Cryptanalysis of Rank 2 Module-LIP for certain number fields

C. Chevignard, T. Espitau, P-A. Fouque, **G. Mureau**,
A. Pellet-Mary, H. Pliatsok, A. Wallet

Joint Seminar ENSL/CWI/KCL/IRISA
April 28th, 2025

Some context

- 2022: Ducas et al. introduced module-LIP and **Hawk**[1]
  Signature scheme, NIST submission
  Based on module-LIP for $\mathcal{O}_K^2$ with K **cyclotomic** number field

---

[1] Hawk: Module LIP makes Lattice Signatures Fast, Compact and Simple (L. Ducas, E. W. Postlethwaite, L. N. Pulles, W. van Woerden)

[2] Cryptanalysis of rank-2 module-LIP in Totally Real Number Fields

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

Some context

- 2022: Ducas et al. introduced module-LIP and **Hawk**[1]
  Signature scheme, NIST submission
  Based on module-LIP for $\mathcal{O}_K^2$ with K **cyclotomic** number field

- 2023: [1], with A. Pellet-Mary, H. Pliatsok and A. Wallet[2]
  Heuristic poly time algorithm solving rank-2 module-LIP over **totally real** number fields (does **not** break Hawk!)

[1] Hawk: Module LIP makes Lattice Signatures Fast, Compact and Simple (L. Ducas, E. W. Postlethwaite, L. N. Pulles, W. van Woerden)
[2] Cryptanalysis of rank-2 module-LIP in Totally Real Number Fields
[3] A reduction from Hawk to the principal ideal problem in a quaternion algebra

Some context

- 2022: Ducas et al. introduced module-LIP and **Hawk**[1]
  Signature scheme, NIST submission
  Based on module-LIP for $\mathcal{O}_K^2$ with K **cyclotomic** number field

- 2023: [1], with A. Pellet-Mary, H. Pliatsok and A. Wallet[2]
  Heuristic poly time algorithm solving rank-2 module-LIP over **totally real** number fields (does **not** break Hawk!)

- 2024: [2], with C. Chevignard, P-A. Fouque, A. Pellet–Mary, A. Wallet[3]
  Poly time reduction for rank-2 module-LIP over **CM** number fields to a variant of PIP in quaternion algebra called nrdPIP (does **not** break Hawk!)

---

[1] Hawk: Module LIP makes Lattice Signatures Fast, Compact and Simple (L. Ducas, E. W. Postlethwaite, L. N. Pulles, W. van Woerden)

[2] Cryptanalysis of rank-2 module-LIP in Totally Real Number Fields

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

This talk

A framework containing both: L either totally real or CM fields, reduce module-LIP for rank 2 modules over L to a problem on rank 1 modules (ideals) in a quadratic extension $\mathcal{A}/L$, called nrdPIP.

This talk

A framework containing both: L either totally real or CM fields, reduce module-LIP for rank 2 modules over L to a problem on rank 1 modules (ideals) in a quadratic extension $\mathcal{A}/L$, called nrdPIP. Also apply to [1]: remove the heuristic argument

This talk

A framework containing both: L either totally real or CM fields, reduce module-LIP for rank 2 modules over L to a problem on rank 1 modules (ideals) in a quadratic extension $\mathcal{A}/L$, called nrdPIP. Also apply to [1]: remove the heuristic argument

For L totally real, efficient algorithm to solve nrdPIP. For CM fields, open question!

This talk

A framework containing both: L either totally real or CM fields, reduce module-LIP for rank 2 modules over L to a problem on rank 1 modules (ideals) in a quadratic extension $\mathcal{A}/L$, called nrdPIP. Also apply to [1]: remove the heuristic argument

For L totally real, efficient algorithm to solve nrdPIP. For CM fields, open question!

Plan of the talk:

1. Background and module-LIP
2. Reducing rank-2 module-LIP to nrdPIP
3. Solving the totally real case

Totally real and CM number fields

Background and module-LIP

- $L \simeq \mathbb{Q}[X]/P(X)$ of degree d has d (complex) embeddings $\sigma : L \to \mathbb{C}$

Background and module-LIP

- $L \simeq \mathbb{Q}[X]/P(X)$ of degree d has d (complex) embeddings $\sigma : L \to \mathbb{C}$

Example: $P(X) = \Phi_n(X)$ cyclotomic, $d = \varphi(n)$ and $\sigma : X \mapsto e^{\frac{2ik\pi}{n}}$, $k \wedge n = 1$

Background and module-LIP

- $L \simeq \mathbb{Q}[X]/P(X)$ of degree d has d (complex) embeddings $\sigma : L \to \mathbb{C}$

Example: $P(X) = \Phi_n(X)$ cyclotomic, $d = \varphi(n)$ and $\sigma : X \mapsto e^{\frac{2ik\pi}{n}}$, $k \wedge n = 1$

- L **totally real** if $\sigma(L) \subset \mathbb{R}$ for all embeddings. **Examples:** $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$

L **totally complex** if $\sigma(L) \not\subset \mathbb{R}$ for all embeddings. **Examples:** $\mathbb{Q}(\zeta_n)$, $n > 2$

Background and module-LIP

- $L \simeq \mathbb{Q}[X]/P(X)$ of degree d has d (complex) embeddings $\sigma : L \to \mathbb{C}$

Example: $P(X) = \Phi_n(X)$ cyclotomic, $d = \varphi(n)$ and $\sigma : X \mapsto e^{\frac{2ik\pi}{n}}$, $k \wedge n = 1$

- L **totally real** if $\sigma(L) \subset \mathbb{R}$ for all embeddings. **Examples:** $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$

L **totally complex** if $\sigma(L) \not\subset \mathbb{R}$ for all embeddings. **Examples:** $\mathbb{Q}(\zeta_n)$, $n > 2$

- L is a **CM** field if totally complex and quadratic extension of F totally real

We say L/F is **CM extension. Examples:** $L/F = \mathbb{Q}(\sqrt{-1})/\mathbb{Q}$, $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n + \zeta_n^{-1})$

Background and module-LIP

- **Notations:** K for a CM field, F totally real field and L generic notation

Background and module-LIP

- **Notations:** K for a CM field, F totally real field and L generic notation

Fact: K/F CM, always have $K = F(\sqrt{a})$ with $a \in F$ s.t. $\sigma(a) < 0, \ \forall \sigma : F \to \mathbb{R}$.

Example: $K = \mathbb{Q}(\zeta_m)$ with $m = 2^e$, then $K = F(\sqrt{-1})$ with $F = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$

Background and module-LIP

- **Notations:** K for a CM field, F totally real field and L generic notation

Fact: K/F CM, always have $K = F(\sqrt{a})$ with $a \in F$ s.t. $\sigma(a) < 0, \ \forall \sigma : F \to \mathbb{R}$.

Example: $K = \mathbb{Q}(\zeta_m)$ with $m = 2^e$, then $K = F(\sqrt{-1})$ with $F = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$

For simplicity, $a = -1$ and $\sqrt{a} = i$ in the rest of the talk

Background and module-LIP

- **Notations:** K for a CM field, F totally real field and L generic notation

Fact: K/F CM, always have $K = F(\sqrt{a})$ with $a \in F$ s.t. $\sigma(a) < 0, \ \forall \sigma : F \to \mathbb{R}$.

Example: $K = \mathbb{Q}(\zeta_m)$ with $m = 2^e$, then $K = F(\sqrt{-1})$ with $F = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$

For simplicity, $a = -1$ and $\sqrt{a} = i$ in the rest of the talk

- K/F CM, $\overline{\cdot} : x + iy \mapsto x - iy$ **complex conjugation** on $K = F(\sqrt{a})$

nrd : $K \to F$; $x = x_1 + ix_2 \mapsto x\bar{x} = x_1^2 + x_2^2$ **reduced norm** on K

If $x \in F$, $\bar{x} = x$ and nrd$(x) = x^2$.

