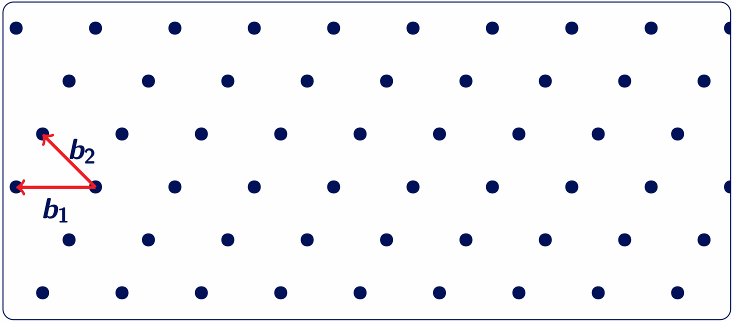
Cryptanalysis of rank-2 module-LIP: a single real embedding is all it takes

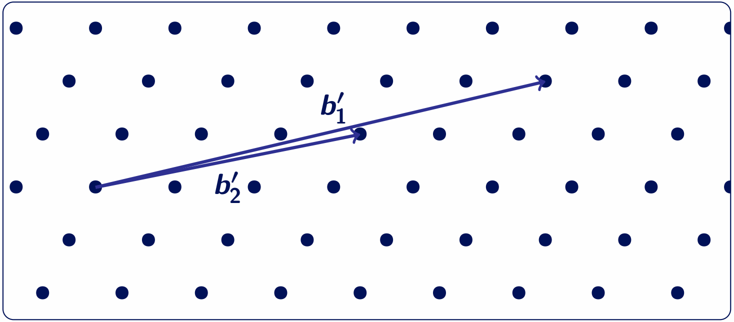
Bill Allombert, Alice Pellet-Mary (Université de Bordeaux),
Wessel van Woerden (Université de Bordeaux & PQShield) .

Lattices

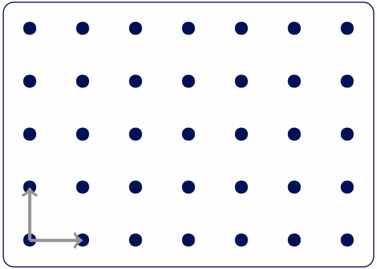


- $\mathcal{L} = \{\sum_{i=1}^{n} x_i b_i \mid \forall i,\, x_i \in \mathbb{Z}\}$ is a lattice
- $(b_1, \ldots, b_n) =: B \in \mathbf{GL}_n(\mathbb{R})$ is a basis (not unique)
- n is the dimension (or rank)

Lattices

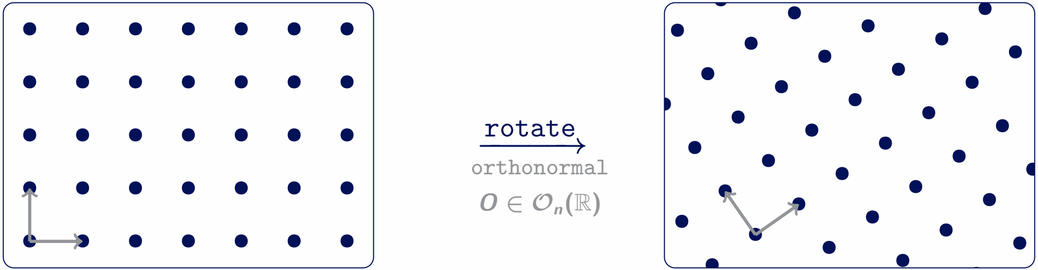


- $\mathcal{L} = \{\sum_{i=1}^{n} x_i b_i \mid \forall i,\ x_i \in \mathbb{Z}\}$ is a lattice
- $(b_1, \ldots, b_n) =: B \in \mathbf{GL}_n(\mathbb{R})$ is a basis (not unique)
- n is the dimension (or rank)



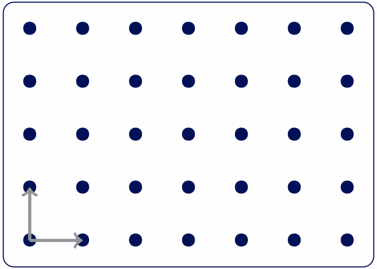
$\mathcal{L}_0 = \mathbb{Z}^n$

The lattice isomorphism problem for $\mathbb{Z}^n$

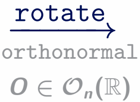


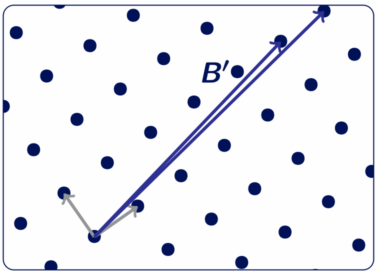
$\mathcal{L}_0 = \mathbb{Z}^n$ $\mathcal{L}_1 = O \cdot \mathbb{Z}^n$

The lattice isomorphism problem for $\mathbb{Z}^n$



$\mathcal{L}_0 = \mathbb{Z}^n$

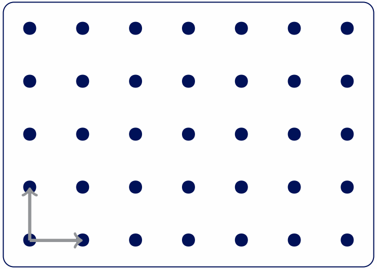




$\mathcal{L}_1 = O \cdot \mathbb{Z}^n$

B' long basis of $\mathcal{L}_1$

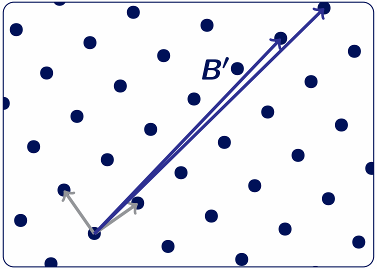
The lattice isomorphism problem for $\mathbb{Z}^n$



rotate $\longrightarrow$

orthonormal

$O \in \mathcal{O}_n(\mathbb{R})$



$\mathcal{L}_0 = \mathbb{Z}^n$

$\mathcal{L}_1 = O \cdot \mathbb{Z}^n$

B' long basis of $\mathcal{L}_1$

Lattice Isomorphism Problem (LIP) assumption

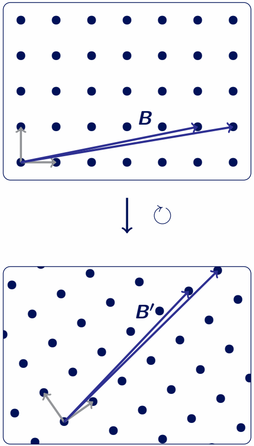
recovering O from B' is hard

B basis of $\mathbb{Z}^n$, $O \in \mathcal{O}_n(\mathbb{R}) : B' = O \cdot B$.

Equivalent formulation with Gram matrices

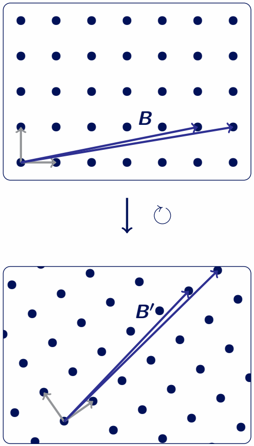
$\mathbb{Z}^n$-LIP: Given $B' = O \cdot B$ with
- $O \in O_n(\mathbb{R})$ orthogonal
- B a basis of $\mathbb{Z}^n$

Find O (equivalently: find B)



$\mathbb{Z}^n$-LIP: Given $B' = O \cdot B$ with
- $O \in O_n(\mathbb{R})$ orthogonal
- B a basis of $\mathbb{Z}^n$

Find O (equivalently: find B)



Gram matrix associated to B':

$$G = (B')^T B' = B^T (O^T O) B = B^T B$$

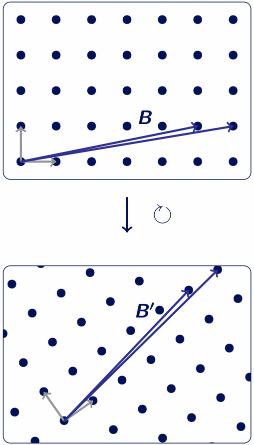
$\Rightarrow$ O has disappeared

Equivalent formulation with Gram matrices

$\mathbb{Z}^n$-LIP: Given $B' = O \cdot B$ with

- $O \in O_n(\mathbb{R})$ orthogonal
- B a basis of $\mathbb{Z}^n$

Find O (equivalently: find B)



Gram matrix associated to B':

$$G = (B')^T B' = B^T (O^T O) B = B^T B$$

$\Rightarrow$ O has disappeared

$\mathbb{Z}^n$-LIP (Gram matrix):

Given $G = B^T B$ with B a basis of $\mathbb{Z}^n$,

find B.

