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

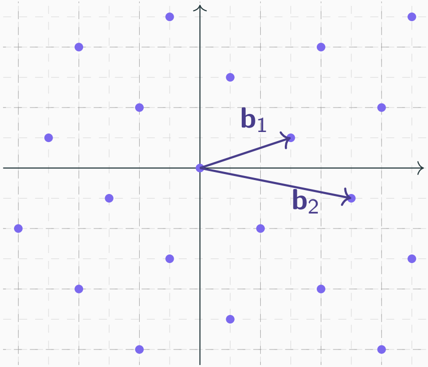
20/05/2025

Clémence Chevignard,

based on a joint work with Guilhem Mureau & Thomas Espitau & Pierre-Alain Fouque & Alice Pellet-Mary & Georges Pliatsok & Alexandre Wallet

Univ. Rennes, Inria, CNRS, Irisa, UMR 6074, France

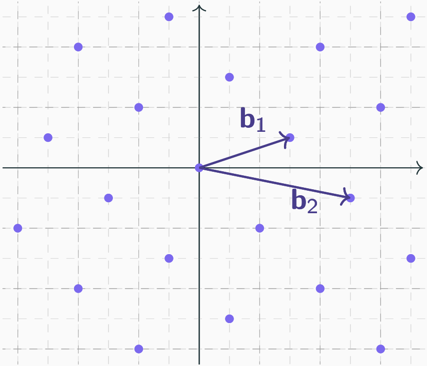
The Lattice Isomorphism Problem over $\mathbb{R}$



$$B = (\mathbf{b}_1 || \mathbf{b}_2) = \begin{pmatrix} 3 & 5 \\ 1 & -1 \end{pmatrix}$$

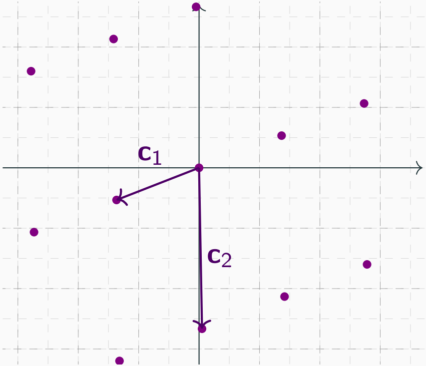
$$G := B^t B$$

The Lattice Isomorphism Problem over $\mathbb{R}$



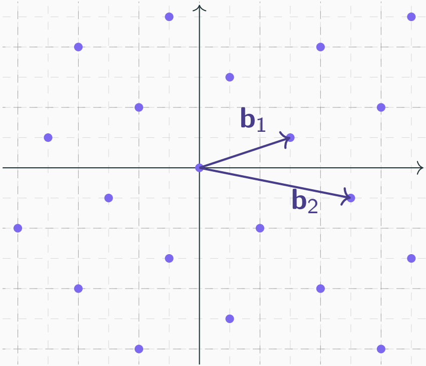
$$B = (\mathbf{b}_1 || \mathbf{b}_2) = \begin{pmatrix} 3 & 5 \\ 1 & -1 \end{pmatrix}$$
$$G := B^t B$$

$$O = \begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}$$
$$U = \begin{pmatrix} 1 & -2 \\ -1 & 1 \end{pmatrix}$$
$$C = OBU$$



$$C = (\mathbf{c}_1 || \mathbf{c}_2) = \begin{pmatrix} -2.73 & 0.10 \\ -1.07 & -5.33 \end{pmatrix}$$
$$G' := C^t C$$

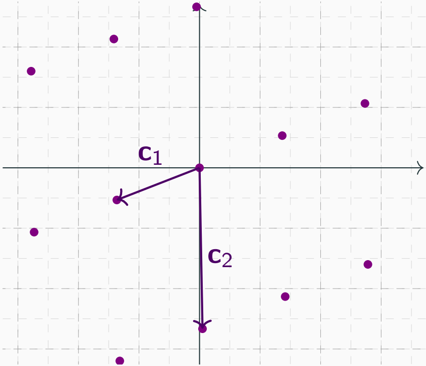
The Lattice Isomorphism Problem over $\mathbb{R}$



$$O = \begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}$$

$$U = \begin{pmatrix} 1 & -2 \\ -1 & 1 \end{pmatrix}$$

$$C = OBU$$



$$B = (\mathbf{b}_1 || \mathbf{b}_2) = \begin{pmatrix} 3 & 5 \\ 1 & -1 \end{pmatrix}$$
$$G := B^t B$$

$$C = (\mathbf{c}_1 || \mathbf{c}_2) = \begin{pmatrix} -2.73 & 0.10 \\ -1.07 & -5.33 \end{pmatrix}$$
$$G' := C^t C$$

Lattice Isomorphism Problem (LIP):

- find some $O \in O_n(\mathbb{R})$, $U \in GL_n(\mathbb{Z})$ such that, $OBU = C$.
- equivalently, find some $U \in GL_n(\mathbb{Z})$ such that $U^t \cdot G \cdot U = G'$.

