JC2 presentation:

Public-Key Encryption from the Lattice Isomorphism Problem

Joint work with Adeline Roux-Langlois (CNRS, Greyc, AmacC)
and Alexandre Wallet (Inria, IRISA, Capsule)

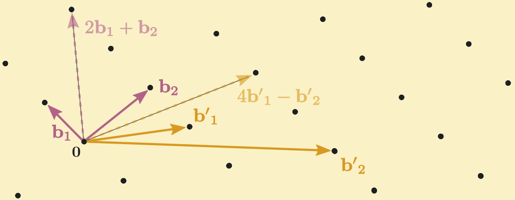
Léo Ackermann

October 2023

Standard lattice-based cryptography

Euclidean lattices

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



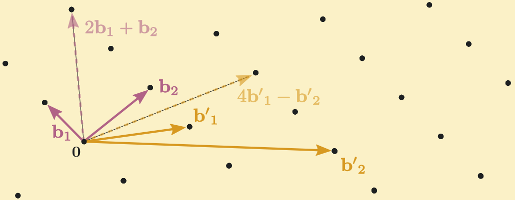
The more the merrier

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

Standard lattice-based cryptography

Euclidean lattices

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

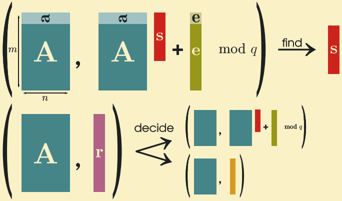


The more the merrier

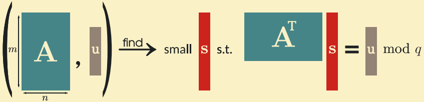
The bases are not unique: $\Lambda(\boldsymbol{B}) = \Lambda(\boldsymbol{B})$.

Hard lattice problems

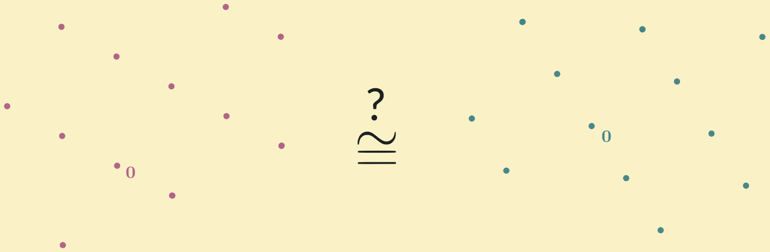
Learning With Errors (LWE).



Short Integer Solution (SIS).



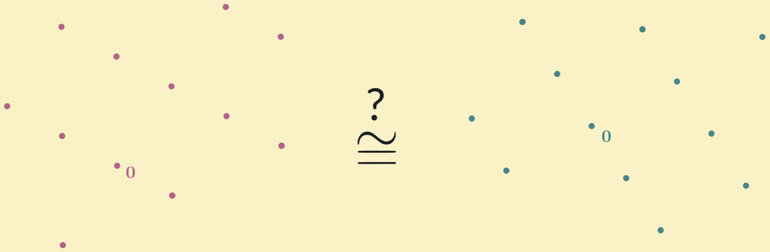
Lattice Isomorphism Problem (LIP)



Lattice Isomorphism Problem

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

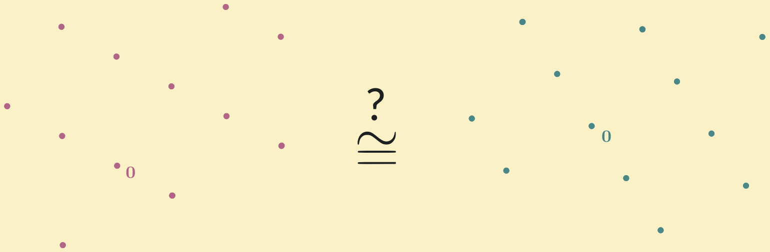
Lattice Isomorphism Problem (LIP)



Lattice Isomorphism Problem

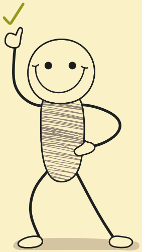
- Given Λ and Λ', find (if any) $O \in \mathcal{O}(\mathbb{R}^n)$ such that $\Lambda = O \cdot \Lambda'$.
- Given B and B', find (if any) $O \in \mathcal{O}(\mathbb{R}^n)$ such that $B = O \cdot B'$.

