Sums-of-squares and module lattice isomorphisms

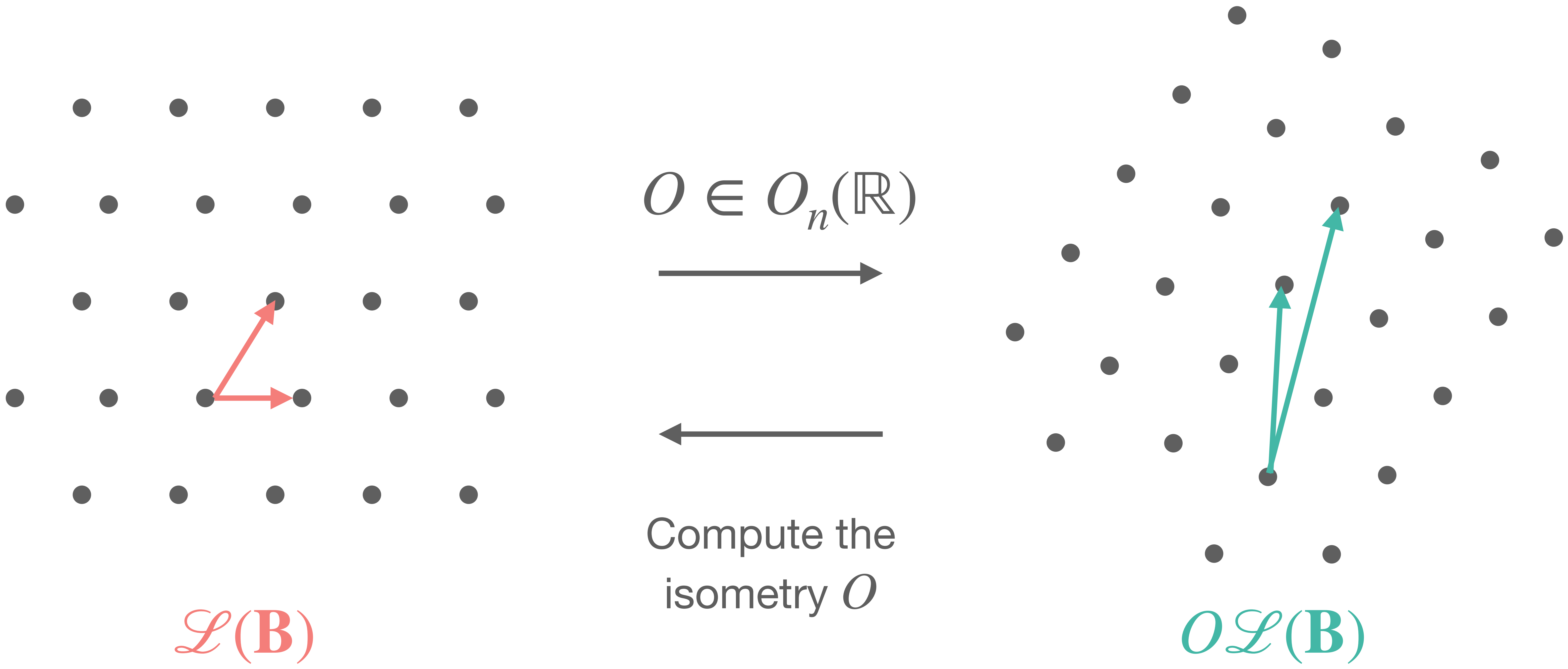
Alexandre Wallet, PQ Shield

Mathematics for PQC Workshop, Budapest, 5-9/08/2024

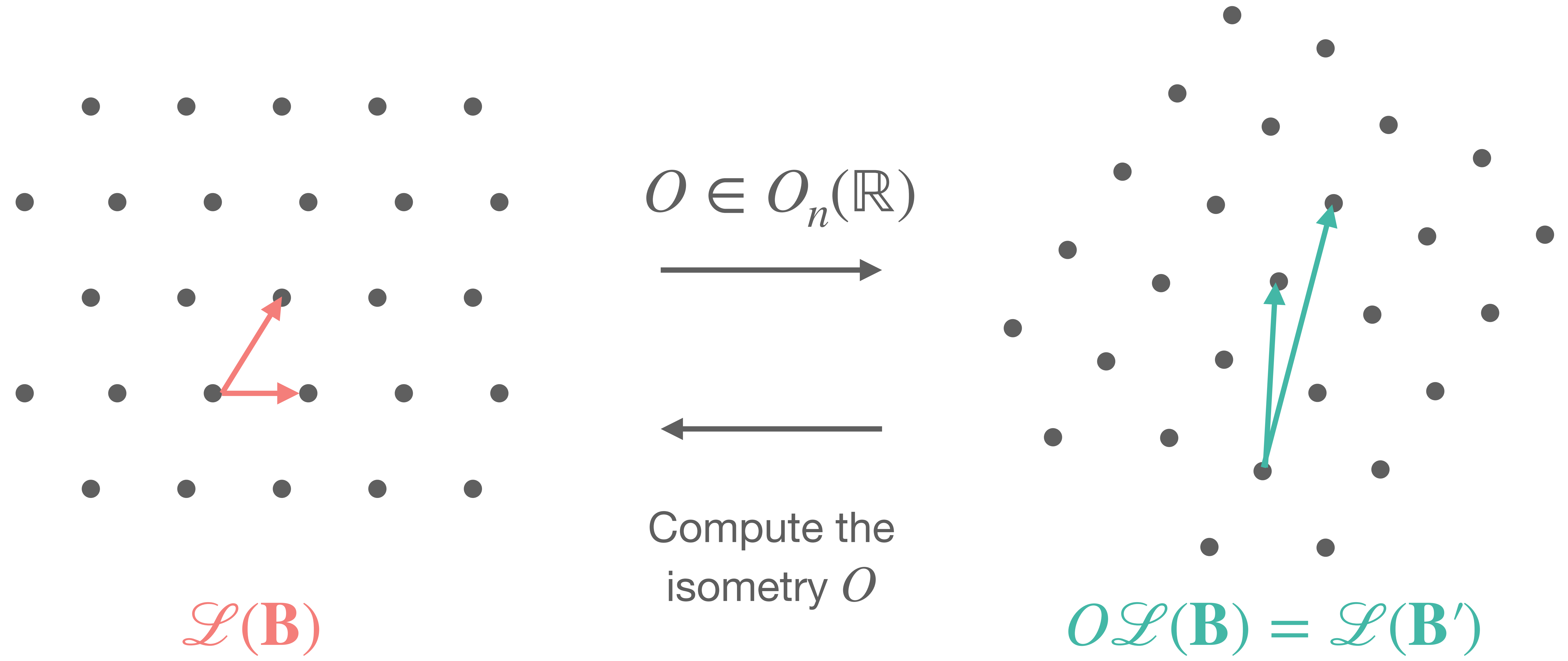
Based on joint works with C. Chevignard, T. Espitau, G. Mureau, A. Pellet—Mary, H. Pliatsok and P.A. Fouque

PQ SHIELD

The Lattice Isomorphism Problem (LIP)



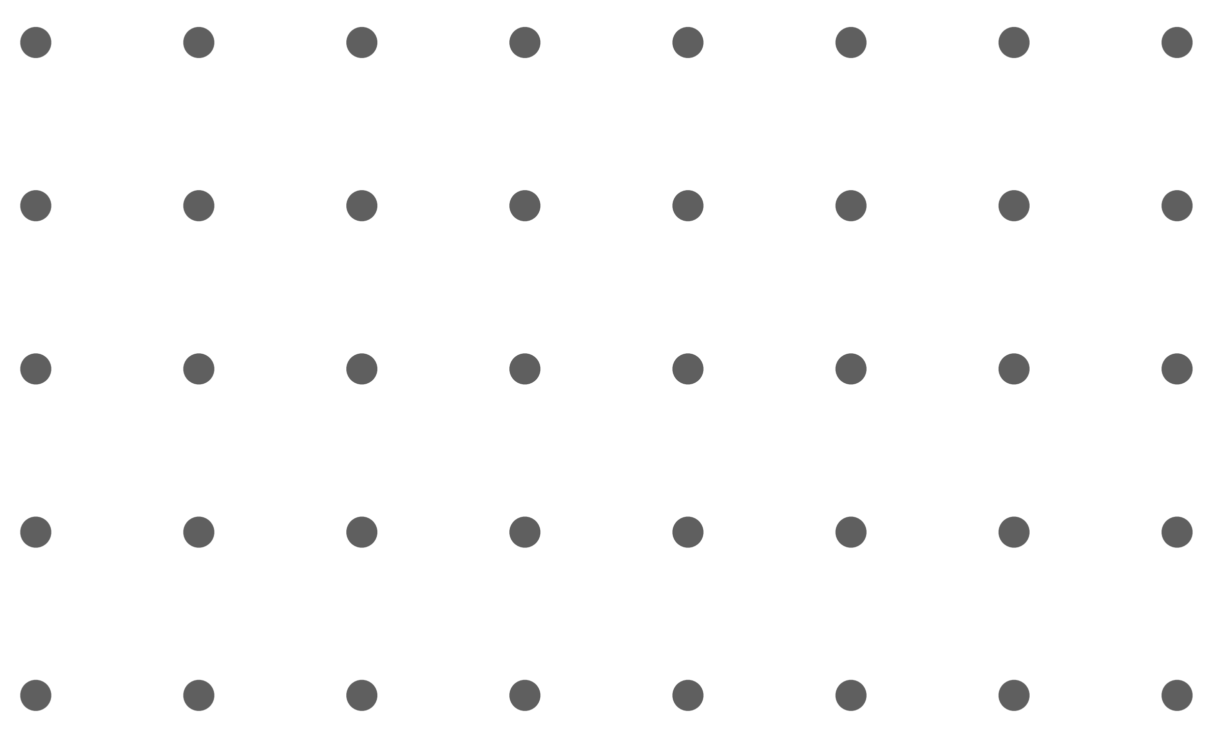
The Lattice Isomorphism Problem (LIP)



A computational version: Given $\mathbf{B}' = \mathbf{OBU}$, with $\mathbf{O}$ orthogonal and $\mathbf{U} \in \mathrm{GL}_n(\mathbb{Z})$, compute $\mathbf{O}$ or $\mathbf{U}$.

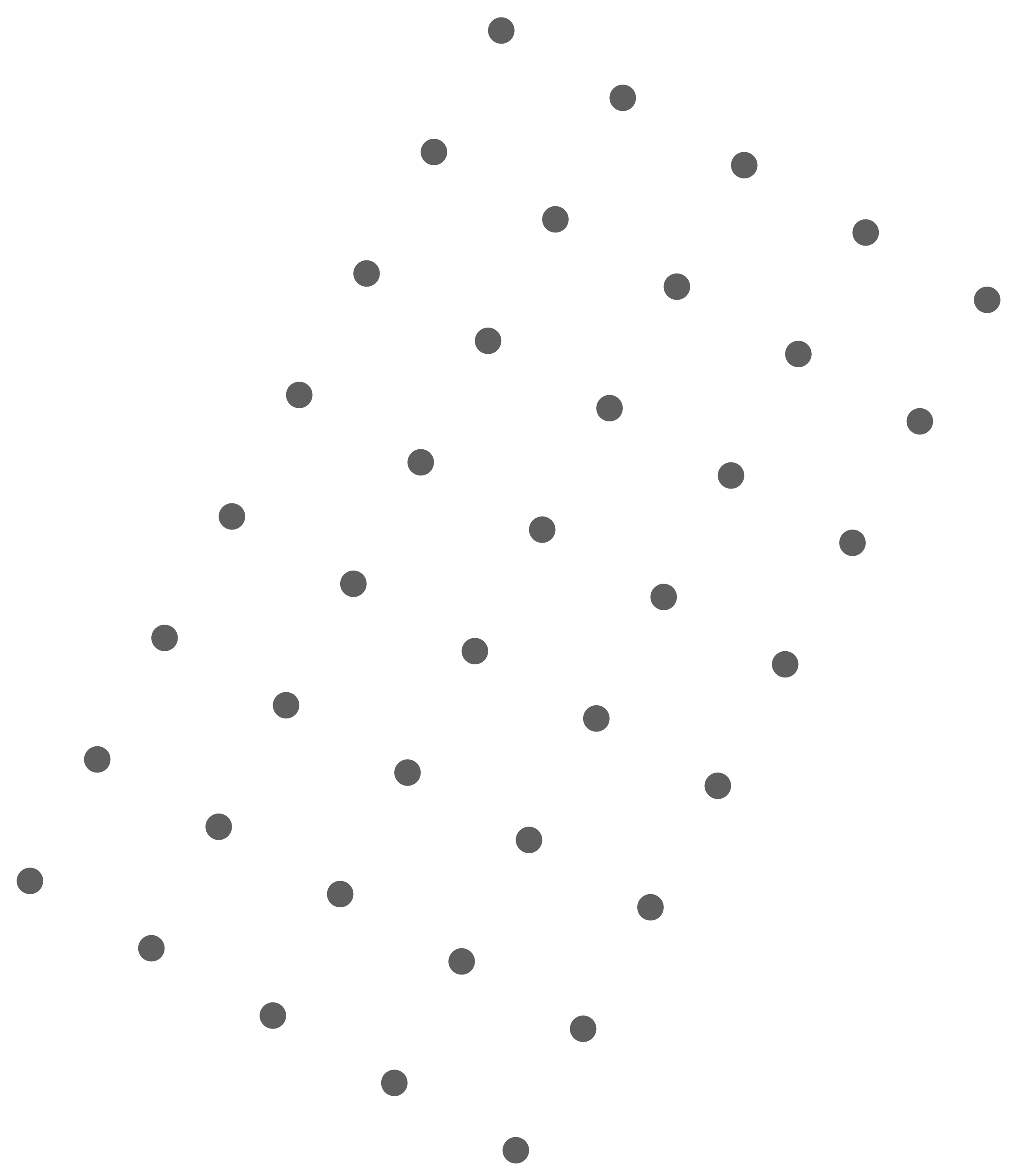
Proof of knowledge from LIP[1]