Module lattices

Background and module-LIP

- Let L either totally real or CM, $\ell \in \mathbb{N}_{>0}$ and V a L-vector space of dim ℓ

Background and module-LIP

- Let L either totally real or CM, $\ell \in \mathbb{N}_{>0}$ and V a L-vector space of dim ℓ

$\Psi : V \to \mathbb{Q} \,;(x_1, \ldots, x_\ell) \mapsto \mathrm{Tr}_{L/\mathbb{Q}} \left(\sum_{i=1}^{\ell} \mathrm{nrd}(x_i) \right)$ positive definite quadratic (or hermitian) form on V

Background and module-LIP

- Let L either totally real or CM, $\ell \in \mathbb{N}_{>0}$ and V a L-vector space of dim ℓ

$\Psi : V \to \mathbb{Q}\,;(x_1,\ldots,x_\ell) \mapsto \mathrm{Tr}_{L/\mathbb{Q}}\left(\sum_{i=1}^{\ell} \mathrm{nrd}(x_i)\right)$ positive definite quadratic (or hermitian) form on V

- **Rank-ℓ (free $\mathcal{O}_L$-)module** in V is any

$$M = \mathcal{O}_L \mathrm{b}_1 + \cdots + \mathcal{O}_L \mathrm{b}_\ell \subset V \text{ **equipped with** } \Psi_{|M},$$

where $B = (\mathrm{b}_1|\cdots|\mathrm{b}_\ell) \in \mathrm{GL}_\ell(L)$ called a **basis** of M

Background and module-LIP

- Let L either totally real or CM, $\ell \in \mathbb{N}_{>0}$ and V a L-vector space of dim ℓ

$\Psi : V \to \mathbb{Q}\,; (x_1, \ldots, x_\ell) \mapsto \mathrm{Tr}_{L/\mathbb{Q}}\left(\sum_{i=1}^{\ell} \mathrm{nrd}(x_i)\right)$ positive definite quadratic (or hermitian) form on V

- **Rank-ℓ (free $\mathcal{O}_L$-)module** in V is any

$$M = \mathcal{O}_L \mathrm{b}_1 + \cdots + \mathcal{O}_L \mathrm{b}_\ell \subset V \textbf{ equipped with } \Psi_{|M},$$

where $B = (\mathrm{b}_1 | \cdots | \mathrm{b}_\ell) \in \mathrm{GL}_\ell(L)$ called a **basis** of M

- **Remark:** Can consider more general objects using pseudo-bases.

Background and module-LIP

- Let $M \subset V \simeq L^\ell$ rank-ℓ module

Background and module-LIP

- Let $M \subset V \simeq L^\ell$ rank-ℓ module

Fact: $B, C \in \mathrm{GL}_\ell(L)$ are both bases of M **iff**

Background and module-LIP

- Let $M \subset V \simeq L^\ell$ rank-ℓ module

Fact: $B, C \in \mathrm{GL}_\ell(L)$ are both bases of M **iff** $\exists U \in \mathrm{GL}_\ell(\mathcal{O}_L)$ s.t. $C = BU$

Background and module-LIP

- Let $M \subset V \simeq L^\ell$ rank-ℓ module

Fact: $B, C \in \mathrm{GL}_\ell(L)$ are both bases of M **iff** $\exists U \in \mathrm{GL}_\ell(\mathcal{O}_L)$ s.t. $C = BU$

- If B basis of M, call $G = B^* B$ (where $B^* =$ transpose–conjugate of B) the **Gram matrix** associated to B

Background and module-LIP

- Let $M \subset V \simeq L^\ell$ rank-ℓ module

Fact: $B, C \in \mathrm{GL}_\ell(L)$ are both bases of M **iff** $\exists U \in \mathrm{GL}_\ell(\mathcal{O}_L)$ s.t. $C = BU$

- If B basis of M, call $G = B^* B$ (where B^* = transpose–conjugate of B) the **Gram matrix** associated to B

Gram matrices are **congruent** if associated to bases of the same module

$$G \sim G' \iff \exists U \in \mathrm{GL}_\ell(\mathcal{O}_L) : G' = U^* G U.$$

Module-LIP

Background and module-LIP

- L either totally real or CM and B basis for $M \subset L^\ell$, G the Gram matrix

Background and module-LIP

- L either totally real or CM and B basis for $M \subset L^{\ell}$, G the Gram matrix

modLIP$_L^B$.

Background and module-LIP

- L either totally real or CM and B basis for $M \subset L^\ell$, G the Gram matrix

modLIP$_L^B$. **Input:** $G' \sim G$

Background and module-LIP

- L either totally real or CM and B basis for $M \subset L^\ell$, G the Gram matrix

<u>**modLIP$_L^B$.**</u> **Input:** $G' \sim G$

Goal: Any $U \in \mathrm{GL}_\ell(\mathcal{O}_L)$ s.t. $G' = U^*GU$ (call it a **congruence** matrix between G and G')

Background and module-LIP

- L either totally real or CM and B basis for $M \subset L^\ell$, G the Gram matrix

<u>**modLIP$_L^B$**</u>. **Input:** $G' \sim G$

Goal: Any $U \in \mathrm{GL}_\ell(\mathcal{O}_L)$ s.t. $G' = U^* G U$ (call it a **congruence** matrix between G and G')

$$\Longleftrightarrow$$

Goal: Any $C \in \mathrm{GL}_2(L)$ **basis** of M with $C^* C = G'$

Background and module-LIP

- L either totally real or CM and B basis for $M \subset L^\ell$, G the Gram matrix

<u>**modLIP$_L^B$.**</u> **Input:** $G' \sim G$

Goal: Any $U \in \mathrm{GL}_\ell(\mathcal{O}_L)$ s.t. $G' = U^* G U$ (call it a **congruence** matrix between G and G')

$$\iff$$

Goal: Any $C \in \mathrm{GL}_2(L)$ **basis** of M with $C^* C = G'$

- **Example:** For $M = \mathcal{O}_L^2$ and $B_0 = I_2$ as in **Hawk**

Background and module-LIP

- L either totally real or CM and B basis for $M \subset L^\ell$, G the Gram matrix

<u>**modLIP$_L^B$.**</u> **Input:** $G' \sim G$

Goal: Any $U \in \mathrm{GL}_\ell(\mathcal{O}_L)$ s.t. $G' = U^* G U$ (call it a **congruence** matrix between G and G')

$$\Longleftrightarrow$$

Goal: Any $C \in \mathrm{GL}_2(L)$ **basis** of M with $C^* C = G'$

- **Example:** For $M = \mathcal{O}_L^2$ and $B_0 = I_2$ as in **Hawk**

<u>**Hawk.**</u> **Input:** $G' \sim I_2$

Goal: Any $U \in \mathrm{GL}_2(\mathcal{O}_L)$ s.t. $G' = U^* U$

Background and module-LIP

- L either totally real or CM and $\ell = \mathbf{2}$

Main observation: $G' = \begin{pmatrix} q_1 & q_2 \\ \overline{q_2} & q_3 \end{pmatrix}$ input and $C = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ solution to modLIP,

Background and module-LIP

- L either totally real or CM and $\ell = \mathbf{2}$

Main observation: $G' = \begin{pmatrix} q_1 & q_2 \\ \overline{q_2} & q_3 \end{pmatrix}$ input and $C = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ solution to modLIP,

$$\begin{pmatrix} q_1 & q_2 \\ \overline{q_2} & q_3 \end{pmatrix} = \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \cdot \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} a\bar{a} + b\bar{b} & \bar{a}c + \bar{b}d \\ a\bar{c} + b\bar{d} & c\bar{c} + d\bar{d} \end{pmatrix}$$