Lattice Isomorphism Problem (LIP)

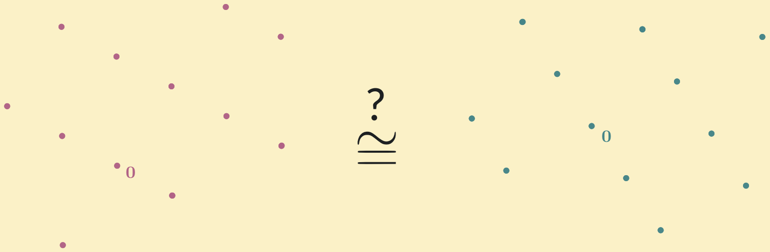


Lattice Isomorphism Problem

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



Lattice Isomorphism Problem (LIP)



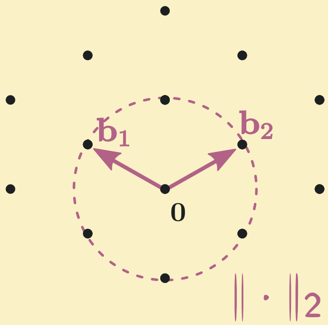
Lattice Isomorphism Problem

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

LIP-based cryptography

LIP flavours

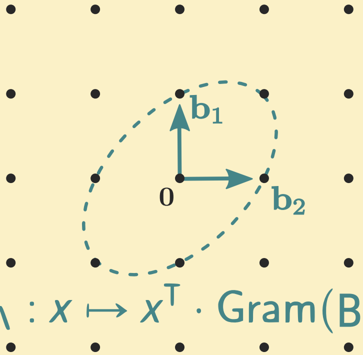
- The *public key* consists in any lattice Λ and a basis B of $O \cdot \Lambda$. The secret key is the rotation O.



LIP-based cryptography

LIP flavours

- The *public key* consists in quadratic forms (Q, Q') such that $Q' = U^{\intercal} Q U$ for $U \in \mathrm{GL}_n(\mathbb{Z})$. The secret key is U.



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

where $\mathrm{Gram}(B) = B^{\intercal} B$

LIP-based cryptography

LIP flavours

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

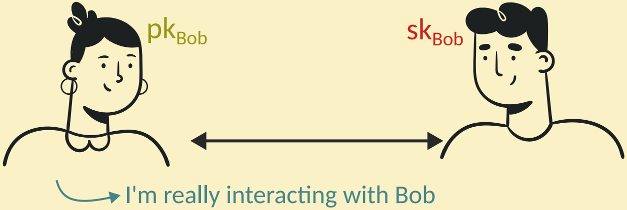
LIP-based cryptography

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.
- Schemes can be instantiated with geometry of *remarkable lattices* (root systems, Barnes-Wall, $\mathbb{Z}^n, \ldots$): smaller gaps, better algorithms.

Existing schemes

- Authentication scheme



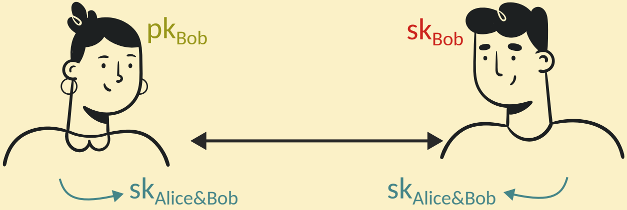
LIP-based cryptography

LIP flavours

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

Existing schemes

- Authentication scheme
- Key-encapsulation mecanism



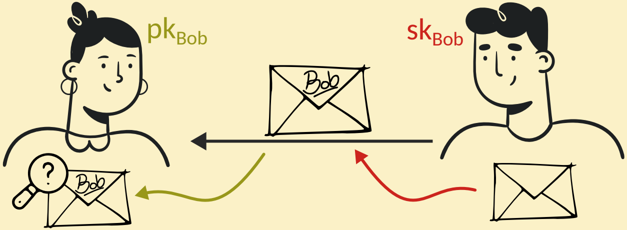
LIP-based cryptography

LIP flavours

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

Existing schemes

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



LIP-based cryptography

LIP flavours

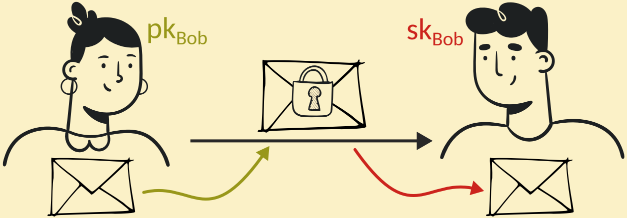
- The *public key* consists in quadratic forms (Q, Q') such that $Q' = U^\top Q U$ for $U \in \mathrm{GL}_n(\mathbb{Z})$. The secret key is U.
- Schemes can be instantiated with geometry of *remarkable lattices* (root systems, Barnes-Wall, $\mathbb{Z}^n, \ldots$): smaller gaps, better algorithms.