$\mathbb{Z}^n$



$\mathbf{G} = \mathbf{U}^t\mathbf{U}$

$\mathbf{OU}$



$O\mathbb{Z}^n$

$\mathbf{O}, \mathbf{U}$ secret

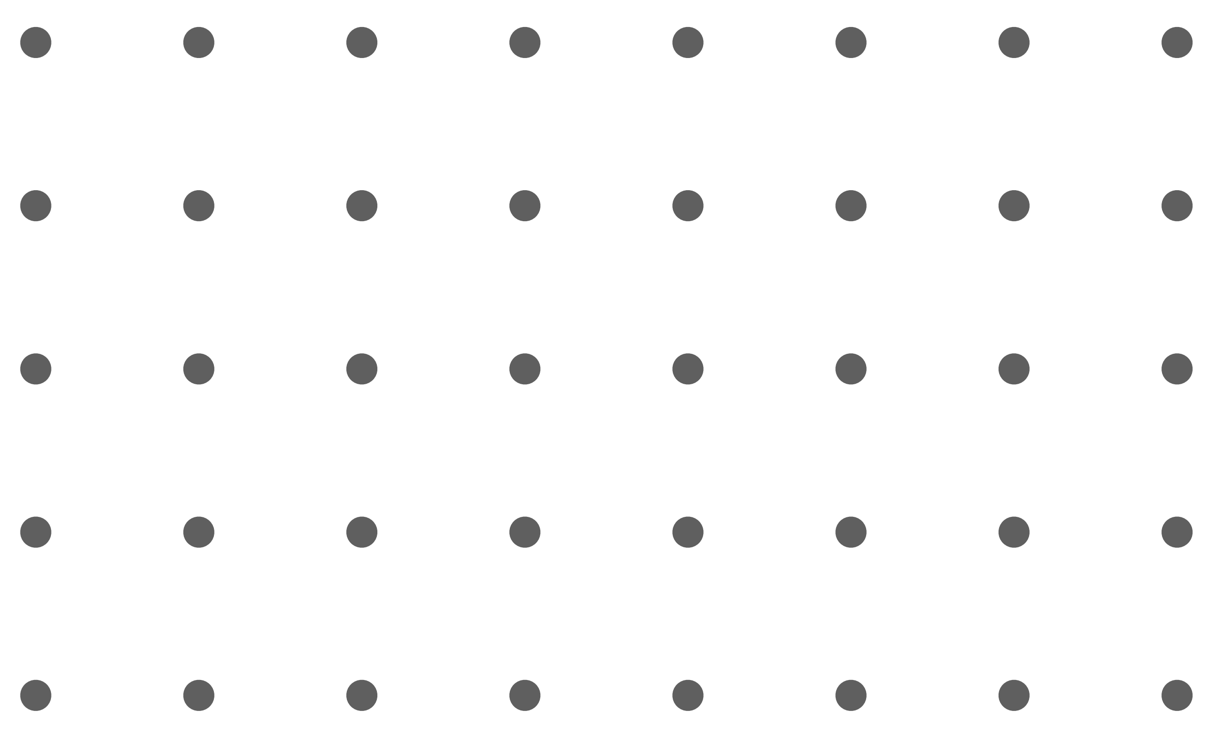
Prover

Verifier

[1] : L. Ducas and W. Van Woerden, e.g. ePrint 2021/1332

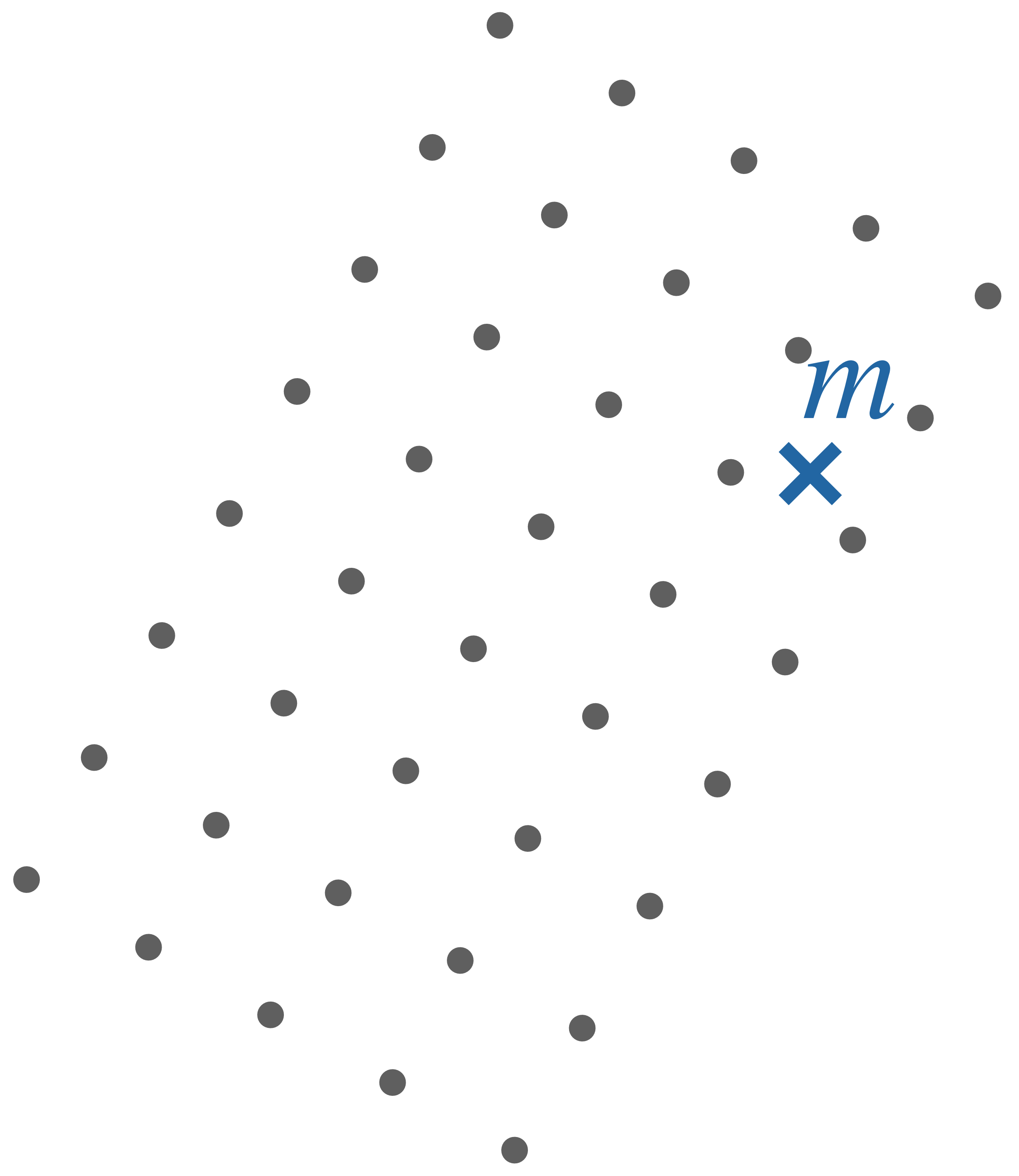
Proof of knowledge from LIP[1]

$\mathbb{Z}^n$



$\mathbf{G} = \mathbf{U}^t\mathbf{U}$

$\mathbf{O}\mathbf{U}$



$O\mathbb{Z}^n$

$\mathbf{O}, \mathbf{U}$ secret

Prover

Verifier

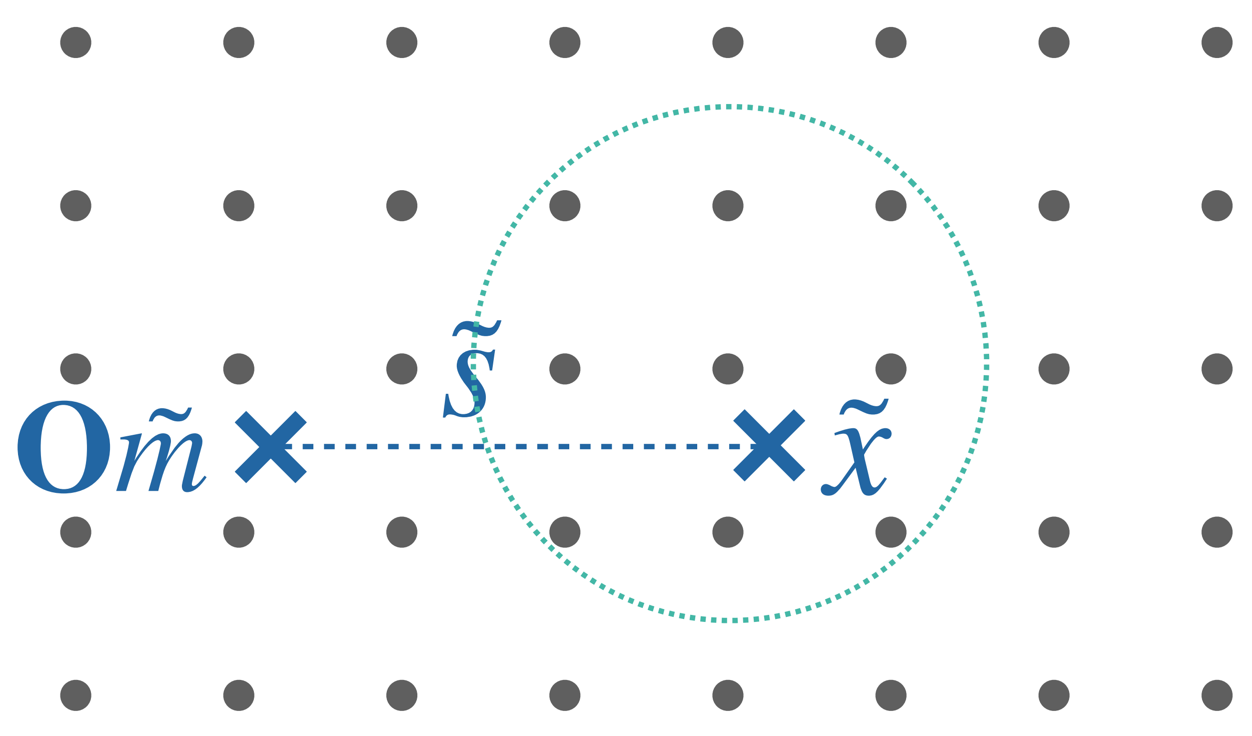
$\tilde{m} = \mathbf{U}m$

m ←

[1] : L. Ducas and W. Van Woerden, e.g. ePrint 2021/1332

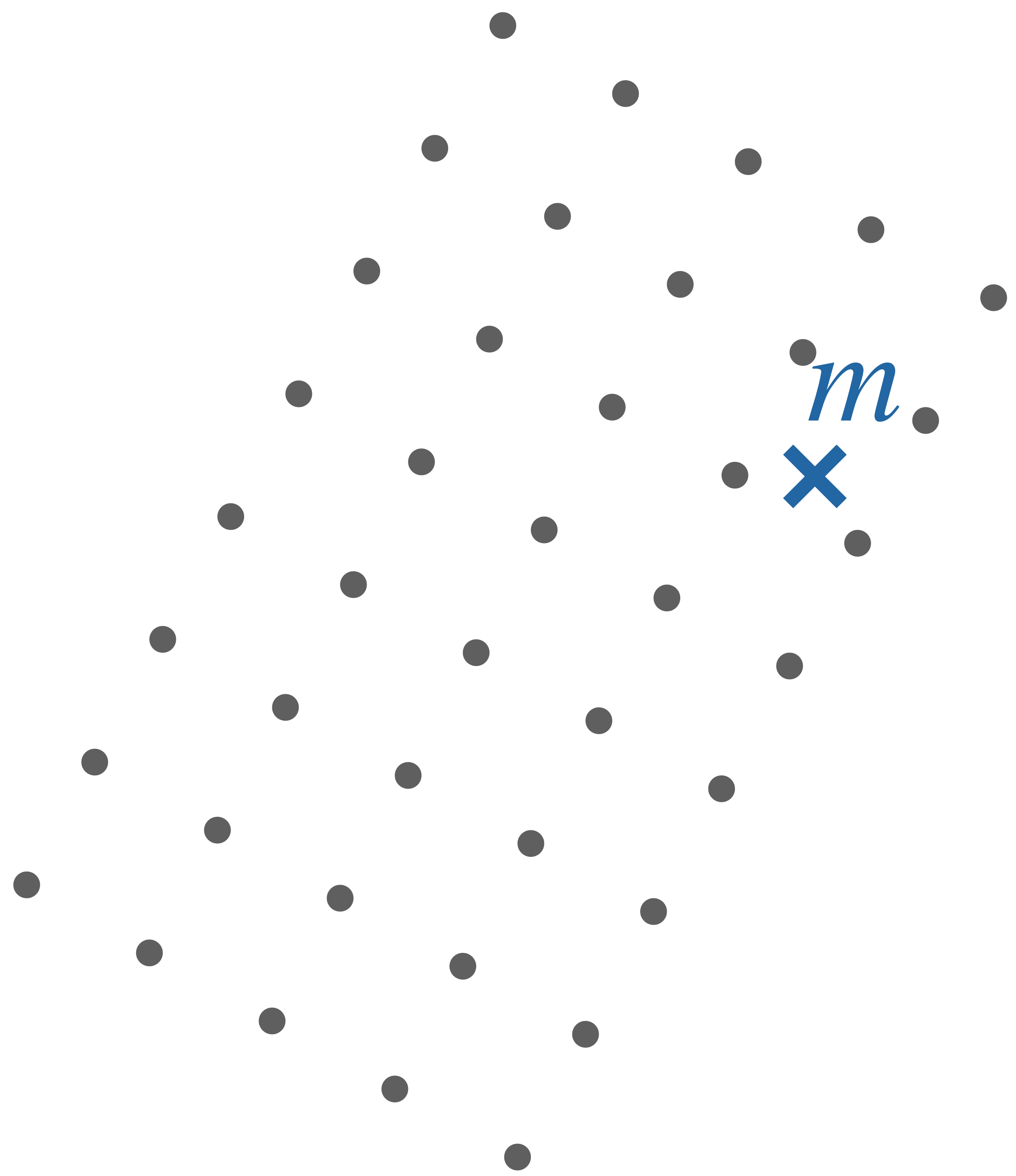
Proof of knowledge from LIP[1]

$\mathbb{Z}^n$



$\mathbf{G} = \mathbf{U}^t\mathbf{U}$

$\mathbf{OU}$



$O\mathbb{Z}^n$

$\mathbf{O}, \mathbf{U}$ secret

Prover

Verifier

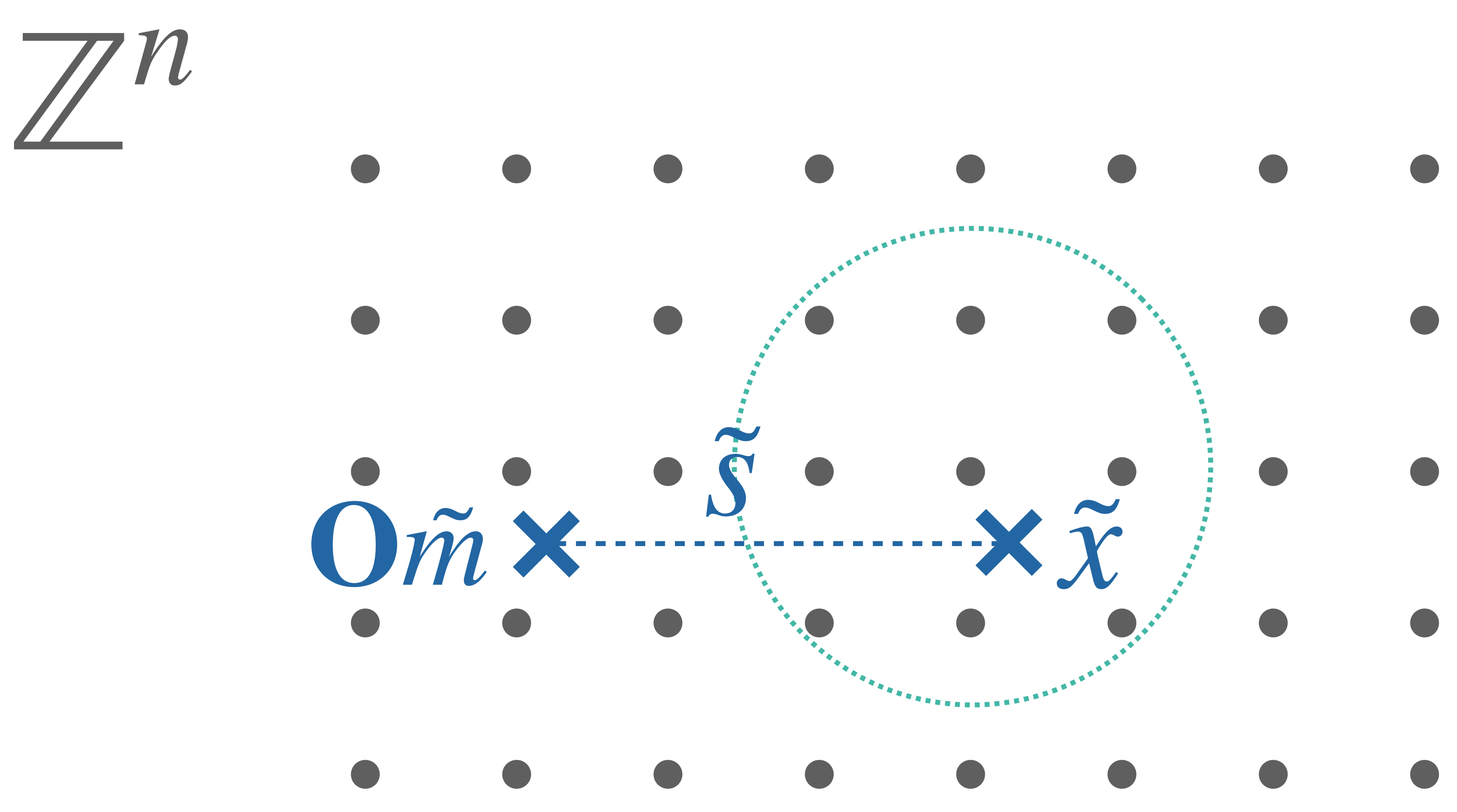
$\tilde{m} = \mathbf{U}m \qquad m \longleftarrow$

Sample short $\tilde{x}$ in $\mathbf{O}\tilde{m} + \mathbb{Z}^n$

$$s = \mathbf{U}^{-1}\mathbf{O}^t\tilde{s} = m - \mathbf{U}^{-1}\mathbf{O}^t\tilde{x}$$

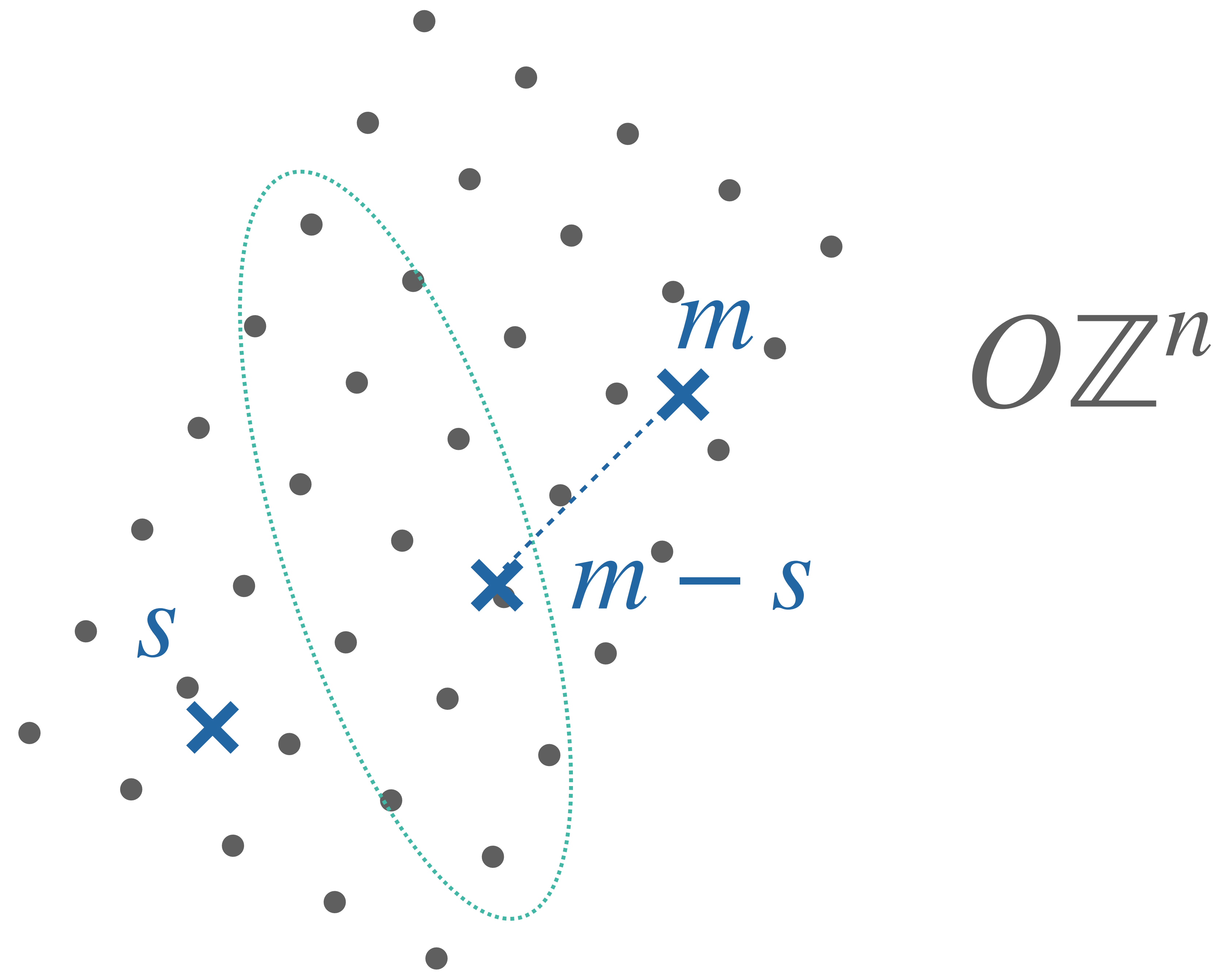
[1] : L. Ducas and W. Van Woerden, e.g. ePrint 2021/1332

