WCC presentation:

Public-key encryption from the lattice isomorphism problem

Presenting **Léo Ackermann** (CNRS, Greyc, Caen)
Joint work with Adeline Roux-Langlois (CNRS, Greyc, Caen)
Alexandre Wallet (Inria, Capsule, Rennes)[1]

[1] Now at PQShield

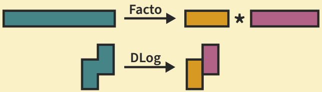
17th June 2024

Lattice-based cryptography

A strong candidate for post-quantum crypto

Cryptographic threat posed by quantum computers

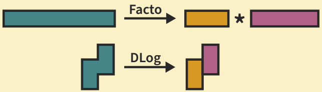
- Shor's algorithm solves the **discrete log** and **factorisation** problems in quantum polynomial time.
- The advent of reasonable quantum computers would **break current cryptosystems** (ECC, RSA).



A strong candidate for post-quantum crypto

Cryptographic threat posed by quantum computers

- Shor's algorithm solves the **discrete log** and **factorisation** problems in quantum polynomial time.
- The advent of reasonable quantum computers would **break current cryptosystems** (ECC, RSA).



The NIST competition (2016 → 2022)

Three out of four of the first standardized algorithms **rely on lattices**.

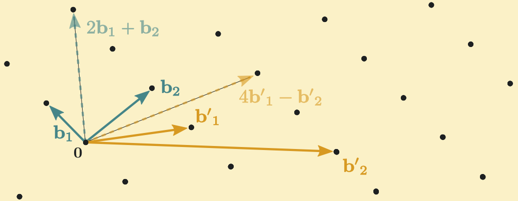
Encryption	Signature
• Crystals-Kyber	• Crystals-Dilithium • Falcon • SPHINCS+

Many lattice-based (and code-based) proposals within the the **extra-round** for **signatures**.

First principles of lattice-based crypto

Euclidean lattices

A lattice Λ is a discrete additive subgroup of $\mathbb{R}^n$.
It can always be written $\Lambda(\boldsymbol{B}) = \sum_i \boldsymbol{b}_i \mathbb{Z}$.

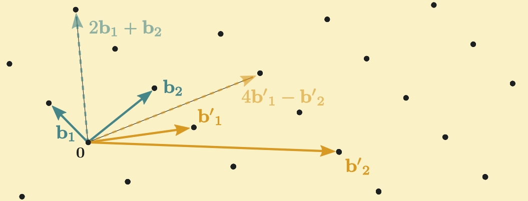


The bases are not unique, eg. $\Lambda(\boldsymbol{B}) = \Lambda(\boldsymbol{B})$.

First principles of lattice-based crypto

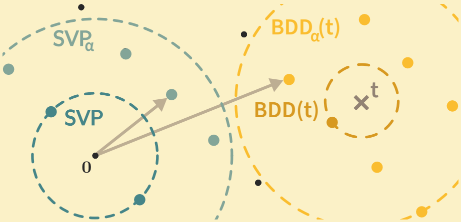
Euclidean lattices

A lattice Λ is a discrete additive subgroup of $\mathbb{R}^n$.
It can always be written $\Lambda(\boldsymbol{B}) = \sum_i \boldsymbol{b}_i\mathbb{Z}$.



The bases are not unique, eg. $\Lambda(\boldsymbol{B}) = \Lambda(\boldsymbol{B})$.

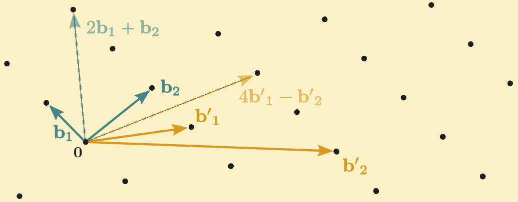
Hard lattice problems



First principles of lattice-based crypto

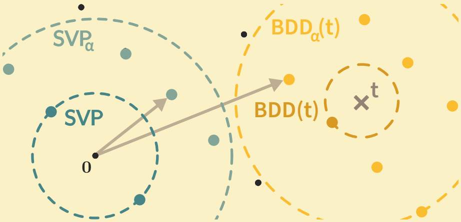
Euclidean lattices

A lattice Λ is a discrete additive subgroup of $\mathbb{R}^n$.
It can always be written $\Lambda(\boldsymbol{B}) = \sum_i \boldsymbol{b}_i \mathbb{Z}$.