The Lattice Isomorphism Problem.

In Mathematics, problem studied [DS+20; HR14; PS97] since 1997.

In Cryptography, several studies and cryptosystems based on LIP: [ARLW24; Ben+23; DW22].

$\rightarrow$ A variant of LIP in complex multiplication fields was presented [Duc+22] in 2022.

Number fields

$F := \mathbb{Q}[X]/\phi(X) \leftarrow$ **number field**.

$\mathcal{O}_F :=$ **ring of integers** of F.

$\rightarrow$ elements $e \in F$ *s.t.* , for some $P(X) \in \mathbb{Z}[X]$, $P(e) = 0$.

Number fields

$F := \mathbb{Q}[X]/\phi(X) \leftarrow$ **number field**.

$\mathcal{O}_F :=$ **ring of integers** of F.

$\rightarrow$ elements $e \in F$ *s.t.* , for some $P(X) \in \mathbb{Z}[X]$, $P(e) = 0$.

$\mathcal{O}_F$-lattice $:= \{c_1\mathbf{b_1} + \ldots + c_d\mathbf{b_d}, \mathbf{b_i} \in F^d, c_i \in \mathcal{O}_F\}$.

Fractional ideal $\mathfrak{a}$ of $F =$ additive subgroup *s.t.*

- $\mathcal{O}_F \cdot \mathfrak{a} \subset \mathfrak{a}$
- $\exists e \in \mathcal{O}_F \backslash \{0\}$ *s.t.* $e \cdot \mathfrak{a} \subset \mathcal{O}_F$

You can add, multiply, and invert them.

$\mathfrak{a}^{-1} \times \mathfrak{a} = \mathcal{O}_F$.

Number fields

$F := \mathbb{Q}[X]/\phi(X) \leftarrow$ **number field**.

All complex roots ζ of $\phi(X)$ define an embedding

$$\begin{aligned}\sigma_\zeta &: F \to \mathbb{C}\\ &: a_0 + a_1 X + \dots a_n X^n \to a_0 + a_1\zeta + \dots a_n \zeta^n\end{aligned}$$

Number fields

$F := \mathbb{Q}[X]/\phi(X) \leftarrow$ **number field**.

All complex roots ζ of $\phi(X)$ define an embedding

$$\sigma_\zeta : F \to \mathbb{C}$$
$$: a_0 + a_1 X + \ldots a_n X^n \to a_0 + a_1 \zeta + \ldots a_n \zeta^n$$

- If for all $\sigma_\zeta(F) \subset \mathbb{R}$, F is totally real. (equivalent to "each $\zeta \in \mathbb{R}$")
  If for all $\sigma_\zeta(F) \not\subset \mathbb{R}$, F is totally complex.
- If $a \in F$ is *s.t.* $\forall \sigma_\zeta$, $\sigma_\zeta(a) < 0$, then a is totally negative.

Complex Multiplication field (CM field)

$F = \mathbb{Q}[X]/\phi(X) \leftarrow$ totally real number field.

$K := F(\sqrt{a})$, with $a \in F$ totally negative $\leftarrow$ CM field, and K is totally complex.

Complex Multiplication field (CM field)

$F = \mathbb{Q}[X]/\phi(X) \leftarrow$ totally real number field.
$K := F(\sqrt{a})$, with $a \in F$ totally negative $\leftarrow$ CM field, and K is totally complex.

- **Complex conjugation on K:** $\overline{x + y\sqrt{a}} := x - y\sqrt{a}$.
- $f = Re(f) + \sqrt{a}Im(f)$.
- **Reduced norm in K:** $\mathrm{nrd}(f) := f\overline{f} = Re(f)^2 - aIm(f)^2$.
- **Hermitian transformation:**

$$\text{Given } B = \begin{pmatrix} b & d \\ c & e \end{pmatrix} \in M_2(K),\ B^* := \overline{B}^t = \begin{pmatrix} \overline{b} & \overline{c} \\ \overline{d} & \overline{e} \end{pmatrix}.$$

$\mathcal{O}_K :=$ ring of integers of K.