Background and module-LIP

- L either totally real or CM and $\ell = \mathbf{2}$

Main observation: $G' = \begin{pmatrix} q_1 & q_2 \\ \overline{q_2} & q_3 \end{pmatrix}$ input and $C = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ solution to modLIP,

$$\begin{pmatrix} q_1 & q_2 \\ \overline{q_2} & q_3 \end{pmatrix} = \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \cdot \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} a\bar{a} + b\bar{b} & \bar{a}c + \bar{b}d \\ a\bar{c} + b\bar{d} & c\bar{c} + d\bar{d} \end{pmatrix}$$

For $L = F$ **totally real**:
$q_1 = a^2 + b^2 = \mathrm{nrd}(a + bi)$,

Background and module-LIP

- L either totally real or CM and $\ell = \mathbf{2}$

Main observation: $G' = \begin{pmatrix} q_1 & q_2 \\ \overline{q_2} & q_3 \end{pmatrix}$ input and $C = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ solution to modLIP,

$$\begin{pmatrix} q_1 & q_2 \\ \overline{q_2} & q_3 \end{pmatrix} = \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \cdot \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} a\bar{a} + b\bar{b} & \bar{a}c + \bar{b}d \\ a\bar{c} + b\bar{d} & c\bar{c} + d\bar{d} \end{pmatrix}$$

For $L = F$ **totally real**:
$q_1 = a^2 + b^2 = \mathrm{nrd}(a + bi)$,
$a + bi \in K = L(i)$ CM field

Background and module-LIP

- L either totally real or CM and $\ell = \mathbf{2}$

Main observation: $G' = \begin{pmatrix} q_1 & q_2 \\ \overline{q_2} & q_3 \end{pmatrix}$ input and $C = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ solution to modLIP,

$$\begin{pmatrix} q_1 & q_2 \\ \overline{q_2} & q_3 \end{pmatrix} = \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \cdot \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} a\bar{a} + b\bar{b} & \bar{a}c + \bar{b}d \\ a\bar{c} + b\bar{d} & c\bar{c} + d\bar{d} \end{pmatrix}$$

For $L = F$ **totally real**:
$q_1 = a^2 + b^2 = \mathrm{nrd}(a + bi)$,
$a + bi \in K = L(i)$ CM field

$\Longrightarrow$ Norm equation in CM extension

Background and module-LIP

- L either totally real or CM and $\ell = \mathbf{2}$

Main observation: $G' = \begin{pmatrix} q_1 & q_2 \\ \overline{q_2} & q_3 \end{pmatrix}$ input and $C = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ solution to modLIP,

$$\begin{pmatrix} q_1 & q_2 \\ \overline{q_2} & q_3 \end{pmatrix} = \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \cdot \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} a\bar{a} + b\bar{b} & \bar{a}c + \bar{b}d \\ a\bar{c} + b\bar{d} & c\bar{c} + d\bar{d} \end{pmatrix}$$

For $L = F$ **totally real**:
$q_1 = a^2 + b^2 = \mathrm{nrd}(a + bi)$,
$a + bi \in K = L(i)$ CM field

$\Longrightarrow$ Norm equation in CM extension

For $L = F(i)$ **CM**:
$q_1 = a_1^2 + a_2^2 + b_1^2 + b_2^2$,

Background and module-LIP

- L either totally real or CM and $\ell = \mathbf{2}$

Main observation: $G' = \begin{pmatrix} q_1 & q_2 \\ \overline{q_2} & q_3 \end{pmatrix}$ input and $C = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ solution to modLIP,

$$\begin{pmatrix} q_1 & q_2 \\ \overline{q_2} & q_3 \end{pmatrix} = \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \cdot \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} a\bar{a} + b\bar{b} & \bar{a}c + \bar{b}d \\ a\bar{c} + b\bar{d} & c\bar{c} + d\bar{d} \end{pmatrix}$$

For $L = F$ **totally real**:
$q_1 = a^2 + b^2 = \mathrm{nrd}(a + bi)$,
$a + bi \in K = L(i)$ CM field

For $L = F(i)$ **CM**:
$q_1 = a_1^2 + a_2^2 + b_1^2 + b_2^2$, reduced norm in quaternion algebra $L + L \cdot j$

$\implies$ Norm equation in CM extension

Background and module-LIP

- L either totally real or CM and $\ell = \mathbf{2}$

Main observation: $G' = \begin{pmatrix} q_1 & q_2 \\ \overline{q_2} & q_3 \end{pmatrix}$ input and $C = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ solution to modLIP,

$$\begin{pmatrix} q_1 & q_2 \\ \overline{q_2} & q_3 \end{pmatrix} = \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \cdot \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} a\bar{a} + b\bar{b} & \bar{a}c + \bar{b}d \\ a\bar{c} + b\bar{d} & c\bar{c} + d\bar{d} \end{pmatrix}$$

For $L = F$ **totally real**:
$q_1 = a^2 + b^2 = \mathrm{nrd}(a + bi)$,
$a + bi \in K = L(i)$ CM field

$\implies$ Norm equation in CM extension

For $L = F(i)$ **CM**:
$q_1 = a_1^2 + a_2^2 + b_1^2 + b_2^2$, reduced norm in quaternion algebra $L + L \cdot j$

$\implies$ Norm equation in quaternion algebra

Quaternion algebras

Background and module-LIP

- Let K/F a CM extension, $K = F(i)$ with $i^2 = -1$

Background and module-LIP

- Let K/F a CM extension, $K = F(i)$ with $i^2 = -1$

$$\mathcal{A} = F + F \cdot i + F \cdot j + F \cdot ij = K + K \cdot j,$$

with $j^2 = -1$ and $ij = -ji$.

Background and module-LIP

- Let K/F a CM extension, $K = F(i)$ with $i^2 = -1$

$$\mathcal{A} = F + F \cdot i + F \cdot j + F \cdot ij = K + K \cdot j,$$

with $j^2 = -1$ and $ij = -ji$. Non-commutative F-algebra of dim 4 (quaternion algebra)

Background and module-LIP

- Let K/F a CM extension, $K = F(i)$ with $i^2 = -1$

$$\mathcal{A} = F + F \cdot i + F \cdot j + F \cdot ij = K + K \cdot j,$$

with $j^2 = -1$ and $ij = -ji$. Non-commutative F-algebra of dim 4 (quaternion algebra)

- $\overline{\cdot} : x + yi + zj + tij \mapsto x - yi - zj - tij$ **complex conjugation** on $\mathcal{A}$

nrd : $\mathcal{A} \to F$; $\alpha = x + yi + zj + tij \mapsto \alpha\bar{\alpha} = x^2 + y^2 + z^2 + t^2$ **reduced norm** on $\mathcal{A}$

Background and module-LIP

- Let K/F a CM extension, $K = F(i)$ with $i^2 = -1$

$$\mathcal{A} = F + F \cdot i + F \cdot j + F \cdot ij = K + K \cdot j,$$

with $j^2 = -1$ and $ij = -ji$. Non-commutative F-algebra of dim 4 (quaternion algebra)

- $\overline{\cdot} : x + yi + zj + tij \mapsto x - yi - zj - tij$ **complex conjugation** on $\mathcal{A}$

nrd : $\mathcal{A} \to F$; $\alpha = x + yi + zj + tij \mapsto \alpha\bar{\alpha} = x^2 + y^2 + z^2 + t^2$ **reduced norm** on $\mathcal{A}$

$\implies$ Extensions of $\overline{\cdot}$ and nrd on K

Background and module-LIP

- **Ideal** in $\mathcal{A}$: rank-4 $\mathcal{O}_F$-module in $\mathcal{A}$ (not necessarily free).