Equivalent formulation with Gram matrices

$\mathbb{Z}^n$-LIP: Given $B' = O \cdot B$ with
- $O \in O_n(\mathbb{R})$ orthogonal
- B a basis of $\mathbb{Z}^n$

Find O (equivalently: find B)

Gram matrix associated to B':

$$G = (B')^T B' = B^T (O^T O) B = B^T B$$

$\Rightarrow$ O has disappeared

$\mathbb{Z}^n$-LIP (Gram matrix):
Given $G = B^T B$ with B a basis of $\mathbb{Z}^n$,

find B.

Example:

- $B = \begin{pmatrix} 1 & 1 \\ 4 & 5 \end{pmatrix}$
- $O = \begin{pmatrix} 0.5 & 0.87 \\ 0.87 & -0.5 \end{pmatrix}$
- $B' = \begin{pmatrix} 3.96 & 4.83 \\ -1.13 & -1.63 \end{pmatrix}$
- $G = \begin{pmatrix} 17 & 21 \\ 21 & 26 \end{pmatrix}$
  $= B^T B = (B')^T B'$

Given G, recover $B \in \mathbb{Z}^{2\times 2}$ with $\det(B) = \pm 1$ such that $B^T B = G$

Module-LIP

Number fields

Number field: $K = \mathbb{Q}[X]/P(X)$ (P irreducible, $\deg(P) = d$)

Number field: $K = \mathbb{Q}[X]/P(X)$ (P irreducible, $\deg(P) = d$)

- $K = \mathbb{Q}$
- $K = \mathbb{Q}[X]/(X^d + 1)$ with $d = 2^\ell$ $\rightsquigarrow$ power-of-two cyclotomic field
- $K = \mathbb{Q}[X]/(X^d - X - 1)$ with d prime $\rightsquigarrow$ NTRUPrime field

Number fields

Number field: $K = \mathbb{Q}[X]/P(X)$ (P irreducible, $\deg(P) = d$)

- $K = \mathbb{Q}$
- $K = \mathbb{Q}[X]/(X^d + 1)$ with $d = 2^\ell$ $\rightsquigarrow$ power-of-two cyclotomic field
- $K = \mathbb{Q}[X]/(X^d - X - 1)$ with d prime $\rightsquigarrow$ NTRUPrime field

Ring of integers: $\mathcal{O}_K \subset K$, for this talk $\mathcal{O}_K = \mathbb{Z}[X]/P(X)$

(more generally $\mathbb{Z}[X]/P(X) \subseteq \mathcal{O}_K$ but $\mathcal{O}_K$ can be larger)

Number fields

Number field: $K = \mathbb{Q}[X]/P(X)$ (P irreducible, $\deg(P) = d$)

- $K = \mathbb{Q}$
- $K = \mathbb{Q}[X]/(X^d + 1)$ with $d = 2^\ell$ $\rightsquigarrow$ power-of-two cyclotomic field
- $K = \mathbb{Q}[X]/(X^d - X - 1)$ with d prime $\rightsquigarrow$ NTRUPrime field

Ring of integers: $\mathcal{O}_K \subset K$, for this talk $\mathcal{O}_K = \mathbb{Z}[X]/P(X)$

(more generally $\mathbb{Z}[X]/P(X) \subseteq \mathcal{O}_K$ but $\mathcal{O}_K$ can be larger)

- $\mathcal{O}_K = \mathbb{Z}$
- $\mathcal{O}_K = \mathbb{Z}[X]/(X^d + 1)$ with $d = 2^\ell$ $\rightsquigarrow$ power-of-two cyclotomic ring
- $\mathcal{O}_K = \mathbb{Z}[X]/(X^d - X - 1)$ with d prime $\rightsquigarrow$ NTRUPrime ring of integers

Embeddings

($K = \mathbb{Q}[X]/P(X)$, $\alpha_1, \cdots, \alpha_d$ complex roots of $P(X)$)

Field embeddings: $\sigma_k : K \to \mathbb{C},\ X \mapsto \alpha_k$

Canonical embedding:
$$\begin{aligned} \sigma : K &\to \mathbb{C}^d \\ y &\mapsto (\sigma_1(y), \cdots, \sigma_d(y)) \end{aligned}$$

Embeddings

$(K = \mathbb{Q}[X]/P(X), \quad \alpha_1, \cdots, \alpha_d$ complex roots of $P(X))$

Field embeddings: $\sigma_k : K \to \mathbb{C}, \; X \mapsto \alpha_k$

Canonical embedding:
$$\begin{aligned} \sigma : K &\to \mathbb{C}^d \\ y &\mapsto (\sigma_1(y), \cdots, \sigma_d(y)) \end{aligned}$$

- real embedding: $\sigma_i(K) \subset \mathbb{R} \subset \mathbb{C}$.

Embeddings

($K = \mathbb{Q}[X]/P(X)$, $\alpha_1, \cdots, \alpha_d$ complex roots of $P(X)$)

Field embeddings: $\sigma_k : K \to \mathbb{C}, \; X \mapsto \alpha_k$

Canonical embedding: $\sigma : K \to \mathbb{C}^d$

$$y \mapsto (\sigma_1(y), \cdots, \sigma_d(y))$$

- real embedding: $\sigma_i(K) \subset \mathbb{R} \subset \mathbb{C}$.
- Otherwise: complex embedding (occur in conjugate pairs)

Embeddings

($K = \mathbb{Q}[X]/P(X)$, $\alpha_1, \cdots, \alpha_d$ complex roots of $P(X)$)

Field embeddings: $\sigma_k : K \to \mathbb{C}, \; X \mapsto \alpha_k$

Canonical embedding:

$$\begin{aligned} \sigma : K &\to \mathbb{C}^d \\ y &\mapsto (\sigma_1(y), \cdots, \sigma_d(y)) \end{aligned}$$

- real embedding: $\sigma_i(K) \subset \mathbb{R} \subset \mathbb{C}$.
- Otherwise: complex embedding (occur in conjugate pairs)
- we can see K as a rank d $\mathbb{Q}$-subspace of $\mathbb{R}^{r_1} \times \mathbb{C}^{2r_2} \subset \mathbb{C}^d$

($K = \mathbb{Q}[X]/P(X)$, $\alpha_1, \cdots, \alpha_d$ complex roots of $P(X)$)

Field embeddings: $\sigma_k : K \to \mathbb{C}, \; X \mapsto \alpha_k$

Canonical embedding:
$$\sigma : K \to \mathbb{C}^d$$
$$y \mapsto (\sigma_1(y), \cdots, \sigma_d(y))$$

- real embedding: $\sigma_i(K) \subset \mathbb{R} \subset \mathbb{C}$.
- Otherwise: complex embedding (occur in conjugate pairs)
- we can see K as a rank d $\mathbb{Q}$-subspace of $\mathbb{R}^{r_1} \times \mathbb{C}^{2r_2} \subset \mathbb{C}^d$
- this induces a geometry on K:

$$\langle a, b \rangle := \langle \sigma(a), \sigma(b) \rangle = \sigma(a)^* \sigma(b) = \sum_{i=1}^{d} \overline{\sigma_i(a)} \sigma_i(b) \in \mathbb{R}$$
$$\|a\|^2 := \|\sigma(a)\|_2^2 = \sum_{i=1}^{d} |\sigma_i(a)|^2 \in \mathbb{R}.$$

(Free) module:

$M = \{B \cdot x \mid x \in \mathcal{O}_K^k\}$ for some matrix $B \in \mathcal{O}_K^{k \times k}$ with $\det_K(B) \neq 0$

Module lattices

(Free) module:

$$M = \{B \cdot x \mid x \in \mathcal{O}_K^k\} \text{ for some matrix } B \in \mathcal{O}_K^{k \times k} \text{ with } \det_K(B) \neq 0$$

- k is the module rank
- B is a module basis of M

  (if the module is not free, it has a ‘‘pseudo-basis’’ instead)

Module lattices

(Free) module:

$$M = \{B \cdot x \mid x \in \mathcal{O}_K^k\} \text{ for some matrix } B \in \mathcal{O}_K^{k \times k} \text{ with } \det_K(B) \neq 0$$

- k is the module rank
- B is a module basis of M

  (if the module is not free, it has a ''pseudo-basis'' instead)

$\sigma(M)$ is a lattice:

- of $\mathbb{Z}$-rank $n := d \cdot k$

(Free) module:

$$M = \{B \cdot x \mid x \in \mathcal{O}_K^k\} \text{ for some matrix } B \in \mathcal{O}_K^{k \times k} \text{ with } \det_K(B) \neq 0$$

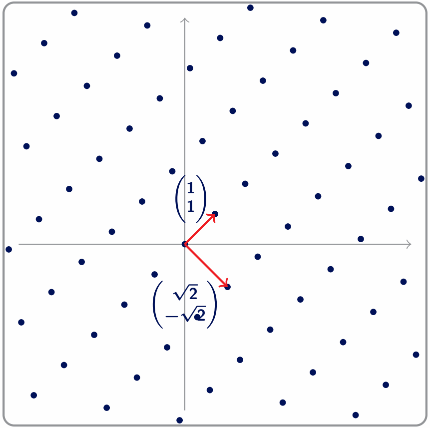
- k is the module rank
- B is a module basis of M
  (if the module is not free, it has a ''pseudo-basis'' instead)

$\sigma(M)$ is a lattice:

- of $\mathbb{Z}$-rank $n := d \cdot k$
- with basis $(\sigma(b_i X^j))_{\substack{1 \leq i \leq k \\ 0 \leq j < d}}$ (b_i columns of B)

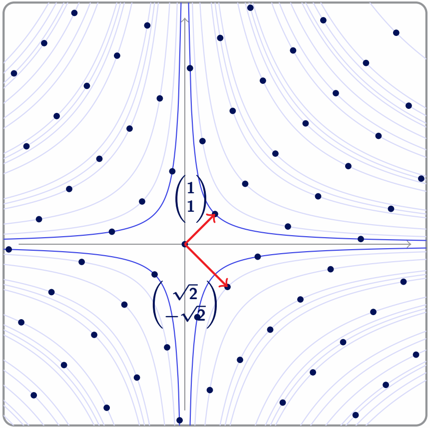
An example

$$K = \mathbb{Q}[X]/(X^2-2)\,, \qquad \mathcal{O}_K = \mathbb{Z}[X]/(X^2-2)\,, \qquad \sigma : a + bX \mapsto \begin{pmatrix} a+b\sqrt{2} \\ a-b\sqrt{2} \end{pmatrix}, \qquad \mathcal{L} = \sigma(\mathcal{O}_K)$$



An example

$K = \mathbb{Q}[X]/(X^2 - 2)$, $\mathcal{O}_K = \mathbb{Z}[X]/(X^2 - 2)$, $\sigma : a + bX \mapsto \begin{pmatrix} a + b\sqrt{2} \\ a - b\sqrt{2} \end{pmatrix}$, $\mathcal{L} = \sigma(\mathcal{O}_K)$



LIP for $\mathbb{Z}^n$:
Given $\boldsymbol{G} = \boldsymbol{B}^T \boldsymbol{B}$ with $\boldsymbol{B}$ a basis of $\mathbb{Z}^n$, find $\boldsymbol{B}$

The module lattice isomorphism problem

LIP for $\mathbb{Z}^n$:
Given $G = B^T B$ with B a basis of $\mathbb{Z}^n$, find B

Module-LIP for $\mathcal{O}_K^n$:
Given $G = \sigma(B)^* \sigma(B)$ with B a basis of $\mathcal{O}_K^n$, find B

The module lattice isomorphism problem

LIP for $\mathbb{Z}^n$:
Given $G = B^T B$ with B a basis of $\mathbb{Z}^n$, find B

Module-LIP for $\mathcal{O}_K^n$:
Given $G = \sigma(B)^* \sigma(B)$ with B a basis of $\mathcal{O}_K^n$, find B

Remarks.

- we consider $\sigma(B)^* = \overline{\sigma(B)}^T$ because we use hermitian norm in $\mathbb{C}^{2d}$
- only rank 2 modules in this talk (and even only $\mathcal{O}_K^2$)

The module lattice isomorphism problem

LIP for $\mathbb{Z}^n$:
Given $G = B^T B$ with B a basis of $\mathbb{Z}^n$, find B

Module-LIP for $\mathcal{O}_K^n$:
Given $G = \sigma(B)^* \sigma(B)$ with B a basis of $\mathcal{O}_K^n$, find B

Remarks.

- we consider $\sigma(B)^* = \overline{\sigma(B)}^T$ because we use hermitian norm in $\mathbb{C}^{2d}$
- only rank 2 modules in this talk (and even only $\mathcal{O}_K^2$)

Hawk relies on
module-LIP for the module $\mathcal{O}_K^2$, in a power-of-two cyclotomic field
($K = \mathbb{Q}[X]/(X^d + 1)$ with $d = 512$ or $d = 1024$)

Notations: $K = \mathbb{Q}[X]/P(X)$, $\mathcal{O}_K = \mathbb{Z}[X]/P(X)$

- We consider the case $\mathcal{L}_0 = z\mathcal{O}_K$ for some $z \in \mathcal{O}_K$
- K a CM-field

Cryptanalysis of rank-1 module-LIP

Notations: $K = \mathbb{Q}[X]/P(X)$, $\mathcal{O}_K = \mathbb{Z}[X]/P(X)$

- We consider the case $\mathcal{L}_0 = z\mathcal{O}_K$ for some $z \in \mathcal{O}_K$
- K a CM-field

Objective: Given $z\mathcal{O}_K$ and $\bar{z}z$, recover z (up to a root of unity)

Notations: $K = \mathbb{Q}[X]/P(X)$, $\mathcal{O}_K = \mathbb{Z}[X]/P(X)$

- We consider the case $\mathcal{L}_0 = z\mathcal{O}_K$ for some $z \in \mathcal{O}_K$
- K a CM-field

Objective: Given $z\mathcal{O}_K$ and $\bar{z}z$, recover z (up to a root of unity)

Gentry-Szydlo algorithm: recovers z in classical polynomial-time

(when K is a cyclotomic field)

Cryptanalysis of rank-1 module-LIP

Notations: $K = \mathbb{Q}[X]/P(X)$, $\mathcal{O}_K = \mathbb{Z}[X]/P(X)$

- We consider the case $\mathcal{L}_0 = z\mathcal{O}_K$ for some $z \in \mathcal{O}_K$
- K a CM-field

Objective: Given $z\mathcal{O}_K$ and $\bar{z}z$, recover z (up to a root of unity)

Gentry-Szydlo algorithm: recovers z in classical polynomial-time

(when K is a cyclotomic field)

Extension by Lenstra-Silverberg: to all CM-fields

Cryptanalysis of rank-1 module-LIP

Notations: $K = \mathbb{Q}[X]/P(X)$, $\mathcal{O}_K = \mathbb{Z}[X]/P(X)$

- We consider the case $\mathcal{L}_0 = z\mathcal{O}_K$ for some $z \in \mathcal{O}_K$
- K a CM-field

Objective: Given $z\mathcal{O}_K$ and $\bar{z}z$, recover z (up to a root of unity)

Gentry-Szydlo algorithm: recovers z in classical polynomial-time

(when K is a cyclotomic field)

Extension by Lenstra-Silverberg: to all CM-fields

Our contribution: generalization to all number fields

(under a light heuristic)

Generalized GS-algorithm: this work

Let K be any field that is GS-friendly. Given $z\mathcal{O}_K$ and $|\sigma_k(z)|$ for all embeddings σ_k, one can recover $z \in \mathcal{O}_K$ in classical polynomial time.

Notations: $K = \mathbb{Q}[X]/P(X)$, $\mathcal{O}_K = \mathbb{Z}[X]/P(X)$, r_1 real, and $2r_2$ complex embeddings

- We consider the case $\mathcal{L}_0 = \mathcal{O}_K^2$.

Cryptanalysis of rank-2 module-LIP

Notations: $K = \mathbb{Q}[X]/P(X)$, $\mathcal{O}_K = \mathbb{Z}[X]/P(X)$, r_1 real, and $2r_2$ complex embeddings

- We consider the case $\mathcal{L}_0 = \mathcal{O}_K^2$.

Objective: Given $G := \sigma(B)^*\sigma(B)$, recover B (where $B = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathcal{O}_K^{2\times 2}$)

Notations: $K = \mathbb{Q}[X]/P(X)$, $\mathcal{O}_K = \mathbb{Z}[X]/P(X)$, r_1 real, and $2r_2$ complex embeddings

- We consider the case $\mathcal{L}_0 = \mathcal{O}_K^2$.

Objective: Given $G := \sigma(B)^*\sigma(B)$, recover B (where $B = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathcal{O}_K^{2\times 2}$)

Current state of cryptanalysis:

Totally real

$(r_1, 2r_2) = (d, 0)$

Broken!

[MPMPW24]

Totally imaginary

$(r_1, 2r_2) = (0, d)$

HAWK (CM field)

Cryptanalysis of rank-2 module-LIP

Notations: $K = \mathbb{Q}[X]/P(X)$, $\mathcal{O}_K = \mathbb{Z}[X]/P(X)$, r_1 real, and $2r_2$ complex embeddings

- We consider the case $\mathcal{L}_0 = \mathcal{O}_K^2$.

Objective: Given $G := \sigma(B)^*\sigma(B)$, recover B (where $B = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathcal{O}_K^{2\times 2}$)

Current state of cryptanalysis:

Totally real	What about here?	Totally imaginary
$(r_1, 2r_2) = (d, 0)$		$(r_1, 2r_2) = (0, d)$
Broken! [MPMPW24]		HAWK (CM field)

Cryptanalysis of rank-2 module-LIP

Notations: $K = \mathbb{Q}[X]/P(X)$, $\mathcal{O}_K = \mathbb{Z}[X]/P(X)$, r_1 real, and $2r_2$ complex embeddings

- We consider the case $\mathcal{L}_0 = \mathcal{O}_K^2$.

Objective: Given $G := \sigma(B)^* \sigma(B)$, recover B (where $B = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathcal{O}_K^{2\times 2}$)

Current state of cryptanalysis:

NTRUPrime field

$(r_1, 2r_2) = (1, d-1)$

Totally real

$(r_1, 2r_2) = (d, 0)$

Broken!