LIP variant we actually study

Module M in K^2: (full-rank)

$$M := \mathfrak{a}_1 \mathbf{b}_1 + \mathfrak{a}_2 \mathbf{b}_2, \quad B := (\mathbf{b}_1 || \mathbf{b}_2) \in GL_2(K), \quad \mathfrak{a}_{1,2} \text{ fractional ideals in } K$$

$$\mathbf{v} \text{ in } M \text{ is of the form } \mathbf{v} = a_1 \mathbf{b}_1 + a_2 \mathbf{b}_2, \quad a_{1,2} \in \mathfrak{a}_{1,2}.$$

- **Pseudo-basis of M: $\mathbf{B}$** $:= (B, \mathfrak{a}_1, \mathfrak{a}_2)$.
- **Pseudo-Gram matrix of M: $\mathbf{G}$** $:= (G = B^* B, \mathfrak{a}_1, \mathfrak{a}_2)$.

LIP variant we actually study

- **Pseudo-basis of** M**:** $\mathbf{B} := (B, \mathfrak{a}_1, \mathfrak{a}_2)$.
- **Pseudo-Gram matrix of** M**:** $\mathbf{G} := (G = B^* B, \mathfrak{a}_1, \mathfrak{a}_2)$.
- **Another pseudo-basis** of M: $\mathbf{C} = (C, \mathfrak{b}_1, \mathfrak{b}_2)$, with pseudo-Gram matrix $\mathbf{G}' = (G' = C^* C, \mathfrak{b}_1, \mathfrak{b}_2)$.

If $\exists U \in GL_2(K)$ *s.t.*

- $U^* G U = G'$.
- $\forall i, j,$ coeffs $U_{i,j} \in \mathfrak{a}_i \mathfrak{b}_j^{-1}$.
- $\prod_i \mathfrak{a}_i = (\det U) \prod_i \mathfrak{b}_i$.

Then G and **G**′are **congruent**.

$\mathrm{Cong}(\mathbf{G}, \mathbf{G}') =$ set of congruence matrices U.

LIP variant we actually study

- **Pseudo-basis of** M**:** $\mathbf{B} := (B, \mathfrak{a}_1, \mathfrak{a}_2)$.
- **Pseudo-Gram matrix of** M**:** $\mathbf{G} := (G = B^* B, \mathfrak{a}_1, \mathfrak{a}_2)$.
- **Another pseudo-basis** of M: $\mathbf{C} = (C, \mathfrak{b}_1, \mathfrak{b}_2)$, with pseudo-Gram matrix $\mathbf{G}' = (G' = C^* C, \mathfrak{b}_1, \mathfrak{b}_2)$.

If $\exists U \in GL_2(K)$ *s.t.*

- $U^* G U = G'$.
- $\forall i, j,$ coeffs $U_{i,j} \in \mathfrak{a}_i \mathfrak{b}_j^{-1}$.
- $\prod_i \mathfrak{a}_i = (\det U) \prod_i \mathfrak{b}_i$.

Then G and **G**′are **congruent**.

$\mathrm{Cong}(\mathbf{G}, \mathbf{G}')$ = set of congruence matrices U.

Module-LIP (modLIP): given **B**, **G**, and **G**′, compute an element of $\mathrm{Cong}(\mathbf{G}, \mathbf{G}')$.

Previous attacks on modLIP

- If K was totally real, Mureau, Pellet-Mary, Pliatsok and Wallet [Mur+24].
- With restrictions on M, Espitau and Pliatsok [EP24].
- In the same setting, Luo, Jiang, Pan, and Wang [Luo+24].

This work: polynomial time reduction to the problem of finding an ideal's generator in a quaternion algebra.

modLIP

- **Pseudo-basis of** M**:** $\mathbf{B} := (B, \mathfrak{a}_1, \mathfrak{a}_2)$.
- **Pseudo-Gram matrix of** M**:** $\mathbf{G} := (G = B^* B, \mathfrak{a}_1, \mathfrak{a}_2)$.
- **Another pseudo-basis** of M: $\mathbf{C} = (C, \mathfrak{b}_1, \mathfrak{b}_2)$, with pseudo-Gram matrix $\mathbf{G}' = (G' = C^* C, \mathfrak{b}_1, \mathfrak{b}_2)$.

$$U^* G U = G' \Leftrightarrow U^* B^* B U = C^* C$$
$$\Leftrightarrow (C' = BU, \mathfrak{b}_1, \mathfrak{b}_2) \text{ is a pseudo-basis of pseudo-Gram matrix } \mathbf{G}'$$

To compute the C':

1. Formalise the problem as a quaternion reduced norm equation.
2. Turn this reduced norm equation into the problem of "finding the generator of an ideal" in a quaternion algebra.