Proof of knowledge from LIP[1]



$\mathbf{G} = \mathbf{U}^t\mathbf{U}$

$\mathbf{OU}$



$\mathbf{O}, \mathbf{U}$ secret

Prover | Verifier

$\tilde{m} = \mathbf{U}m$ $\quad m \leftarrow$

Sample short $\tilde{x}$ in $\mathbf{O}\tilde{m} + \mathbb{Z}^n$

$s = \mathbf{U}^{-1}\mathbf{O}^t\tilde{s} = m - \mathbf{U}^{-1}\mathbf{O}^t\tilde{x}$ $\quad \rightarrow s$

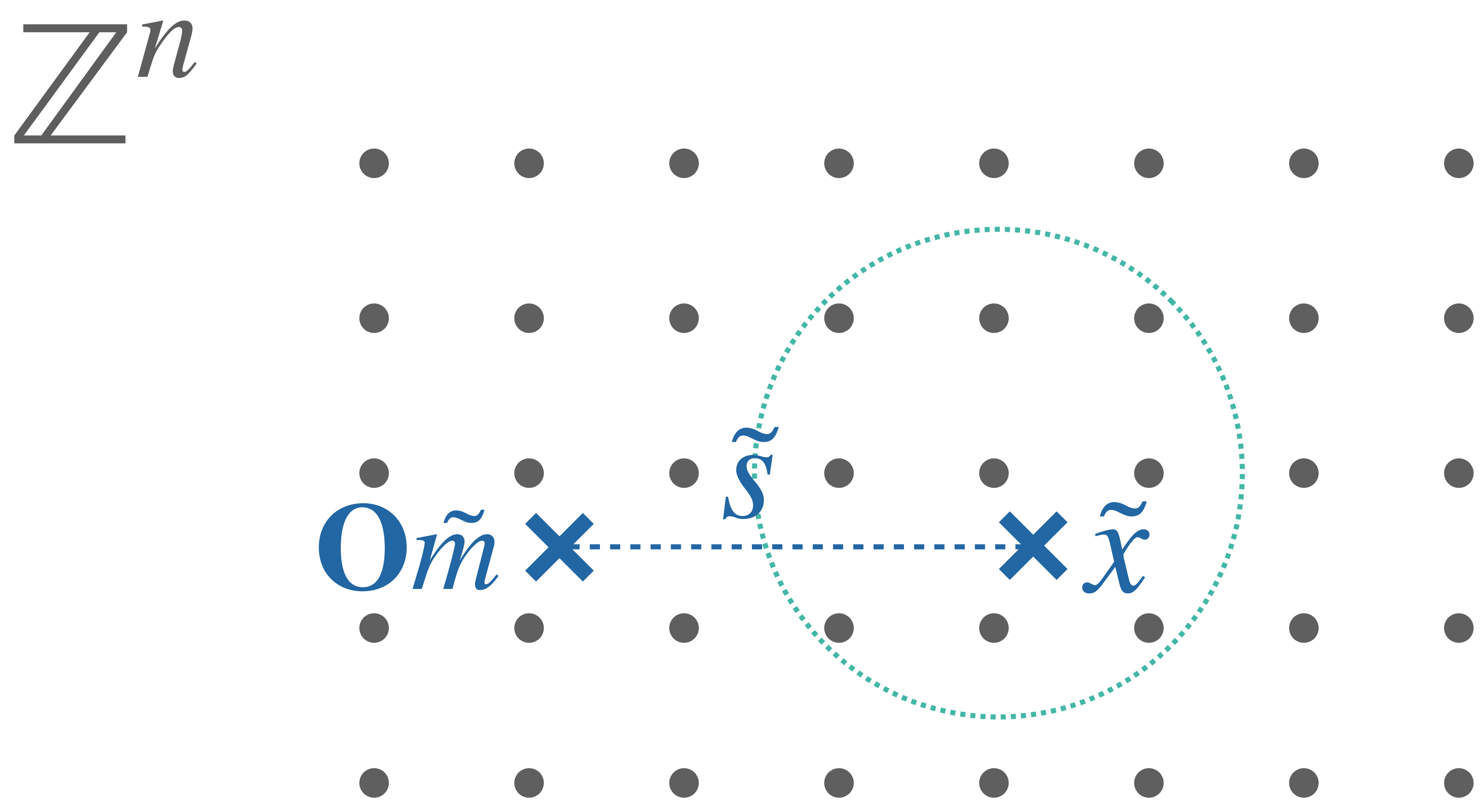
1) $\mathbf{OU}s \in \mathbf{Z}^n$? 2) $(m-s)^t\mathbf{G}(m-s)$ is short? (where $(m-s)^t\mathbf{G}(m-s) = \|\tilde{x}\|^2$)

Yes both: the verifier is convinced!

(in the end, we do not care so much for O)

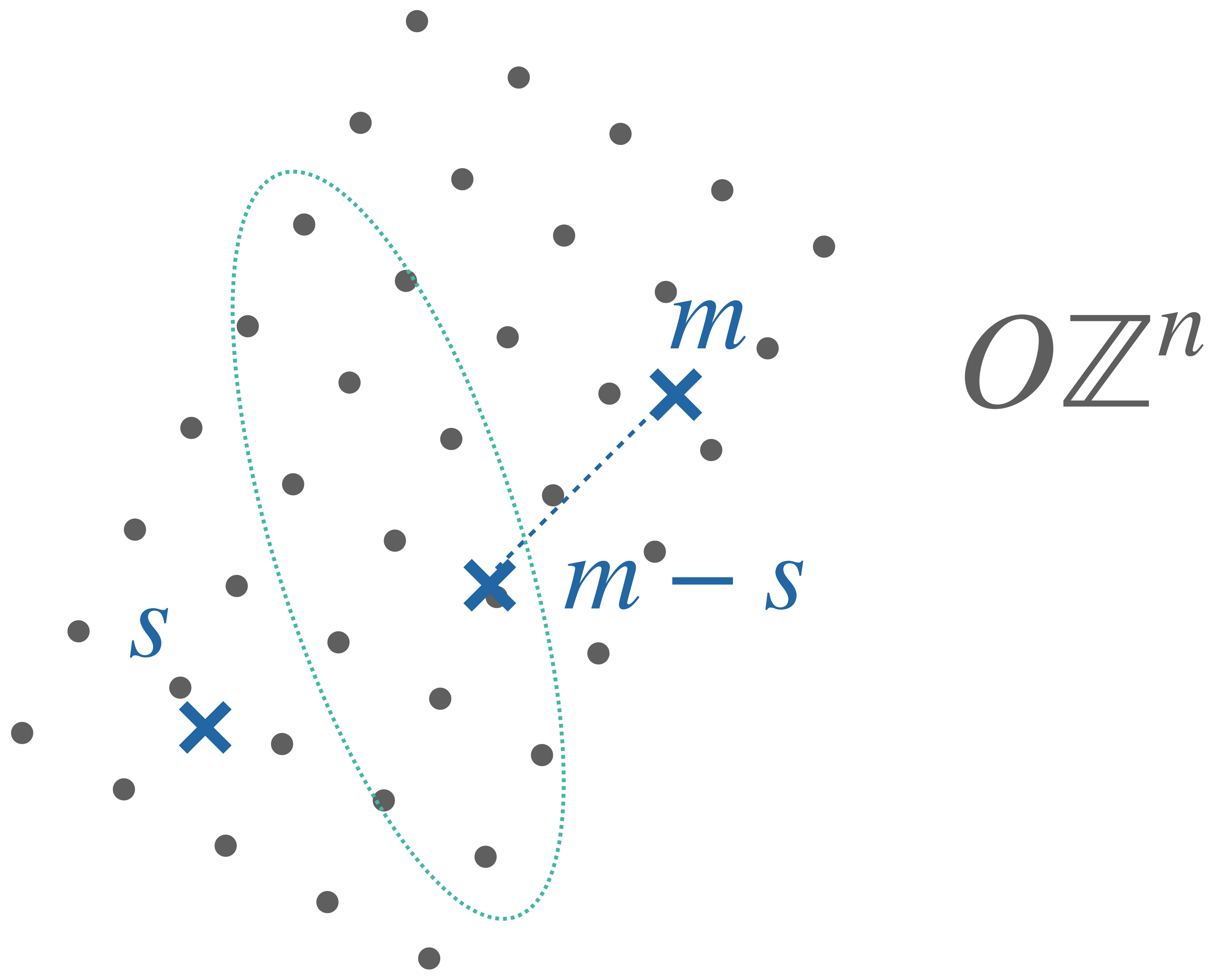
[1] : L. Ducas and W. Van Woerden, e.g. ePrint 2021/1332

Proof of knowledge from LIP[1]



$\mathbf{G} = \mathbf{U}^t\mathbf{U}$

$\mathbf{OU}$



$\mathbf{O}, \mathbf{U}$ secret

Prover | **Verifier**

$\tilde{m} = \mathbf{U}m$ ⟵ m

Sample short $\tilde{x}$ in $\mathbf{O}\tilde{m} + \mathbb{Z}^n$

$s = \mathbf{U}^{-1}\mathbf{O}^t\tilde{s} = m - \mathbf{U}^{-1}\mathbf{O}^t\tilde{x}$ ⟶ s

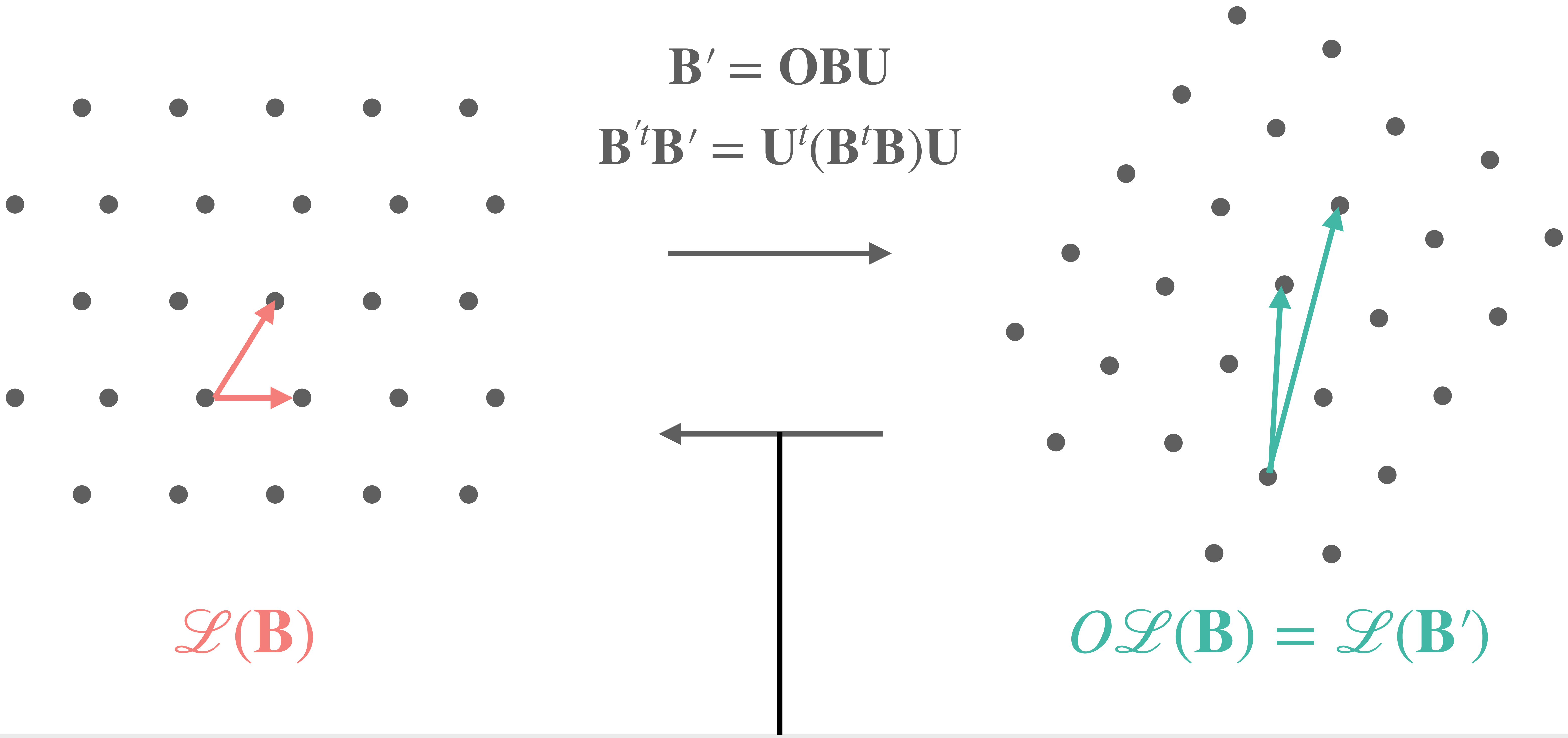
Observation:

Any $\mathbf{V} \in GL_n(\mathbb{Z})$ such that $\mathbf{V}^t\mathbf{V} = \mathbf{G}$ allows to convince the verifier.

(Run the protocol with $\mathbf{V}$ instead of $\mathbf{U}$).

[1] : L. Ducas and W. Van Woerden, e.g. ePrint 2021/1332

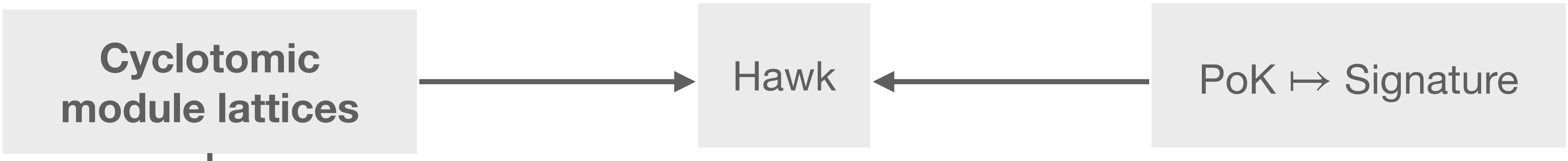
The Lattice Isomorphism Problem (LIP), with quadratic forms



Two quadratic forms $\mathbf{G}, \mathbf{G}'$ are integrally congruent when $\mathbf{G}' = \mathbf{U}^t\mathbf{G}\mathbf{U}$ for some congruence matrix $\mathbf{U} \in \mathrm{GL}_n(\mathbb{Z})$.

LIP$^{\mathbf{B}}$: *Given* $\mathbf{B}$, $\mathbf{G} = \mathbf{B}^t\mathbf{B}$ *and* $\mathbf{G}' \sim_{\mathbb{Z}} \mathbf{G}$, *find any congruence matrix* $\mathbf{U}$ *between* $\mathbf{G}$ *and* $\mathbf{G}'$.

Hawk[1] and module lattices



<u>New context:</u>

$m = 2^\ell$, $K = \mathbb{Q}(\zeta_m)$, and $\mathcal{O}_K := \mathbb{Z}[\zeta_m]$ (for ζ_m primitive).

Identify $\mathbb{Z}^m$ with $\mathcal{O}_K^2$, **a free module lattice of rank 2.**

Transpose becomes conjugate-transpose

Two forms $\mathbf{G}, \mathbf{G}'$ are $\mathcal{O}_K$-congruent when $\mathbf{G}' = \mathbf{U}^*\mathbf{G}\mathbf{U}$ for some congruence matrix $\mathbf{U} \in \mathrm{GL}_n(\mathcal{O}_K)$.

*(Free-)*Mod-LIP$_K^{\mathbf{B}}$: *Given $\mathbf{B}$, $\mathbf{G} = \mathbf{B}^*\mathbf{B}$ and $\mathbf{G}' \sim_{\mathcal{O}_K} \mathbf{G}$, find any congruence matrix $\mathbf{U}$ between $\mathbf{G}$ and $\mathbf{G}'$.*

[1] : https://hawk-sign.info, also ePrint 2022/1155 (L. Ducas, E. Postlethwaite, L. Pulles and W. Van Woerden. See also Wessel's talk!

Hawk[1] and module lattices

Cyclotomic module lattices → **Hawk** ← PoK $\mapsto$ Signature

<u>New context:</u>

$m = 2^\ell$, $K = \mathbb{Q}(\zeta_m)$, and $\mathcal{O}_K := \mathbb{Z}[\zeta_m]$ (for ζ_m primitive).

Identify $\mathbb{Z}^m$ with $\mathcal{O}_K^2$, **a free module lattice of rank 2.**

Transpose becomes conjugate-transpose

Could be extended to many number fields K

Don't do it in rank 1!

Two forms $\mathbf{G}, \mathbf{G}'$ are $\mathcal{O}_K$-congruent when $\mathbf{G}' = \mathbf{U}^*\mathbf{G}\mathbf{U}$ for some congruence matrix $\mathbf{U} \in \mathrm{GL}_n(\mathcal{O}_K)$.

*(Free-)*Mod-LIP$_K^{\mathbf{B}}$: *Given* $\mathbf{B}$, $\mathbf{G} = \mathbf{B}^*\mathbf{B}$ *and* $\mathbf{G}' \sim_{\mathcal{O}_K} \mathbf{G}$, *find any congruence matrix* $\mathbf{U}$ *between* $\mathbf{G}$ *and* $\mathbf{G}'$.