[MPMPW24]

What about here?

Totally imaginary

$(r_1, 2r_2) = (0, d)$

HAWK (CM field)

Notations: $K = \mathbb{Q}[X]/P(X)$, $\mathcal{O}_K = \mathbb{Z}[X]/P(X)$, r_1 real, and $2r_2$ complex embeddings

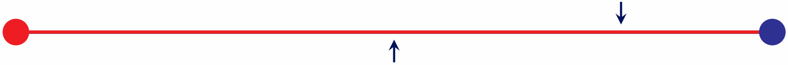
- We consider the case $\mathcal{L}_0 = \mathcal{O}_K^2$.

Objective: Given $G := \sigma(B)^*\sigma(B)$, recover B (where $B = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathcal{O}_K^{2\times 2}$)

Current state of cryptanalysis:

NTRUPrime field

$(r_1, 2r_2) = (1, d-1)$



Totally real

$(r_1, 2r_2) = (d, 0)$

Broken!

[MPMPW24]

What about here?

also broken!

(this work)

Totally imaginary

$(r_1, 2r_2) = (0, d)$

HAWK (CM field)

Plan of attack

(1) Reconstruction

Recover $B^\top B$ from $\sigma(B)^*\sigma(B)$.

(where $B = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathcal{O}_K^{2\times 2}$)

$B^\top B$

(2) Ideal recovery

$z_1 := a + bi$

recover $z_1\mathcal{O}_{L_1}$.

(where $L_1 = K(i)$)

$B^\top B$

(3) Absolute recovery

$\sigma_{k,\pm} : L_1 \to \mathbb{C}$

recover some $|\sigma_{k,\pm}(z_1)|$

$z_1\mathcal{O}_{L_1}$

$|\sigma_{k,\pm}(z_1)|$

(4) Ideal-LIP

Recover $z_1 = a + bi$.

(1) Cryptanalysis of module-LIP: when P has a real root

Notations: $K = \mathbb{Q}[X]/P(X)$, $\mathcal{O}_K = \mathbb{Z}[X]/P(X)$

Objective: Given $G := \sigma(B)^*\sigma(B)$, recover B (where $B = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathcal{O}_K^{2\times 2}$)

(1) Cryptanalysis of module-LIP: when P has a real root

Notations: $K = \mathbb{Q}[X]/P(X)$, $\mathcal{O}_K = \mathbb{Z}[X]/P(X)$

Objective: Given $G := \sigma(B)^* \sigma(B)$, recover B (where $B = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathcal{O}_K^{2\times 2}$)

Key point: if P has at least 1 real root, then from G we can recover

$$B^T B = \begin{pmatrix} a^2 + b^2 & ac + bd \\ ac + bd & c^2 + d^2 \end{pmatrix} =: \begin{pmatrix} q_1 & q_2 \\ q_2 & q_4 \end{pmatrix} \in \mathcal{O}_K^2$$

(1) Cryptanalysis of module-LIP: when P has a real root

Notations: $K = \mathbb{Q}[X]/P(X)$, $\mathcal{O}_K = \mathbb{Z}[X]/P(X)$

Objective: Given $G := \sigma(B)^* \sigma(B)$, recover B (where $B = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathcal{O}_K^{2\times 2}$)

Key point: if P has at least 1 real root, then from G we can recover

$$B^T B = \begin{pmatrix} a^2 + b^2 & ac + bd \\ ac + bd & c^2 + d^2 \end{pmatrix} =: \begin{pmatrix} q_1 & q_2 \\ q_2 & q_4 \end{pmatrix} \in \mathcal{O}_K^2$$

Idea: For a real embedding $\sigma_1 : K \to \mathbb{R} \subset \mathbb{C}$ we have

$$\boxed{\sigma_1(B)^* \sigma_1(B) = \sigma_1(B)^\top \sigma_1(B) = \sigma_1(B^\top B)}$$

Todo: recover $B^\top B$ from $\sigma_1(B^\top B)$

(1) Recovery of $B^\top B$ from a single real embedding

- Goal: recover $\boldsymbol{q} \in \mathcal{O}_K$ from real embedding(s) $\boldsymbol{\sigma_i(q)}$.

(1) Recovery of $B^\top B$ from a single real embedding

- Goal: recover $q \in \mathcal{O}_K$ from real embedding(s) $\sigma_i(q)$.
- Each embedding $\sigma_i : K \to \mathbb{R}$ is injective. (with infinite precision)

(1) Recovery of $B^\top B$ from a single real embedding

- Goal: recover $q \in \mathcal{O}_K$ from real embedding(s) $\sigma_i(q)$.
- Each embedding $\sigma_i : K \to \mathbb{R}$ is injective. (with infinite precision)
- $\mathbb{Z}$-basis $o_1, \ldots, o_d$ of $\mathcal{O}_K$, $q = \sum_{i=1}^{d} x_i o_i$

(1) Recovery of $B^\top B$ from a single real embedding

- Goal: recover $q \in \mathcal{O}_K$ from real embedding(s) $\sigma_i(q)$.
- Each embedding $\sigma_i : K \to \mathbb{R}$ is injective. (with infinite precision)
- $\mathbb{Z}$-basis $o_1, \ldots, o_d$ of $\mathcal{O}_K$, $q = \sum_{i=1}^{d} x_i o_i$
- Totally real: $\sigma(q) = \sum_{i=1}^{d} x_i \cdot \sigma(o_i) \in \mathbb{R}^d$

  d unknowns, d equations $\implies$ recover x_i with linear algebra

(1) Recovery of $B^\top B$ from a single real embedding

- Goal: recover $q \in \mathcal{O}_K$ from real embedding(s) $\sigma_i(q)$.
- Each embedding $\sigma_i : K \to \mathbb{R}$ is injective. (with infinite precision)
- $\mathbb{Z}$-basis $o_1, \ldots, o_d$ of $\mathcal{O}_K$, $q = \sum_{i=1}^{d} x_i o_i$
- Totally real: $\sigma(q) = \sum_{i=1}^{d} x_i \cdot \sigma(o_i) \in \mathbb{R}^d$

  d unknowns, d equations $\Longrightarrow$ recover x_i with linear algebra
- One real embedding: $\sigma_1(q) = \sum_{i=1}^{d} x_i \cdot \sigma_1(o_i) \in \mathbb{R}$

  d unknowns, **1** equation...

(1) Recovery of $B^\top B$ from a single real embedding

- Goal: recover $q \in \mathcal{O}_K$ from real embedding(s) $\sigma_i(q)$.
- Each embedding $\sigma_i : K \to \mathbb{R}$ is injective. (with infinite precision)
- $\mathbb{Z}$-basis $o_1, \ldots, o_d$ of $\mathcal{O}_K$, $q = \sum_{i=1}^d x_i o_i$
- Totally real: $\sigma(q) = \sum_{i=1}^d x_i \cdot \sigma(o_i) \in \mathbb{R}^d$

  d unknowns, d equations $\implies$ recover x_i with linear algebra
- One real embedding: $\sigma_1(q) = \sum_{i=1}^d x_i \cdot \sigma_1(o_i) \in \mathbb{R}$

  d unknowns, 1 equation...
- Assume: x_i are small

(1) Recovery of $B^\top B$ from a single real embedding

- Goal: recover $q \in \mathcal{O}_K$ from real embedding(s) $\sigma_i(q)$.
- Each embedding $\sigma_i : K \to \mathbb{R}$ is injective. (with infinite precision)
- $\mathbb{Z}$-basis $o_1, \ldots, o_d$ of $\mathcal{O}_K$, $q = \sum_{i=1}^{d} x_i o_i$
- Totally real: $\sigma(q) = \sum_{i=1}^{d} x_i \cdot \sigma(o_i) \in \mathbb{R}^d$

  d unknowns, d equations $\implies$ recover x_i with linear algebra
- One real embedding: $\sigma_1(q) = \sum_{i=1}^{d} x_i \cdot \sigma_1(o_i) \in \mathbb{R}$

  d unknowns, 1 equation...
- Assume: x_i are small
- Find small integer combination of x_i such that

$$\tilde{\sigma}_1(q) \underset{2^{-\lambda}}{\approx} \sum_{i=1}^{d} x_i \cdot \tilde{\sigma}_1(o_i)$$

(1) Recovery of $B^\top B$ from a single real embedding

- Goal: recover $q \in \mathcal{O}_K$ from real embedding(s) $\sigma_i(q)$.
- Each embedding $\sigma_i : K \to \mathbb{R}$ is injective. (with infinite precision)
- $\mathbb{Z}$-basis $o_1, \ldots, o_d$ of $\mathcal{O}_K$, $q = \sum_{i=1}^d x_i o_i$
- Totally real: $\sigma(q) = \sum_{i=1}^d x_i \cdot \sigma(o_i) \in \mathbb{R}^d$

  d unknowns, d equations $\implies$ recover x_i with linear algebra
- One real embedding: $\sigma_1(q) = \sum_{i=1}^d x_i \cdot \sigma_1(o_i) \in \mathbb{R}$

  d unknowns, 1 equation...
- Assume: x_i are small
- Find small integer combination of x_i such that

$$\tilde{\sigma}_1(q) \underset{2^{-\lambda}}{\approx} \sum_{i=1}^d x_i \cdot \tilde{\sigma}_1(o_i)$$