Background and module-LIP

- **Ideal** in $\mathcal{A}$: rank-4 $\mathcal{O}_F$-module in $\mathcal{A}$ (not necessarily free). **Order** in $\mathcal{A}$: ideal in $\mathcal{A}$ with ring structure. Said **maximal** if not contained in a strictly bigger order

Background and module-LIP

- **Ideal** in $\mathcal{A}$: rank-4 $\mathcal{O}_F$-module in $\mathcal{A}$ (not necessarily free). **Order** in $\mathcal{A}$: ideal in $\mathcal{A}$ with ring structure. Said **maximal** if not contained in a strictly bigger order

Example: $F = \mathbb{Q}$, order $\mathcal{O} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}ij$ (not maximal!)

Background and module-LIP

- **Ideal** in $\mathcal{A}$: rank-4 $\mathcal{O}_F$-module in $\mathcal{A}$ (not necessarily free). **Order** in $\mathcal{A}$: ideal in $\mathcal{A}$ with ring structure. Said **maximal** if not contained in a strictly bigger order

Example: $F = \mathbb{Q}$, order $\mathcal{O} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}ij$ (not maximal!)

- $I \subset \mathcal{A}$ an ideal, $\mathcal{O}_\ell(I) := \{\alpha \in \mathcal{A} \mid \alpha I \subseteq I\}$ **left order** of I. Same way, define **right order** $\mathcal{O}_r(I)$ of I

Background and module-LIP

- **Ideal** in $\mathcal{A}$: rank-4 $\mathcal{O}_F$-module in $\mathcal{A}$ (not necessarily free). **Order** in $\mathcal{A}$: ideal in $\mathcal{A}$ with ring structure. Said **maximal** if not contained in a strictly bigger order

Example: $F = \mathbb{Q}$, order $\mathcal{O} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}ij$ (not maximal!)

- $I \subset \mathcal{A}$ an ideal, $\mathcal{O}_\ell(I) := \{\alpha \in \mathcal{A} \mid \alpha I \subseteq I\}$ **left order** of I. Same way, define **right order** $\mathcal{O}_r(I)$ of I

An ideal $I \subset \mathcal{A}$ is a left $\mathcal{O}$-ideal if $\mathcal{O}_\ell(I) = \mathcal{O}$. Same way, define right $\mathcal{O}$-ideals

Background and module-LIP

- **Ideal** in $\mathcal{A}$: rank-4 $\mathcal{O}_F$-module in $\mathcal{A}$ (not necessarily free). **Order** in $\mathcal{A}$: ideal in $\mathcal{A}$ with ring structure. Said **maximal** if not contained in a strictly bigger order

Example: $F = \mathbb{Q}$, order $\mathcal{O} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}ij$ (not maximal!)

- $I \subset \mathcal{A}$ an ideal, $\mathcal{O}_\ell(I) := \{\alpha \in \mathcal{A} \mid \alpha I \subseteq I\}$ **left order** of I. Same way, define **right order** $\mathcal{O}_r(I)$ of I

An ideal $I \subset \mathcal{A}$ is a left $\mathcal{O}$-ideal if $\mathcal{O}_\ell(I) = \mathcal{O}$. Same way, define right $\mathcal{O}$-ideals

- **Fact:** If $\mathcal{O}$ is maximal and I a left $\mathcal{O}$-ideal, I is **invertible** : $\exists!\, J$ ideal s.t. $IJ = \mathcal{O}$

Also, J is efficiently computable from I

Reducing rank-2 module-LIP

Reducing rank-2 module-LIP

- **Recall:** Solve norm equations (in CM extensions or quaternion algebras) to reconstruct solutions

Reducing rank-2 module-LIP

- **Recall:** Solve norm equations (in CM extensions or quaternion algebras) to reconstruct solutions

Totally real case: [1]
Randomize input to ensure few solutions

Reducing rank-2 module-LIP

- **Recall:** Solve norm equations (in CM extensions or quaternion algebras) to reconstruct solutions

Totally real case: [1]
Randomize input to ensure few solutions
Can compute them efficiently

Reducing rank-2 module-LIP

- **Recall:** Solve norm equations (in CM extensions or quaternion algebras) to reconstruct solutions

Totally real case: [1]
Randomize input to ensure few solutions
Can compute them efficiently

$\implies$ Heuristic poly time algorithm

Reducing rank-2 module-LIP

- **Recall:** Solve norm equations (in CM extensions or quaternion algebras) to reconstruct solutions

Totally real case: [1]
Randomize input to ensure few solutions
Can compute them efficiently

$\Longrightarrow$ Heuristic poly time algorithm

CM case:
Too many solutions (even with randomization)!

Reducing rank-2 module-LIP

- **Recall:** Solve norm equations (in CM extensions or quaternion algebras) to reconstruct solutions

Totally real case: [1]
Randomize input to ensure few solutions
Can compute them efficiently

$\Longrightarrow$ Heuristic poly time algorithm

CM case:
Too many solutions (even with randomization)!
Don't know how to compute one...

Reducing rank-2 module-LIP

- **Recall:** Solve norm equations (in CM extensions or quaternion algebras) to reconstruct solutions

Totally real case: [1]
Randomize input to ensure few solutions
Can compute them efficiently

$\Longrightarrow$ Heuristic poly time algorithm

CM case:
Too many solutions (even with randomization)!
Don't know how to compute one...

$\Longrightarrow$ *Sad reactions in the audience*

Reducing rank-2 module-LIP

- **Recall:** Solve norm equations (in CM extensions or quaternion algebras) to reconstruct solutions

Totally real case: [1]
Randomize input to ensure few solutions
Can compute them efficiently

$\Longrightarrow$ Heuristic poly time algorithm

CM case:
Too many solutions (even with randomization)!
Don't know how to compute one...

$\Longrightarrow$ *Sad reactions in the audience*

- **Strategy [2]:** First, use info from non-diagonal coeff to add constraints on the solutions $\Rightarrow$ at most **two** solutions to norm equation needed

Reducing rank-2 module-LIP

- **Recall:** Solve norm equations (in CM extensions or quaternion algebras) to reconstruct solutions

Totally real case: [1]
Randomize input to ensure few solutions
Can compute them efficiently

$\Longrightarrow$ Heuristic poly time algorithm

CM case:
Too many solutions (even with randomization)!
Don't know how to compute one...

$\Longrightarrow$ *Sad reactions in the audience*

- **Strategy [2]:** First, use info from non-diagonal coeff to add constraints on the solutions $\Rightarrow$ at most **two** solutions to norm equation needed

Build these solutions as generators of principal ideals

Reducing rank-2 module-LIP

- Denote $(L, \mathcal{A})$ **either:**

$(L = F$ totally real, $\mathcal{A} = L(j)$ CM$)$ **or** $(L = K$ CM, $\mathcal{A} = K + K \cdot j$ quaternion algebra$)$

Reducing rank-2 module-LIP

- Denote $(L, \mathcal{A})$ **either:**

$(L = F$ totally real, $\mathcal{A} = L(j)$ CM) **or** $(L = K$ CM, $\mathcal{A} = K + K \cdot j$ quaternion algebra)

Lemma [2]

Let $C = \begin{pmatrix} c_1 & c_3 \\ c_2 & c_4 \end{pmatrix}$, $G' = \begin{pmatrix} q_1 & q_2 \\ \overline{q_2} & q_3 \end{pmatrix} \in \mathrm{GL}_2(L)$ and $\alpha = c_1 + c_2 j,\ \beta = c_3 + c_4 j \in \mathcal{A}$.