[1] : https://hawk-sign.info, also ePrint 2022/1155 (L. Ducas, E. Postlethwaite, L. Pulles and W. Van Woerden. See also Wessel's talk!

Why not using ideal lattices?

Say $K = \mathbb{Q}(\zeta)$, a cyclotomic field, the lattice is $\mathcal{O}_K$.

We pick a private unit $u \in \mathcal{O}_K^\times$, and publish the **totally real** element $g = u^* u$.

For all $\sigma : K \to \mathbb{C}$
$\sigma(g) \in \mathbb{R}_+$

Observation:
The congruence class is then the set of solutions of **the relative norm equation**

$$N(x) = g,$$

where $N : K \to F, N(a) = a^* a$.

F is the field fixed by $\cdot^*$
(A totally real field)

Do not use ideal lattice because there are polynomial time algorithms[1] for this!

(But this information is useful for the rest of the talk!)

[1] :Gentry-Szydlo's algorithm for cyclotomic fields, Lenstra-Silverberg for general « CM-orders ».

Now what's the plan for today?

Target: ModLIP **over Rank 2, Free, module** lattices

Mod-LIP$_K^{\mathbf{B}}$: *Given* $\mathbf{B}$, $\mathbf{G} = \mathbf{B}^*\mathbf{B}$ *and* $\mathbf{G}' \sim_{\mathcal{O}_K} \mathbf{G}$, *find any congruence matrix* $\mathbf{U}$ *between* $\mathbf{G}$ *and* $\mathbf{G}'$.

1. Fermat's two squares problem
2. A heuristic polynomial time algorithm to solve ModLIP over totally real number fields
3. Lagrange's four square theorem, quaternions: new reductions for ModLIP over CM-extension fields
4. State of affairs, perspectives, open questions

ModLIP in rank 2
over totally real fields

aka.

Fermat’s « two squares » theorem

The totally real version of ModLip

1

Now, we let K be a totally real number field (all embeddings map to $\mathbb{R}$) and $\mathbf{B} = \begin{bmatrix} x & z \\ y & w \end{bmatrix}$

$$\mathbf{G}_{pub} = \begin{bmatrix} g_0 & \star \\ \star & g_1 \end{bmatrix} = \begin{bmatrix} x^2 + y^2 & \star \\ \star & z^2 + w^2 \end{bmatrix} = \mathbf{B}^* \mathbf{B}$$

So we can recover the key if we can compute all sums of two squares giving g_0, g_1.

The totally real version of ModLip

1

Now, we let K be a totally real number field (all embeddings map to $\mathbb{R}$) and $\mathbf{B} = \begin{bmatrix} x & z \\ y & w \end{bmatrix}$

$$\mathbf{G}_{pub} = \begin{bmatrix} g_0 & \star \\ \star & g_1 \end{bmatrix} = \begin{bmatrix} x^2 + y^2 & \star \\ \star & z^2 + w^2 \end{bmatrix} = \mathbf{B}^*\mathbf{B}$$

So we can recover the key if we can compute all sums of two squares giving g_0, g_1.

This links back to ***Fermat's two squares theorem:***

- A prime integer p is the sum of two integers squared if and only if $p \equiv 1\ [4]$.
- The set of integers that can be written as the sums of two squares is:

$$S_2(\mathbb{Z}) := \{2^e \cdot \prod_{p \equiv 1\ [4]} p^{v_p} \cdot \prod_{p \equiv 3\ [4]} p^{2v_p} \ : e, v_p \in \mathbb{N}\}$$

We need:

- An **algorithmic** version of it
- An extension to **algebraic integers**

Two classic proofs strategies

$S_2(\mathbb{Z})$ is stable by multiplication. With unique factorization into primes, the main task is understanding primes that are in $S_2(\mathbb{Z})$.

Proof with geometry
We look at $p = x^2 + y^2$, that is $x^2 \equiv -y^2\ [p]$.

Two classic proofs strategies

$S_2(\mathbb{Z})$ is stable by multiplication. With unique factorization into primes, the main task is understanding primes that are in $S_2(\mathbb{Z})$.

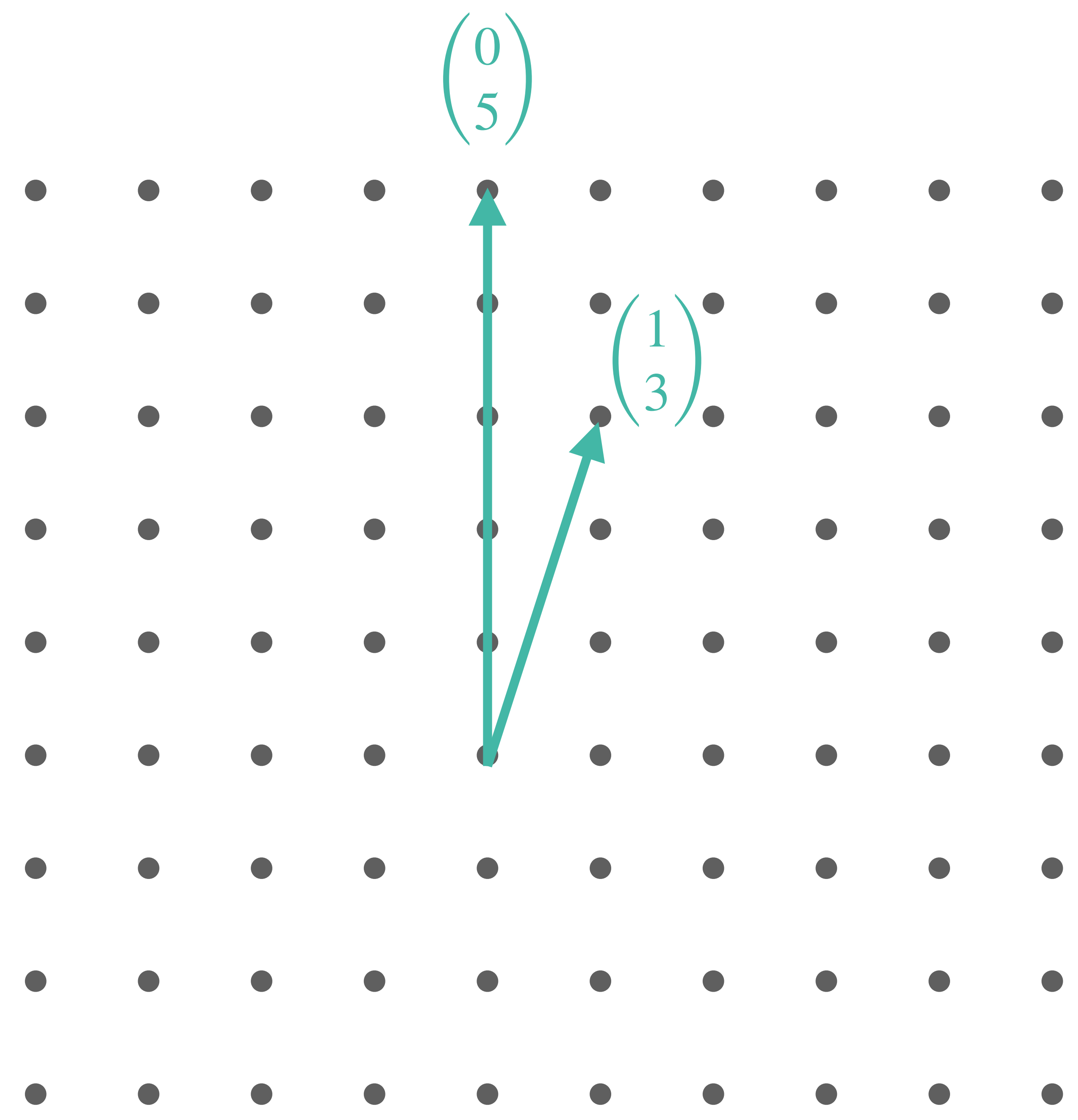
Proof with geometry

We look at $p = x^2 + y^2$, that is $x^2 \equiv -y^2\,[p]$.

1. -1 is a square mod p $\Leftrightarrow p \equiv 1\,[4]$.
   Let $u^2 \equiv -1\,[p]$.

2. Define $\mathscr{L}(p) = \{(a,b) \in \mathbb{Z}^2 \,:\, au - b \equiv 0\,[p]\}$.
   For $v \in \mathscr{L}(p)$, we have $\|v\|^2 = a^2 + b^2 \in p\mathbb{Z}$.

   A basis is $\begin{bmatrix} 1 & 0 \\ u & p \end{bmatrix}$.



Two classic proofs strategies

$S_2(\mathbb{Z})$ is stable by multiplication. With unique factorization into primes, the main task is understanding primes that are in $S_2(\mathbb{Z})$.

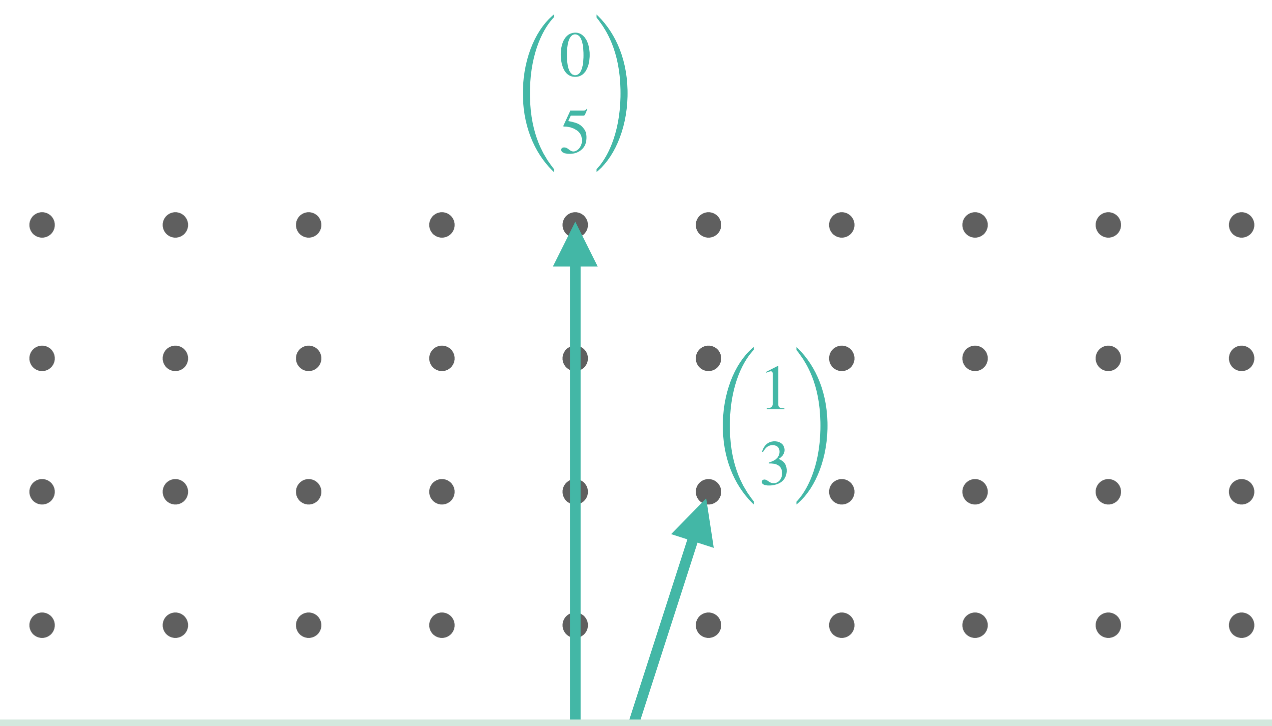
Proof with geometry

We look at $p = x^2 + y^2$, that is $x^2 \equiv -y^2\,[p]$.

1. -1 is a square mod $p \Leftrightarrow p \equiv 1\,[4]$.
   Let $u^2 \equiv -1\,[p]$.

2. Define $\mathscr{L}(p) = \{(a,b) \in \mathbb{Z}^2 \,:\, au - b \equiv 0\,[p]\}$.
   For $v \in \mathscr{L}(p)$, we have $\|v\|^2 = a^2 + b^2 \in p\mathbb{Z}$.

   A basis is $\begin{bmatrix} 1 & 0 \\ u & p \end{bmatrix}$. And we have $\lambda_1(\mathscr{L}(p))^2 < 2p$.



Minkowski's theorem (in rank 2)
Let $\mathscr{L}$ be a lattice of rank 2. The shortest vector in $\mathscr{L}\setminus\{0\}$ has length:

$$\lambda_1(\mathscr{L})^2 \leq \frac{4}{\pi} \cdot \det(\mathscr{L}).$$

Two classic proofs strategies

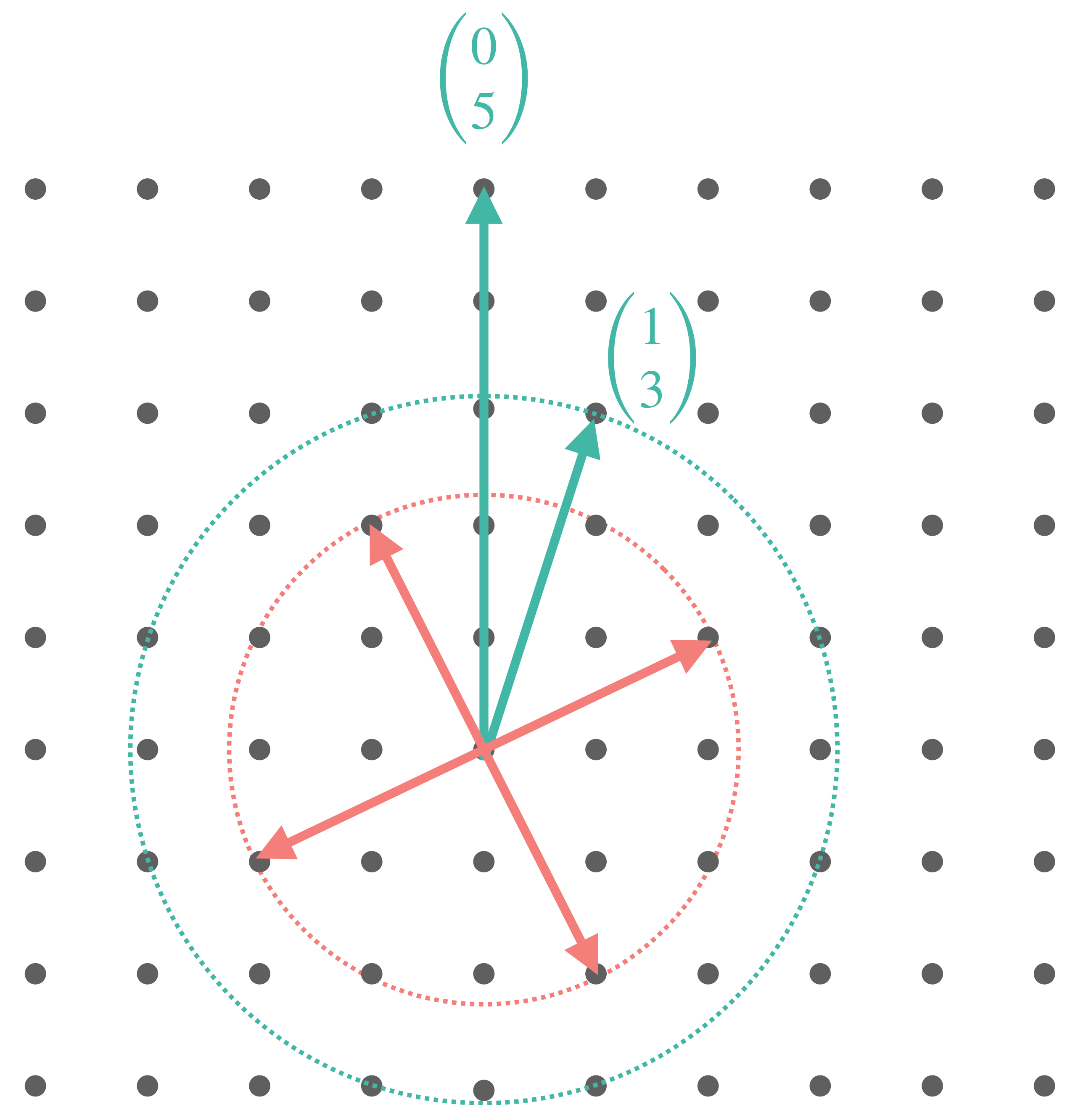
$S_2(\mathbb{Z})$ is stable by multiplication. With unique factorization into primes, the main task is understanding primes that are in $S_2(\mathbb{Z})$.

Proof with geometry

We look at $p = x^2 + y^2$, that is $x^2 \equiv -y^2\,[p]$.

1. -1 is a square mod $p \;\Leftrightarrow p \equiv 1\,[4]$.
   Let $u^2 \equiv -1\,[p]$.
2. Define $\mathscr{L}(p) = \{(a,b) \in \mathbb{Z}^2 \,:\, au - b \equiv 0\,[p]\}$.
   For $v \in \mathscr{L}(p)$, we have $\|v\|^2 = a^2 + b^2 \in p\mathbb{Z}$.

   A basis is $\begin{bmatrix} 1 & 0 \\ u & p \end{bmatrix}$. And we have $\lambda_1(\mathscr{L}(p))^2 < 2p$.
3. Any shortest vector gives a two-square sum for p.
   Compute them with Gauss-Lagrange's algorithm.



($\mathscr{L}(p)$ is similar to $\mathbb{Z}^2$)

Two classic proofs strategies

$S_2(\mathbb{Z})$ is stable by multiplication. With unique factorization into primes, the main task is understanding primes that are in $S_2(\mathbb{Z})$.

Proof with geometry

We look at $p = x^2 + y^2$, that is $x^2 \equiv -y^2\,[p]$.