- This is a lattice problem!

$$A = \begin{pmatrix} 2^\lambda \cdot \tilde{\sigma}_1(q) & 2^\lambda \cdot \tilde{\sigma}_1(o_1) & \dots & 2^\lambda \cdot \tilde{\sigma}_1(o_d) \\ 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}.$$

Note that

$$\|A \cdot (-1, x_1, \dots, x_d)\|^2 = 2^{2\lambda} \cdot \underbrace{(\tilde{\sigma}_1(q) - \sum_j x_j \tilde{\sigma}_1(o_j))^2}_{< \mathrm{poly}(d, |x_i|) \cdot 2^{-\mathtt{precision}}} + \sum_j x_j^2 < 1 + \sum_j x_j^2$$

$$A = \begin{pmatrix} 2^\lambda \cdot \tilde{\sigma}_1(q) & 2^\lambda \cdot \tilde{\sigma}_1(o_1) & \dots & 2^\lambda \cdot \tilde{\sigma}_1(o_d) \\ 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}.$$

Note that

$$\|A \cdot (-1, x_1, \dots, x_d)\|^2 = 2^{2\lambda} \cdot \underbrace{(\tilde{\sigma}_1(q) - \sum_j x_j \tilde{\sigma}_1(o_j))^2}_{< \mathrm{poly}(d, |x_i|) \cdot 2^{-\texttt{precision}}} + \sum_j x_j^2 < 1 + \sum_j x_j^2$$

- Increasing λ makes the lattice $\mathcal{L}(A)$ sparser

(1) Recovery via lattice reduction

$$A = \begin{pmatrix} 2^\lambda \cdot \tilde{\sigma}_1(q) & 2^\lambda \cdot \tilde{\sigma}_1(o_1) & \dots & 2^\lambda \cdot \tilde{\sigma}_1(o_d) \\ 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}.$$

Note that

$$\|A \cdot (-1, x_1, \dots, x_d)\|^2 = 2^{2\lambda} \cdot \underbrace{(\tilde{\sigma}_1(q) - \sum_j x_j \tilde{\sigma}_1(o_j))^2}_{< \text{poly}(d, |x_i|) \cdot 2^{-\text{precision}}} + \sum_j x_j^2 < 1 + \sum_j x_j^2$$

- Increasing λ makes the lattice $\mathcal{L}(A)$ sparser
- $v := A \cdot (-1, x_1, \dots, x_d)$ is short

(1) Recovery via lattice reduction

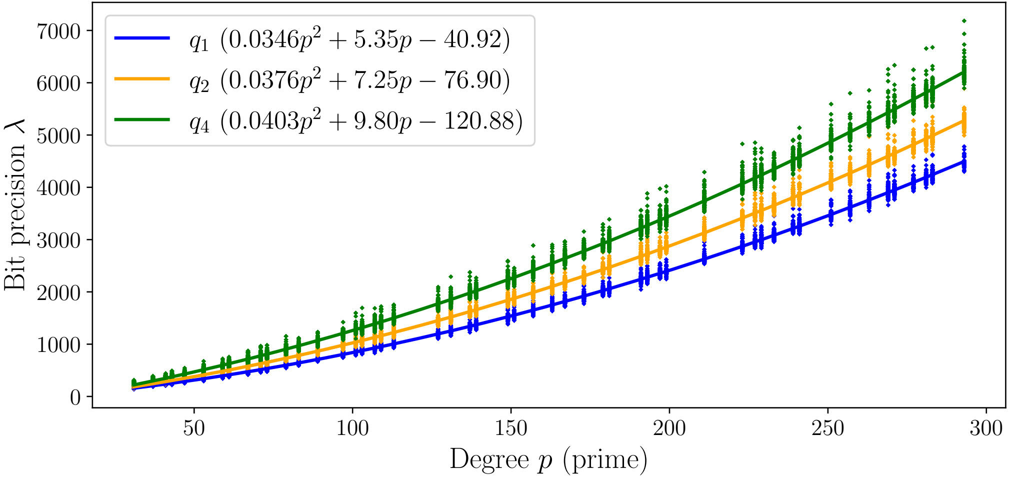
$$A = \begin{pmatrix} 2^\lambda \cdot \tilde{\sigma}_1(q) & 2^\lambda \cdot \tilde{\sigma}_1(o_1) & \dots & 2^\lambda \cdot \tilde{\sigma}_1(o_d) \\ 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}.$$

Note that

$$\|A \cdot (-1, x_1, \dots, x_d)\|^2 = 2^{2\lambda} \cdot \underbrace{(\tilde{\sigma}_1(q) - \sum_j x_j \tilde{\sigma}_1(o_j))^2}_{<\mathrm{poly}(d, |x_i|) \cdot 2^{-\mathrm{precision}}} + \sum_j x_j^2 < 1 + \sum_j x_j^2$$

- Increasing λ makes the lattice $\mathcal{L}(A)$ sparser
- $v := A \cdot (-1, x_1, \dots, x_d)$ is short
- For sufficiently large $\lambda = \mathrm{poly}(d, \log |x_i|)$, LLL will recover v

(1) Required precision for NTRUPrime field



(1) Reconstruction

Recover $B^\top B$ from $\sigma(B)^*\sigma(B)$.

(where $B = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathcal{O}_K^{2\times 2}$)

$B^\top B$

(2) Ideal recovery

$z_1 := a + bi$

recover $z_1\mathcal{O}_{L_1}$.

(where $L_1 = K(i)$)

$z_1\mathcal{O}_{L_1}$

$B^\top B$

(3) Absolute recovery

$\sigma_{k,\pm} : L_1 \to \mathbb{C}$

recover some $|\sigma_{k,\pm}(z_1)|$

$|\sigma_{k,\pm}(z_1)|$

(4) Ideal-LIP

Recover $z_1 = a + bi$.

(2) Ideal recovery

- Note that $\boldsymbol{i} \notin \boldsymbol{K}$ (as then $\sigma_1(\boldsymbol{i})^2 = -\mathbf{1}$ but $\sigma_1(\boldsymbol{i}) \in \mathbb{R}$)

(2) Ideal recovery

- Note that $i \notin K$ (as then $\sigma_1(i)^2 = -1$ but $\sigma_1(i) \in \mathbb{R}$)
- Let $L_1 := K(i)$

(2) Ideal recovery

- Note that $i \notin K$ (as then $\sigma_1(i)^2 = -1$ but $\sigma_1(i) \in \mathbb{R}$)
- Let $L_1 := K(i)$
- Note that $a^2 + b^2 = N_{L_1/K}(a + bi)$ (norm equation!)

(2) Ideal recovery

- Note that $i \notin K$ (as then $\sigma_1(i)^2 = -1$ but $\sigma_1(i) \in \mathbb{R}$)
- Let $L_1 := K(i)$
- Note that $a^2 + b^2 = N_{L_1/K}(a + bi)$ (norm equation!)

Objective: Given $Q := B^\top B$, recover $(a + bi)\mathcal{O}_{L_1}$ $\left(B = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathcal{O}_K^{2\times 2}\right)$

- Note that $i \notin K$ (as then $\sigma_1(i)^2 = -1$ but $\sigma_1(i) \in \mathbb{R}$)
- Let $L_1 := K(i)$
- Note that $a^2 + b^2 = N_{L_1/K}(a + bi)$ (norm equation!)

Objective: Given $Q := B^\top B$, recover $(a + bi)\mathcal{O}_{L_1}$ $\left(B = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathcal{O}_K^{2\times 2}\right)$

Notation: $Q = \begin{pmatrix} q_1 & q_2 \\ q_2 & q_4 \end{pmatrix}$, $z_1 = a + bi$, $z_2 = c + di$

Lemma: Ideal recovery [CMEPMPW25, Lemma 3.5]

Let $I_{\mathcal{M}} := z_1\mathcal{O}_{L_1} + z_2\mathcal{O}_{L_1}$, then

$$z_1(\det(B)i + q_2) = q_1 z_2,$$

and $z_1\mathcal{O}_{L_1} = I_{\mathcal{M}} \cap z_1 z_2^{-1} I_{\mathcal{M}} = I_{\mathcal{M}} \cap q_1(\det(B)i + q_2)^{-1} I_{\mathcal{M}}$.