Reducing rank-2 module-LIP

- Denote $(L, \mathcal{A})$ **either:**

$(L = F$ totally real, $\mathcal{A} = L(j)$ CM$)$ **or** $(L = K$ CM, $\mathcal{A} = K + K \cdot j$ quaternion algebra$)$

Lemma [2]

Let $C = \begin{pmatrix} c_1 & c_3 \\ c_2 & c_4 \end{pmatrix}$, $G' = \begin{pmatrix} q_1 & q_2 \\ \overline{q_2} & q_3 \end{pmatrix} \in \mathrm{GL}_2(L)$ and $\alpha = c_1 + c_2 j$, $\beta = c_3 + c_4 j \in \mathcal{A}$.

$$G' = C^* C \iff \begin{cases} \mathrm{nrd}(\alpha) = q_1 \\ \alpha\beta^{-1} = q_3^{-1}(\overline{q_2} - \det(C) \cdot j) \end{cases}$$

Reducing rank-2 module-LIP

- Denote $(L, \mathcal{A})$ **either:**

$(L = F$ totally real, $\mathcal{A} = L(j)$ CM) **or** $(L = K$ CM, $\mathcal{A} = K + K \cdot j$ quaternion algebra)

Lemma [2]

Let $C = \begin{pmatrix} c_1 & c_3 \\ c_2 & c_4 \end{pmatrix}$, $G' = \begin{pmatrix} q_1 & q_2 \\ \overline{q_2} & q_3 \end{pmatrix} \in \mathrm{GL}_2(L)$ and $\alpha = c_1 + c_2 j,\ \beta = c_3 + c_4 j \in \mathcal{A}$.

$$G' = C^* C \iff \begin{cases} \mathrm{nrd}(\alpha) = q_1 \\ \alpha\beta^{-1} = q_3^{-1}(\overline{q_2} - \det(C) \cdot j) \end{cases}$$

Know everything on the r.h.s. (compute $\det(C)$ easily up to root of unity in L).
Getting α determines β, so a whole solution!

Reducing rank-2 module-LIP

- **Next step:** Get a principal ideal $\alpha\mathcal{O}$ from $\alpha\beta^{-1}$?

Reducing rank-2 module-LIP

- **Next step:** Get a principal ideal $\alpha\mathcal{O}$ from $\alpha\beta^{-1}$?

Remark: $a, b \in \mathbb{Z}$ unknown, $\dfrac{a}{b}$ known. Get $a\mathbb{Z}$ from $\dfrac{a}{b}$?

Reducing rank-2 module-LIP

- **Next step:** Get a principal ideal $\alpha\mathcal{O}$ from $\alpha\beta^{-1}$?

Remark: $a, b \in \mathbb{Z}$ unknown, $\dfrac{a}{b}$ known. Get $a\mathbb{Z}$ from $\dfrac{a}{b}$?

If $a \wedge b = 1$, $\dfrac{a}{b}\mathbb{Z} \cap \mathbb{Z} = a\mathbb{Z}$

Reducing rank-2 module-LIP

- **Next step:** Get a principal ideal $\alpha\mathcal{O}$ from $\alpha\beta^{-1}$?

Remark: $a, b \in \mathbb{Z}$ unknown, $\dfrac{a}{b}$ known. Get $a\mathbb{Z}$ from $\dfrac{a}{b}$?

If $a \wedge b = 1$, $\dfrac{a}{b}\mathbb{Z} \cap \mathbb{Z} = a\mathbb{Z}$

If $a \wedge b = d$, write $a = a'd$ and $b = b'd$, then $d\mathbb{Z}\left(\dfrac{a'}{b'}\mathbb{Z} \cap \mathbb{Z}\right) = a\mathbb{Z}$

Reducing rank-2 module-LIP

- **Next step:** Get a principal ideal $\alpha\mathcal{O}$ from $\alpha\beta^{-1}$?

Remark: $a, b \in \mathbb{Z}$ unknown, $\dfrac{a}{b}$ known. Get $a\mathbb{Z}$ from $\dfrac{a}{b}$?

If $a \wedge b = 1$, $\dfrac{a}{b}\mathbb{Z} \cap \mathbb{Z} = a\mathbb{Z}$

If $a \wedge b = d$, write $a = a'd$ and $b = b'd$, then $d\mathbb{Z}\left(\dfrac{a'}{b'}\mathbb{Z} \cap \mathbb{Z}\right) = a\mathbb{Z}$

$\Rightarrow$ Need a "gcd ideal" of α and β?

Reducing rank-2 module-LIP

- **Embed** $M \subset L^2$ into an **ideal** in $\mathcal{A} = L + L \cdot j$ using

$$\begin{aligned} \Phi : L^2 &\longrightarrow \mathcal{A} \\ \begin{pmatrix} x \\ y \end{pmatrix} &\longmapsto x + yj \end{aligned}$$

Reducing rank-2 module-LIP

- **Embed** $M \subset L^2$ into an **ideal** in $\mathcal{A} = L + L \cdot j$ using

$$\begin{aligned} \Phi : L^2 &\longrightarrow \mathcal{A} \\ \begin{pmatrix} x \\ y \end{pmatrix} &\longmapsto x + yj \end{aligned}$$

Fix $\mathcal{O} \subset \mathcal{A}$ maximal order containing $\mathcal{O}_L + \mathcal{O}_L \cdot j$.

Reducing rank-2 module-LIP

- **Embed** $M \subset L^2$ into an **ideal** in $\mathcal{A} = L + L \cdot j$ using

$$\Phi : L^2 \longrightarrow \mathcal{A}$$
$$\begin{pmatrix} x \\ y \end{pmatrix} \longmapsto x + yj$$

Fix $\mathcal{O} \subset \mathcal{A}$ maximal order containing $\mathcal{O}_L + \mathcal{O}_L \cdot j$. Put

$$I_M = \text{ left } \mathcal{O}\text{-ideal generated by } \Phi(M)$$

Reducing rank-2 module-LIP

- **Embed** $M \subset L^2$ into an **ideal** in $\mathcal{A} = L + L \cdot j$ using

$$\Phi : L^2 \longrightarrow \mathcal{A}$$
$$\begin{pmatrix} x \\ y \end{pmatrix} \longmapsto x + yj$$

Fix $\mathcal{O} \subset \mathcal{A}$ maximal order containing $\mathcal{O}_L + \mathcal{O}_L \cdot j$. Put

$$I_M = \text{ left } \mathcal{O}\text{-ideal generated by } \Phi(M)$$

Fact: If $B = (b_1|b_2)$ basis for M, then

$$I_M = \mathcal{O}\alpha + \mathcal{O}\beta,$$

where $\alpha = \Phi(b_1)$, $\beta = \Phi(b_2) \in \mathcal{A}$

Reducing rank-2 module-LIP

- **Embed** $M \subset L^2$ into an **ideal** in $\mathcal{A} = L + L \cdot j$ using

$$\Phi : L^2 \longrightarrow \mathcal{A}$$
$$\begin{pmatrix} x \\ y \end{pmatrix} \longmapsto x + yj$$

Fix $\mathcal{O} \subset \mathcal{A}$ maximal order containing $\mathcal{O}_L + \mathcal{O}_L \cdot j$. Put

$$I_M = \text{ left } \mathcal{O}\text{-ideal generated by } \Phi(M)$$

Fact: If $B = (b_1 | b_2)$ basis for M, then

$$I_M = \mathcal{O}\alpha + \mathcal{O}\beta,$$

where $\alpha = \Phi(b_1)$, $\beta = \Phi(b_2) \in \mathcal{A}$ $\implies$ I_M efficiently computable from **any** basis

Reducing rank-2 module-LIP

Proposition [2]

Let $C = (c_1|c_2)$ basis for a module $M \subset L^2$ and $\alpha = \Phi(c_1), \beta = \Phi(c_2)$. Let $\mathcal{O}$ maximal order in $\mathcal{A}$ containing $\mathcal{O}_L + \mathcal{O}_L \cdot j$. Put $\mathcal{O}' = I_M^{-1} I_M$ maximal order,

Reducing rank-2 module-LIP

Proposition [2]