1. -1 is a square mod p $\Leftrightarrow p \equiv 1\,[4]$.
   Let $u^2 \equiv -1\,[p]$.
2. Define $\mathscr{L}(p) = \{(a,b) \in \mathbb{Z}^2 \;:\; au - b \equiv 0\,[p]\}$.
3. Any shortest vector gives a two-square sum for p.
   Compute them with Gauss-Lagrange's algorithm.

Proof with arithmetic

In the Gauss integers $\mathbb{Z}[i]$, we have:

$$p = N(x+iy) := (x+iy)(x-iy).$$

1. p factors $\Leftrightarrow T^2 + 1$ factors modulo p
   Its discriminant is $\Delta = -4$. It is a square mod p iff -1 is a square modulo p.

Two classic proofs strategies

1

$S_2(\mathbb{Z})$ is stable by multiplication. With unique factorization into primes, the main task is understanding primes that are in $S_2(\mathbb{Z})$.

Proof with geometry

We look at $p = x^2 + y^2$, that is $x^2 \equiv -y^2\,[p]$.

1. -1 is a square mod $p \;\Leftrightarrow p \equiv 1\,[4]$.
   Let $u^2 \equiv -1\,[p]$.
2. Define $\mathscr{L}(p) = \{(a,b) \in \mathbb{Z}^2 \;:\; au - b \equiv 0\,[p]\}$.
3. Any shortest vector gives a two-square sum for p.
   Compute them with Gauss-Lagrange's algorithm.

Proof with arithmetic

In the Gauss integers $\mathbb{Z}[i]$, we have:

$$p = N(x+iy) := (x+iy)(x-iy).$$

1. p factors $\Leftrightarrow -1$ is a square modulo p.
2. Then $T^2 + 1 = (T-a)(T-b)$ mod p.
   Two conjugate primes above p. One is $\mathfrak{p} = \langle p, i-a \rangle$.

Two classic proofs strategies

1

$S_2(\mathbb{Z})$ is stable by multiplication. With unique factorization into primes, the main task is understanding primes that are in $S_2(\mathbb{Z})$.

Proof with geometry

We look at $p = x^2 + y^2$, that is $x^2 \equiv -y^2\,[p]$.

1. -1 is a square mod $p \Leftrightarrow p \equiv 1\,[4]$.
   Let $u^2 \equiv -1\,[p]$.
2. Define $\mathcal{L}(p) = \{(a,b) \in \mathbb{Z}^2 \,:\, au - b \equiv 0\,[p]\}$.
3. Any shortest vector gives a two-square sum for p.
   Compute them with Gauss-Lagrange's algorithm.

Proof with arithmetic

In the Gauss integers $\mathbb{Z}[i]$, we have:

$$p = N(x+iy) := (x+iy)(x-iy).$$

1. p factors $\Leftrightarrow -1$ is a square modulo p.
2. Then $T^2 + 1 = (T-a)(T-b)$ mod p.
   Two conjugate primes above p. One is $\mathfrak{p} = \langle p, i-a \rangle$.
3. $\mathbb{Z}[i]$ is *Euclidean*: compute gcd of p and $i-a$ with Euclidean division to obtain a generator $x+iy$ of $\mathfrak{p}$.
4. Do the same for $\mathfrak{p}^*$, loop over all units in $\mathbb{Z}[i]$ to get all generators.

Two classic proofs strategies

$S_2(\mathbb{Z})$ is stable by multiplication. With unique factorization into primes, the main task is understanding primes that are in $S_2(\mathbb{Z})$.

Proof with geometry	Proof with arithmetic
We look at $p = x^2 + y^2$, that is $x^2 \equiv -y^2\,[p]$.	In $\mathbb{Z}[i]$, we have $p = N(x+iy) := (x+iy)(x-iy)$.
1. -1 is a square mod $p \Leftrightarrow p \equiv 1\,[4]$. Let $u^2 \equiv -1\,[p]$.	1. p factors $\Leftrightarrow -1$ is a square modulo p.
2. Define $\mathscr{L}(p) = \{(a,b) \in \mathbb{Z}^2 \,:\, au - b \equiv 0\,[p]\}$.	2. Compute $p\mathbb{Z}[i] = \mathfrak{p}\mathfrak{p}^*$ by factoring $T^2 + 1$ mod p.
3. Any shortest vector gives a two-square sum for p. Compute them with Gauss-Lagrange's algorithm.	3. Compute generators of $\mathfrak{p}, \mathfrak{p}^*$. Products of them and units give two-square sums.

Two classic proofs strategies

1

$S_2(\mathbb{Z})$ is stable by multiplication. With unique factorization into primes, the main task is understanding primes that are in $S_2(\mathbb{Z})$.

Proof with geometry

We look at $p = x^2 + y^2$, that is $x^2 \equiv -y^2\,[p]$.

1. -1 is a square mod $p \Leftrightarrow p \equiv 1\,[4]$.
   Let $u^2 \equiv -1\,[p]$.
2. Define $\mathscr{L}(p) = \{(a,b) \in \mathbb{Z}^2 : au - b \equiv 0\,[p]\}$.
3. Any shortest vector gives a two-square sum for p.
   Compute them with Gauss-Lagrange's algorithm.

Gauss-Lagrange is very similar to Euclidean division

Reciprocity

Proof with arithmetic

In $\mathbb{Z}[i]$, we have $p = N(x+iy) := (x+iy)(x-iy)$.

1. p factors $\Leftrightarrow -1$ is a square modulo p.
2. Compute $p\mathbb{Z}[i] = \mathfrak{p}\mathfrak{p}^*$ by factoring $T^2 + 1 \bmod p$.
3. Compute generators of $\mathfrak{p}, \mathfrak{p}^*$.
   Products of them and units give two-square sums.

This works because Euclidean ⇒ ***Principal*** ⇒UFD.

Extension to totally real fields

Let $F = \mathbb{Q}(\zeta + \zeta^{-1})$, with ζ a primitive root of unity, and $\mathcal{O}_F = \mathbb{Z}[\zeta + \zeta^{-1}]$.

We have $\alpha = x^2 + y^2$, for some $x, y \in \mathcal{O}_F$. ***No unique factorization anymore.***

Instead we have unique factorization in **prime ideals**: $\alpha\mathcal{O}_F = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}}$.

Extension to totally real fields

Let $F = \mathbb{Q}(\zeta + \zeta^{-1})$, with ζ a primitive root of unity, and $\mathcal{O}_F = \mathbb{Z}[\zeta + \zeta^{-1}]$.

We have $\alpha = x^2 + y^2$, for some $x, y \in \mathcal{O}_F$. ***No unique factorization anymore.***

Instead we have unique factorization in **prime ideals**: $\alpha\mathcal{O}_F = \prod_{\mathfrak{p}} \mathfrak{p}^{v_\mathfrak{p}}$.

Analog of $\mathbb{Q}(i)$ is $F(i)$, and reciprocity is now factoring $T^2 + 1$ modulo $\mathfrak{p}$.

That is, $\mathfrak{p}$ splits when Δ is a square in the finite field $\mathcal{O}_F/\mathfrak{p}$.

Extension to totally real fields

1

Let $F = \mathbb{Q}(\zeta + \zeta^{-1})$, with ζ a primitive root of unity, and $\mathcal{O}_F = \mathbb{Z}[\zeta + \zeta^{-1}]$.

We have $\alpha = x^2 + y^2$, for some $x, y \in \mathcal{O}_F$. ***No unique factorization anymore.***

Instead we have unique factorization in **prime ideals**: $\alpha\mathcal{O}_F = \prod_{\mathfrak{p}} \mathfrak{p}^{v_\mathfrak{p}}$.

Above, we have $\alpha\mathcal{O}_{F(i)} = (x + iy)\mathcal{O}_{F(i)} \cdot (x - iy)\mathcal{O}_{F(i)}$.

$$\mathfrak{p}\mathcal{O}_{F(i)} = \begin{cases} \mathfrak{P}\mathfrak{P}^* & \text{, if } \mathfrak{p} \text{ splits} \\ \mathfrak{p} & \text{, if } \mathfrak{p} \text{ is inert} \\ (\mathfrak{P}^2 & \text{, if } \mathfrak{p} \text{ ramifies)} \end{cases}$$

These ideals: 1) must share the prime factors of α
2) have **conjugated** prime factors.

This implies $\alpha\mathcal{O}_{F(i)} = \prod_{\mathfrak{p}\ splits} (\mathfrak{P}\mathfrak{P}^*)^{v_\mathfrak{P}} \cdot \prod_{\mathfrak{p}\ inert} \mathfrak{p}^{2v_\mathfrak{p}}$.

Extension to totally real fields

Let $F = \mathbb{Q}(\zeta + \zeta^{-1})$, with ζ a primitive root of unity, and $\mathcal{O}_F = \mathbb{Z}[\zeta + \zeta^{-1}]$.

We have $\alpha = x^2 + y^2$, for some $x, y \in \mathcal{O}_F$. ***No unique factorization anymore.***

Instead we have unique factorization in **prime ideals**: $\alpha\mathcal{O}_F = \prod_{\mathfrak{p}} \mathfrak{p}^{v_\mathfrak{p}}$.

Above, we have $\alpha\mathcal{O}_{F(i)} = (x+iy)\mathcal{O}_{F(i)} \cdot (x-iy)\mathcal{O}_{F(i)}$

$$= \prod_{\mathfrak{p}\ splits} (\mathfrak{P}\mathfrak{P}^*)^{v_\mathfrak{P}} \cdot \prod_{\mathfrak{p}\ inert} \mathfrak{p}^{2v_\mathfrak{p}}.$$

$$\mathfrak{p}\mathcal{O}_{F(i)} = \begin{cases} \mathfrak{P}\mathfrak{P}^* & \text{, if } \mathfrak{p} \text{ splits} \\ \mathfrak{p} & \text{, if } \mathfrak{p} \text{ is inert} \\ (\mathfrak{P}^2 & \text{, if } \mathfrak{p} \text{ ramifies)} \end{cases}$$

Theorem (up to ramification):
The set of elements in $\mathcal{O}_F$ that can be written as the sum of two $\mathcal{O}_F$-squares is

$$S_2(\mathcal{O}_F) = \{\alpha \in \mathcal{O}_F \,:\, \alpha\mathcal{O}_F = \prod_{\mathfrak{p}\ splits} \mathfrak{p}^{v_\mathfrak{p}} \cdot \prod_{\mathfrak{p}\ inert} \mathfrak{p}^{2v_\mathfrak{p}}\}$$

From two-squares to module lattices isomorphisms

Computing sums of squares

$$S_2(\mathcal{O}_F) = \{\alpha \in \mathcal{O}_F \,:\, \alpha\mathcal{O}_F = \prod_{\mathfrak{p}\; splits} \mathfrak{p}^{v_\mathfrak{p}} \cdot \prod_{\mathfrak{p}\; inert} \mathfrak{p}^{2v_\mathfrak{p}}\}$$

Observations:

1) We can compute these primes given α
2) Must be at least **one principal ideal** $(x + iy)\mathcal{O}_{F(i)}$ among all meaningful products of these primes

Computing sums of squares

2

$$S_2(\mathcal{O}_F) = \{\alpha \in \mathcal{O}_F \,:\, \alpha\mathcal{O}_F = \prod_{\mathfrak{p}\ splits} \mathfrak{p}^{v_\mathfrak{p}} \cdot \prod_{\mathfrak{p}\ inert} \mathfrak{p}^{2v_\mathfrak{p}}\}$$

Observations:

1) We can compute these primes given α
2) Must be at least **one principal ideal** $(x + iy)\mathcal{O}_{F(i)}$ among all meaningful products of these primes

To test if an ideal is principal in number fields and to compute a generator is a (classically) hard problem!

And we may not even find the correct generator…

Computing sums of squares

2

$$S_2(\mathcal{O}_F) = \{\alpha \in \mathcal{O}_F \,:\, \alpha\mathcal{O}_F = \prod_{\mathfrak{p}\ splits} \mathfrak{p}^{v_\mathfrak{p}} \cdot \prod_{\mathfrak{p}\ inert} \mathfrak{p}^{2v_\mathfrak{p}}\}$$

Observations:

1) We can compute these primes given α
2) Must be at least **one principal ideal** $(x+iy)\mathcal{O}_{F(i)}$ among all meaningful products of these primes
3) We know the relative norm $N_{F(i)|F}(x+iy) = \alpha$.

Recover generators up to **roots of unity**

Computing sums of squares

2

$$S_2(\mathcal{O}_F) = \{\alpha \in \mathcal{O}_F \,:\, \alpha\mathcal{O}_F = \prod_{\mathfrak{p}\ splits} \mathfrak{p}^{v_\mathfrak{p}} \cdot \prod_{\mathfrak{p}\ inert} \mathfrak{p}^{2v_\mathfrak{p}}\}$$

Observations:

1) We can compute these primes given α
2) Must be at least **one principal ideal** $(x+iy)\mathcal{O}_{F(i)}$ among all meaningful products of these primes
3) We know the relative norm $N_{F(i)|F}(x+iy) = \alpha$.

Recover generators up to **roots of unity**

Gentry-Szydlo's algorithm:

There is a **polynomial time** algorithm that, given a basis of an ideal I in a cyclotomic field, and a candidate β for the relative norm of a potential generator g of I:

1) Decides if I is principal;
2) If it is, returns an element $g' = \rho g$ where ρ is a root of unity in the field.

Computing sums of squares

2

$$S_2(\mathcal{O}_F) = \{\alpha \in \mathcal{O}_F \,:\, \alpha\mathcal{O}_F = \prod_{\mathfrak{p}\ splits} \mathfrak{p}^{v_\mathfrak{p}} \cdot \prod_{\mathfrak{p}\ inert} \mathfrak{p}^{2v_\mathfrak{p}}\}$$

Observations:

1) We can compute these primes given α
2) Must be at least **one principal ideal** $(x+iy)\mathcal{O}_{F(i)}$ among all meaningful products of these primes
3) We know the relative norm $N_{F(i)|F}(x+iy) = \alpha$.
4) We can also compute the roots of unity in $F(i)$.

Recover all **useful** generators, in **polynomial time,** by solving **relative norm equations**

An algorithm to compute sums-of-squares

Input: $\alpha \in \mathcal{O}_F$

Output : the set $S_2(\alpha)$ of all possible $(x, y) \in \mathcal{O}_F^2$ such that $x^2 + y^2 = \alpha$.

1. Factor $\alpha\mathcal{O}_F = \prod_{splits} \mathfrak{p}^{v_\mathfrak{p}} \cdot \prod_{inerts} \mathfrak{q}^{v_\mathfrak{q}}$; set $\mathcal{S} = \emptyset$; if one $v_\mathfrak{q}$ is not even, return $\mathcal{S}$.
2. For all $0 \leq e_\mathfrak{p} \leq v_\mathfrak{p}$, do:
   a. Compute $I = \prod_{splitters} \mathfrak{P}^{e_\mathfrak{P}}(\mathfrak{P}*)^{v_\mathfrak{P}-e_\mathfrak{P}} \cdot \prod_{inerts} \mathfrak{q}^{v_\mathfrak{q}/2}$ and set $\mathcal{G} = \emptyset$
   b. $g \leftarrow$ GentrySzydlo(I, α);
   c. If $g \neq \perp$, set $\mathcal{G} = \{\rho \cdot g \ : \ \rho$ root of unity in $F(i)\}$.
   d. For all $g' \in \mathcal{G}$, write $g' = x + iy$ and $\mathcal{S} = \mathcal{S} \cup \{(x, y)\}$
3. Return $\mathcal{S} \cap \mathcal{O}_F^2$.

An algorithm to compute sums-of-squares

Input: $\alpha \in \mathcal{O}_F$

Output : the set $S_2(\alpha)$ of all possible $(x, y) \in \mathcal{O}_F^2$ such that $x^2 + y^2 = \alpha$.

1. Factor $\alpha\mathcal{O}_F = \prod_{splits} \mathfrak{p}^{v_\mathfrak{p}} \cdot \prod_{inerts} \mathfrak{q}^{v_\mathfrak{q}}$; set $\mathcal{S} = \varnothing$; if one $v_\mathfrak{q}$ is not even, return $\mathcal{S}$.
2. For all $0 \leq e_\mathfrak{p} \leq v_\mathfrak{p}$, do:
   a. Compute $I = \prod_{splitters} \mathfrak{P}^{e_\mathfrak{P}}(\mathfrak{P}*)^{v_\mathfrak{P} - e_\mathfrak{P}} \cdot \prod_{inerts} \mathfrak{q}^{v_\mathfrak{q}/2}$ and set $\mathcal{G} = \varnothing$
   b. $g \leftarrow$ GentrySzydlo(I, α);
   c. If $g \neq \perp$, set $\mathcal{G} = \{\rho \cdot g \ : \ \rho$ root of unity in $F(i)\}$.
   d. For all $g' \in \mathcal{G}$, write $g' = x + iy$ and $\mathcal{S} = \mathcal{S} \cup \{(x, y)\}$
3. Return $\mathcal{S} \cap \mathcal{O}_F^2$.

Not polynomial time if the factorization is not given.

Possibly **many** combinations

$\mathcal{O}_F + i\mathcal{O}_F \subsetneq \mathcal{O}_{F(i)}$ in general

An algorithm to solve totally real modLIP

2

Input: the public Gram matrix $\mathbf{G} = \mathbf{B}^t\mathbf{B} = \begin{bmatrix} g_0 & \star \\ \star & g_1 \end{bmatrix}$ and a matrix $\mathbf{C}$ such that $\mathbf{C}^t\mathbf{C} = \mathbf{U}^t\mathbf{G}\mathbf{U}$

Output : the set of $\mathbf{U} \in GL_2(\mathcal{O}_F)$ describing the congruence class of $\mathbf{G}$

1. For $b \in \{0,1\}$:
   a. $\mathcal{S}_b \leftarrow$ TwoSquares(g_b)
2. Let $\mathcal{U} = \emptyset$.
   For all $(a, b), (a', b') \in \mathcal{S}_0 \times \mathcal{S}_1$:
   a. $\mathbf{D} \leftarrow \begin{bmatrix} a & a' \\ b & b' \end{bmatrix}$
   b. If $\mathbf{V} = \mathbf{C}^{-1}\mathbf{D}$ is a congruence matrix for $\mathbf{G}$, set $\mathcal{U} = \mathcal{U} \cup \{\mathbf{V}\}$.
3. Return $\mathcal{U}$.

