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) .

Context

We continue on from the previous talk.

Context

We continue on from the previous talk.

Eurocrypt 2024: solve rank-$\mathbf{2}$ module-LIP over totally real fields

(Mureau, Pellet-Mary, Pliatsok, Wallet)

Context

We continue on from the previous talk.

Eurocrypt 2024: solve rank-2 module-LIP over totally real fields

(Mureau, Pellet-Mary, Pliatsok, Wallet)

Previous talk: reduces rank-2 module-LIP for CM fields to nrdPIP over a quaternion algebra.

Context

We continue on from the previous talk.

Eurocrypt 2024: solve rank-2 module-LIP over totally real fields

(Mureau, Pellet-Mary, Pliatsok, Wallet)

Previous talk: reduces rank-2 module-LIP for CM fields to nrdPIP over a quaternion algebra.

This talk: What about other number fields?

Number fields and module-LIP

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

- $K = \mathbb{Q}[X]/(X^d - X - 1)$ with d prime $\rightsquigarrow$ NTRU Prime field

Number fields and module-LIP

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

- $K = \mathbb{Q}[X]/(X^d - X - 1)$ with d prime $\rightsquigarrow$ NTRU Prime field

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

- $\mathcal{O}_K = \mathbb{Z}[X]/(X^d - X - 1)$ with d prime $\rightsquigarrow$ NTRU Prime ring of integers

Number fields and module-LIP

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

- $K = \mathbb{Q}[X]/(X^d - X - 1)$ with d prime $\rightsquigarrow$ NTRU Prime field

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

- $\mathcal{O}_K = \mathbb{Z}[X]/(X^d - X - 1)$ with d prime $\rightsquigarrow$ NTRU Prime ring of integers

Problem: Rank-2 module-LIP for $\mathcal{O}_K^2$

Given $G = B^* B$ with B a basis of $\mathcal{O}_K^2$, find B

Number fields and module-LIP

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

- $K = \mathbb{Q}[X]/(X^d - X - 1)$ with d prime $\rightsquigarrow$ NTRU Prime field

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

- $\mathcal{O}_K = \mathbb{Z}[X]/(X^d - X - 1)$ with d prime $\rightsquigarrow$ NTRU Prime ring of integers

Problem: Rank-2 module-LIP for $\mathcal{O}_K^2$

Given $G = B^* B$ with B a basis of $\mathcal{O}_K^2$, find B

Difficulty: Conjugation $B^* := \overline{B}^\top$ isn't always properly defined in K!

(if not totally real or CM field)

Number fields and module-LIP

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

- $K = \mathbb{Q}[X]/(X^d - X - 1)$ with d prime $\rightsquigarrow$ NTRU Prime field

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

- $\mathcal{O}_K = \mathbb{Z}[X]/(X^d - X - 1)$ with d prime $\rightsquigarrow$ NTRU Prime ring of integers

Problem: Rank-2 module-LIP for $\mathcal{O}_K^2$

Given $G = B^* B$ with B a basis of $\mathcal{O}_K^2$, find B

Difficulty: Conjugation $B^* := \overline{B}^\top$ isn't always properly defined in K!

(if not totally real or CM field)

- Cause of most technical problems in this work

Embeddings

Complex roots of $\boldsymbol{P(X)}$: $\boldsymbol{\alpha_1, \cdots, \alpha_d} \in \mathbb{C}$

Embeddings

Complex roots of $P(X)$: $\alpha_1, \cdots, \alpha_d \in \mathbb{C}$

Field embeddings: $\sigma_k : \quad K = \mathbb{Q}[X]/P(X) \quad \to \quad \mathbb{C}, \quad X \mapsto \alpha_k$

Embeddings

Complex roots of $P(X)$: $\alpha_1, \cdots, \alpha_d \in \mathbb{C}$

Field embeddings: $\sigma_k : K = \mathbb{Q}[X]/P(X) \to \mathbb{C}, \quad X \mapsto \alpha_k$

Canonical embedding:
$$\begin{aligned} \sigma : K = \mathbb{Q}[X]/P(X) &\to \mathbb{C}^d \\ y &\mapsto (\sigma_1(y), \cdots, \sigma_d(y)) \end{aligned}$$

Complex roots of $P(X)$: $\alpha_1, \cdots, \alpha_d \in \mathbb{C}$

Field embeddings: $\sigma_k : K = \mathbb{Q}[X]/P(X) \to \mathbb{C},\ X \mapsto \alpha_k$

Canonical embedding:
$$\begin{aligned} \sigma : K = \mathbb{Q}[X]/P(X) &\to \mathbb{C}^d \\ y &\mapsto (\sigma_1(y), \cdots, \sigma_d(y)) \end{aligned}$$

- real embedding: $\sigma_k(X) = \alpha_k \in \mathbb{R}$.