The bases are not unique, eg. $\Lambda(\boldsymbol{B}) = \Lambda(\boldsymbol{B})$.

Hard lattice problems



Computational hardness

- $\alpha \in \omega(\sqrt{n}) \Rightarrow \texttt{runtime} \in 2^{\Omega(n)}$.
- $\alpha \in 2^{\Omega(n)} \Rightarrow \texttt{runtime} \in poly(n)$.

Cryptographic assumption

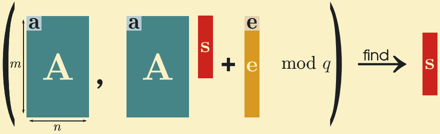
- $\alpha \in poly(n) \Rightarrow \texttt{runtime} \in 2^{\Omega(n)}$.

Lattice-based crypto, legacy approach

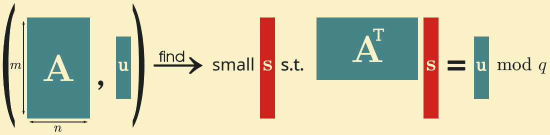
$$\begin{cases} a_{1,1}s_1 & + & \cdots & + & a_{1,n}s_n & = & b_1 \\ \vdots & + & \ddots & + & \vdots & = & \vdots \\ a_{m,1}s_1 & + & \cdots & + & a_{m,n}s_n & = & b_m \end{cases}$$

Lattice-based crypto, legacy approach

Learning With Errors (LWE)



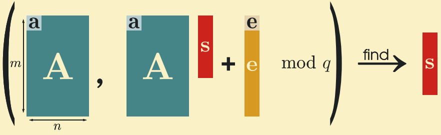
Inhomogeneous Short Integer Solution (ISIS)



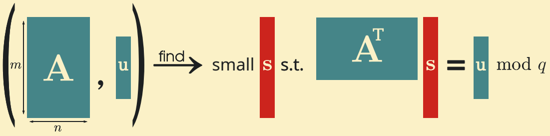
$$\begin{cases} a_{1,1}s_1 & + & \cdots & + & a_{1,n}s_n & = & b_1 \\ \vdots & + & \ddots & + & \vdots & = & \vdots \\ a_{m,1}s_1 & + & \cdots & + & a_{m,n}s_n & = & b_m \end{cases}$$

Lattice-based crypto, legacy approach

Learning With Errors (LWE)



Inhomogeneous Short Integer Solution (ISIS)



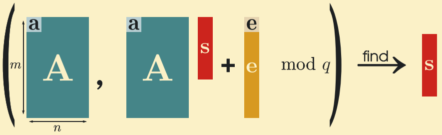
↔ Hardness of LWE and ISIS

Those problems enjoy **worst-case average-case reductions** from hard lattice problems, namely **SVP** and **BDD**.

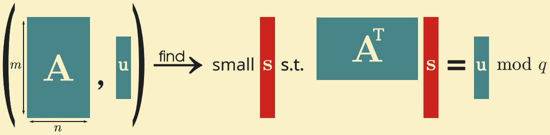
- LWE $\equiv$ Bounded Distance Decoding over
  $$\Lambda = \{\mathbf{x} \in \mathbb{Z}^m \mid \exists \mathbf{s} \in \mathbb{Z}, \mathbf{x} = \mathbf{A}\mathbf{s} \mod q\}.$$
- ISIS $\equiv$ Shortest Vector Problem over
  $$\Lambda = \{\mathbf{s} \in \mathbb{Z}^m \mid \mathbf{A}^\mathsf{T}\mathbf{s} = \mathbf{u} \mod q\}.$$

Lattice-based crypto, legacy approach

Learning With Errors (LWE)



Inhomogeneous Short Integer Solution (ISIS)



⟷ Hardness of LWE and ISIS

Those problems enjoy **worst-case average-case reductions** from hard lattice problems, namely **SVP** and **BDD**.