Notation: $K = \mathbb{Q}(\alpha_{r_1+1}), \sigma_1, \ldots, \sigma_d, L_1 = K(i)$

- L_1 has embeddings $\sigma_{k,\pm}$ given by

$$\sigma_{k,\pm}(a + bi) = \sigma_k(a) \pm i\sigma_k(b) \quad \text{for } k = 1, \ldots, d, \pm \in \{+, -\}.$$

(3) Absolute embeddings

Notation: $K = \mathbb{Q}(\alpha_{r_1+1}), \sigma_1, \ldots, \sigma_d, L_1 = K(i)$

- L_1 has embeddings $\sigma_{k,\pm}$ given by

$$\sigma_{k,\pm}(a + bi) = \sigma_k(a) \pm i\sigma_k(b) \quad \text{for } k = 1, \ldots, d, \pm \in \{+, -\}.$$

- Goal: recover (some) $|\sigma_{k,\pm}(z_1)|$ (where $z_1 = a + bi$)

(3) Absolute embeddings

Notation: $K = \mathbb{Q}(\alpha_{r_1+1}), \sigma_1, \ldots, \sigma_d, L_1 = K(i)$

- L_1 has embeddings $\sigma_{k,\pm}$ given by

$$\sigma_{k,\pm}(a + bi) = \sigma_k(a) \pm i\sigma_k(b) \quad \text{for } k = 1, \ldots, d, \pm \in \{+, -\}.$$

- Goal: recover (some) $|\sigma_{k,\pm}(z_1)|$ (where $z_1 = a + bi$)
- We know $\delta_k := \sigma_k(a)^2 + \sigma_k(b)^2$ and $\gamma_k := |\sigma_k(a)|^2 + |\sigma_k(b)|^2$

Notation: $K = \mathbb{Q}(\alpha_{r_1+1}), \sigma_1, \ldots, \sigma_d, L_1 = K(i)$

- L_1 has embeddings $\sigma_{k,\pm}$ given by

$$\sigma_{k,\pm}(a + bi) = \sigma_k(a) \pm i\sigma_k(b) \quad \text{for } k = 1, \ldots, d, \pm \in \{+, -\}.$$

- Goal: recover (some) $|\sigma_{k,\pm}(z_1)|$ (where $z_1 = a + bi$)
- We know $\delta_k := \sigma_k(a)^2 + \sigma_k(b)^2$ and $\gamma_k := |\sigma_k(a)|^2 + |\sigma_k(b)|^2$
- For real embedding $\sigma_k(K) \subset \mathbb{R}$, we have $|\sigma_{k,\pm}(z_1)|^2 = |\sigma_k(a) \pm i\sigma_k(b)|^2 = \sigma_k(a^2 + b^2)$

(3) Absolute embeddings

Notation: $K = \mathbb{Q}(\alpha_{r_1+1}), \sigma_1, \ldots, \sigma_d, L_1 = K(i)$

- L_1 has embeddings $\sigma_{k,\pm}$ given by

$$\sigma_{k,\pm}(a + bi) = \sigma_k(a) \pm i\sigma_k(b) \quad \text{for } k = 1, \ldots, d, \pm \in \{+, -\}.$$

- Goal: recover (some) $|\sigma_{k,\pm}(z_1)|$ (where $z_1 = a + bi$)
- We know $\delta_k := \sigma_k(a)^2 + \sigma_k(b)^2$ and $\gamma_k := |\sigma_k(a)|^2 + |\sigma_k(b)|^2$
- For real embedding $\sigma_k(K) \subset \mathbb{R}$, we have
  $|\sigma_{k,\pm}(z_1)|^2 = |\sigma_k(a) \pm i\sigma_k(b)|^2 = \sigma_k(a^2 + b^2)$

Lemma: Absolute recovery (up to pairwise swaps)

The polynomial $f(t) = t^2 - 2\gamma_k t + |\delta_k|^2$,
has real roots $\{|\sigma_{k,+}(z_1)|^2, |\sigma_{k,-}(z_1)|^2\}$.

(3) Absolute embeddings

$$f_k(t) = t^2 - 2(|\sigma_k(a)|^2 + |\sigma_k(b)|^2) + |\sigma_k(a^2+b^2)|^2$$

$f_1(t_1) = 0$ $\quad$ $f_k(t_{k,\pm}) = 0$ $\quad$ $f_d(t_{d,\pm}) = 0$

$|\sigma_{1,+}(z_1)|^2 = |\sigma_{1,-}(z_1)|^2 = t_1$

real embeddings ✓

$|\sigma_{k,+}(z_1)|^2 \overset{?}{\longleftrightarrow} |\sigma_{k,-}(z_1)|^2$ $\quad$ $|\sigma_{d,+}(z_1)|^2 \overset{?}{\longleftrightarrow} |\sigma_{d,-}(z_1)|^2$

complex embeddings (up to pairwise swaps) ✗

(3) Absolute embeddings (if 2-transitive)

Notation: $K = \mathbb{Q}(\alpha_{r_1+1})$, roots $\alpha_1, \ldots, \alpha_d$, embeddings $\sigma_k : \alpha_{r_1+1} \mapsto \alpha_k$

- Assume $\mathrm{Gal}(P)$ is 2-transitive (any pair of roots maps to any pair)

(3) Absolute embeddings (if 2-transitive)

Notation: $K = \mathbb{Q}(\alpha_{r_1+1})$, roots $\alpha_1, \ldots, \alpha_d$, embeddings $\sigma_k : \alpha_{r_1+1} \mapsto \alpha_k$

- Assume $\mathbf{Gal}(P)$ is 2-transitive (any pair of roots maps to any pair)
- True for NTRU Prime and most number fields

(3) Absolute embeddings (if 2-transitive)

Notation: $K = \mathbb{Q}(\alpha_{r_1+1})$, roots $\alpha_1, \ldots, \alpha_d$, embeddings $\sigma_k : \alpha_{r_1+1} \mapsto \alpha_k$

- Assume $\mathrm{Gal}(P)$ is 2-transitive (any pair of roots maps to any pair)
- True for NTRU Prime and most number fields
- $K_2 := \mathbb{Q}(\alpha_{r_1+1}, \overline{\alpha_{r_1+1}})$ is a degree $d-1$ extension of K.

(3) Absolute embeddings (if 2-transitive)

Notation: $K = \mathbb{Q}(\alpha_{r_1+1})$, roots $\alpha_1, \ldots, \alpha_d$, embeddings $\sigma_k : \alpha_{r_1+1} \mapsto \alpha_k$

- Assume $\mathbf{Gal}(P)$ is 2-transitive (any pair of roots maps to any pair)
- True for NTRU Prime and most number fields
- $K_2 := \mathbb{Q}(\alpha_{r_1+1}, \overline{\alpha_{r_1+1}})$ is a degree $d-1$ extension of K.
- $a^2 + b^2, \overline{a}a + \overline{b}b \in K_2$

(3) Absolute embeddings (if 2-transitive)

Notation: $K = \mathbb{Q}(\alpha_{r_1+1})$, roots $\alpha_1, \ldots, \alpha_d$, embeddings $\sigma_k : \alpha_{r_1+1} \mapsto \alpha_k$

- Assume $\mathbf{Gal}(P)$ is 2-transitive (any pair of roots maps to any pair)
- True for NTRU Prime and most number fields
- $K_2 := \mathbb{Q}(\alpha_{r_1+1}, \overline{\alpha_{r_1+1}})$ is a degree $d-1$ extension of K.
- $a^2 + b^2, \bar{a}a + \bar{b}b \in K_2$
- K_2 has $d(d-1)$ complex embeddings

$$\sigma_{k,l} : \alpha_{r_1+1} \mapsto \alpha_k, \overline{\alpha_{r_1+1}} \mapsto \alpha_l$$

(3) Absolute embeddings (if 2-transitive)

Notation: $K = \mathbb{Q}(\alpha_{r_1+1})$, roots $\alpha_1, \ldots, \alpha_d$, embeddings $\sigma_k : \alpha_{r_1+1} \mapsto \alpha_k$

- Assume $\mathrm{Gal}(P)$ is 2-transitive (any pair of roots maps to any pair)
- True for NTRU Prime and most number fields
- $K_2 := \mathbb{Q}(\alpha_{r_1+1}, \overline{\alpha_{r_1+1}})$ is a degree $d-1$ extension of K.
- $a^2 + b^2, \overline{a}a + \overline{b}b \in K_2$
- K_2 has $d(d-1)$ complex embeddings

$$\sigma_{k,l} : \alpha_{r_1+1} \mapsto \alpha_k, \overline{\alpha_{r_1+1}} \mapsto \alpha_l$$

- $L_2 = K_2(i)$, $\sigma_{k,l,\pm} : i \mapsto \pm i$ (if $i \notin K_2$)

(3) Absolute embeddings (if 2-transitive)

Notation: $K = \mathbb{Q}(\alpha_{r_1+1})$, roots $\alpha_1, \ldots, \alpha_d$, embeddings $\sigma_k : \alpha_{r_1+1} \mapsto \alpha_k$

- Assume $\mathrm{Gal}(P)$ is 2-transitive (any pair of roots maps to any pair)
- True for NTRU Prime and most number fields
- $K_2 := \mathbb{Q}(\alpha_{r_1+1}, \overline{\alpha_{r_1+1}})$ is a degree $d-1$ extension of K.
- $a^2 + b^2, \bar{a}a + \bar{b}b \in K_2$
- K_2 has $d(d-1)$ complex embeddings

$$\sigma_{k,l} : \alpha_{r_1+1} \mapsto \alpha_k, \overline{\alpha_{r_1+1}} \mapsto \alpha_l$$

- $L_2 = K_2(i)$, $\sigma_{k,l,\pm} : i \mapsto \pm i$ (if $i \notin K_2$)