Retrieve C'.

Factoring G′

$K = F(\sqrt{a})$.

$$\text{If } C = \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix}, \quad G' = \begin{pmatrix} q_{1,1} & q_{1,2} \\ \overline{q_{1,2}} & q_{2,2} \end{pmatrix}, \text{ then}$$

$$x_2\overline{x_1} + y_2\overline{y_1} = q_{1,2}, x_2\overline{x_2} + y_2\overline{y_2} = q_{2,2}$$

$$\text{and } x_1\overline{x_1} + y_1\overline{y_1} = q_{1,1}$$

$$i.e. \;\; Re(x_1)^2 - aIm(x_1)^2 + Re(y_1)^2 - aIm(y_1)^2 = q_{1,1}$$

Quaternion algebras

$K = F(\sqrt{a})$.

Quaternion Algebra $\mathcal{A} \simeq F + iF + jF + ijF$, of basis $\{1, i, j, ij\}$, with

$$i^2 = a, \quad j^2 = -1, \quad \boldsymbol{ij = -ji}$$

For $f = x + iy + jz + ijt \in \mathcal{A}$,

$$\overline{f} := x - iy - jz - ijt$$
$$\mathrm{nrd}(f) := f\overline{f} = x^2 - ay^2 + z^2 - at^2$$

Quaternion algebras

$K = F(\sqrt{a})$. Quaternion Algebra $\mathcal{A} \simeq F + iF + jF + ijF$, of basis $\{1, i, j, ij\}$, with $ij = -ji$..

Order $\mathcal{O}$ of $\mathcal{A}$:
(full rank) $\mathcal{O}_F$-lattice of $\mathcal{A}$ + ring

$\rightarrow$

Left $\mathcal{O}$-ideal I in $\mathcal{A}$:
(full rank) $\mathcal{O}_F$-lattice of $\mathcal{A}$ + $\forall x \in \mathcal{O},\ xI \subset I$

Quaternion algebras

$K = F(\sqrt{a})$. Quaternion Algebra $\mathcal{A} \simeq F + iF + jF + ijF$, of basis $\{1, i, j, ij\}$, with $ij = -ji$..

Order $\mathcal{O}$ of $\mathcal{A}$:

(full rank) $\mathcal{O}_F$-lattice of $\mathcal{A}$ + ring

$\vdots$

$\mathcal{O}$ is maximal if not contained in a bigger order

$\rightarrow$

Left $\mathcal{O}$-ideal I in $\mathcal{A}$:

(full rank) $\mathcal{O}_F$-lattice of $\mathcal{A}$ + $\forall x \in \mathcal{O},\ xI \subset I$

$\vdots$

Left (resp. right) order of I is

$\mathcal{O}_\ell(I) := \{x \in \mathcal{A}\ s.t.\ xI \subset I\}$ (resp $s.t.\ Ix \subset I$)

From now on, $\mathcal{O}$ always maximal.

Quaternion algebras

Order $\mathcal{O} = \mathcal{O}_F$-lattice + subring of $\mathcal{A}$.
Left $\mathcal{O}$-Ideal $I = \mathcal{O}_F$-lattice + $\mathcal{O}I \subset I$.

- $nrd(I) := \{nrd(a), a \in I\}\mathcal{O}_F$.
- I is **principal** iff $I = \mathcal{O}g$, $g \in \mathcal{A}^\times$.

nrd Principal Ideal Problem (nrdPIP): Given I and $\mathrm{nrd}(g)$, find g.

Quaternion algebras

Order $\mathcal{O} = \mathcal{O}_F$-lattice $+$ subring of $\mathcal{A}$.
Left $\mathcal{O}$-Ideal $I = \mathcal{O}_F$-lattice $+ \mathcal{O}I \subset I$.

- $nrd(I) := \{nrd(a), a \in I\}\mathcal{O}_F$.
- I is **principal** iff $I = \mathcal{O}g$, $g \in \mathcal{A}^\times$.

nrd Principal Ideal Problem (nrdPIP): Given I and $\mathrm{nrd}(g)$, find g.

- You can add and multiply quaternion ideals.
- I is “invertible”, *i.e.* $I^{-1} \times I = \mathcal{O}_r(I)$.
- $(I + J)^{-1} = I^{-1} \cap J^{-1}$.