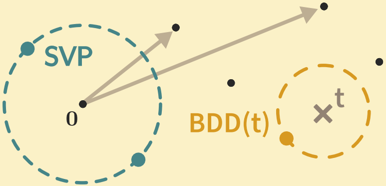
- LWE $\equiv$ Bounded Distance Decoding over
  $\Lambda = \{\mathbf{x} \in \mathbb{Z}^m \mid \exists \mathbf{s} \in \mathbb{Z}, \mathbf{x} = \mathbf{A}\mathbf{s} \mod q\}$.
- ISIS $\equiv$ Shortest Vector Problem over
  $\Lambda = \{\mathbf{s} \in \mathbb{Z}^m \mid \mathbf{A}^\top \mathbf{s} = \mathbf{u} \mod q\}$.

Large variety of constructions

Ranging from simple **encryption** or digital **signature** scheme to **anonymous credentials** and **fully homomorphic encryption**.

Breaking lattice-based crypto

Attacking fundamental lattice problems



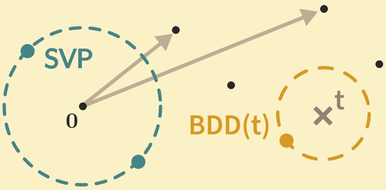
SVP Find the *shortest* non-zero vector, of length $\lambda_1(\Lambda) := \min_{\Lambda \setminus \{0\}} \|x\|_2$.

BDD Find v, given a target $t = v + e$, with $v \in \Lambda$ and $\|e\| \leq \lambda_1(\Lambda)/2$.

The **concrete hardness** of those problems is driven by the **gap** $gap(\Lambda)$ between the **actual shortest length** and the upper bound given by **Gaussian heuristics**.

Breaking lattice-based crypto

Attacking fundamental lattice problems



SVP Find the *shortest* non-zero vector, of length $\lambda_1(\Lambda) := \min_{\Lambda \setminus \{0\}} \|x\|_2$.

BDD Find v, given a target $t = v + e$, with $v \in \Lambda$ and $\|e\| \leq \lambda_1(\Lambda)/2$.

The **concrete hardness** of those problems is driven by the **gap** $gap(\Lambda)$ between the **actual shortest length** and the upper bound given by **Gaussian heuristics**.

Deceptive aspect of lattice-based crypto

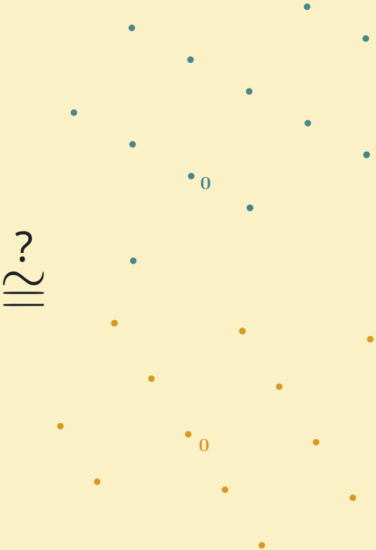
LWE-lattice: $gap(\Lambda) \geq \Omega(\sqrt{n})$. Prime-lattice: $gap(\Lambda) = \Theta(\log(n))$.

Hypotheses on **random lattices** and subsequent constructions **barely connect** with the luxuriant litterature on **remarkable lattices**.

Public-key encryption from LIP

The lattice isomorphism problem (LIP)

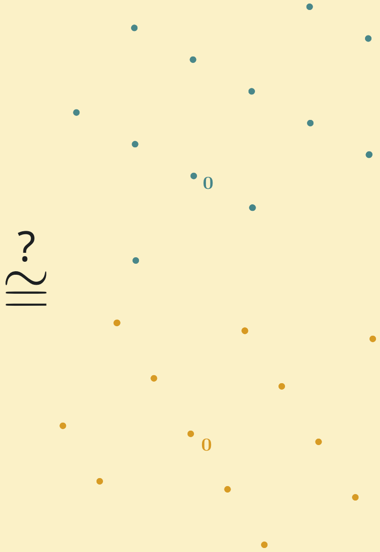
The lattice isomorphism problem (LIP)



Flavours of lattice isomorphisms

- (Unpractical) Given Λ and Λ', find (if any) $O \in \mathcal{O}(\mathbb{R}^n)$ such that $\Lambda = O \cdot \Lambda'$.