Let $C = (c_1|c_2)$ basis for a module $M \subset L^2$ and $\alpha = \Phi(c_1), \beta = \Phi(c_2)$. Let $\mathcal{O}$ maximal order in $\mathcal{A}$ containing $\mathcal{O}_L + \mathcal{O}_L \cdot j$. Put $\mathcal{O}' = I_M^{-1} I_M$ maximal order, then

$$\alpha \mathcal{O}' = I_M \cap \alpha\beta^{-1} I_M$$

Reducing rank-2 module-LIP

Proposition [2]

Let $C = (c_1|c_2)$ basis for a module $M \subset L^2$ and $\alpha = \Phi(c_1), \beta = \Phi(c_2)$. Let $\mathcal{O}$ maximal order in $\mathcal{A}$ containing $\mathcal{O}_L + \mathcal{O}_L \cdot j$. Put $\mathcal{O}' = I_M^{-1} I_M$ maximal order, then

$$\alpha\mathcal{O}' = I_M \cap \alpha\beta^{-1} I_M$$

Proof.

$$\begin{aligned} I_M = \mathcal{O}\alpha + \mathcal{O}\beta &\Longrightarrow I_M^{-1} = \alpha^{-1}\mathcal{O} \cap \beta^{-1}\mathcal{O} \\ &\Longrightarrow \alpha I_M^{-1} = \mathcal{O} \cap \alpha\beta^{-1}\mathcal{O} \\ &\Longrightarrow \alpha\mathcal{O}' = I_M \cap \alpha\beta^{-1} I_M \end{aligned}$$

$\square$

Reducing rank-2 module-LIP

- **modLIP** instance

$$B = (b_1|b_2) \text{ basis of } M \subset L^2 \text{ (known)}$$
$$C = (c_1|c_2) \text{ basis of } M \subset L^2 \text{ (unknown)}$$
$$G' \text{ Gram matrix with } G' = C^*C \text{ (known)}$$

Reducing rank-2 module-LIP

- **modLIP** instance

$$B = (b_1|b_2) \text{ basis of } M \subset L^2 \text{ (known)}$$
$$C = (c_1|c_2) \text{ basis of } M \subset L^2 \text{ (unknown)}$$
$$G' \text{ Gram matrix with } G' = C^*C \text{ (known)}$$

- What do we know now?

Reducing rank-2 module-LIP

- **modLIP** instance

$$B = (b_1 | b_2) \text{ basis of } M \subset L^2 \text{ (known)}$$
$$C = (c_1 | c_2) \text{ basis of } M \subset L^2 \text{ (unknown)}$$
$$G' \text{ Gram matrix with } G' = C^* C \text{ (known)}$$

- What do we know now?

Lemma $\Rightarrow$ know $\alpha\beta^{-1}$ where $\alpha = \Phi(c_1), \beta = \Phi(c_2)$. Getting α is enough.

Reducing rank-2 module-LIP

- **modLIP** instance

$$B = (b_1|b_2) \text{ basis of } M \subset L^2 \text{ (known)}$$
$$C = (c_1|c_2) \text{ basis of } M \subset L^2 \text{ (unknown)}$$
$$G' \text{ Gram matrix with } G' = C^*C \text{ (known)}$$

- What do we know now?

Lemma $\Rightarrow$ know $\alpha\beta^{-1}$ where $\alpha = \Phi(c_1), \beta = \Phi(c_2)$. Getting α is enough.
From B compute I_M and $\mathcal{O}' = I_M^{-1} I_M$
Proposition $\Rightarrow$ know $\alpha\mathcal{O}'$. Also know $\mathrm{nrd}(\alpha) = q_1$

Reducing rank-2 module-LIP

- **modLIP** instance

$$B = (b_1|b_2) \text{ basis of } M \subset L^2 \text{ (known)}$$
$$C = (c_1|c_2) \text{ basis of } M \subset L^2 \text{ (unknown)}$$
$$G' \text{ Gram matrix with } G' = C^*C \text{ (known)}$$

- What do we know now?

Lemma $\Rightarrow$ know $\alpha\beta^{-1}$ where $\alpha = \Phi(c_1), \beta = \Phi(c_2)$. Getting α is enough.
From B compute I_M and $\mathcal{O}' = I_M^{-1} I_M$
Proposition $\Rightarrow$ know $\alpha\mathcal{O}'$. Also know $\mathrm{nrd}(\alpha) = q_1$

$\mathcal{O}$-nrdPIP, definition

Parameter: $\mathcal{O} \subset \mathcal{A}$ maximal order

Reducing rank-2 module-LIP

- **modLIP** instance

$$B = (b_1|b_2) \text{ basis of } M \subset L^2 \text{ (known)}$$
$$C = (c_1|c_2) \text{ basis of } M \subset L^2 \text{ (unknown)}$$
$$G' \text{ Gram matrix with } G' = C^*C \text{ (known)}$$

- What do we know now?

Lemma $\Rightarrow$ know $\alpha\beta^{-1}$ where $\alpha = \Phi(c_1), \beta = \Phi(c_2)$. Getting α is enough.
From B compute I_M and $\mathcal{O}' = I_M^{-1} I_M$
Proposition $\Rightarrow$ know $\alpha\mathcal{O}'$. Also know $\mathrm{nrd}(\alpha) = q_1$

$\mathcal{O}$-nrdPIP, definition

Parameter: $\mathcal{O} \subset \mathcal{A}$ maximal order
Input: $I \subset \mathcal{A}$ principal right $\mathcal{O}$-ideal and $q \in F$

Reducing rank-2 module-LIP

- **modLIP instance**

$$B = (b_1|b_2) \text{ basis of } M \subset L^2 \text{ (known)}$$
$$C = (c_1|c_2) \text{ basis of } M \subset L^2 \text{ (unknown)}$$
$$G' \text{ Gram matrix with } G' = C^*C \text{ (known)}$$

- What do we know now?

Lemma $\Rightarrow$ know $\alpha\beta^{-1}$ where $\alpha = \Phi(c_1), \beta = \Phi(c_2)$. Getting α is enough.
From B compute I_M and $\mathcal{O}' = I_M^{-1} I_M$
Proposition $\Rightarrow$ know $\alpha\mathcal{O}'$. Also know $\mathrm{nrd}(\alpha) = q_1$

$\mathcal{O}$-nrdPIP, definition

Parameter: $\mathcal{O} \subset \mathcal{A}$ maximal order
Input: $I \subset \mathcal{A}$ principal right $\mathcal{O}$-ideal and $q \in F$
Goal: A right generator α of I with $\mathrm{nrd}(\alpha) = q$ (if it exists)

Reducing rank-2 module-LIP

Theorem (general reduction)

Let $(L, \mathcal{A}) = (F, K)$ or $(K, K + K \cdot j)$ and B basis of $M \subset L^2$

Reducing rank-2 module-LIP

Theorem (general reduction)

Let $(L, \mathcal{A}) = (F, K)$ or $(K, K + K \cdot j)$ and B basis of $M \subset L^2$
$\exists$ a poly time reduction from modLIP$_L^B$ to $\mathcal{O}'$-nrdPIP where $\mathcal{O}' \subset \mathcal{A}$ depends only on M

Reducing rank-2 module-LIP

Theorem (general reduction)

Let $(L, \mathcal{A}) = (F, K)$ or $(K, K + K \cdot j)$ and B basis of $M \subset L^2$
$\exists$ a poly time reduction from modLIP_L^B to $\mathcal{O}'$-nrdPIP where $\mathcal{O}' \subset \mathcal{A}$ depends only on M

- **Hawk:** $L = \mathbb{Q}(\zeta_m)$ cyclotomic, $M = \mathcal{O}_L^2$, we have $I_M = \mathcal{O}$ and $\mathcal{O}' = I_M^{-1} I_M = \mathcal{O}$