Quaternion algebras

Set $\mathcal{O} \supset \mathcal{O}_K + \mathcal{O}_K \times j$, and $C^*C = G'$.

$$Re(x_1)^2 - aIm(x_1)^2 + Re(y_1)^2 - aIm(y_1)^2 = q_{1,1}$$
$$\Leftrightarrow \mathrm{nrd}(x_1 + y_1 \times j) = q_{1,1}$$

[KV10, Alg. 6.3]: Finding $x_1 + y_1 j$ from $q_{1,1} \rightarrow$ **solving nrdPIP, given** $\mathcal{O}(x_1 + y_1 j)$ **and** $q_{1,1}$.

Quaternion algebras

Set $\mathcal{O} \supset \mathcal{O}_K + \mathcal{O}_K \times j$, and $C^* C = G'$.

$$Re(x_1)^2 - aIm(x_1)^2 + Re(y_1)^2 - aIm(y_1)^2 = q_{1,1}$$
$$\Leftrightarrow \mathrm{nrd}(x_1 + y_1 \times j) = q_{1,1}$$

[KV10, Alg. 6.3]: Finding $x_1 + y_1 j$ from $q_{1,1} \to$ **solving nrdPIP, given $\mathcal{O}(x_1 + y_1 j)$ and $q_{1,1}$.**

Computational steps:

1. **$C = BU$'s determinant.**
2. A useful quaternion.
3. A useful ideal.
4. **$\mathcal{O}(x_1 + y_1 j)$.**

Step 1/4: Compute C's determinant

$U =$ congruence matrix between **G** and **G**$'$, $G = B^*B$, $G' = C^*C$.

- **Clue 1:** $\prod_i \mathfrak{a}_i = (\det U) \prod_i \mathfrak{b}_i$
- **Clue 2:** $U^* G U = G'$.

$$\Rightarrow (\det U)\mathcal{O}_K = \left(\prod_i \mathfrak{a}_i\right)\left(\prod_i \mathfrak{b}_i\right)^{-1}, \text{ and } \det(U^*U) = \mathrm{nrd}(\det U) = \det G' / \det G.$$

Lenstra-Silverberg [LS14] $\rightarrow$ We get $\det U$ and $\det C = \det B \det U$ up to a root of unity in $\mathcal{O}_K$ in polynomial time.

Step 2/4: compute $\alpha\beta^{-1}$

With $C = \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix}$, $G' = \begin{pmatrix} q_{1,1} & q_{1,2} \\ \overline{q_{1,2}} & q_{2,2} \end{pmatrix}$, set $\alpha := x_1 + y_1 j$, $\beta = x_2 + y_2 j$.

$$\alpha\overline{\beta} = \ldots = \overline{q_{1,2}} - \det(C)j,$$

$$\text{so } \boldsymbol{\alpha\beta^{-1}} = \underbrace{q_{2,2}^{-1}(\overline{q_{1,2}} - \mathbf{det}(\boldsymbol{C})j)}_{\text{public datas}}$$

Step 3/4: compute an intermediary ideal

$\mathbf{B} = (B, \mathfrak{a}_1, \mathfrak{a}_2)$ with $B^*B = G$, and $\mathbf{C} = (C, \mathfrak{b}_1, \mathfrak{b}_2)$ with $C^*C = G'$ $\to$ two pseudo-bases of a module M.

$C = \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix}$, $\alpha := x_1 + y_1 j$, $\beta = x_2 + y_2 j$.

Set $I_M := \mathcal{O} \cdot \{x + yj,\ \begin{pmatrix} x \\ y \end{pmatrix} \in M\}$.

Step 3/4: compute an intermediary ideal

$\mathbf{B} = (B, \mathfrak{a}_1, \mathfrak{a}_2)$ with $B^* B = G$, and $\mathbf{C} = (C, \mathfrak{b}_1, \mathfrak{b}_2)$ with $C^* C = G'$ $\rightarrow$ two pseudo-bases of a module M.
$C = \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix}$, $\alpha := x_1 + y_1 j$, $\beta = x_2 + y_2 j$.

Set $I_M := \mathcal{O} \cdot \{x + yj, \ \begin{pmatrix} x \\ y \end{pmatrix} \in M\}$.

1. $\mathcal{O} \supset \mathcal{O}_K + \mathcal{O}_K j$ pre-computed with [Voi13, Algorithm 7.9, 7.10].