Idea: find root $\overline{z_1} z_1 \in L_2$ of $f(t) = t^2 - 2(\bar{a}a + \bar{b}b) + (a^2 + b^2)$

(3) Absolute embeddings (if 2-transitive)

Notation: $K = \mathbb{Q}(\alpha_{r_1+1})$, roots $\alpha_1, \ldots, \alpha_d$, embeddings $\sigma_k : \alpha_{r_1+1} \mapsto \alpha_k$

- Assume $\mathrm{Gal}(P)$ is 2-transitive (any pair of roots maps to any pair)
- True for NTRU Prime and most number fields
- $K_2 := \mathbb{Q}(\alpha_{r_1+1}, \overline{\alpha_{r_1+1}})$ is a degree $d-1$ extension of K.
- $a^2 + b^2, \bar{a}a + \bar{b}b \in K_2$
- K_2 has $d(d-1)$ complex embeddings

$$\sigma_{k,l} : \alpha_{r_1+1} \mapsto \alpha_k, \overline{\alpha_{r_1+1}} \mapsto \alpha_l$$

- $L_2 = K_2(i)$, $\sigma_{k,l,\pm} : i \mapsto \pm i$ (if $i \notin K_2$)

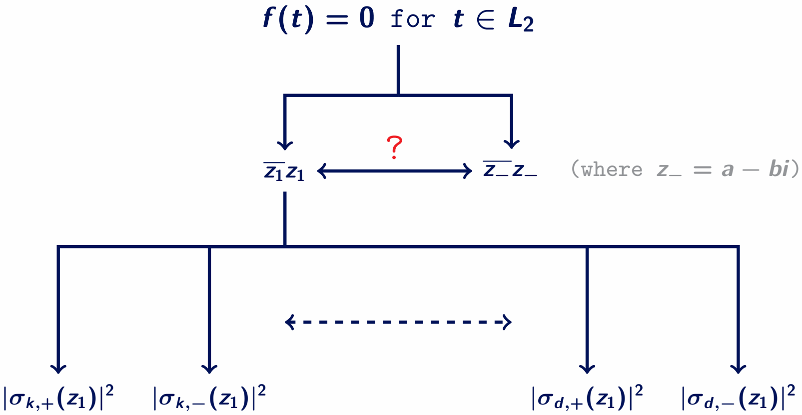
Idea: find root $\overline{z_1} z_1 \in L_2$ of $f(t) = t^2 - 2(\bar{a}a + \bar{b}b) + (a^2 + b^2)$

Then use embeddings to obtain $|\sigma_{k,\pm}(z_1)|$ for all k and $\pm \in \{+, 0\}$:

$$|\sigma_{k,\pm}(z_1)|^2 = \sigma_{k,\bar{k},\pm}(\overline{z_1} z_1)$$

(3) Absolute embeddings (if 2-transitive)

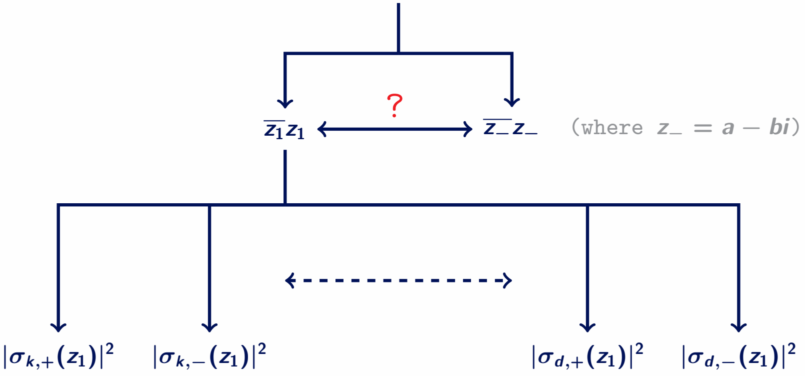
$$f(t) = t^2 - 2(\bar{a}a + \bar{b}b) + (a^2 + b^2)$$



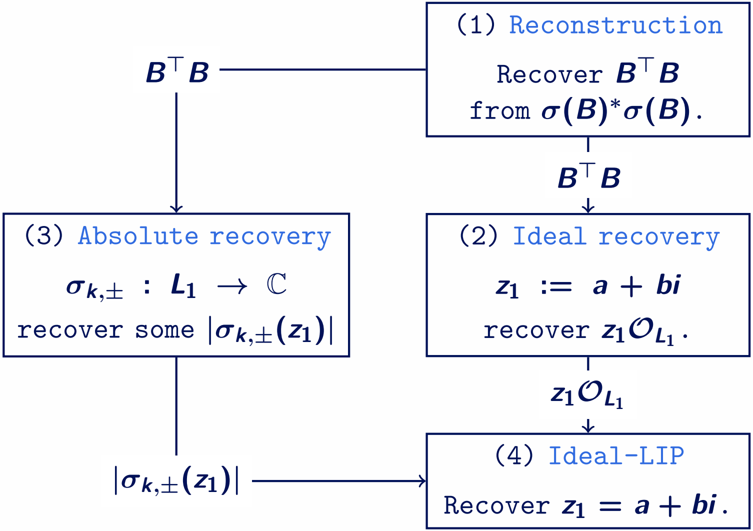
(3) Absolute embeddings (if 2-transitive)

$$f(t) = t^2 - 2(\bar{a}a + \bar{b}b) + (a^2 + b^2)$$

$f(t) = 0$ for $t \in L_2$

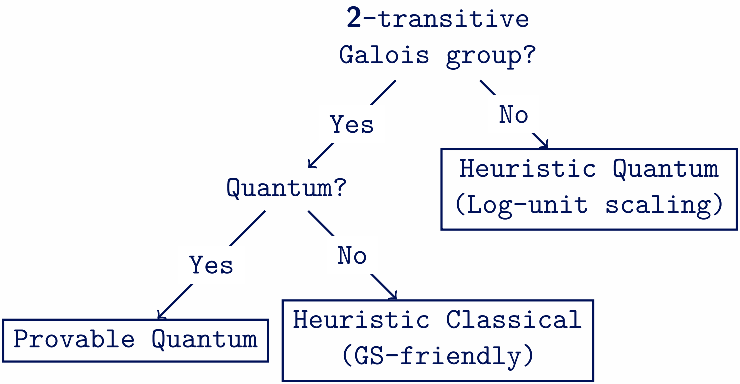


only one (optional) choice



(where $B = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathcal{O}_K^{2\times 2}$)

(where $L_1 = K(i)$)


2-transitive
Galois group?
Yes
No
Heuristic Quantum
(Log-unit scaling)
Quantum?
Yes
No
Provable Quantum
Heuristic Classical
(GS-friendly)

(4) Ideal-LIP (if 2-transitive)

From (2): (generators of) $z_1 \mathcal{O}_{L_1}$

From (3): all absolute embeddings $|\sigma_{k,\pm}(z_1)|$

(4) Ideal-LIP (if 2-transitive)

From (2): (generators of) $z_1\mathcal{O}_{L_1}$

From (3): all absolute embeddings $|\sigma_{k,\pm}(z_1)|$

rank-1 module-LIP!

(4) Ideal-LIP (if 2-transitive)

From (2): (generators of) $z_1 \mathcal{O}_{L_1}$

From (3): all absolute embeddings $|\sigma_{k,\pm}(z_1)|$

rank-1 module-LIP!

Final step: use generalized Gentry-Szydlo algorithm to recover z_1

(4) Ideal-LIP (if 2-transitive)

From (2): (generators of) $z_1\mathcal{O}_{L_1}$

From (3): all absolute embeddings $|\sigma_{k,\pm}(z_1)|$

rank-1 module-LIP!

Final step: use generalized Gentry-Szydlo algorithm to recover z_1

Heuristic assumption: all number fields are GS-friendly.

(4) Ideal-LIP (if 2-transitive)

From (2): (generators of) $z_1\mathcal{O}_{L_1}$

From (3): all absolute embeddings $|\sigma_{k,\pm}(z_1)|$

rank-1 module-LIP!

Final step: use generalized Gentry-Szydlo algorithm to recover z_1

Heuristic assumption: all number fields are GS-friendly.

Main result (1): heuristic classical if 2-transitive

Let $K = \mathbb{Q}[X]/P(X)$ be a number field with at least one real embedding and such that $\mathrm{Gal}(P)$ acts 2-transitively on the roots of P. Then there is a heuristic polynomial time classical algorithm that solves the rank-2 module-LIP problem on $\mathcal{O}_K$.