Embeddings

Complex roots of $P(X)$: $\alpha_1, \cdots, \alpha_d \in \mathbb{C}$

Field embeddings: $\sigma_k : K = \mathbb{Q}[X]/P(X) \to \mathbb{C}, \; X \mapsto \alpha_k$

Canonical embedding:
$$\begin{aligned} \sigma : K = \mathbb{Q}[X]/P(X) &\to \mathbb{C}^d \\ y &\mapsto (\sigma_1(y), \cdots, \sigma_d(y)) \end{aligned}$$

- real embedding: $\sigma_k(X) = \alpha_k \in \mathbb{R}$.
- complex embedding: $\sigma_k(X) = \alpha_k \in \mathbb{C} \setminus \mathbb{R}$ (occur in conjugate pairs)

Complex roots of $P(X)$: $\alpha_1, \cdots, \alpha_d \in \mathbb{C}$

Field embeddings: $\sigma_k : K = \mathbb{Q}[X]/P(X) \to \mathbb{C}, \quad X \mapsto \alpha_k$

Canonical embedding:
$$\begin{aligned} \sigma : K = \mathbb{Q}[X]/P(X) &\to \mathbb{C}^d \\ y &\mapsto (\sigma_1(y), \cdots, \sigma_d(y)) \end{aligned}$$

- real embedding: $\sigma_k(X) = \alpha_k \in \mathbb{R}$.
- complex embedding: $\sigma_k(X) = \alpha_k \in \mathbb{C} \setminus \mathbb{R}$ (occur in conjugate pairs)

Conjugation: we have conjugation in $\mathbb{C}^d$!

Lift to K: $\overline{y} := \sigma^{-1}(\overline{\sigma(y)})$

Embeddings

Complex roots of $P(X)$: $\alpha_1, \cdots, \alpha_d \in \mathbb{C}$

Field embeddings: $\sigma_k : K = \mathbb{Q}[X]/P(X) \to \mathbb{C},\ X \mapsto \alpha_k$

Canonical embedding:
$$\begin{aligned} \sigma : K = \mathbb{Q}[X]/P(X) &\to \mathbb{C}^d \\ y &\mapsto (\sigma_1(y), \cdots, \sigma_d(y)) \end{aligned}$$

- real embedding: $\sigma_k(X) = \alpha_k \in \mathbb{R}$.
- complex embedding: $\sigma_k(X) = \alpha_k \in \mathbb{C} \setminus \mathbb{R}$ (occur in conjugate pairs)

Conjugation: we have conjugation in $\mathbb{C}^d$!

Lift to K: $\bar{y} := \sigma^{-1}(\overline{\sigma(y)}) \in K_{\mathbb{R}} := K \otimes \mathbb{R}$.

Embeddings

Complex roots of $P(X)$: $\alpha_1, \cdots, \alpha_d \in \mathbb{C}$

Field embeddings: $\sigma_k : K = \mathbb{Q}[X]/P(X) \to \mathbb{C},\ X \mapsto \alpha_k$

Canonical embedding:
$$\begin{aligned}\sigma : K = \mathbb{Q}[X]/P(X) &\to \mathbb{C}^d \\ y &\mapsto (\sigma_1(y), \cdots, \sigma_d(y))\end{aligned}$$

- real embedding: $\sigma_k(X) = \alpha_k \in \mathbb{R}$.
- complex embedding: $\sigma_k(X) = \alpha_k \in \mathbb{C} \setminus \mathbb{R}$ (occur in conjugate pairs)

Conjugation: we have conjugation in $\mathbb{C}^d$!

Lift to K: $\bar{y} := \sigma^{-1}(\overline{\sigma(y)}) \in K_{\mathbb{R}} := K \otimes \mathbb{R}$.

Problem: Rank-2 module-LIP for $\mathcal{O}_K^2$

Given $G = \sigma(B)^*\sigma(B)$ with B a basis of $\mathcal{O}_K^2$, find B

Cryptanalysis of rank-2 module-LIP

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

Cryptanalysis of rank-2 module-LIP

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

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

Current state of cryptanalysis:

Totally real

Broken!

[MPMPW24]

Totally imaginary

HAWK (CM field)

Previous talk!

Cryptanalysis of rank-2 module-LIP

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

Current state of cryptanalysis:

Totally real

Broken!

[MPMPW24]

Totally imaginary

HAWK (CM field)

Previous talk!

So4S: $a_1^2 + a_2^2 + b_1^2 + b_2^2$

Cryptanalysis of rank-2 module-LIP

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

Current state of cryptanalysis:

Totally real	Totally imaginary
Broken!	HAWK (CM field)
[MPMPW24]	Previous talk!
So2S: $a^2 + b^2$	So4S: $a_1^2 + a_2^2 + b_1^2 + b_2^2$

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

Current state of cryptanalysis:

What about here?

Totally real	Totally imaginary
Broken!	HAWK (CM field)
[MPMPW24]	Previous talk!
So2S: $a^2 + b^2$	So4S: $a_1^2 + a_2^2 + b_1^2 + b_2^2$

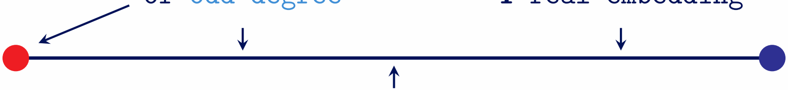
Notations: $K = \mathbb{Q}[X]/P(X)$, $\mathcal{O}_K = \mathbb{Z}[X]/P(X)$

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

Current state of cryptanalysis:

Number field of odd degree

NTRU Prime field 1 real embedding



What about here?

Totally real	Totally imaginary
Broken!	HAWK (CM field)
[MPMPW24]	Previous talk!
So2S: $a^2 + b^2$	So4S: $a_1^2 + a_2^2 + b_1^2 + b_2^2$

Cryptanalysis of rank-2 module-LIP

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

Current state of cryptanalysis:

Number field of odd degree

NTRU Prime field 1 real embedding

Totally real

Broken!

[MPMPW24]

So2S: $a^2 + b^2$

What about here?

also broken!

(this work)

Totally imaginary

HAWK (CM field)

Previous talk!