Reducing rank-2 module-LIP

Theorem (general reduction)

Let $(L, \mathcal{A}) = (F, K)$ or $(K, K + K \cdot j)$ and B basis of $M \subset L^2$
$\exists$ a poly time reduction from modLIP$_L^B$ to $\mathcal{O}'$-nrdPIP where $\mathcal{O}' \subset \mathcal{A}$ depends only on M

- **Hawk:** $L = \mathbb{Q}(\zeta_m)$ cyclotomic, $M = \mathcal{O}_L^2$, we have $I_M = \mathcal{O}$ and $\mathcal{O}' = I_M^{-1} I_M = \mathcal{O}$

Theorem (reduction, special case)

$L = \mathbb{Q}(\zeta_m)$ cyclotomic and $\mathcal{O}$ maximal order in $L + L \cdot j$ containing $\mathcal{O}_L + \mathcal{O}_L \cdot j$
$\exists$ a poly time **Karp** reduction from modLIP$_L^{I_2}$ to $\mathcal{O}$-nrdPIP

Reducing rank-2 module-LIP

Theorem (general reduction)

Let $(L, \mathcal{A}) = (F, K)$ or $(K, K + K \cdot j)$ and B basis of $M \subset L^2$
$\exists$ a poly time reduction from modLIP$_L^B$ to $\mathcal{O}'$-nrdPIP where $\mathcal{O}' \subset \mathcal{A}$ depends only on M

- **Hawk:** $L = \mathbb{Q}(\zeta_m)$ cyclotomic, $M = \mathcal{O}_L^2$, we have $I_M = \mathcal{O}$ and $\mathcal{O}' = I_M^{-1} I_M = \mathcal{O}$

Theorem (reduction, special case)

$L = \mathbb{Q}(\zeta_m)$ cyclotomic and $\mathcal{O}$ maximal order in $L + L \cdot j$ containing $\mathcal{O}_L + \mathcal{O}_L \cdot j$
$\exists$ a poly time **Karp** reduction from modLIP$_L^{I_2}$ to $\mathcal{O}$-nrdPIP

Remark: When $L = \mathbb{Q}(\zeta_m)$ cyclotomic, $\mathcal{O}_L + \mathcal{O}_L \cdot j$ already maximal for most m.
Otherwise, $\exists$ poly time algo to compute $\mathcal{O}$

Reducing rank-2 module-LIP

Let $(L, \mathcal{A}) = (F, K)$ or $(K = \mathbb{Q}(\zeta_m), K + K \cdot j)$

Reducing rank-2 module-LIP

Let $(L, \mathcal{A}) = (F, K)$ or $(K = \mathbb{Q}(\zeta_m), K + K \cdot j)$
Parameters: B basis of $\mathcal{O}_L^2$, $G = B^* B$. **Input:** $G' \sim G$

Reducing rank-2 module-LIP

Let $(L, \mathcal{A}) = (F, K)$ or $(K = \mathbb{Q}(\zeta_m), K + K \cdot j)$
Parameters: B basis of $\mathcal{O}_L^2$, $G = B^* B$. **Input:** $G' \sim G$

Algorithm reduction for $\mathcal{O}_L^2$

1: Compute $\mathcal{O} \supset \mathcal{O}_L + \mathcal{O}_L \cdot j$ maximal order
2: From $\mathbf{G}, \mathbf{G}'$ compute a candidate δ for $\delta = \det(C)$
3: $q = q_3^{-1}(\overline{q_2} - \delta \cdot j) \quad (= \alpha\beta^{-1})$
4: $I = \mathcal{O} \cap q\mathcal{O} \quad (= \alpha\mathcal{O}')$
5: Call an oracle solving $\mathcal{O}'$-nrdPIP on (I, q), get α
6: From α get a solution $C \in \mathrm{GL}_2(\mathrm{L})$

Reducing rank-2 module-LIP

Let $(L, \mathcal{A}) = (F, K)$ or $(K = \mathbb{Q}(\zeta_m), K + K \cdot j)$
Parameters: B basis of $\mathcal{O}_L^2$, $G = B^* B$. **Input:** $G' \sim G$

Algorithm reduction for $\mathcal{O}_L^2$

1: Compute $\mathcal{O} \supset \mathcal{O}_L + \mathcal{O}_L \cdot j$ maximal order
2: From $\mathbf{G}, \mathbf{G}'$ compute a candidate δ for $\delta = \det(C)$
3: $q = q_3^{-1}(\overline{q_2} - \delta \cdot j) \quad (= \alpha\beta^{-1})$
4: $I = \mathcal{O} \cap q\mathcal{O} \quad (= \alpha\mathcal{O}')$
5: Call an oracle solving $\mathcal{O}'$-nrdPIP on (I, q), get α
6: From α get a solution $C \in \mathrm{GL}_2(\mathrm{L})$

- Can be adapted to compute **all** the solutions for modLIP on $\mathcal{O}_L^2$, still with **one** call to the oracle (act by Aut$(\mathcal{O}_L^2)$, explicit group)

Reducing rank-2 module-LIP

- In general, our algorithm computes **all** the solutions to module-LIP with at most **two** calls to the oracle.

Reducing rank-2 module-LIP

- In general, our algorithm computes **all** the solutions to module-LIP with at most **two** calls to the oracle. Can bound the number of solutions and since

$$\begin{aligned} \{C \text{ solutions to modLIP}\} &\longrightarrow \{\text{solutions to nrdPIP}\} \\ (c_1|c_2) &\longmapsto \Phi(c_1) \end{aligned}$$

is **injective**, get a bound on $|\{\text{solutions to modLIP}\}|$

Reducing rank-2 module-LIP

- In general, our algorithm computes **all** the solutions to module-LIP with at most **two** calls to the oracle. Can bound the number of solutions and since

$$\{C \text{ solutions to modLIP}\} \longrightarrow \{\text{solutions to nrdPIP}\}$$
$$(c_1|c_2) \longmapsto \Phi(c_1)$$

is **injective**, get a bound on $|\{\text{solutions to modLIP}\}| = |\mathrm{Aut}(M)|$, where $\mathrm{Aut}(M) = \{\Theta \in \mathrm{GL}_2(L) \,|\, \Theta(M) = M \text{ and } \Theta \cdot \Theta^* = I_2\}$

Reducing rank-2 module-LIP

- In general, our algorithm computes **all** the solutions to module-LIP with at most **two** calls to the oracle. Can bound the number of solutions and since

$$\{C \text{ solutions to modLIP}\} \longrightarrow \{\text{solutions to nrdPIP}\}$$
$$(c_1|c_2) \longmapsto \Phi(c_1)$$

is **injective**, get a bound on $|\{\text{solutions to modLIP}\}| = |\mathrm{Aut}(M)|$, where $\text{Aut}(M) = \{\Theta \in \mathrm{GL}_2(L) \,|\, \Theta(M) = M \text{ and } \Theta \cdot \Theta^* = I_2\}$

Proposition [2]

Let $M \subset L^2$ a rank 2 module, then $|\mathrm{Aut}(M)| \leq 64d^4$, where $d = [L : \mathbb{Q}]$

Reducing rank-2 module-LIP

- In general, our algorithm computes **all** the solutions to module-LIP with at most **two** calls to the oracle. Can bound the number of solutions and since

$$\begin{aligned}\{C \text{ solutions to modLIP}\} &\longrightarrow \{\text{solutions to nrdPIP}\}\\ (c_1|c_2) &\longmapsto \Phi(c_1)\end{aligned}$$

is **injective**, get a bound on $|\{\text{solutions to modLIP}\}| = |\mathrm{Aut}(M)|$, where $\mathrm{Aut}(M) = \{\Theta \in \mathrm{GL}_2(L) \,|\, \Theta(M) = M \text{ and } \Theta \cdot \Theta^* = I_2\}$

Proposition [2]

Let $M \subset L^2$ a rank 2 module, then $|\mathrm{Aut}(M)| \leq 64d^4$, where $d = [L : \mathbb{Q}]$

- In comparison, the lattice $\mathbb{Z}^n \subset \mathbb{R}^n$ has $2^{O(n)}$ automorphisms (isometries)

Solving the totally real case

Solving the totally real case

- K/F CM extension and $I = g \cdot \mathcal{O}_K$ principal ideal. Finding a generator is a well-known problem (PIP): sub-exponential classical or polynomial quantum.

