo's Laptop

PQC forum Sept. 12:
'HAWK is a very cool scheme'

Cryptanalysis



Cryptanalysis

Cryptanalysis

Algebraic Structure

rank 2 attacks

(symplectic) automorphisms

[LJPW24,vGP25]

Geometric Structure

Invariants

Cryptanalysis

Cryptanalysis

Algebraic Structure

rank 2 attacks

(symplectic) automorphisms

[LJPW24,vGP25]

Geometric Structure

hull attacks [DG23]

provable reduction [D23,BN24]

Search to distinguish [vG**vW**25]

Invariants

Cryptanalysis

Cryptanalysis

Algebraic Structure

rank 2 attacks

(symplectic) automorphisms [LJPW24,vGP25]

Geometric Structure

hull attacks [DG23]

provable reduction [D23,BN24]

Search to distinguish [vG**vW**25]

Invariants

algebraic genus

special/spinor genus

Algebraic Structure

Cryptography is a trade-off between $\underbrace{\text{efficiency}}_{\text{structure}}$ and security

Algebraic Structure

Cryptography is a trade-off between $\underbrace{\text{efficiency}}_{\text{structure}}$ and security

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

Algebraic Structure

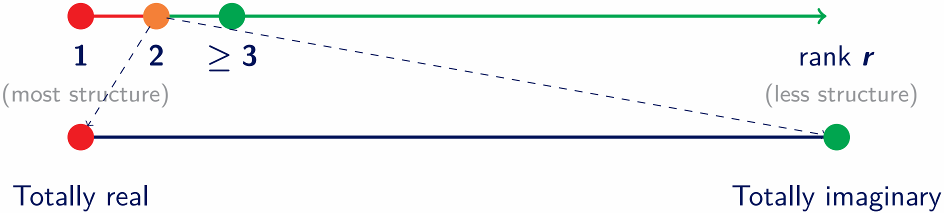
Cryptography is a trade-off between $\underbrace{\text{efficiency}}_{\text{structure}}$ and security

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

Cryptography is a trade-off between efficiency and security
(efficiency ⟶ structure)

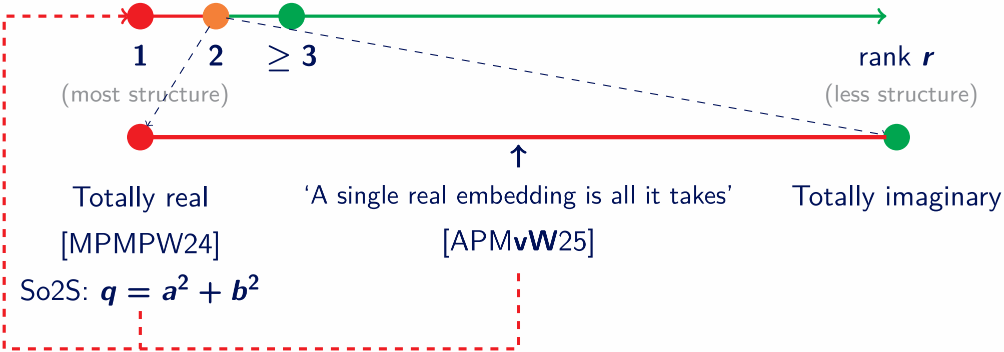
Module-LIP: replace $\mathcal{L} = B \cdot \mathbb{Z}^n$ by $\mathcal{L} = B \cdot O_K^r$ for ring of integers O_K.



Algebraic Structure

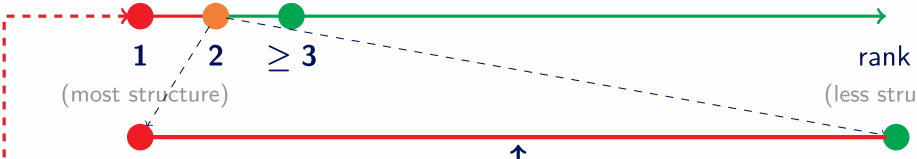
Cryptography is a trade-off between efficiency (structure) and security

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



Cryptography is a trade-off between $\underbrace{\text{efficiency}}_{\text{structure}}$ and security

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]

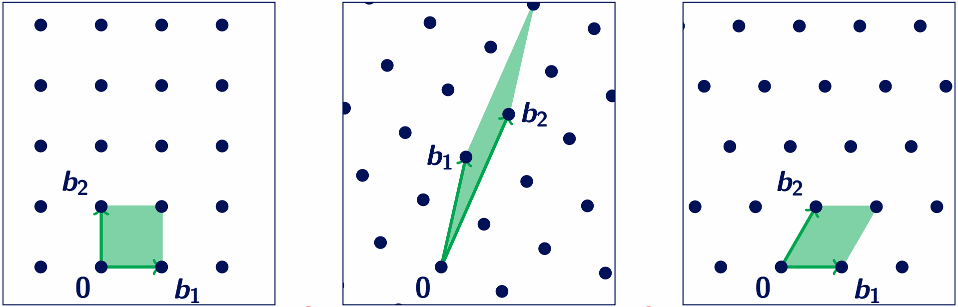
Totally imaginary

HAWK (CM field)