So4S: $a_1^2 + a_2^2 + b_1^2 + b_2^2$

Totally real:

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

When P has a real root

Totally real:

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

- Recovers $a^2 + b^2 = q_1$! But...above is not the case in general

When P has a real root

Totally real:

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

- Recovers $a^2 + b^2 = q_1$! But...above is not the case in general

Main idea: For a real embedding $\sigma_{\mathbb{R}} : K \to \mathbb{R} \subset \mathbb{C}$ we do have

$$\boxed{\sigma_{\mathbb{R}}(a^2 + b^2) = \sigma_{\mathbb{R}}(\overline{a}a + \overline{b}b) = \sigma_{\mathbb{R}}(q_1)}$$

When P has a real root

Totally real:

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

- Recovers $a^2 + b^2 = q_1$! But...above is not the case in general

Main idea: For a real embedding $\sigma_{\mathbb{R}} : K \to \mathbb{R} \subset \mathbb{C}$ we do have

$$\boxed{\sigma_{\mathbb{R}}(a^2 + b^2) = \sigma_{\mathbb{R}}(\bar{a}a + \bar{b}b) = \sigma_{\mathbb{R}}(q_1)}$$

Question: can we recover $a^2 + b^2 \in \mathcal{O}_K$ from $\sigma_{\mathbb{R}}(a^2 + b^2)$?

When P has a real root

Totally real:

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

- Recovers $a^2 + b^2 = q_1$! But...above is not the case in general

Main idea: For a real embedding $\sigma_{\mathbb{R}} : K \to \mathbb{R} \subset \mathbb{C}$ we do have

$$\boxed{\sigma_{\mathbb{R}}(a^2 + b^2) = \sigma_{\mathbb{R}}(\overline{a}a + \overline{b}b) = \sigma_{\mathbb{R}}(q_1)}$$

Question: can we recover $a^2 + b^2 \in \mathcal{O}_K$ from $\sigma_{\mathbb{R}}(a^2 + b^2)$? Yes!

Recovery from a single real embedding

- Goal: recover $a^2 + b^2 \in \mathcal{O}_K$ from $\sigma_{\mathbb{R}}(a^2 + b^2)$.

Recovery from a single real embedding

- Goal: recover $a^2 + b^2 \in \mathcal{O}_K$ from $\sigma_{\mathbb{R}}(a^2 + b^2)$.
- In theory: ✓ each embedding is injective (with infinite precision)

Recovery from a single real embedding

- Goal: recover $a^2 + b^2 \in \mathcal{O}_K$ from $\sigma_{\mathbb{R}}(a^2 + b^2)$.
- In theory: ✓ each embedding is injective (with infinite precision)
- $\mathbb{Z}$-basis $o_1, \ldots, o_d$ of $\mathcal{O}_K$, $a^2 + b^2 = \sum_{i=1}^{d} x_i o_i$

Recovery from a single real embedding

- Goal: recover $a^2 + b^2 \in \mathcal{O}_K$ from $\sigma_{\mathbb{R}}(a^2 + b^2)$.
- In theory: ✓ each embedding is injective (with infinite precision)
- $\mathbb{Z}$-basis $o_1, \ldots, o_d$ of $\mathcal{O}_K$, $a^2 + b^2 = \sum_{i=1}^{d} x_i o_i$
- d unknowns...1 equation: $\sigma_{\mathbb{R}}(a^2 + b^2) = \sum_{i=1}^{d} x_i \cdot \sigma_{\mathbb{R}}(o_i) \in \mathbb{R}$

Recovery from a single real embedding

- Goal: recover $a^2 + b^2 \in \mathcal{O}_K$ from $\sigma_{\mathbb{R}}(a^2 + b^2)$.
- In theory: ✓ each embedding is injective (with infinite precision)
- $\mathbb{Z}$-basis $o_1, \ldots, o_d$ of $\mathcal{O}_K$, $a^2 + b^2 = \sum_{i=1}^{d} x_i o_i$
- d unknowns... 1 equation: $\sigma_{\mathbb{R}}(a^2 + b^2) = \sum_{i=1}^{d} x_i \cdot \sigma_{\mathbb{R}}(o_i) \in \mathbb{R}$
- Assume: x_i are small (follows when $o_1, \ldots, o_d$ is LLL reduced)

Recovery from a single real embedding

- Goal: recover $a^2 + b^2 \in \mathcal{O}_K$ from $\sigma_{\mathbb{R}}(a^2 + b^2)$.
- In theory: ✓ each embedding is injective (with infinite precision)
- $\mathbb{Z}$-basis $o_1, \ldots, o_d$ of $\mathcal{O}_K$, $a^2 + b^2 = \sum_{i=1}^{d} x_i o_i$
- d unknowns... 1 equation: $\sigma_{\mathbb{R}}(a^2 + b^2) = \sum_{i=1}^{d} x_i \cdot \sigma_{\mathbb{R}}(o_i) \in \mathbb{R}$
- Assume: x_i are small (follows when $o_1, \ldots, o_d$ is LLL reduced)
- Find small integer combination of x_i such that:

$$\boxed{\tilde{\sigma}_{\mathbb{R}}(a^2 + b^2) \approx \sum_{i=1}^{d} x_i \cdot \tilde{\sigma}_{\mathbb{R}}(o_i)}$$