Theorem (Mureau, Pellet—Mary, Pliatsok, W.)

This algorithm returns (a description of) the congruence class of $\mathbf{G}$.

Possibly **many** steps.

Towards polynomial time: the randomization step (1/2)

Goal: avoid factoring and control loops to achieve (classic) polynomial time

With $\mathbf{G} = \mathbf{B}^t\mathbf{B}$, from vectors in $\mathcal{O}_F^2$ we can learn the norm of vectors in $\mathcal{L}(\mathbf{B})$:

$$(x, y)\mathbf{G}(x, y)^t = (x, y)\mathbf{B}^t \cdot \mathbf{B}(x, y)^t = a^2 + b^2$$

If we have two that are linearly independent, we deduce congruence matrices by linear algebra:

$$\mathbf{D} = \mathbf{CV} \sim \mathbf{D}' = \mathbf{CVX}$$

$$(a, b) = \mathbf{B}(x, y)$$

$$\mathbf{X} = \begin{bmatrix} x & x' \\ y & y' \end{bmatrix}$$

<u>Lemma:</u> we can sample Gaussians $(x, y) \in \mathcal{O}_F^2$ so that $\mathbf{B}(x, y)$ is spherical, without knowing $\mathbf{B}$.

(This way we have at least *some* control over (a, b))

Towards polynomial time: the randomization step (2/2)

Goal: avoid factoring and control loops to achieve (classic) polynomial time

Randomization step: feed *random* vectors $(x, y) \in \mathcal{O}_F^2$ to $\mathbf{G}$ until:

- Two of them span the space
- These two have a prime relative norm, that is, $(x, y)\mathbf{G}(x, y)^t = a^2 + b^2$ is a prime in $\mathcal{O}_F$.

$\Rightarrow$ compute the corresponding sum of squares **without having to factor!**

$\Rightarrow$ primes in F have at most two divisors in $F(i)$ so poly($[F : \mathbb{Q}]$) steps in the loop at worst.

Heuristic assumption:

With large enough width, $q := a^2 + b^2$ behaves like a « uniformly random » principal ideal.

(GRH) Proba$\big(q$ is prime$\big) \approx \dfrac{1}{\rho_F \cdot \ln N(q)}$, ρ_F residue at 1 of the Dedekind zeta function of F.

Conclusion for modLIP over totally real fields

Theorem (Mureau, Pellet—Mary, Pliatsok, W.)
Let F be a totally real number field with ring of integers $\mathcal{O}_F$.
There is an algorithm that solves modLIP over rank 2 free $\mathcal{O}_F$-modules in heuristic polynomial-time (in ρ_F, $[F:\mathbb{Q}]$).

- The full algorithm is implemented for cyclotomic fields with conductor $m = 4k$.
  https://gitlab.inria. fr/capsule/code-for-module-lip

- In the paper[1], we provide an algorithm for rank 2 (non-free) modules and its tools. It also runs in polynomial-time (depending on an additional, precomputable quantity).

[1] : ePrint 2024/441

ModLIP in rank 2, over CM-extensions

Alexandre Wallet, Maths for PQC workshop, 5/08/2024

Back to the general case (or almost)

For simplicity: let $K = \mathbb{Q}(\zeta)$ where ζ is a primitive root of unity, and $F = \mathbb{Q}(\zeta + \zeta^{-1})$. Assume $i \in K$.

$$\mathbf{G}_{pub} = \begin{bmatrix} g_0 & \star \\ \star & g_1 \end{bmatrix} = \begin{bmatrix} x^*x + y^*y & \star \\ \star & z^*z + w^*w \end{bmatrix} = \mathbf{B}^*\mathbf{B}$$

We can write $x = x_{\mathbb{R}} + ix_{\mathbb{I}} \in K = F + iF$ and $x^*x = x_{\mathbb{R}}^2 + x_{\mathbb{I}}^2$ (and similarly for y, z, w).

So we can recover $\mathbf{B}$ if we can compute all **sums of four squares** that give g_0, g_1.

Back to the general case (or almost)

For simplicity: let $K = \mathbb{Q}(\zeta)$ where ζ is a primitive root of unity, and $F = \mathbb{Q}(\zeta + \zeta^{-1})$. Assume $i \in K$.

$$\mathbf{G}_{pub} = \begin{bmatrix} g_0 & \star \\ \star & g_1 \end{bmatrix} = \begin{bmatrix} x^*x + y^*y & \star \\ \star & z^*z + w^*w \end{bmatrix} = \mathbf{B}^*\mathbf{B}$$

We can write $x = x_{\mathbb{R}} + ix_{\mathbb{I}} \in K = F + iF$ and $x^*x = x_{\mathbb{R}}^2 + x_{\mathbb{I}}^2$ (and similarly for y, z, w).

So we can recover $\mathbf{B}$ if we can compute all **sums of four squares** that give g_0, g_1.

This links to **Lagrange's four square theorem:** Every integer can be written as the sum of four integers squared.

At least two proofs:

- a **geometric** one with short vectors (mostly for prime integers)
- an algebraic proof using **quaternions**

We need:

- An **algorithmic** version of it
- An extension to **cyclotomic integers**

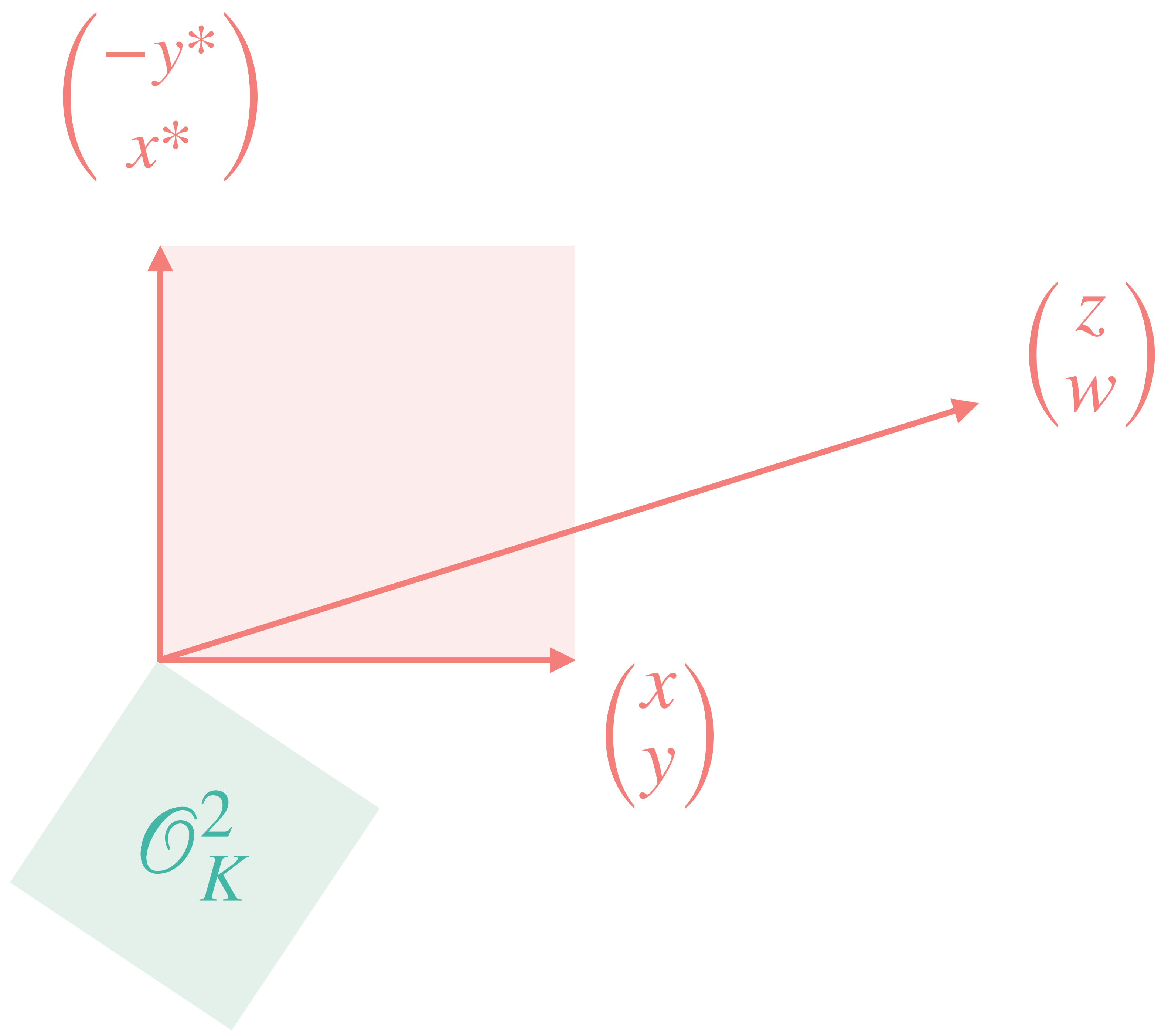
The nice case: cyclotomic modLIP over $\mathcal{O}_K^2$ (1/2)

Geometric view[1]

$\mathbf{G} = \mathbf{B}^*\mathbf{B}$ with $\mathbf{B} = \begin{bmatrix} x & z \\ y & w \end{bmatrix}$ and $\det \mathbf{B} = 1$ (a basis of $\mathcal{O}_K^2$)

Another interesting basis: $\mathbf{S} = \begin{bmatrix} x & -y^* \\ y & x^* \end{bmatrix}$.

It is essentially unitary: $\mathbf{S}^*\mathbf{S} = g_0 \cdot \mathbf{I}_2$



[1] : Thomas and Heorhii, ePrint 2024/1148

The nice case: cyclotomic modLIP over $\mathcal{O}_K^2$ (1/2)

Geometric view[1]

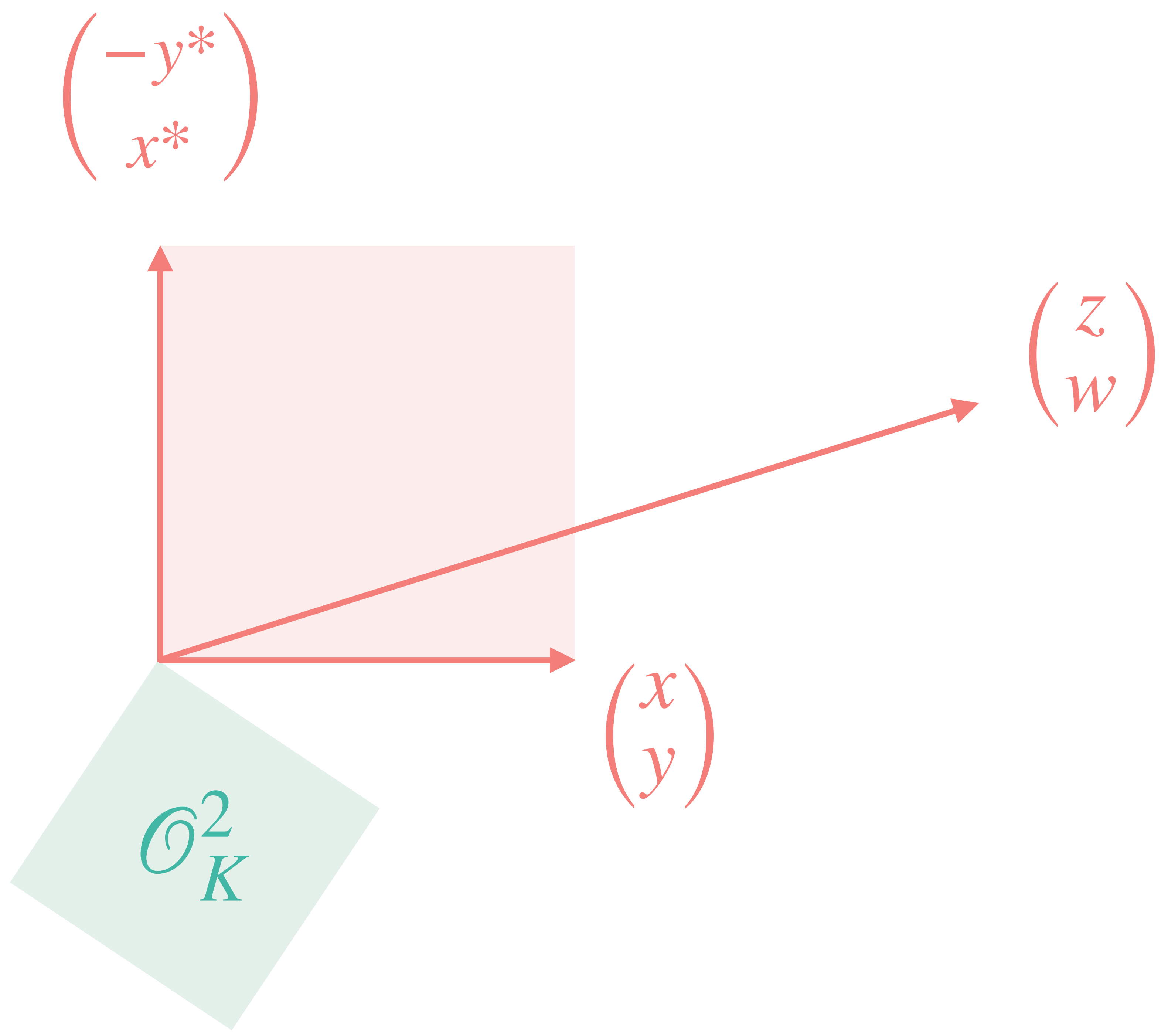
$\mathbf{G} = \mathbf{B}^*\mathbf{B}$ with $\mathbf{B} = \begin{bmatrix} x & z \\ y & w \end{bmatrix}$ and $\det \mathbf{B} = 1$ (a basis of $\mathcal{O}_K^2$)

Another interesting basis: $\mathbf{S} = \begin{bmatrix} x & -y^* \\ y & x^* \end{bmatrix}$.

It is essentially unitary: $\mathbf{S}^*\mathbf{S} = g_0 \cdot \mathbf{I}_2$.

Coordinate-wise: $\mathbf{B}^{-1}\mathbf{S} = \begin{bmatrix} 1 & -g_{01} \\ 0 & g_0 \end{bmatrix} =: \mathbf{T}$

$\Rightarrow \mathscr{L}(\mathbf{T}^*)$ is a public hypercubic lattice, and it has a secret orthogonal basis $\mathbf{S}^*$.



[1] : Thomas and Heorhii, ePrint 2024/1148

The nice case: cyclotomic modLIP over $\mathcal{O}_K^2$

Geometric view[1]

The lattice spanned by $\mathbf{T}^* = \begin{bmatrix} 1 & 0 \\ -g_{01}^* & g_0 \end{bmatrix}$ is similar to lattices from two-squares:

$$\mathcal{L}(g_0) = \{(a, b) \in \mathcal{O}_K^2 \ : \ g_{01}^* a - b = 0 \ [g_0]\}$$

where $g_{01}^* g_{01} \equiv -1 \ [g_0]$: -1 is a two-squares sums mod g_0

Conclusion[1]:

An oracle to compute an orthogonal basis in a hyper cubic lattice recovers (x, y).

Observation:

$\mathbf{S} = \begin{bmatrix} x & -y^* \\ y & x^* \end{bmatrix}$ is actually a matrix representation for a **quaternion.**

[1] : Thomas and Heorhii, ePrint 2024/1148

Sprinkles of quaternion algebra

Let $i^2 = -1$, and j such that $-ji = ij =: k$ and $j^2 = k^2 = -1$.