$\rightarrow$ polytime reducible to a factorisation of ideal in F.

Step 3/4: compute an intermediary ideal

$\mathbf{B} = (B, \mathfrak{a}_1, \mathfrak{a}_2)$ with $B^*B = G$, and $\mathbf{C} = (C, \mathfrak{b}_1, \mathfrak{b}_2)$ with $C^*C = G'$ $\to$ two pseudo-bases of a module M.

$C = \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix}$, $\alpha := x_1 + y_1 j$, $\beta = x_2 + y_2 j$.

Set $I_M := \mathcal{O} \cdot \{x + yj,\ \begin{pmatrix} x \\ y \end{pmatrix} \in M\}$.

1. $\mathcal{O} \supset \mathcal{O}_K + \mathcal{O}_K j$ pre-computed with [Voi13, Algorithm 7.9, 7.10].

$\to$ polytime reducible to a factorisation of ideal in F.

2. $\boldsymbol{I_M = \mathcal{O}\mathfrak{b}_1\alpha + \mathcal{O}\mathfrak{b}_2\beta}$.

$\to$ with α_B and β_B equivalents of α and β for B, $I_M = \mathcal{O}\mathfrak{a}_1\alpha_B + \mathcal{O}\mathfrak{a}_2\beta_B$.

Step 4/4: compute an ideal generated by α

$\mathbf{B} = (B, \mathfrak{a}_1, \mathfrak{a}_2)$ with $B^* B = G$, and $\mathbf{C} = (C, \mathfrak{b}_1, \mathfrak{b}_2)$ with $C^* C = G' \to$ two pseudo-bases of a module M.

$C = \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix}$, $\alpha := x_1 + y_1 j$, $\beta = x_2 + y_2 j$.

Set $I_M := \mathcal{O} \cdot \{x + yj,\ \begin{pmatrix} x \\ y \end{pmatrix} \in M\}$ and $\mathcal{O}' = \mathcal{O}_r(I_M) = I_M^{-1} \times I_M$.

$$\boldsymbol{\alpha \mathcal{O}' = \mathfrak{b}_1^{-1} I_M \cap \alpha \beta^{-1} \mathfrak{b}_2^{-1} I_M}.$$

Step 4/4: compute an ideal generated by α

$\mathbf{B} = (B, \mathfrak{a}_1, \mathfrak{a}_2)$ with $B^* B = G$, and $\mathbf{C} = (C, \mathfrak{b}_1, \mathfrak{b}_2)$ with $C^* C = G'$ $\rightarrow$ two pseudo-bases of a module M.

$C = \left(\begin{smallmatrix} x_1 & x_2 \\ y_1 & y_2 \end{smallmatrix}\right)$, $\alpha := x_1 + y_1 j$, $\beta = x_2 + y_2 j$.

Set $I_M := \mathcal{O} \cdot \{x + yj,\ \left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) \in M\}$ and $\mathcal{O}' = \mathcal{O}_r(I_M) = I_M^{-1} \times I_M$.

$$\boldsymbol{\alpha \mathcal{O}' = \mathfrak{b}_1^{-1} I_M \cap \alpha \beta^{-1} \mathfrak{b}_2^{-1} I_M}.$$

$$\begin{aligned} I_M^{-1} &= (\mathcal{O}\mathfrak{b}_1 \alpha + \mathcal{O}\mathfrak{b}_2 \beta)^{-1} \\ &= (\mathcal{O}\mathfrak{b}_1 \alpha)^{-1} \cap (\mathcal{O}\mathfrak{b}_2 \beta)^{-1} \\ &= \alpha^{-1} \mathfrak{b}_1^{-1} \mathcal{O} \cap \beta^{-1} \mathfrak{b}_2^{-1} \mathcal{O} \end{aligned}$$

$$\Rightarrow \alpha \times I_M^{-1} \times I_M = \mathfrak{b}_1^{-1} I_M \cap \alpha \beta^{-1} \mathfrak{b}_2^{-1} I_M = \alpha \mathcal{O}'$$

Recover C *s.t.* $(C, \mathfrak{b}_1, \mathfrak{b}_2)$ pseudo basis of M, and $C^*C = G'$

$$\boldsymbol{\alpha\mathcal{O}'} = \mathfrak{b}_1^{-1} I_M \cap \alpha\beta^{-1}\mathfrak{b}_2^{-1} I_M$$

1. nrdPIP oracle in $\mathcal{A} \to$ recover α.
2. $\beta = (\alpha\beta^{-1})^{-1} \times \alpha \to$ We have one C *s.t.* $C^*C = G'$.
3. For all $f \in \mathcal{O}'$ *s.t.* $\mathrm{nrd}(f) = 1$, $\alpha' := \alpha \times f$, $\beta' = (\alpha\beta^{-1})^{-1} \times \alpha'$.
   $\to$ We get all the other C *s.t.* $C^*C = G'$.