[CMEPMPW25,CM25]:

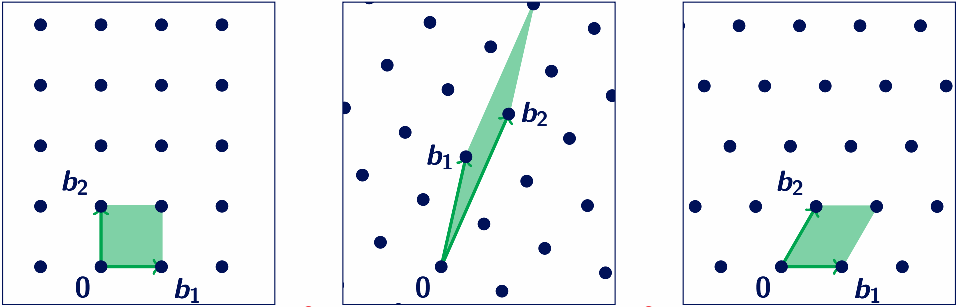
So4S: $q = a^2 + b^2 + c^2 + d^2$

attack does not work



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

Invariants

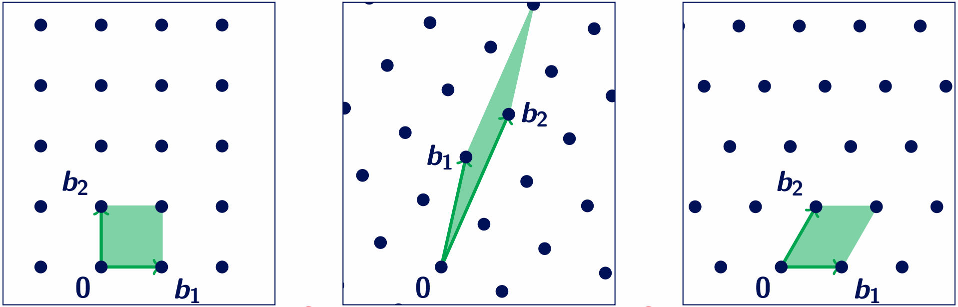


$\det(\mathcal{L}_1) \stackrel{?}{=} \det(O \cdot \mathcal{L}_b) \stackrel{?}{=} \det(\mathcal{L}_2)$

Lemma:

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

Invariants



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

Lemma:

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

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

Genus Invariant

[BDG23] SIS lattices concentrate in only two genera.

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

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

Genus Invariant

[BDG23] SIS lattices concentrate in only two genera.

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

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

Module structure + Genus?

[LLM24] **Spinor genus** stronger when rank $\boldsymbol{r} = \mathbf{2}$ and totally real.

[vG25] $> \mathbf{2^{1050}}$ module lattices have the same genus as HAWK.

[M25] $> \mathbf{2^{850}}$ module lattices have the same **special genus** as HAWK.

Genus Invariant

[BDG23] SIS lattices concentrate in only two genera.

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

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

Module structure + Genus?

[LLM24] **Spinor genus** stronger when rank $r = 2$ and totally real.

[vG25] $> 2^{1050}$ module lattices have the same genus as HAWK.

[M25] $> 2^{850}$ module lattices have the same **special genus** as HAWK.

Conclusion: invariants do not seem to affect security.

Constructions

KEM&PKEs

$\mathbb{Z}^{\boldsymbol{n}}$ or $\mathrm{BW}_{\boldsymbol{n}} + \boldsymbol{\Delta}$LIP

[ARLW24,CBZIPC24]

Constructions

KEM&PKEs

$\mathbb{Z}^{\boldsymbol{n}}$ or $\mathrm{BW}_{\boldsymbol{n}} + \boldsymbol{\Delta}$LIP

[ARLW24,CBZIPC24]

Various **Commitment Schemes**

LIP (group action)

[JWLLGPW25,LJPW25]

Constructions

KEM&PKEs

$\mathbb{Z}^n$ or $\mathsf{BW}_n + \Delta$LIP

[ARLW24,CBZIPC24]

Various **Commitment Schemes**

LIP (group action)

[JWLLGPW25,LJPW25]

Unbounded Updatable Encryption

ΔPCE [ABL25] or ΔLIP (WIP)

Constructions

KEM&PKEs

$\mathbb{Z}^n$ or $\mathrm{BW}_n + \mathbf{\Delta}$LIP

[ARLW24,CBZIPC24]

Various **Commitment Schemes**

LIP (group action)

[JWLLGPW25,LJPW25]

Unbounded Updatable Encryption

ΔPCE [ABL25] or **Δ**LIP (WIP)

Fully Homomorphic Encryption

ΔLIP [BMM25,LR**vW**25]

Constructions

KEM&PKEs

$\mathbb{Z}^n$ or BW_n + **Δ**LIP

[ARLW24,CBZIPC24]

Various **Commitment Schemes**

LIP (group action)

[JWLLGPW25,LJPW25]