Quaternion algebra	$\mathscr{A} := F\langle i, j\rangle$	$\sim F + iF + jF + kF$
	$\cup$	
CM-extension of F	$K = F(i)$	$\sim F + iF$
	$\cup$	
Totally real number field	F	

There is an involution extending the conjugation:

$$(a + ib + jc + kd)^* = a - ib - jc - kd$$

There is a norm map extending the relative norm from $F(i) \mid F$:

$$\mathrm{Nrd}(a + ib + jc + kd) = a^2 + b^2 + c^2 + d^2 \in F$$

Using that $\mathscr{A} = K + Kj$, we can represent elements as matrices of multiplication:

$$x + yj \mapsto \begin{bmatrix} x & -y^* \\ y & x^* \end{bmatrix}$$

Now that we have more algebra:

$$\mathbf{G}_{pub} = \begin{bmatrix} g_0 & g_{01} \\ \cdot & g_1 \end{bmatrix} = \begin{bmatrix} x^*x + y^*y & x^*z + y^*w \\ \cdot & z^*z + w^*w \end{bmatrix} = \mathbf{B}^*\mathbf{B}$$

Observations:

- We have not used the anti-diagonal term g_{01} yet
- As we reduced to sums-of-squares computations, maybe we can mimic the previous strategy

Now that we have more algebra:

$$\mathbf{G}_{pub} = \begin{bmatrix} g_0 & g_{01} \\ \cdot & g_1 \end{bmatrix} = \begin{bmatrix} x^*x + y^*y & x^*z + y^*w \\ \cdot & z^*z + w^*w \end{bmatrix} = \mathbf{B}^*\mathbf{B}$$

Observations:

- We have not used the anti-diagonal term g_{01} yet
- As we reduced to sums-of-squares computations, maybe we can mimic the previous strategy

The non commutative-settings brings a lot of inconveniences:

	$F(i)$	$F\langle i, j\rangle$
Unique factorisation in prime ideals	Yes	Not for sided ideals
Maximal ring of integers	1	Many
Roots of unity	Straightforward	Depends on the subring
Algorithms for norm equations	Some poly-time	All known exp-time

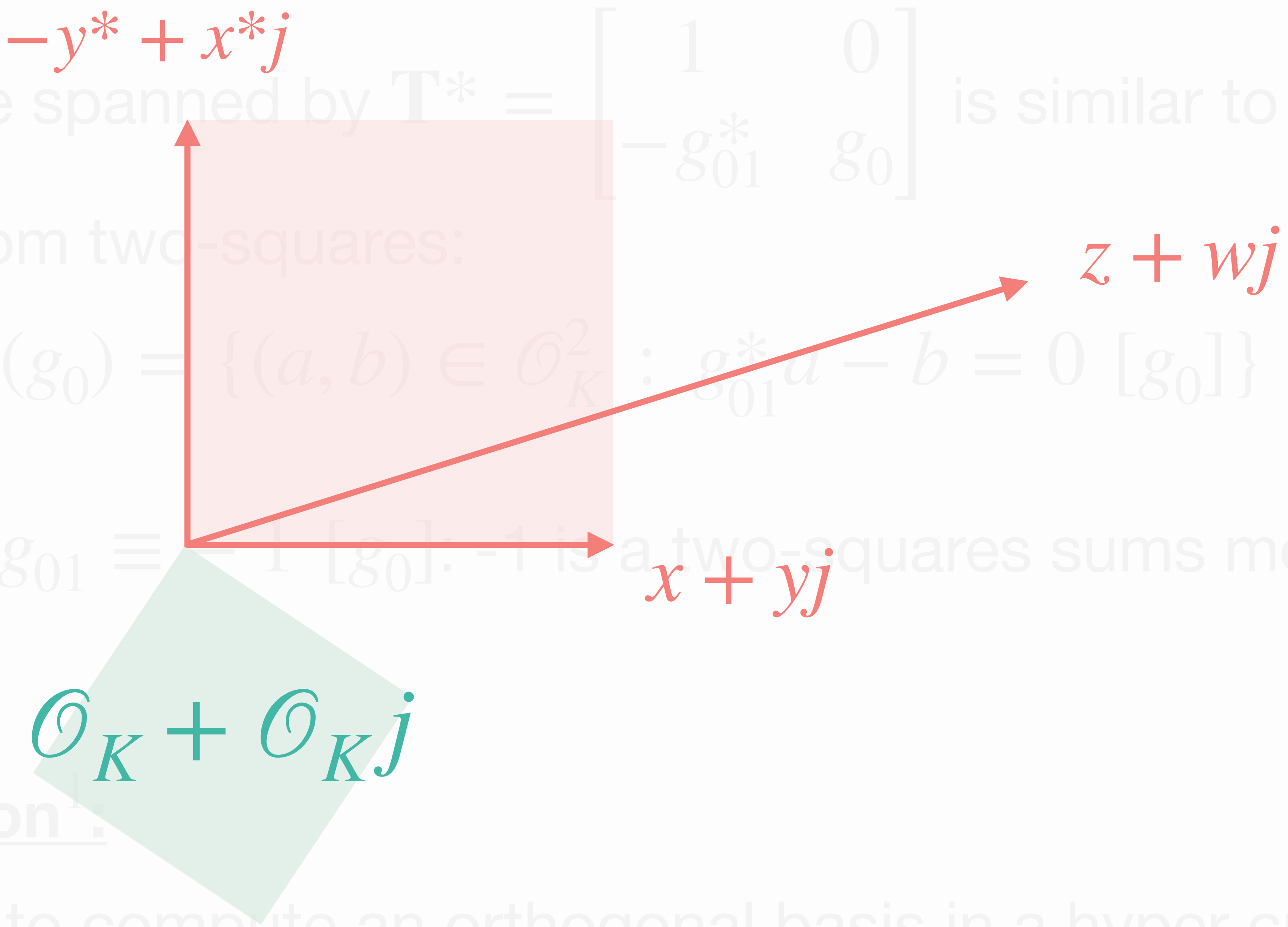
The nice case: cyclotomic modLIP over $\mathcal{O}_K^2$ (2/2)

Geometric view[1]

The lattice spanned by $\mathbf{T}^* = \begin{bmatrix} 1 & 0 \\ -g_{01}^* & g_0 \end{bmatrix}$ is similar to lattices from two-squares:

$$\mathcal{L}(g_0) = \{(a,b) \in \mathcal{O}_K^2 \ : \ g_{01}^* a - b = 0 \ [g_0]\}$$

where $g_{01}^* g_{01} \equiv -1 \ [g_0]$: -1 is a two-squares sums mod g_0



Conclusion[1]:

An oracle to compute an orthogonal basis in a hyper cubic lattice recovers (x, y).

Quaternion view[2]

- $\mathcal{O}_K^2$ identifies to the maximal order $\mathcal{O}_K + \mathcal{O}_K j$.
  It is generated by $\alpha = x + yj$ and $\beta = z + wj$.
- The matrix $\mathbf{S}$ represents the quaternion $x + yj$, so:

$$\mathbf{S}^{-1}\mathbf{B} = \mathbf{T} \ \Rightarrow \alpha^{-1}\beta = g_0^{-1}(g_{01} + j)$$

Lemma: we can compute a basis of $\alpha(\mathcal{O}_K + \mathcal{O}_K j)$ from the public data.

[1] : Thomas and Heorhii, ePrint 2024/1148

[2] : with Clémence, Guilhem, Alice and Pierre-Alain, ePrint 2024/1147

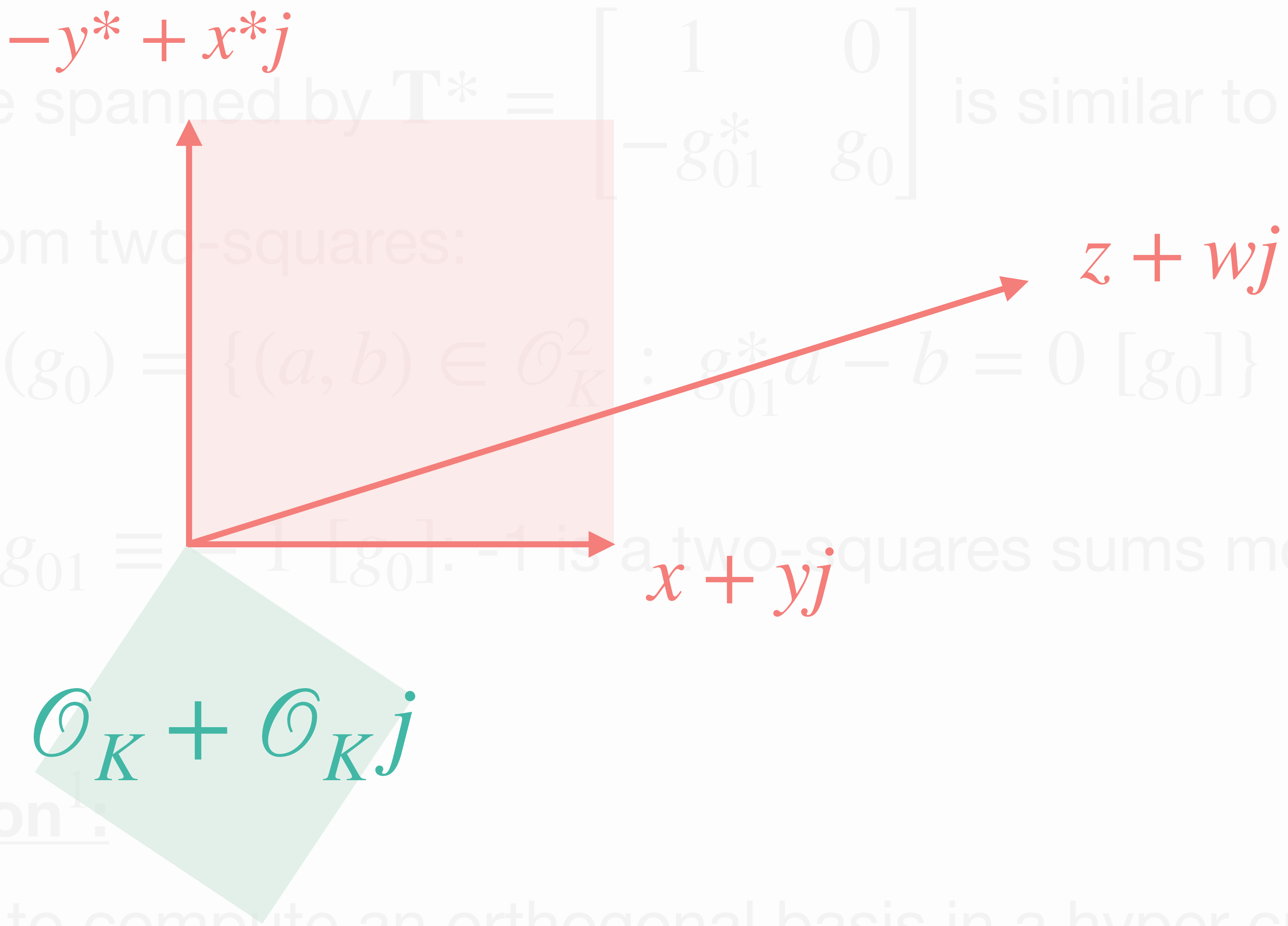
The nice case: cyclotomic modLIP over $\mathcal{O}_K^2$ (2/2)

Geometric view[1]

The lattice spanned by $\mathbf{T}^* = \begin{bmatrix} 1 & 0 \\ -g_{01}^* & g_0 \end{bmatrix}$ is similar to lattices from two-squares:

$$\mathcal{L}(g_0) = \{(a,b) \in \mathcal{O}_K^2 \ : \ g_{01}^* a - b = 0 \ [g_0]\}$$

where $g_{01}^* g_{01} \equiv -1 \ [g_0]$: -1 is a two-squares sums mod g_0



<u>Conclusion</u>[1]:

An oracle to compute an orthogonal basis in a hyper cubic lattice recovers (x, y).

Quaternion view[2]

- $\mathcal{O}_K^2$ identifies to the maximal order $\mathcal{O}_K + \mathcal{O}_K j$.
  It is generated by $\alpha = x + yj$ and $\beta = z + wj$.
- The matrix $\mathbf{S}$ represents the quaternion $x + yj$, so:

$$\mathbf{S}^{-1}\mathbf{B} = \mathbf{T} \ \Rightarrow \alpha^{-1}\beta = g_0^{-1}(g_{01} + j)$$

<u>Lemma:</u> we can compute a basis of $\alpha(\mathcal{O}_K + \mathcal{O}_K j)$ from the public data.

We have the norm of α since $\mathrm{Nrd}(\alpha) = g_0$.

$\Rightarrow$ **we recover α if we can compute generators of principal ideals given their relative norm.**

[1] : Thomas and Heorhii, ePrint 2024/1148

[2] : with Clémence, Guilhem, Alice and Pierre-Alain, ePrint 2024/1147

The nice case: cyclotomic modLIP over $\mathcal{O}_K^2$

3

Geometric view[1]	Quaternion view[2]

Geometric view[1]

The lattice spanned by $\mathbf{T}^* = \begin{bmatrix} 1 & 0 \\ -g_{01}^* & g_0 \end{bmatrix}$ is hyper-cubic:

$$\mathscr{L}(g_0) = \{(a,b) \in \mathcal{O}_K^2 \ : \ g_{01}^* a - b = 0 \ [g_0]\}$$

Conclusion[1]:

An oracle to compute an orthogonal basis in a hyper cubic lattice recovers (x, y).

*(We do not know efficient algorithms to compute orthogonal bases **in large dimension**.)*

Quaternion view[2]

The public data gives a principal ideal $(x + yj)\mathcal{O}$, and we know the reduced norm of this generator.

Conclusion[2]:

Cyclotomic modLIP over $\mathcal{O}_K^2$ reduces to the quaternion version of the Principal Ideal with Relative Norm Problem.

*(We do not know an extension of Gentry-Szydlo's algorithm for this **non-commutative setting**)*

[1] : Thomas and Heorhii, ePrint 2024/1148

[2] : with Clémence, Guilhem, Alice and Pierre-Alain, ePrint 2024/1147

Conclusion for modLIP over CM-extensions

Theorem(s) ([insert the list of peeps]):

Let $K \mid F$ be a CM-extension with ring of integers $\mathcal{O}_K$.

ModLIP over rank 2 free $\mathcal{O}_K$-modules reduces to:
- Computing short orthogonal bases of hypercubic lattices
- Solving the Principal (Left)-ideal problem given the reduced norm of a generator (in quaternion algebras)

- In ePrint 2024/1147, we extend the reduction to rank 2 non-free modules.

- The reduction technique works as well directly over F totally real:
  - ✓No need for randomization anymore
  - ✓This gives a *provable* polynomial time algorithm for totally real modLIP!
    (see also an independent work[1] for an equivalent result with a different approach)

[1] : H. Luo, K. Jiang, Y. Pan and A. Wang, ePrint 2024/1173

Time to wrap-up!

Another reduction (ePrint 2024/1173)

Theorem[1]**:** Let $K \mid F$ be a CM-extension. If an additional symplectic automorphism ϕ_j of $\mathcal{O}_K^2$ is given, then free-modLIP$_K^{\mathbf{B}}$ can be solved in polynomial time.

Very high level idea:

- Knowing ϕ_j , one can construct a CM-order $\mathfrak{O}$ in which $\mathcal{O}_K^2$ is a principal ideal lattice.
- **Lenstra-Silverberg's**[2] applies: it computes a generator of $\mathcal{O}_K^2$ in polynomial time.
- This generator essentially corresponds to a column of the secret basis, up to an isometry of $\mathcal{O}_K^2$.
- (Consequence of Kronecker) Isom($\mathcal{O}_K^2$) is a known finite group of polynomial size.

[1] : H. Luo, K. Jiang, Y. Pan and A. Wang, ePrint 2024/1173

[2] : H. Lenstra, A. Silverberg: arXiv 1706.07373

Another reduction (ePrint 2024/1173)

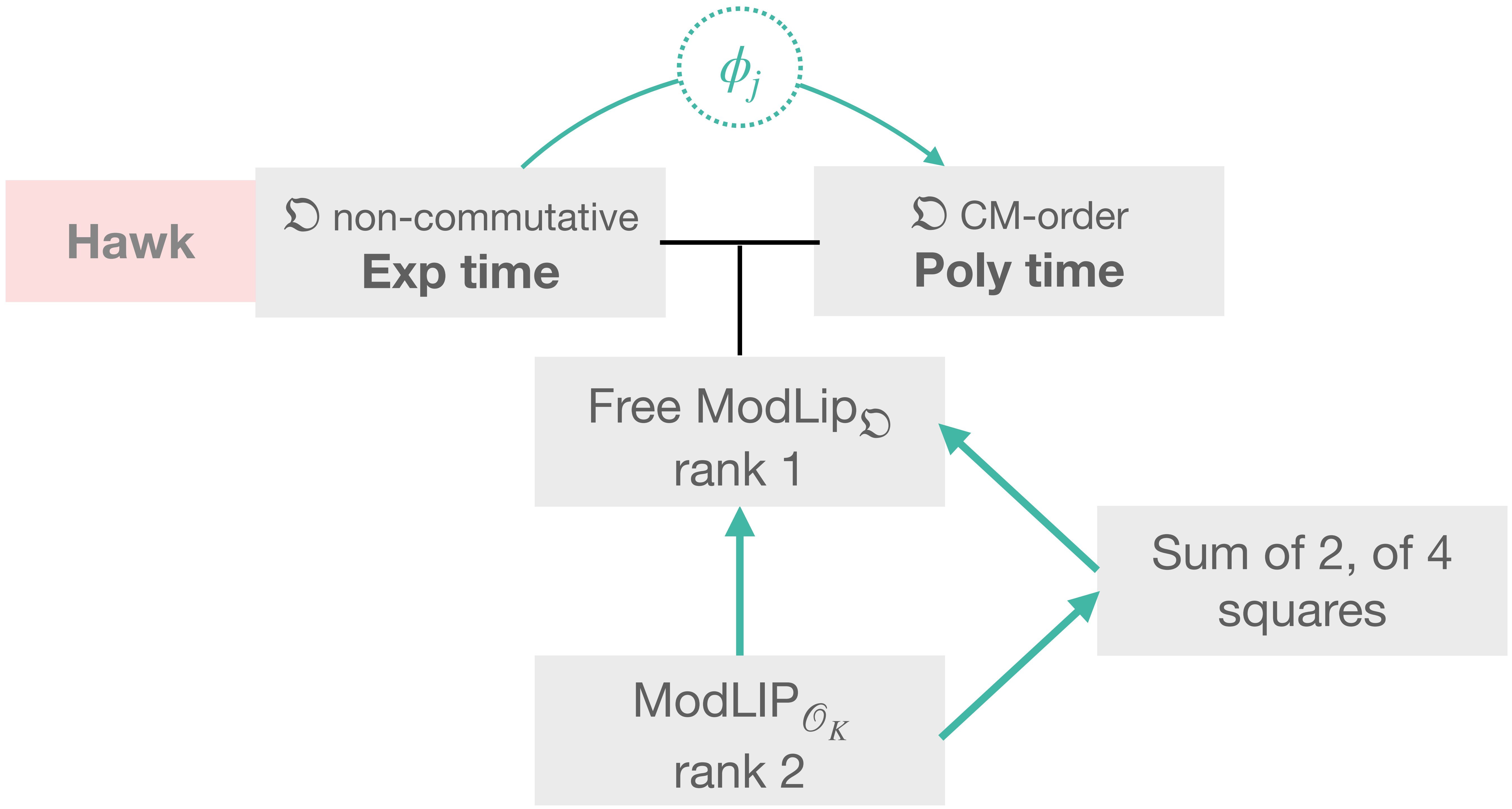
Theorem[1]**:** Let $K | F$ be a CM-extension. If an additional symplectic automorphism ϕ_j of $\mathcal{O}_K^2$ is given, then free-modLIP$_K^{\mathbf{B}}$ can be solved in polynomial time.