Recovery from a single real embedding

- Goal: recover $a^2 + b^2 \in \mathcal{O}_K$ from $\sigma_{\mathbb{R}}(a^2 + b^2)$.
- In theory: ✓ each embedding is injective (with infinite precision)
- $\mathbb{Z}$-basis $o_1, \ldots, o_d$ of $\mathcal{O}_K$, $a^2 + b^2 = \sum_{i=1}^{d} x_i o_i$
- d unknowns. . . 1 equation: $\sigma_{\mathbb{R}}(a^2 + b^2) = \sum_{i=1}^{d} x_i \cdot \sigma_{\mathbb{R}}(o_i) \in \mathbb{R}$
- Assume: x_i are small (follows when $o_1, \ldots, o_d$ is LLL reduced)
- Find small integer combination of x_i such that:

$$\boxed{\tilde{\sigma}_{\mathbb{R}}(a^2 + b^2) \approx \sum_{i=1}^{d} x_i \cdot \tilde{\sigma}_{\mathbb{R}}(o_i)}$$

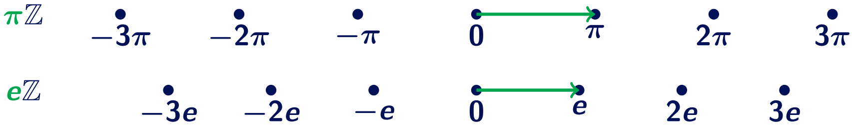
- This is a lattice problem!

Recovery from a single real embedding

Suppose we know (an approximation of) $\boldsymbol{v} = \boldsymbol{x}_1 \cdot \pi + \boldsymbol{x}_2 \cdot \boldsymbol{e} \in \mathbb{R}$ with $\boldsymbol{x}_i \in \mathbb{Z}$.

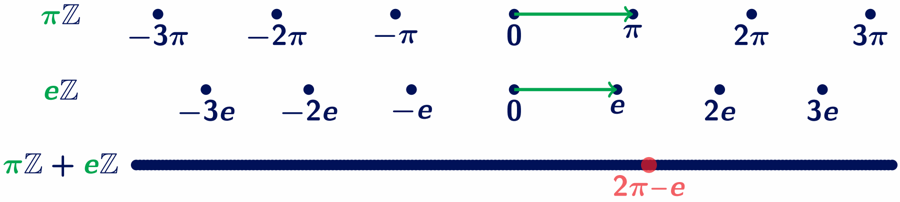
Recovery from a single real embedding

Suppose we know (an approximation of) $v = x_1 \cdot \pi + x_2 \cdot e \in \mathbb{R}$ with $x_i \in \mathbb{Z}$.

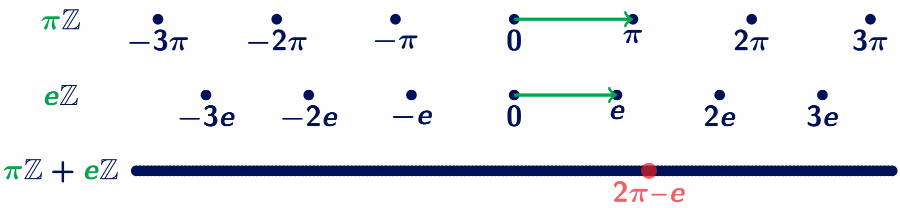


Recovery from a single real embedding

Suppose we know (an approximation of) $v = x_1 \cdot \pi + x_2 \cdot e \in \mathbb{R}$ with $x_i \in \mathbb{Z}$.

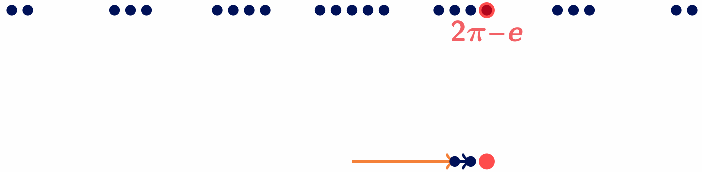


Suppose we know (an approximation of) $v = x_1 \cdot \pi + x_2 \cdot e \in \mathbb{R}$ with $x_i \in \mathbb{Z}$.



Small combinations only ($S = \{-2, -1, 0, 1, 2\}$)