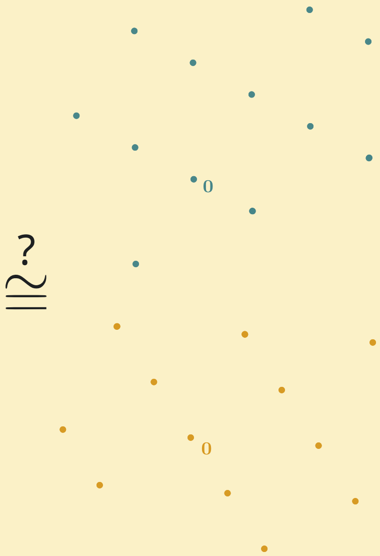
The lattice isomorphism problem (LIP)



Flavours of lattice isomorphisms

- (Unpractical) Given Λ and Λ', find (if any) $O \in \mathcal{O}(\mathbb{R}^n)$ such that $\Lambda = O \cdot \Lambda'$.
- (Search var.) Given $\mathbf{B}$ and $\mathbf{B'}$, find (if any) $O \in \mathcal{O}(\mathbb{R}^n)$ such that $\mathbf{B} = O \cdot \mathbf{B'}$.

The lattice isomorphism problem (LIP)



Flavours of lattice isomorphisms

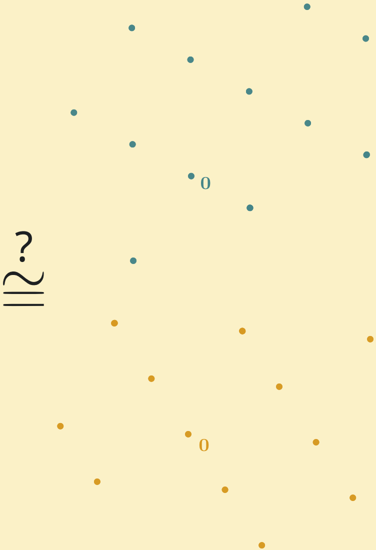
- (Unpractical) Given Λ and Λ', find (if any) $O \in \mathcal{O}(\mathbb{R}^n)$ such that $\Lambda = O \cdot \Lambda'$.
- (Search var.) Given $\boldsymbol{B}$ and $\boldsymbol{B'}$, find (if any) $O \in \mathcal{O}(\mathbb{R}^n)$, $U \in GL(\mathbb{Z}^n)$ such that $\boldsymbol{B} = O \cdot \boldsymbol{B'} \cdot U$.

The lattice isomorphism problem (LIP)

Flavours of lattice isomorphisms

- (Unpractical) Given Λ and Λ', find (if any) $O \in \mathcal{O}(\mathbb{R}^n)$ such that $\Lambda = O \cdot \Lambda'$.
- (Search var.) Given $\boldsymbol{B}$ and $\boldsymbol{B'}$, find (if any) $O \in \mathcal{O}(\mathbb{R}^n)$, $U \in GL(\mathbb{Z}^n)$ such that $\boldsymbol{B} = O \cdot \boldsymbol{B'} \cdot U$.
- (Decision var., dLIP) Given $\boldsymbol{B}$ and $\boldsymbol{B'}$, decide whether $\Lambda(\boldsymbol{B}) \cong \Lambda(\boldsymbol{B'})$ or not.

The lattice isomorphism problem (LIP)

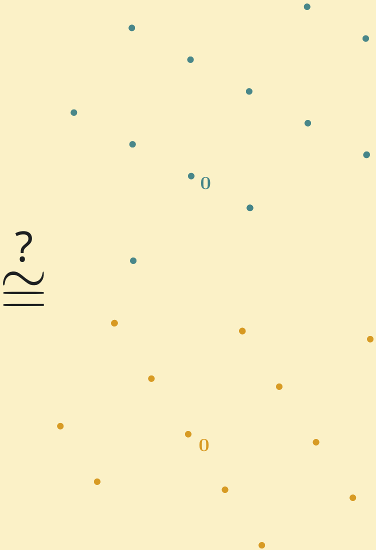


Flavours of lattice isomorphisms

- (Unpractical) Given Λ and Λ', find (if any) $O \in \mathcal{O}(\mathbb{R}^n)$ such that $\Lambda = O \cdot \Lambda'$.
- (Search var.) Given $\boldsymbol{B}$ and $\boldsymbol{B'}$, find (if any) $O \in \mathcal{O}(\mathbb{R}^n)$, $U \in GL(\mathbb{Z}^n)$ such that $\boldsymbol{B} = O \cdot \boldsymbol{B'} \cdot U$.
- (Decision var., dLIP) Given $\boldsymbol{B}$ and $\boldsymbol{B'}$, decide whether $\Lambda(\boldsymbol{B}) \cong \Lambda(\boldsymbol{B'})$ or not.