Existing schemes

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

Our work

- Public-key encryption scheme



LIP-based PKE

High-level idea

Follows *Dual-Regev* cryptosystem flavour:

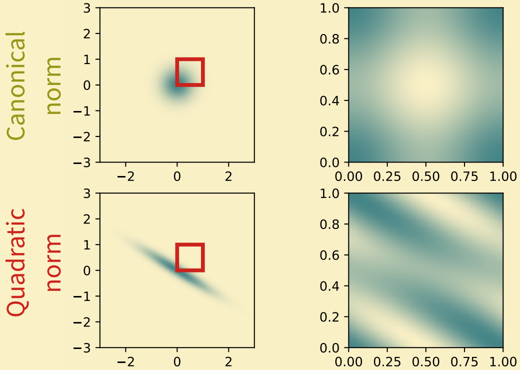
- $\mathcal{C} = (0,1)^n$, $\mathsf{Enc}(0) \sim (D_\Lambda \mod \mathcal{C})$, $\mathsf{Enc}(1) \sim \mathcal{U}(\mathcal{C})$

LIP-based PKE

High-level idea

Follows *Dual-Regev* cryptosystem flavour:

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



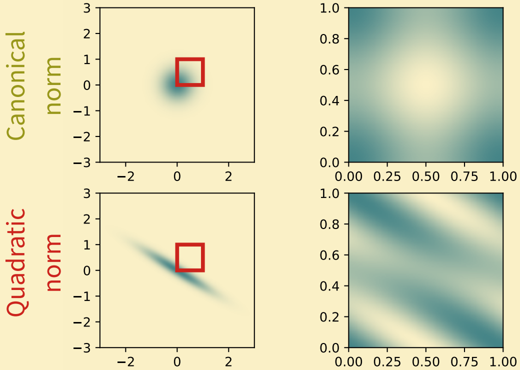
Distribution of encryptions of 0

LIP-based PKE

High-level idea

Follows *Dual-Regev* cryptosystem flavour:

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



Distribution of encryptions of 0

Correctness

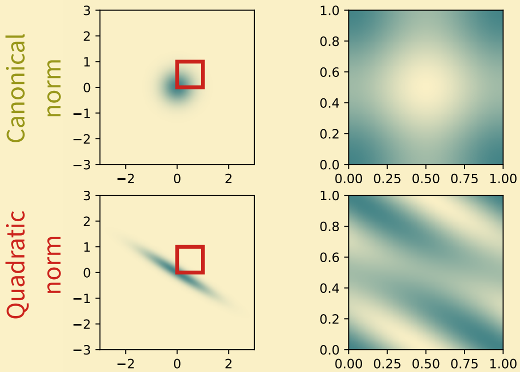
With overwhelming probability, Enc(1) is far enough from $(0,1)^n$ vertices

LIP-based PKE

High-level idea

Follows *Dual-Regev* cryptosystem flavour:

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



Distribution of encryptions of 0

Correctness

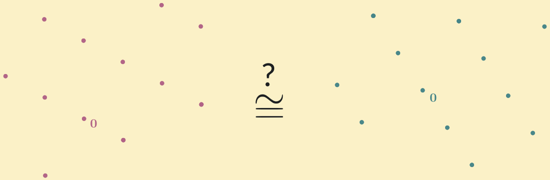
With overwhelming probability, $\mathsf{Enc}(1)$ is far enough from $(0,1)^n$ vertices

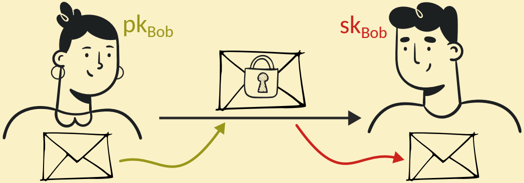
Security

Under ΔLIP_{pke} hypothesis, the scheme is IND-CPA secure

JC2 presentation:

Public-Key Encryption from the Lattice Isomorphism Problem





Credits

- Figures are either mine or free pictures from **Freepik**.
- The colors are from the **Gruvbox** color palette.