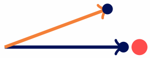
$eS + \pi S$



integer combination π and e close to v

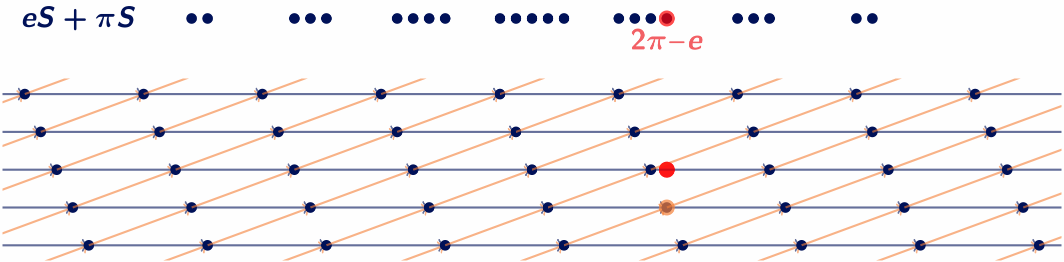
Recovery from a single real embedding

$eS + \pi S$ 



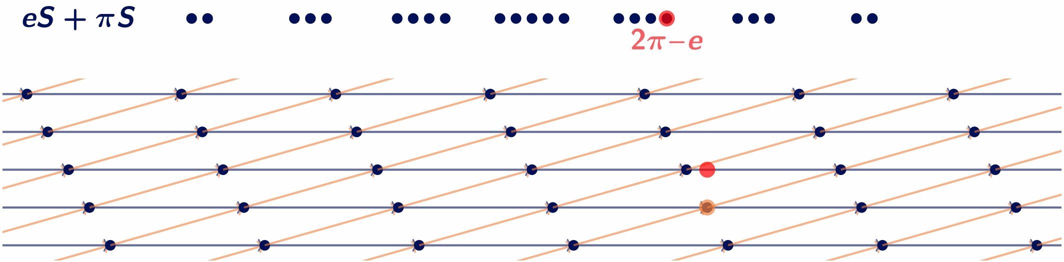
integer combination $\begin{pmatrix}\pi\\0\end{pmatrix}$ and $\begin{pmatrix}e\\1\end{pmatrix}$ close to $\begin{pmatrix}v\\0\end{pmatrix}$

Recovery from a single real embedding



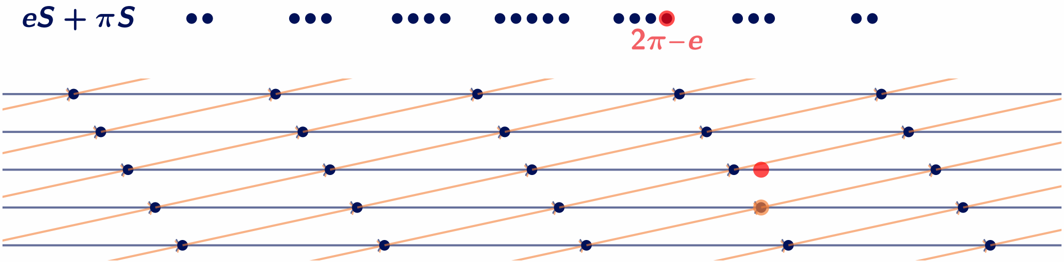
integer combination $\begin{pmatrix} \pi \\ 0 \end{pmatrix}$ and $\begin{pmatrix} e \\ 1 \end{pmatrix}$ close to $\begin{pmatrix} v \\ 0 \end{pmatrix}$

Recovery from a single real embedding



integer combination $\begin{pmatrix} 2^\lambda \pi \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 2^\lambda e \\ 1 \end{pmatrix}$ close to $\begin{pmatrix} 2^\lambda v \\ 0 \end{pmatrix}$

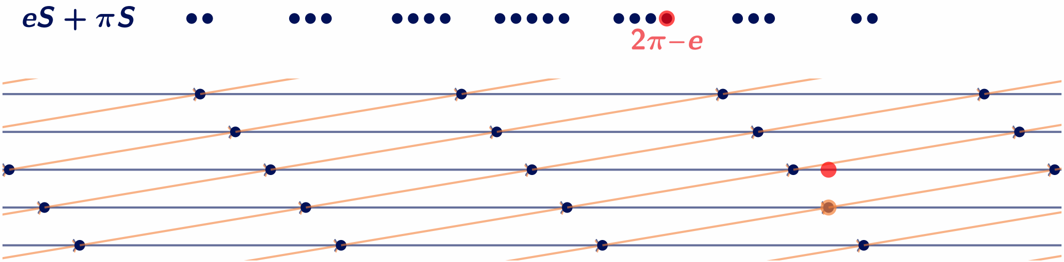
Recovery from a single real embedding



integer combination $\begin{pmatrix} 2^\lambda \pi \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 2^\lambda e \\ 1 \end{pmatrix}$ close to $\begin{pmatrix} 2^\lambda v \\ 0 \end{pmatrix}$

- Increasing λ moves wrong combinations further away
- Distance to correct combination $\approx$ same

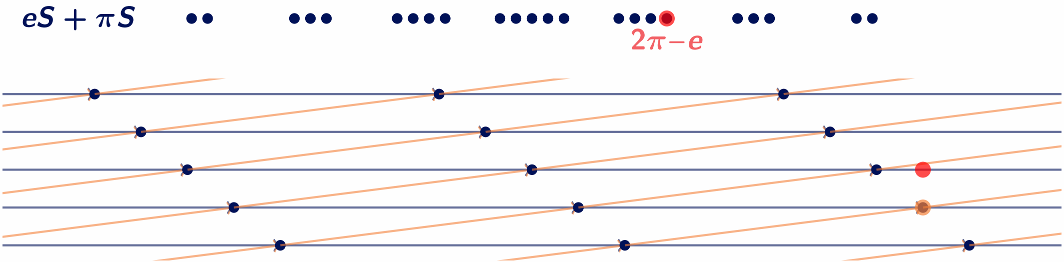
Recovery from a single real embedding



integer combination $\begin{pmatrix} 2^{\lambda}\pi \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 2^{\lambda}e \\ 1 \end{pmatrix}$ close to $\begin{pmatrix} 2^{\lambda}v \\ 0 \end{pmatrix}$

- Increasing λ moves wrong combinations further away
- Distance to correct combination $\approx$ same