- (Distinguish var., ΔLIP) Given $\boldsymbol{B}$, $\boldsymbol{B_0}$ and $\boldsymbol{B_1}$, decide whether $\Lambda(\boldsymbol{B}) \cong \Lambda(\boldsymbol{B_0})$ or $\Lambda(\boldsymbol{B}) \cong \Lambda(\boldsymbol{B_1})$.

The lattice isomorphism problem (LIP)



Flavours of lattice isomorphisms

- (Unpractical) Given Λ and Λ', find (if any) $O \in \mathcal{O}(\mathbb{R}^n)$ such that $\Lambda = O \cdot \Lambda'$.
- (Search var.) Given $\boldsymbol{B}$ and $\boldsymbol{B'}$, find (if any) $O \in \mathcal{O}(\mathbb{R}^n)$, $U \in GL(\mathbb{Z}^n)$ such that $\boldsymbol{B} = O \cdot \boldsymbol{B'} \cdot U$.
- (Decision var., dLIP) Given $\boldsymbol{B}$ and $\boldsymbol{B'}$, decide whether $\Lambda(\boldsymbol{B}) \cong \Lambda(\boldsymbol{B'})$ or not.
- (Distinguish var., ΔLIP) Given $\boldsymbol{B}$, $\boldsymbol{B_0}$ and $\boldsymbol{B_1}$, decide whether $\Lambda(\boldsymbol{B}) \cong \Lambda(\boldsymbol{B_0})$ or $\Lambda(\boldsymbol{B}) \cong \Lambda(\boldsymbol{B_1})$.

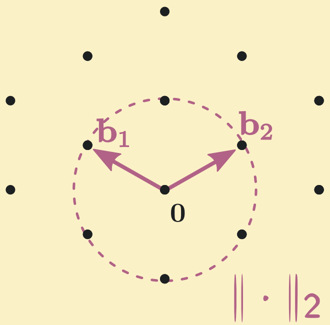
LIP hardness

LIP benefits from **worst-case average-case** self-reduction within an instantiation class, and its **connection with the graph isomorphism problem** accounts for its assumed hardness.

LIP-based crypto

LIP flavours

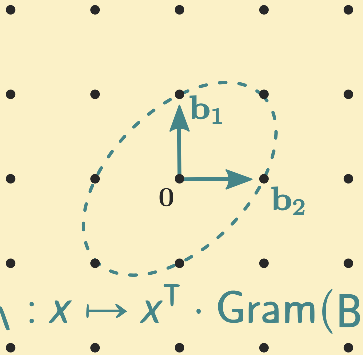
- The **public key** consists in any lattice Λ and a basis $\boldsymbol{B}$ of $O \cdot \Lambda$.
  The **secret key** is the rotation O.



LIP-based crypto

LIP flavours

- The **public key** consists in quadratic forms (Q, Q') such that $Q' = U^{\mathsf{T}} Q U$ for $U \in \mathrm{GL}_n(\mathbb{Z})$. The **secret key** is U.



$$\|\cdot\|_\Lambda : x \mapsto x^{\mathsf{T}} \cdot \mathrm{Gram}(B) \cdot x$$

where $\mathrm{Gram}(\mathbf{B}) = \mathbf{B}^{\mathsf{T}}\mathbf{B}$.

LIP-based crypto

LIP flavours

- The **public key** consists in quadratic forms (Q, Q') such that $Q' = U^\top Q U$ for $U \in \mathrm{GL}_n(\mathbb{Z})$. The **secret key** is U.
- LIP-based schemes can be instantiated with geometry of **remarkable lattices** (root systems, Barnes-Wall, $\mathbb{Z}^n, \ldots$): smaller gaps, **better algorithms**.

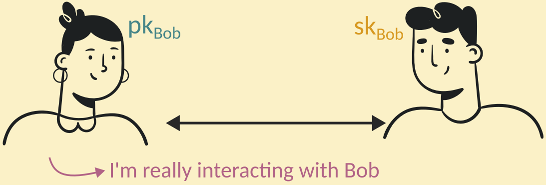
LIP-based crypto

LIP flavours

- The **public key** consists in quadratic forms (Q, Q') such that $Q' = U^\top QU$ for $U \in \mathrm{GL}_n(\mathbb{Z})$. The **secret key** is U.
- LIP-based schemes can be instantiated with geometry of **remarkable lattices** (root systems, Barnes-Wall, $\mathbb{Z}^n, \ldots$): smaller gaps, **better algorithms**.