(4) Ideal-LIP (alternative)

From (2): (generators of) $z_1 \mathcal{O}_{L_1}$

From (3): all absolute embeddings $|\sigma_{k,\pm}(z_1)|$

1. Compute principal generator $g \in \mathcal{O}_{L_1}$ of $z_1 \mathcal{O}_{K_1}$ (quantum)

(4) Ideal-LIP (alternative)

From (2): (generators of) $z_1\mathcal{O}_{L_1}$

From (3): all absolute embeddings $|\sigma_{k,\pm}(z_1)|$

1. Compute principal generator $g \in \mathcal{O}_{L_1}$ of $z_1\mathcal{O}_{K_1}$ (quantum)
2. Compute generators of $\mathcal{O}_{L_1}^*$ and basis of $\mathrm{Log}(|\sigma_{L_1}(\mathcal{O}_{L_1}^*)|)$ (quantum)

(4) Ideal-LIP (alternative)

From (2): (generators of) $z_1 \mathcal{O}_{L_1}$

From (3): all absolute embeddings $|\sigma_{k,\pm}(z_1)|$

1. Compute principal generator $g \in \mathcal{O}_{L_1}$ of $z_1 \mathcal{O}_{K_1}$ (quantum)
2. Compute generators of $\mathcal{O}_{L_1}^*$ and basis of $\mathrm{Log}(|\sigma_{L_1}(\mathcal{O}_{L_1}^*)|)$ (quantum)
3. Then $g \cdot z_1^{-1} = u$ for a unit $u \in \mathcal{O}_{L_1}^*$

(4) Ideal-LIP (alternative)

From (2): (generators of) $z_1 \mathcal{O}_{L_1}$

From (3): all absolute embeddings $|\sigma_{k,\pm}(z_1)|$

1. Compute principal generator $g \in \mathcal{O}_{L_1}$ of $z_1 \mathcal{O}_{K_1}$ (quantum)
2. Compute generators of $\mathcal{O}_{L_1}^*$ and basis of $\mathrm{Log}(|\sigma_{L_1}(\mathcal{O}_{L_1}^*)|)$ (quantum)
3. Then $g \cdot z_1^{-1} = u$ for a unit $u \in \mathcal{O}_{L_1}^*$
4. Then $\mathrm{Log}(|\sigma_{L_1}(g)|) - \mathrm{Log}(|\sigma_{L_1}(z_1)|) = \mathrm{Log}(|\sigma_{L_1}(u)|)$

(4) Ideal-LIP (alternative)

From (2): (generators of) $z_1\mathcal{O}_{L_1}$

From (3): all absolute embeddings $|\sigma_{k,\pm}(z_1)|$

1. Compute principal generator $g \in \mathcal{O}_{L_1}$ of $z_1\mathcal{O}_{K_1}$ (quantum)
2. Compute generators of $\mathcal{O}_{L_1}^*$ and basis of $\mathrm{Log}(|\sigma_{L_1}(\mathcal{O}_{L_1}^*)|)$ (quantum)
3. Then $g \cdot z_1^{-1} = u$ for a unit $u \in \mathcal{O}_{L_1}^*$
4. Then $\mathrm{Log}(|\sigma_{L_1}(g)|) - \mathrm{Log}(|\sigma_{L_1}(z_1)|) = \mathrm{Log}(|\sigma_{L_1}(u)|)$
5. Recover u from $\mathrm{Log}(|\sigma(u)|)$ (up to a root of unity)

(4) Ideal-LIP (alternative)

From (2): (generators of) $z_1\mathcal{O}_{L_1}$

From (3): all absolute embeddings $|\sigma_{k,\pm}(z_1)|$

1. Compute principal generator $g \in \mathcal{O}_{L_1}$ of $z_1\mathcal{O}_{K_1}$ (quantum)
2. Compute generators of $\mathcal{O}_{L_1}^*$ and basis of $\mathrm{Log}(|\sigma_{L_1}(\mathcal{O}_{L_1}^*)|)$ (quantum)
3. Then $g \cdot z_1^{-1} = u$ for a unit $u \in \mathcal{O}_{L_1}^*$
4. Then $\mathrm{Log}(|\sigma_{L_1}(g)|) - \mathrm{Log}(|\sigma_{L_1}(z_1)|) = \mathrm{Log}(|\sigma_{L_1}(u)|)$
5. Recover u from $\mathrm{Log}(|\sigma(u)|)$ (up to a root of unity)

Main result (2): provable quantum if 2-transitive

Let $K = \mathbb{Q}[X]/P(X)$ be a number field with at least one real embedding and such that $\mathrm{Gal}(P)$ acts 2-transitively on the roots of P. Then there is a polynomial time quantum algorithm that solves the rank-2 module-LIP problem on $\mathcal{O}_K$.

(4) Ideal-LIP (alternative)

From (2): (generators of) $z_1\mathcal{O}_{L_1}$

From (3): one absolute embedding $|\sigma_{1,+}(z_1)|$ (actually two)

(4) Ideal-LIP (alternative)

From (2): (generators of) $z_1\mathcal{O}_{L_1}$

From (3): one absolute embedding $|\sigma_{1,+}(z_1)|$ (actually two)

1. Compute principal generator $g \in \mathcal{O}_{L_1}$ of $z_1\mathcal{O}_{K_1}$ (quantum)
2. Compute generators of $\mathcal{O}_{L_1}^*$ and basis of $\mathrm{Log}(|\sigma(\mathcal{O}_{L_1}^*)|)$ (quantum)
3. Then $g \cdot z_1^{-1} = u$ for a unit $u \in \mathcal{O}_{L_1}^*$

(4) Ideal-LIP (alternative)

From (2): (generators of) $z_1 \mathcal{O}_{L_1}$

From (3): one absolute embedding $|\sigma_{1,+}(z_1)|$ (actually two)

1. Compute principal generator $g \in \mathcal{O}_{L_1}$ of $z_1 \mathcal{O}_{K_1}$ (quantum)
2. Compute generators of $\mathcal{O}_{L_1}^*$ and basis of $\mathrm{Log}(|\sigma(\mathcal{O}_{L_1}^*)|)$ (quantum)
3. Then $g \cdot z_1^{-1} = u$ for a unit $u \in \mathcal{O}_{L_1}^*$
4. Then $\log(|\sigma_{1,+}(g)|) - \log(|\sigma_{1,+}(z_1)|) = \log(|\sigma_{1,+}(u)|)$

(4) Ideal-LIP (alternative)

From (2): (generators of) $z_1 \mathcal{O}_{L_1}$

From (3): one absolute embedding $|\sigma_{1,+}(z_1)|$ (actually two)

1. Compute principal generator $g \in \mathcal{O}_{L_1}$ of $z_1 \mathcal{O}_{K_1}$ (quantum)
2. Compute generators of $\mathcal{O}_{L_1}^*$ and basis of $\mathrm{Log}(|\sigma(\mathcal{O}_{L_1}^*)|)$ (quantum)
3. Then $g \cdot z_1^{-1} = u$ for a unit $u \in \mathcal{O}_{L_1}^*$
4. Then $\log(|\sigma_{1,+}(g)|) - \log(|\sigma_{1,+}(z_1)|) = \log(|\sigma_{1,+}(u)|)$
5. Recover u from $\log(|\sigma_{1,+}(u)|)$ (heuristic!)

(4) Ideal-LIP (alternative)

From (2): (generators of) $z_1 \mathcal{O}_{L_1}$

From (3): one absolute embedding $|\sigma_{1,+}(z_1)|$ (actually two)

1. Compute principal generator $g \in \mathcal{O}_{L_1}$ of $z_1 \mathcal{O}_{K_1}$ (quantum)
2. Compute generators of $\mathcal{O}_{L_1}^*$ and basis of $\mathrm{Log}(|\sigma(\mathcal{O}_{L_1}^*)|)$ (quantum)
3. Then $g \cdot z_1^{-1} = u$ for a unit $u \in \mathcal{O}_{L_1}^*$
4. Then $\log(|\sigma_{1,+}(g)|) - \log(|\sigma_{1,+}(z_1)|) = \log(|\sigma_{1,+}(u)|)$
5. Recover u from $\log(|\sigma_{1,+}(u)|)$ (heuristic!)

Main result (3): heuristic quantum

Let $K = \mathbb{Q}[X]/P(X)$ be a number field with at least one real embedding. Then there is a heuristic polynomial time quantum algorithm that solves the rank-2 module-LIP problem on $\mathcal{O}_K$.

Conclusion

- Security of rank-2 module-LIP depends on the number field
- Real embeddings can cause problems

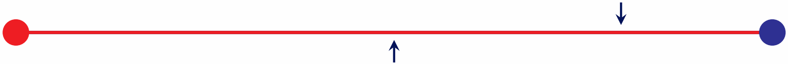
Conclusion

- Security of rank-**2** module-LIP depends on the number field
- Real embeddings can cause problems

New state of cryptanalysis:

NTRUPrime field

$(r_1, 2r_2) = (1, d-1)$



Totally real

$(r_1, 2r_2) = (d, 0)$

Broken!

At least one real embedding

also broken!

Totally imaginary

$(r_1, 2r_2) = (0, d)$

HAWK (CM field)

Conclusion

- Security of rank-2 module-LIP depends on the number field
- Real embeddings can cause problems

New state of cryptanalysis:

NTRUPrime field

$(r_1, 2r_2) = (1, d-1)$

Totally real

$(r_1, 2r_2) = (d, 0)$

Broken!

At least one real embedding

also broken!

Totally imaginary

$(r_1, 2r_2) = (0, d)$

HAWK (CM field)

Thank you!