[4] Cryptanalysis of the Revised NTRU Signature Scheme

Solving the totally real case

- K/F CM extension and $I = g \cdot \mathcal{O}_K$ principal ideal. Finding a generator is a well-known problem (PIP): sub-exponential classical or polynomial quantum. However, if the reduced norm of the generator is known:

[4] Cryptanalysis of the Revised NTRU Signature Scheme

Solving the totally real case

- K/F CM extension and $I = g \cdot \mathcal{O}_K$ principal ideal. Finding a generator is a well-known problem (PIP): sub-exponential classical or polynomial quantum. However, if the reduced norm of the generator is known:

`LenstraSilverberg` algorithm[a]

[a] Testing isomorphism of lattices over CM-orders

$\exists$ a poly time algorithm s.t. given $I = g \cdot \mathcal{O}_K$ principal and $q = g\bar{g}$, the algorithm computes a generator g of I with $\mathrm{nrd}(g) = q$

[4] Cryptanalysis of the Revised NTRU Signature Scheme

Solving the totally real case

- K/F CM extension and $I = g \cdot \mathcal{O}_K$ principal ideal. Finding a generator is a well-known problem (PIP): sub-exponential classical or polynomial quantum. However, if the reduced norm of the generator is known:

`LenstraSilverberg` algorithm[a]

[a] Testing isomorphism of lattices over CM-orders

$\exists$ a poly time algorithm s.t. given $I = g \cdot \mathcal{O}_K$ principal and $q = g\bar{g}$, the algorithm computes a generator g of I with $\mathrm{nrd}(g) = q$

It is a generalization of an algorithm by Gentry and Szydlo[4] for cyclotomic fields

[4] Cryptanalysis of the Revised NTRU Signature Scheme

Solving the totally real case

- Let $K = \mathbb{Q}(\zeta_m)$ and $F = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ with $m = 2^e$. Fix $g \in \mathcal{O}_K$

`GentrySzydlo`

Input : A basis of $g \cdot \mathcal{O}_L$ and $g\bar{g} \in \mathcal{O}_F$
Output : g, up to a root of unity of K

Solving the totally real case

- Let $K = \mathbb{Q}(\zeta_m)$ and $F = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ with $m = 2^e$. Fix $g \in \mathcal{O}_K$

`GentrySzydlo`

Input : A basis of $g \cdot \mathcal{O}_L$ and $g\bar{g} \in \mathcal{O}_F$
Output : g, up to a root of unity of K

- Find a "good" prime $P \in \mathbb{N}$
- Compute a basis of $(g \cdot \mathcal{O}_K)^{P-1} = g^{P-1} \cdot \mathcal{O}_L$ using LLL

Solving the totally real case

- Let $K = \mathbb{Q}(\zeta_m)$ and $F = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ with $m = 2^e$. Fix $g \in \mathcal{O}_K$

`GentrySzydlo`

Input : A basis of $g \cdot \mathcal{O}_L$ and $g\bar{g} \in \mathcal{O}_F$
Output : g, up to a root of unity of K

- Find a "good" prime $P \in \mathbb{N}$
- Compute a basis of $(g \cdot \mathcal{O}_K)^{P-1} = g^{P-1} \cdot \mathcal{O}_L$ using LLL
  At each step, divide the basis by $g\bar{g}$ to avoid coefficient blow-up

Solving the totally real case

- Let $K = \mathbb{Q}(\zeta_m)$ and $F = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ with $m = 2^e$. Fix $g \in \mathcal{O}_K$

GentrySzydlo

Input : A basis of $g \cdot \mathcal{O}_L$ and $g\bar{g} \in \mathcal{O}_F$
Output : g, up to a root of unity of K

- Find a "good" prime $P \in \mathbb{N}$
- Compute a basis of $(g \cdot \mathcal{O}_K)^{P-1} = g^{P-1} \cdot \mathcal{O}_L$ using LLL
  At each step, divide the basis by $g\bar{g}$ to avoid coefficient blow-up
- The first basis vector is $g^{P-1} \cdot v$ with v **short**. Reduce modulo P
- By Fermat's theorem, $g^{P-1} = 1 \pmod P$, so we get $v \pmod P$

Solving the totally real case

- Let $K = \mathbb{Q}(\zeta_m)$ and $F = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ with $m = 2^e$. Fix $g \in \mathcal{O}_K$

GentrySzydlo

Input : A basis of $g \cdot \mathcal{O}_L$ and $g\bar{g} \in \mathcal{O}_F$
Output : g, up to a root of unity of K

- Find a "good" prime $P \in \mathbb{N}$
- Compute a basis of $(g \cdot \mathcal{O}_K)^{P-1} = g^{P-1} \cdot \mathcal{O}_L$ using LLL
  At each step, divide the basis by $g\bar{g}$ to avoid coefficient blow-up
- The first basis vector is $g^{P-1} \cdot v$ with v **short**. Reduce modulo P
- By Fermat's theorem, $g^{P-1} = 1 \pmod P$, so we get $v \pmod P$

Solving the totally real case

- If P is **big enough**, get v exactly and deduce g^{P-1}

Solving the totally real case

- If P is **big enough**, get v exactly and deduce g^{P-1}
- With some trick, reduce the exponent and deduce g^m

Solving the totally real case

- If P is **big enough**, get v exactly and deduce g^{P-1}
- With some trick, reduce the exponent and deduce g^m
- Compute a m-th root and get g, up to a root of unity

Solving the totally real case

- If P is **big enough**, get v exactly and deduce g^{P-1}
- With some trick, reduce the exponent and deduce g^m
- Compute a m-th root and get g, up to a root of unity

We did an implementation in `SageMath` for [1]. Adapting this algorithm for quaternion algebras seems **very hard** !

Sum-up

When L either totally real or CM, reduce rank-2 module-LIP over L to nrdPIP in a quadratic extension of L (may be non commutative)

[5] Algorithmic enumeration of ideal classes for quaternion orders, M. Kirschmer, J. Voight

Sum-up

When L either totally real or CM, reduce rank-2 module-LIP over L to nrdPIP in a quadratic extension of L (may be non commutative)

If L totally real, efficient algorithm for nrdPIP (poly time attack on modLIP)

[5] Algorithmic enumeration of ideal classes for quaternion orders, M. Kirschmer, J. Voight

Sum-up

When L either totally real or CM, reduce rank-2 module-LIP over L to nrdPIP in a quadratic extension of L (may be non commutative)

If L totally real, efficient algorithm for nrdPIP (poly time attack on modLIP)

If L is CM, state-of-the-art for nrdPIP: SVP in $I \subset \mathcal{A}$, rank $2d$ lattice[5]

[5] Algorithmic enumeration of ideal classes for quaternion orders, M. Kirschmer, J. Voight

Sum-up

When L either totally real or CM, reduce rank-2 module-LIP over L to nrdPIP in a quadratic extension of L (may be non commutative)

If L totally real, efficient algorithm for nrdPIP (poly time attack on modLIP)

If L is CM, state-of-the-art for nrdPIP: SVP in $I \subset \mathcal{A}$, rank $2d$ lattice[5]

Thanks for your attention! Any question?

[5] Algorithmic enumeration of ideal classes for quaternion orders, M. Kirschmer, J. Voight