Existing constructions

- Authentication scheme



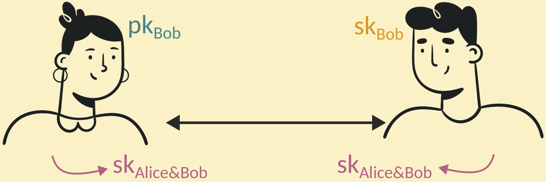
LIP-based crypto

LIP flavours

- The **public key** consists in quadratic forms (Q, Q') such that $Q' = U^\top Q U$ for $U \in \mathrm{GL}_n(\mathbb{Z})$. The **secret key** is U.
- LIP-based schemes can be instantiated with geometry of **remarkable lattices** (root systems, Barnes-Wall, $\mathbb{Z}^n, \ldots$): smaller gaps, **better algorithms**.

Existing constructions

- Authentication scheme
- Key-encapsulation mecanism



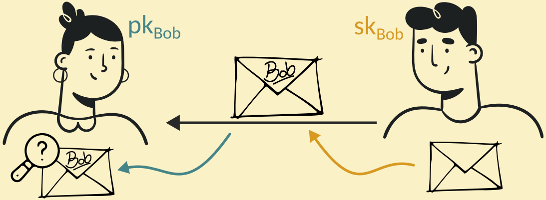
LIP-based crypto

LIP flavours

- The **public key** consists in quadratic forms (Q, Q') such that $Q' = U^\top QU$ for $U \in \mathrm{GL}_n(\mathbb{Z})$. The **secret key** is U.
- LIP-based schemes can be instantiated with geometry of **remarkable lattices** (root systems, Barnes-Wall, $\mathbb{Z}^n, \ldots$): smaller gaps, **better algorithms**.

Existing constructions

- Authentication scheme
- Key-encapsulation mecanism
- Signature (including Hawk submission)



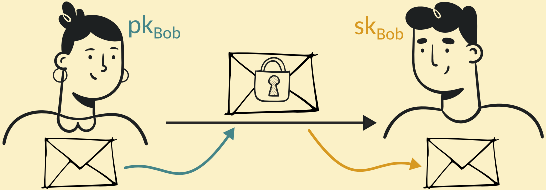
LIP-based crypto

LIP flavours

- The **public key** consists in quadratic forms (Q, Q') such that $Q' = U^\top Q U$ for $U \in \mathrm{GL}_n(\mathbb{Z})$. The **secret key** is U.
- LIP-based schemes can be instantiated with geometry of **remarkable lattices** (root systems, Barnes-Wall, $\mathbb{Z}^n, \ldots$): smaller gaps, **better algorithms**.

Existing constructions

- Authentication scheme
- Key-encapsulation mecanism
- Signature (including Hawk submission)



A missing primitive

We propose the first **direct construction** of a PKE relying on **LIP**.

LIP-based public-key encryption scheme

High-level idea

Follows **Dual-Regev** cryptosystem flavour:

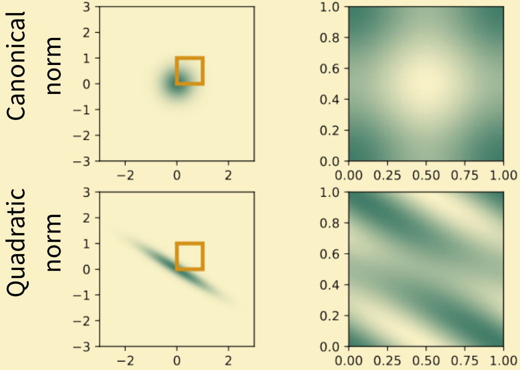
- $\mathcal{C} = (0,1)^n$, $\mathsf{Enc}(0) \sim (D_\Lambda \mod \mathcal{C})$, $\mathsf{Enc}(1) \sim \mathcal{U}(\mathcal{C})$.

LIP-based public-key encryption scheme

High-level idea

Follows **Dual-Regev** cryptosystem flavour:

- $\mathcal{C} = (0,1)^n$, $\mathrm{Enc}(0) \sim (D_\Lambda \mod \mathcal{C})$, $\mathrm{Enc}(1) \sim \mathcal{U}(\mathcal{C})$.