Unbounded Updatable Encryption

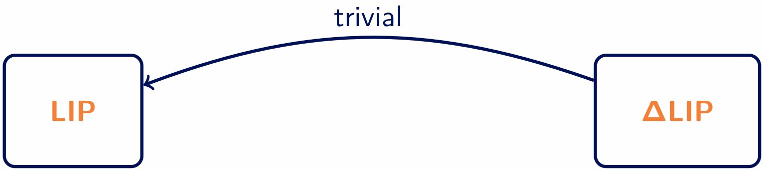
ΔPCE [ABL25] or **Δ**LIP (WIP)

Fully Homomorphic Encryption

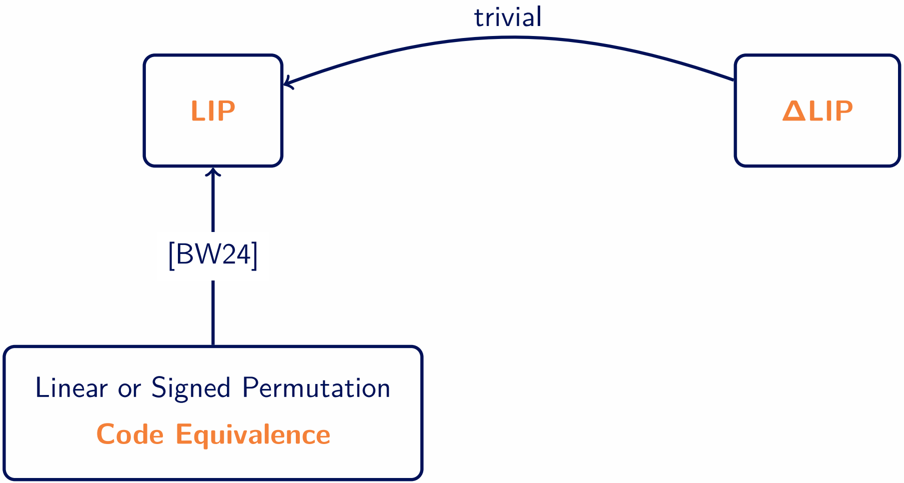
ΔLIP [BMM25,LR**vW**25]

Allows for **Advanced Cryptographic Constructions**

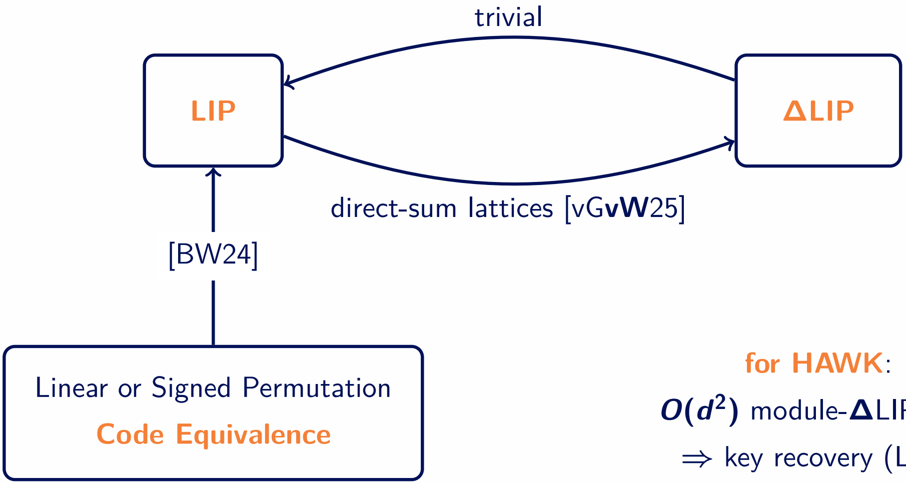
Reductions



Reductions


trivial
LIP
ΔLIP
[BW24]
Linear or Signed Permutation
Code Equivalence

Reductions



for HAWK:

$O(d^2)$ module-**Δ**LIP calls

$\Rightarrow$ key recovery (LIP).

The Future of LIP?

LIP+$\mathbb{Z}^n$ is enough to **match and improve** on LWE and NTRU.

The Future of LIP?

LIP+$\mathbb{Z}^n$ is enough to **match and improve** on LWE and NTRU.

Better lattices $\Rightarrow$ smaller keys and ciphertexts

The Future of LIP?

LIP+$\mathbb{Z}^n$ is enough to **match and improve** on LWE and NTRU.

Better lattices $\Rightarrow$ smaller keys and ciphertexts

Reductions: WC $\rightarrow$ AC within genus?

LIP $\leftrightarrow$ ΔLIP?

The Future of LIP?

LIP+$\mathbb{Z}^n$ is enough to **match and improve** on LWE and NTRU.

Better lattices $\Rightarrow$ smaller keys and ciphertexts

Reductions: WC $\rightarrow$ AC within genus?
LIP $\leftrightarrow$ ΔLIP?

Cryptanalysis: module-LIP & remarkable lattices

The Future of LIP?

LIP+$\mathbb{Z}^n$ is enough to **match and improve** on LWE and NTRU.

Better lattices $\Rightarrow$ smaller keys and ciphertexts

Reductions: WC $\rightarrow$ AC within genus?
LIP $\leftrightarrow$ ΔLIP?

Cryptanalysis: module-LIP & 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

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

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