Recovery from a single real embedding

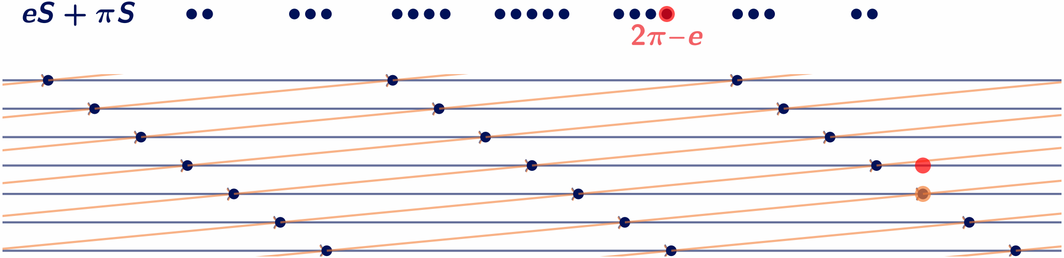


$$\text{integer combination } \begin{pmatrix} 2^\lambda \pi \\ 0 \end{pmatrix} \text{ and } \begin{pmatrix} 2^\lambda e \\ 1 \end{pmatrix} \text{ close to } \begin{pmatrix} 2^\lambda v \\ 0 \end{pmatrix}$$

- Increasing λ moves wrong combinations further away
- Distance to correct combination $\approx$ same

Recovery from a single real embedding

$eS + \pi S$

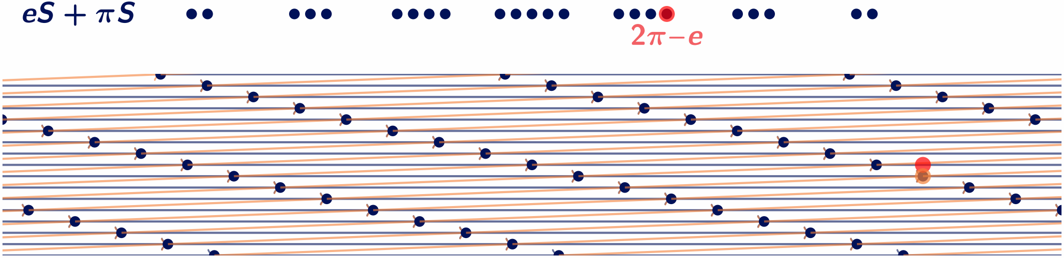


integer combination $\begin{pmatrix} 2^\lambda \pi \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 2^\lambda e \\ 1 \end{pmatrix}$ close to $\begin{pmatrix} 2^\lambda v \\ 0 \end{pmatrix}$

- Increasing λ moves wrong combinations further away
- Distance to correct combination $\approx$ same

Recovery from a single real embedding

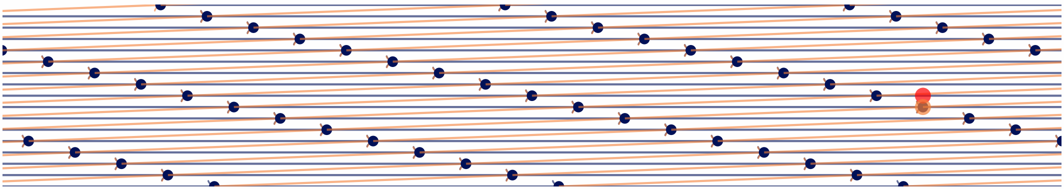
$eS + \pi S$



integer combination $\begin{pmatrix} 2^{\lambda}\pi \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 2^{\lambda}e \\ 1 \end{pmatrix}$ close to $\begin{pmatrix} 2^{\lambda}v \\ 0 \end{pmatrix}$

- Increasing λ moves wrong combinations further away
- Distance to correct combination $\approx$ same

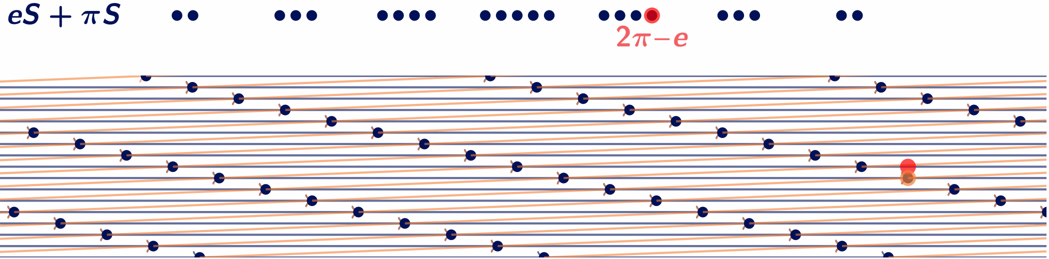
Recovery from a single real embedding



integer combination $\begin{pmatrix} 2^\lambda \pi \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 2^\lambda e \\ 1 \end{pmatrix}$ close to $\begin{pmatrix} 2^\lambda v \\ 0 \end{pmatrix}$

- Increasing λ moves wrong combinations further away
- Distance to correct combination $\approx$ same
- For large enough λ LLL recovers the closest combination