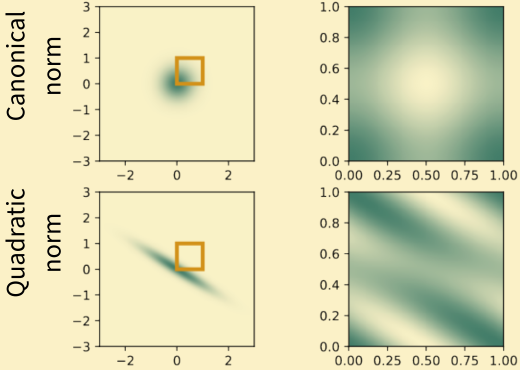
Distribution of encryptions of 0

LIP-based public-key encryption scheme

High-level idea

Follows **Dual-Regev** cryptosystem flavour:

- $\mathcal{C} = (0,1)^n$, $\mathrm{Enc}(0) \sim (D_\Lambda \mod \mathcal{C})$, $\mathrm{Enc}(1) \sim \mathcal{U}(\mathcal{C})$.



Distribution of encryptions of 0

Correctness

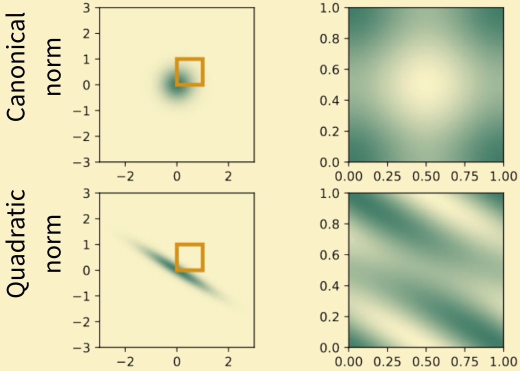
With overwhelming probability, $\mathrm{Enc}(1)$ is far enough from $(0,1)^n$ vertices.

LIP-based public-key encryption scheme

High-level idea

Follows **Dual-Regev** cryptosystem flavour:

- $\mathcal{C} = (0,1)^n$, $\mathrm{Enc}(0) \sim (D_\Lambda \mod \mathcal{C})$, $\mathrm{Enc}(1) \sim \mathcal{U}(\mathcal{C})$.



Distribution of encryptions of 0

Correctness

With overwhelming probability, $\mathrm{Enc}(1)$ is far enough from $(0,1)^n$ vertices.

Security

Under $\Delta LIP_{\mathrm{pke}}$ hypothesis, the scheme is **IND-CPA** secure.

Cryptanalysis of the $\Delta\mathrm{LIP}_{\mathrm{pke}}$ hypothesis

A reasonable hypothesis

The $\Delta\mathrm{LIP}_{\mathrm{pke}}$ hypothesis seems as strong as $\Delta\mathrm{LIP}$: the class restriction **does not improve existing attacks**, and **does not create new ones** neither.

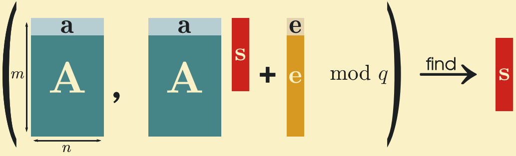
A reasonable conjecture for falsifiability

For $n \geq 85$, there exists at least one unimodular lattice Λ of rank n that verifies $\lambda_1(\Lambda)^2 \geq \sqrt{72n}$.

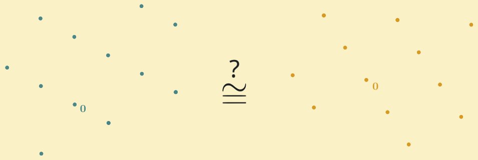
Discussion

What could we expect from LIP?

Legacy approach



LIP approach



Large *gap*(Λ) on random lattices
Hard time with Gaussian sampling
Plenty of constructions
Approximate variants of hypotheses

Small *gap*(Λ) on remarkable lattices
Easy implementation (eg. Hawk)
Only a few constructions
Fragile hypotheses

Thank you for your attention!

Léo Ackermann
Adeline Roux-Langlois
Alexandre Wallet

WCC presentation:

Public-key encryption from the lattice isomorphism problem