Recover C *s.t.* $(C, \mathfrak{b}_1, \mathfrak{b}_2)$ pseudo basis of M, and $C^*C = G'$

$$\boldsymbol{\alpha\mathcal{O}'} = \mathfrak{b}_1^{-1} I_M \cap \alpha\beta^{-1}\mathfrak{b}_2^{-1} I_M$$

1. nrdPIP oracle in $\mathcal{A}$ $\to$ recover α.
2. $\beta = (\alpha\beta^{-1})^{-1} \times \alpha$ $\to$ We have one C *s.t.* $C^*C = G'$.
3. For all $f \in \mathcal{O}'$ *s.t.* $\mathrm{nrd}(f) = 1$, $\alpha' := \alpha \times f$, $\beta' = (\alpha\beta^{-1})^{-1} \times \alpha'$.
   $\to$ We get all the other C *s.t.* $C^*C = G'$.

! det C is known **up to a root of unity.**

$\to$ Two calls to the nrdPIP oracle.

Specific case, including Hawk

Assume that

- K is a cyclotomic field instead of just any CM field.
- $M = \mathcal{O}_K^2$.

Then, given $U \in \mathrm{Cong}(\mathbf{G}, \mathbf{G}')$, and μ a root of unity in $\mathcal{O}_K$:

$$U' = B^{-1} \cdot \mathrm{diag}(\mu, 1) \cdot B \cdot U \in \mathrm{Cong}(\mathbf{G}, \mathbf{G}')$$

Specific case, including Hawk

Assume that

- K is a cyclotomic field instead of just any CM field.
- $M = \mathcal{O}_K^2$.

Then, given $U \in \mathrm{Cong}(\mathbf{G}, \mathbf{G}')$, and μ a root of unity in $\mathcal{O}_K$:

$$U' = B^{-1} \cdot \mathrm{diag}(\mu, 1) \cdot B \cdot U \in \mathrm{Cong}(\mathbf{G}, \mathbf{G}')$$

$\Rightarrow \det U' = \mu \det U$.

$\Rightarrow$ Only one call to nrdPIP oracle to compute all $\mathrm{Cong}(\mathbf{G}, \mathbf{G}')$.

Algorithm recapitulation and complexity

$\mathbf{B} = (B, \mathfrak{a}_1, \mathfrak{a}_2)$ with $B^*B = G$, and $\mathbf{C} = (C, \mathfrak{b}_1, \mathfrak{b}_2)$ with $C^*C = G'$.
$C = \left(\begin{smallmatrix} x_1 & x_2 \\ y_1 & y_2 \end{smallmatrix}\right)$, $\alpha := x_1 + y_1 j$, $\beta = x_2 + y_2 j$.

$\mathcal{O}$ is pre-computed.

Reduction from modLIP to nrdPIP:

1. Get $\det U$ and $\det C$ up to a root of unity in $\mathcal{O}_K \leftarrow$ Lenstra-Silverberg [LS14].
2. $\alpha\beta^{-1} \leftarrow q_{2,2}^{-1}(\overline{q_{1,2}} - \mathbf{det}(\boldsymbol{C})j)$.
3. $I_M := \mathcal{O} \cdot \{x + yj,\ \left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) \in M\}$.
4. $\mathcal{O}' = \mathcal{O}_r(I_M)$, $\alpha\mathcal{O}' = \mathfrak{b}_1^{-1} I_M \cap \alpha\beta^{-1}\mathfrak{b}_2^{-1} I_M$.
5. nrdPIP oracle $\rightarrow \alpha$, then C, then $U = B^{-1}C$.

(Steps 3–4: basic operations on modules.)

Previous attacks on modLIP

- If K was totally real, Mureau, Pellet-Mary, Pliatsok and Wallet [Mur+24].
  $\rightarrow$ completely solves the problem in polynomial time.
- With restrictions on M, Espitau and Pliatsok [EP24].
  $\rightarrow$ polynomial time reduction to an instance of module-SVP, for "free primitive" M.
- In the same setting, Luo, Jiang, Pan, and Wang [Luo+24].
  $\rightarrow$ polynomial time reduction to the problem of finding "pseudo symplectic automorphisms" of M.