Recovery from a single real embedding

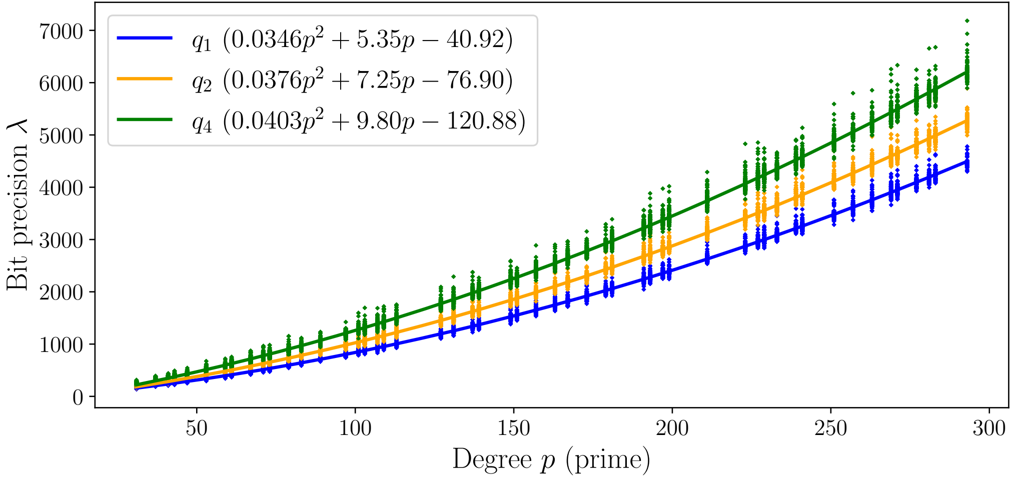


integer combination $\begin{pmatrix} \lfloor 2^\lambda \pi \rceil \\ 0 \end{pmatrix}$ and $\begin{pmatrix} \lfloor 2^\lambda e \rceil \\ 1 \end{pmatrix}$ close to $\begin{pmatrix} \lfloor 2^\lambda v \rceil \\ 0 \end{pmatrix}$

- Increasing λ moves wrong combinations further away
- Distance to correct combination $\approx$ same
- For large enough λ LLL recovers the closest combination

Required precision for NTRU Prime field

Lemma [PMS21]: $\boldsymbol{\lambda \geq \mathrm{poly}(\log(|\Delta_K|), \log\|P\|, \log(\|x\|))}$ is sufficient



Solving the sum of 2 squares equation

- We have recovered $\boldsymbol{B}^\top \boldsymbol{B}$, in particular we know $a^2 + b^2$

Solving the sum of 2 squares equation

- We have recovered $\boldsymbol{B}^\top \boldsymbol{B}$, in particular we know $a^2 + b^2$
- We now proceed as in totally real attack and previous talk... with additional technical obstacles

Solving the sum of 2 squares equation

- We have recovered $B^\top B$, in particular we know $a^2 + b^2$
- We now proceed as in totally real attack and previous talk... with additional technical obstacles

The easy part:

- Note that $i \notin K$ (contrary to previous talk) , let $L := K(i)$, then:

$$\boxed{a^2 + b^2 = \overline{(a + bi)}(a + bi) =: N_{L/K}(a + bi)}$$ norm equation!

Solving the sum of 2 squares equation

- We have recovered $B^\top B$, in particular we know $a^2 + b^2$
- We now proceed as in totally real attack and previous talk... with additional technical obstacles

The easy part:

- Note that $i \notin K$ (contrary to previous talk) , let $L := K(i)$, then:

$$\boxed{a^2 + b^2 = \overline{(a + bi)}(a + bi) =: N_{L/K}(a + bi)}$$ norm equation!

- No need to go to quaternions

Solving the sum of 2 squares equation

- We have recovered $B^\top B$, in particular we know a^2+b^2
- We now proceed as in totally real attack and previous talk... with additional technical obstacles

The easy part:

- Note that $i \notin K$ (contrary to previous talk) , let $L := K(i)$, then:

$$\boxed{a^2+b^2 = \overline{(a+bi)}(a+bi) =: N_{L/K}(a+bi)}$$ norm equation!

- No need to go to quaternions
- Use trick from previous talk to recover ideal $(a+bi)\mathcal{O}_L$

Notation: $z = a+bi$, $z' = c+di$

Lemma: Ideal recovery (previous talk!)

$$z\mathcal{O}_L = \mathcal{O}_L \cap zz'^{-1}\mathcal{O}_L = \mathcal{O}_L \cap q_1(\det(B)i + q_2)^{-1}\mathcal{O}_L.$$

Generalized Gentry-Szydlo algorithm

When L is a CM field Gentry-Szydlo recovers z from $z\mathcal{O}_L$ and $\bar{z}z$.

Generalized Gentry-Szydlo algorithm

When L is a CM field Gentry-Szydlo recovers z from $z\mathcal{O}_L$ and $\bar{z}z$.

Contribution: Generalized GS-algorithm

Let L be any field that is GS-friendly. Given $z\mathcal{O}_L$ and $|\tau_j(z)|$ for all embeddings $\tau_j : L \to \mathbb{C}$, one can recover $z \in \mathcal{O}_L$ in polynomial time.

Generalized Gentry-Szydlo algorithm

When L is a CM field Gentry-Szydlo recovers z from $z\mathcal{O}_L$ and $\bar{z}z$.

Contribution: Generalized GS-algorithm

Let L be any field that is GS-friendly. Given $z\mathcal{O}_L$ and $|\tau_j(z)|$ for all embeddings $\tau_j : L \to \mathbb{C}$, one can recover $z \in \mathcal{O}_L$ in polynomial time.

Conjecture/Heuristic: all fields are GS-friendly

(experimentally verified for $K =$ NTRU Prime and $L =$ cyclotomics or random field)

Generalized Gentry-Szydlo algorithm

When L is a CM field Gentry-Szydlo recovers z from $z\mathcal{O}_L$ and $\bar{z}z$.

Contribution: Generalized GS-algorithm

Let L be any field that is GS-friendly. Given $z\mathcal{O}_L$ and $|\tau_j(z)|$ for all embeddings $\tau_j : L \to \mathbb{C}$, one can recover $z \in \mathcal{O}_L$ in polynomial time.