My very rough understanding is:

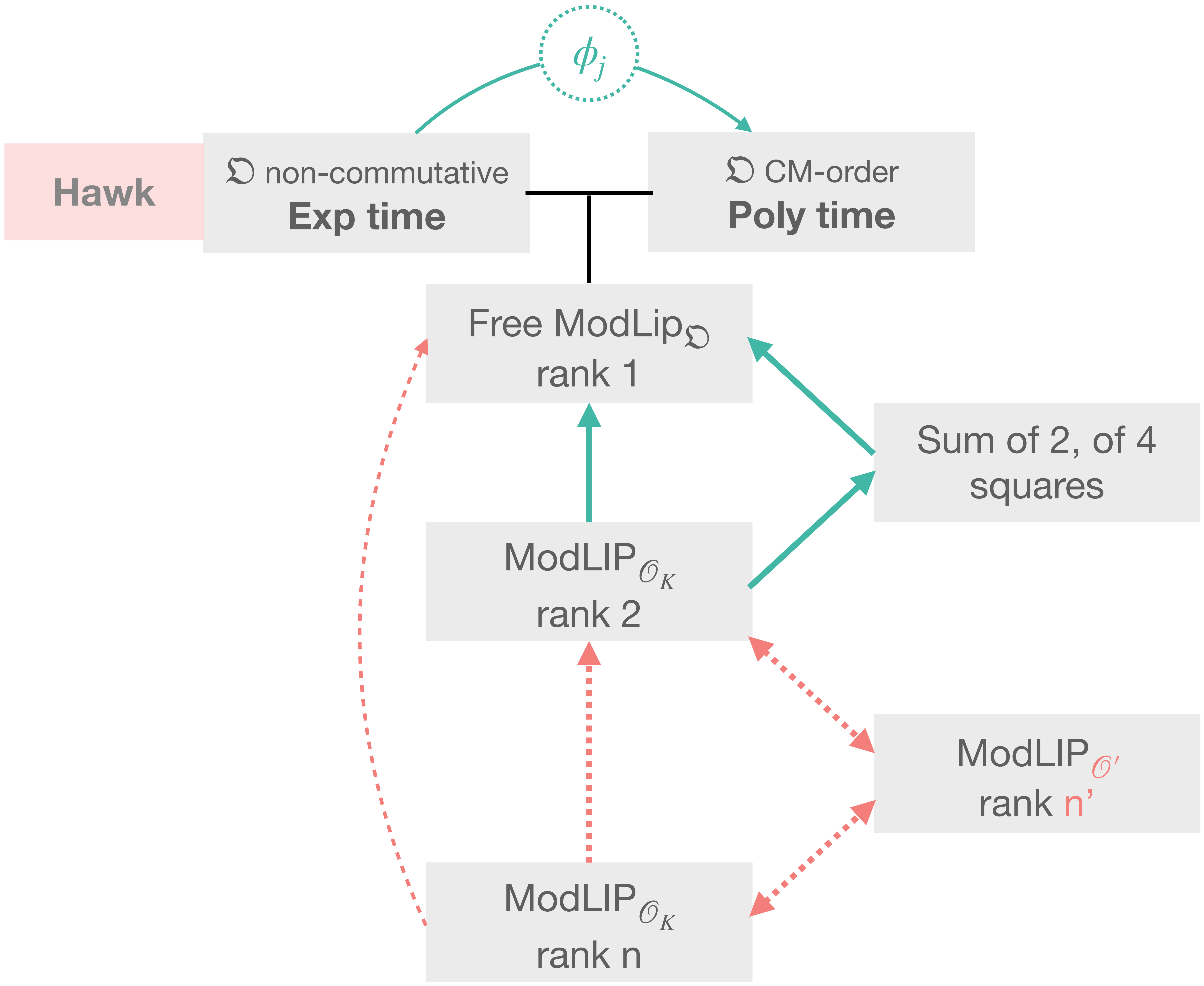
- ϕ_j corresponds to j in the quaternion.
- We need to know its action over the secret basis, but we only know its action in « the canonical one ».
- The article shows that one can easily compute the action of $\tau := [j] \circ \cdot^*$ in the secret basis from public data.

[1] : H. Luo, K. Jiang, Y. Pan and A. Wang, ePrint 2024/1173

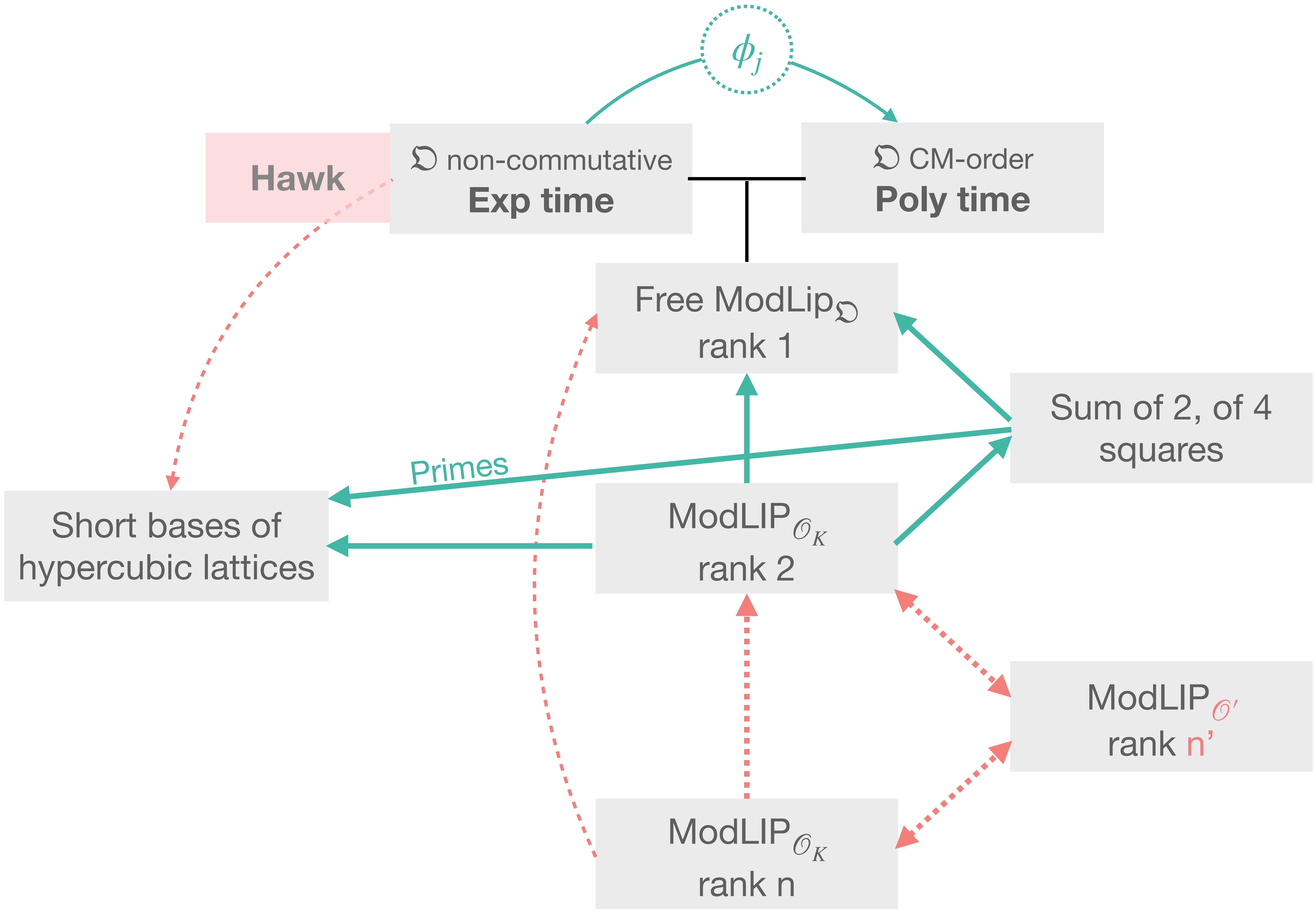
[2] : H. Lenstra, A. Silverberg: arXiv 1706.07373

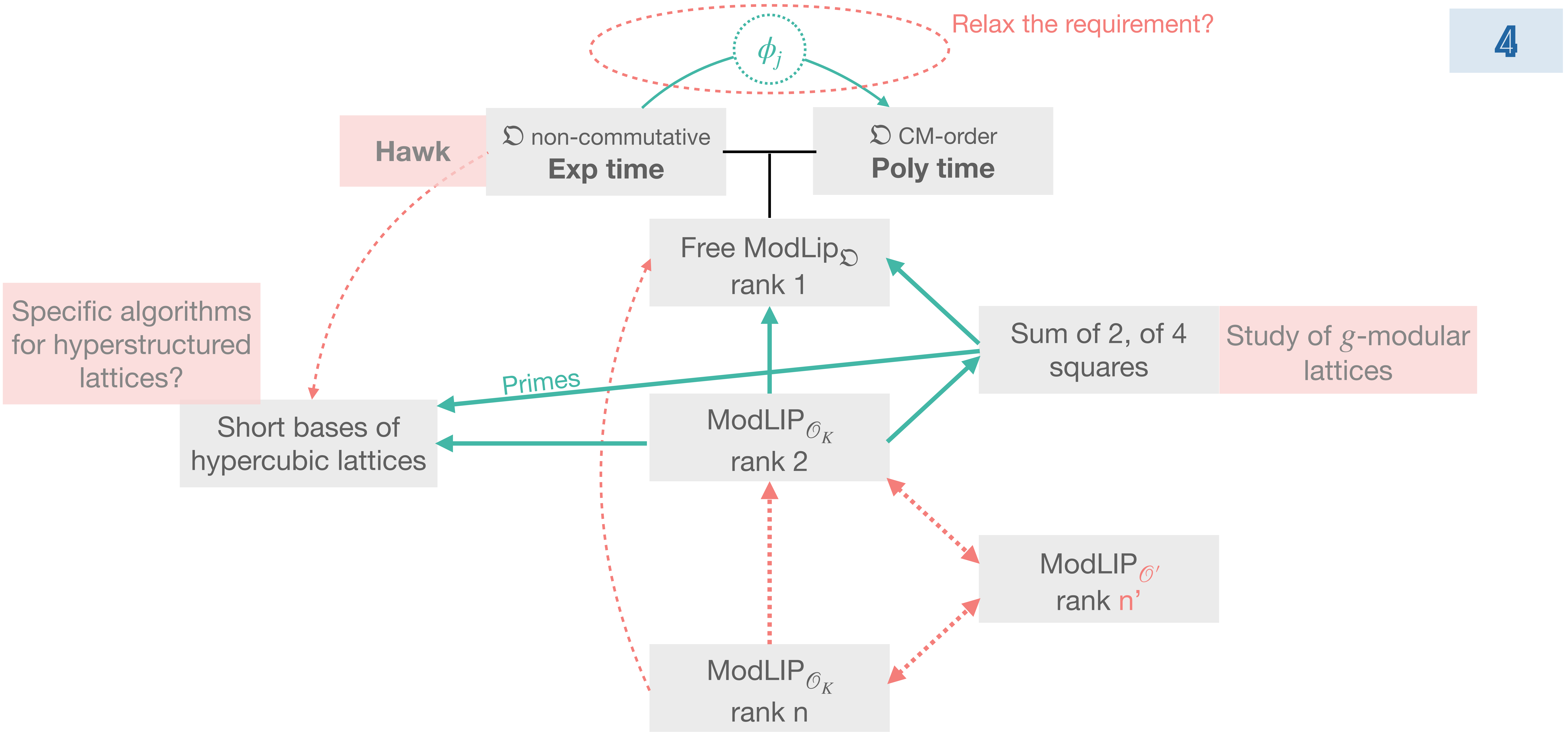

ϕ_j
Hawk
$\mathfrak{O}$ non-commutative
Exp time
$\mathfrak{O}$ CM-order
Poly time
Free ModLip$_{\mathfrak{O}}$
rank 1
Sum of 2, of 4
squares
ModLIP$_{\mathcal{O}_K}$
rank 2

4



ϕ_j
Hawk
𝔒 non-commutative
Exp time
𝔒 CM-order
Poly time
Free ModLip$_{\mathfrak{O}}$
rank 1
Sum of 2, of 4
squares
ModLIP$_{\mathcal{O}_K}$
rank 2
ModLIP$_{\mathcal{O}'}$
rank n'
ModLIP$_{\mathcal{O}_K}$
rank n


ϕ_j
Hawk
$\mathfrak{O}$ non-commutative
Exp time
$\mathfrak{O}$ CM-order
Poly time
Free ModLip$_{\mathfrak{O}}$
rank 1
Sum of 2, of 4
squares
Primes
Short bases of
hypercubic lattices
ModLIP$_{\mathcal{O}_K}$
rank 2
ModLIP$_{\mathcal{O}'}$
rank n'
ModLIP$_{\mathcal{O}_K}$
rank n



Relax the requirement?
ϕ_j
4
Hawk
non-commutative
Exp time
CM-order
Poly time
Free ModLip
rank 1
Specific algorithms for hyperstructured lattices?
Sum of 2, of 4 squares
Study of g-modular lattices
Primes
Short bases of hypercubic lattices
ModLIP$_{\mathcal{O}_K}$
rank 2
ModLIP$_{\mathcal{O}'}$
rank n'
ModLIP$_{\mathcal{O}_K}$
rank n

Relax the requirement?

ϕ_j

Hawk

↻ non-commutative
Exp time

↻ CM-order
Poly time

Free ModLip$_{↻}$
rank 1

Specific algorithms for hyperstructured lattices?

Sum of 2, of 4 squares

Study of g-modular lattices

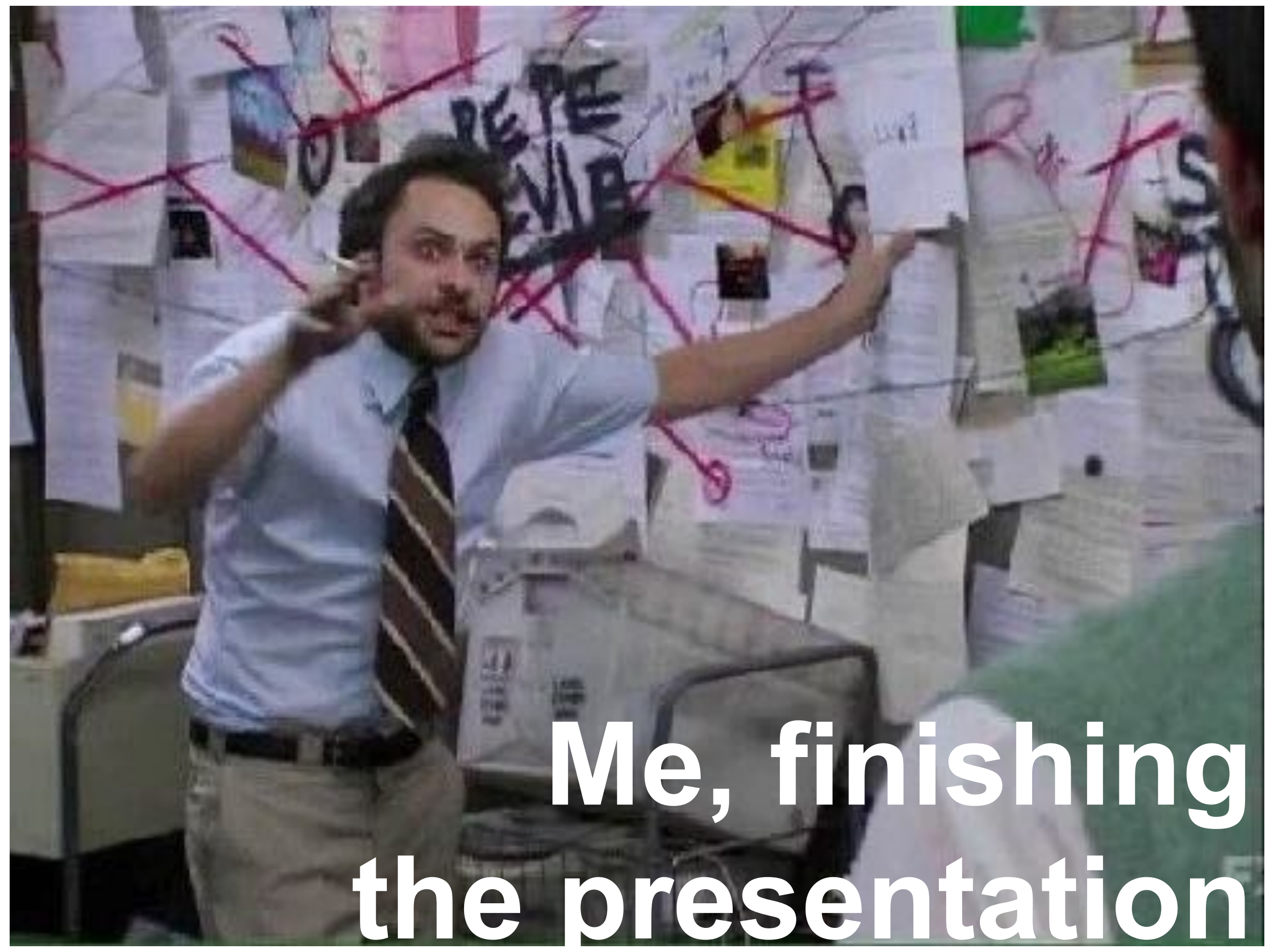
Primes

Short bases of hypercubic lattices

ModLIP$_{\mathcal{O}_K}$
rank 2

ModLIP$_{\mathcal{O}}$
rank n'

ModLIP$_{\mathcal{O}_K}$
rank n



THANK YOU!