Conclusion

Given $\mathbf{B}$, and $\mathbf{G}$ and $\mathbf{G}'$ two pseudo-Gram matrices of a module M:

- **Polynomial time reduction from modLIP to nrdPIP in a quaternion algebra.**
  $\rightarrow$ Two calls to nrdPIP oracle suffice to compute $\mathrm{Cong}(\mathbf{G}, \mathbf{G}')$.
- If K is cyclotomic and $M = \mathcal{O}_K^2$, one call to nrdPIP oracle suffices.
- **This does not break modLIP**, but it broadens the attack surface.

Question time!

References

[ARLW24] Léo Ackermann, Adeline Roux-Langlois, and Alexandre Wallet. **"Public-key encryption from LIP".** In: *International Workshop on Coding and Cryptography (WCC)*. 2024.

[Ben+23] Huck Bennett et al. **"Just how hard are rotations of $\mathbb{Z}^n$? algorithms and cryptography with the simplest lattice".** In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2023, pp. 252–281.

[DS+20] Mathieu Dutour Sikirić et al. **"A canonical form for positive definite matrices".** In: *Open Book Series* 4.1 (2020), pp. 179–195.

[Duc+22] Léo Ducas et al. **"Hawk: Module LIP Makes Lattice Signatures Fast, Compact and Simple".** In: Lecture Notes in Computer Science 13794 (2022). Ed. by Shweta Agrawal and Dongdai Lin, pp. 65–94. DOI: 10.1007/978-3-031-22972-5_3. URL: https://doi.org/10.1007/978-3-031-22972-5_3.

[DW22] Léo Ducas and Wessel P. J. van Woerden. **"On the Lattice Isomorphism Problem, Quadratic Forms, Remarkable Lattices, and Cryptography".** In: *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III*. Ed. by Orr Dunkelman and Stefan Dziembowski. Vol. 13277. Lecture Notes in Computer Science. Springer, 2022, pp. 643–673.

[EP24] Thomas Espitau and Heorhii Pliatsok. ***On hermitian decomposition lattices and the module-LIP problem in rank 2.*** Cryptology ePrint Archive, Paper 2024/1148. 2024. URL: https://eprint.iacr.org/2024/1148.

[HR14] Ishay Haviv and Oded Regev. **"On the Lattice Isomorphism Problem".** In: (2014). Ed. by Chandra Chekuri, pp. 391–404. DOI: 10.1137/1.9781611973402.29. URL: https://doi.org/10.1137/1.9781611973402.29.

[KV10] Markus Kirschmer and John Voight. **"Algorithmic enumeration of ideal classes for quaternion orders".** In: *SIAM Journal on Computing* 39.5 (2010), pp. 1714–1747.

[LS14] Hendrik W. Jr Lenstra and Alice Silverberg. **"Revisiting the Gentry-Szydlo Algorithm".** In: Lecture Notes in Computer Science 8616 (2014). Ed. by Juan A. Garay and Rosario Gennaro, pp. 280–296.

[Luo+24] Hengyi Luo et al. ***Cryptanalysis of Rank-2 Module-LIP with Symplectic Automorphisms.*** Cryptology ePrint Archive, Paper 2024/1173, accepted at Asiacrypt 2024. 2024. URL: https://eprint.iacr.org/2024/1173.

[Mur+24] Guilhem Mureau et al. **"Cryptanalysis of Rank-2 Module-LIP in Totally Real Number Fields".** In: *Advances in Cryptology - EUROCRYPT 2024 - 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26-30, 2024, Proceedings, Part VI*. Ed. by Marc Joye and Gregor Leander. Vol. 14656. Lecture Notes in Computer Science. Springer, 2024, pp. 226–255. DOI: 10.1007/978-3-031-58754-2_9. URL: https://doi.org/10.1007/978-3-031-58754-2_9.

[PS97] Wilhelm Plesken and Bernd Souvignier. **"Computing isometries of lattices".** In: *Journal of Symbolic Computation* 24.3-4 (1997), pp. 327–334.

[Voi13] John Voight. **"Identifying the Matrix Ring: Algorithms for Quaternion Algebras and Quadratic Forms".** In: *Quadratic and Higher Degree Forms*. Ed. by Krishnaswami Alladi et al. New York, NY: Springer New York, 2013, pp. 255–298. ISBN: 978-1-4614-7488-3. DOI: 10.1007/978-1-4614-7488-3_10. URL: https://doi.org/10.1007/978-1-4614-7488-3_10.