Conjecture/Heuristic: all fields are GS-friendly

(experimentally verified for $K =$ NTRU Prime and $L =$ cyclotomics or random field)

The difficult part:

$$|\tau_j(a+bi)|^2 = \overline{\tau_j(a+bi)}\tau_j(a+bi) \neq \tau_j(a^2+b^2) \text{ or } \tau_j(\bar{a}a+\bar{b}b)$$

Generalized Gentry-Szydlo algorithm

When L is a CM field Gentry-Szydlo recovers z from $z\mathcal{O}_L$ and $\bar{z}z$.

Contribution: Generalized GS-algorithm

Let L be any field that is GS-friendly. Given $z\mathcal{O}_L$ and $|\tau_j(z)|$ for all embeddings $\tau_j : L \to \mathbb{C}$, one can recover $z \in \mathcal{O}_L$ in polynomial time.

Conjecture/Heuristic: all fields are GS-friendly

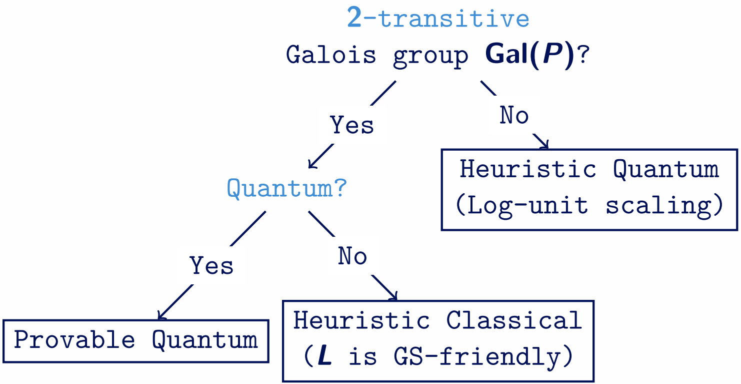
(experimentally verified for $K =$ NTRU Prime and $L =$ cyclotomics or random field)

The difficult part:

$$|\tau_j(a+bi)|^2 = \overline{\tau_j(a+bi)}\tau_j(a+bi) \neq \tau_j(a^2+b^2) \text{ or } \tau_j(\bar{a}a+\bar{b}b)$$

We have 3 approaches to solve this.

Make your choice

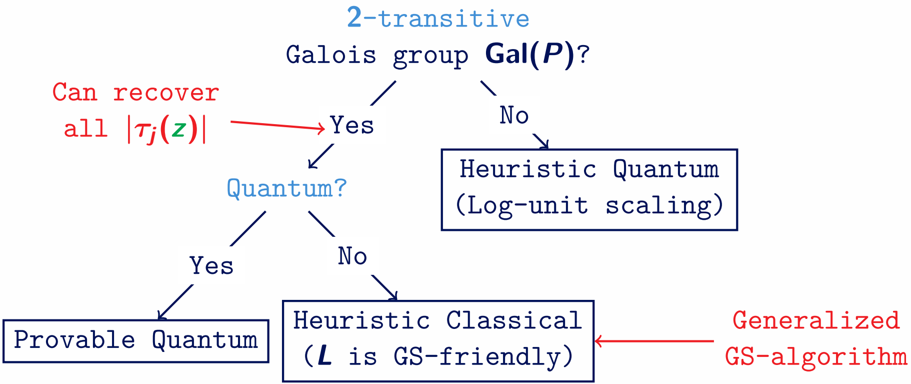


Make your choice

2-transitive
Galois group $\mathbf{Gal}(P)$?

- Yes — Can recover all $|\tau_j(z)|$
  - Quantum?
    - Yes → Provable Quantum
    - No → Heuristic Classical (L is GS-friendly)
- No → Heuristic Quantum (Log-unit scaling)

Make your choice



Make your choice

2-transitive
Galois group $\mathbf{Gal}(P)$?

Can recover
all $|\tau_j(z)|$

Yes

No

Heuristic Quantum
(Log-unit scaling)

Quantum?

Yes

No

Provable Quantum

Heuristic Classical
(L is GS-friendly)

Generalized
GS-algorithm

PIP + log-unit lattice

Make your choice

2-transitive
Galois group $\mathsf{Gal}(P)$?

Use only one $|\tau_j(z)|$ & LLL
(similar to first step)

Can recover all $|\tau_j(z)|$

Yes

No

Heuristic Quantum
(Log-unit scaling)

Quantum?

Yes

No

Provable Quantum

Heuristic Classical
(L is GS-friendly)

Generalized GS-algorithm

PIP + log-unit lattice

Conclusion

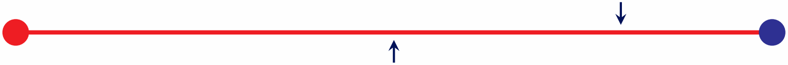
- Security of rank-2 module-LIP depends on the number field
- Real embeddings cause problems

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

New state of cryptanalysis:

NTRU Prime field

1 real embedding



Totally real

Broken!
[MPMPW24]

What about here?

also broken!

Totally imaginary

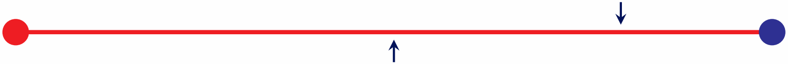
HAWK (CM field)
previous talk:
quaternions!

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

New state of cryptanalysis:

NTRU Prime field

1 real embedding



Totally real

Broken!

[MPMPW24]

What about here?

also broken!

Totally imaginary

HAWK (CM field)

previous talk:

quaternions!

Thank you!