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

May 5th, Eurocrypt 2025, Madrid

Clémence Chevignard, Guilhem Mureau, Thomas Espitau,
Alice Pellet-Mary, Heorhii Pliatsok and Alexandre Wallet

A bit of context...

2022: module-LIP and **Hawk** (Ducas, Postlethwaite, Pulles, van Woerden, [2]).

- NIST candidate (additional call for signatures)
- based on module-LIP over **cyclotomic fields**
- efficient and compact

A bit of context...

2022: module-LIP and **Hawk** (Ducas, Postlethwaite, Pulles, van Woerden, [2]).

- NIST candidate (additional call for signatures)
- based on module-LIP over **cyclotomic fields**
- efficient and compact

2023: Heuristic poly-time algorithm solving module-LIP over **totally real** fields (M., Pellet-Mary, Pliatsok, Wallet, [4] at Eurocrypt 2024). Does **not** break Hawk!

A bit of context...

2022: module-LIP and **Hawk** (Ducas, Postlethwaite, Pulles, van Woerden, [2]).

- NIST candidate (additional call for signatures)
- based on module-LIP over **cyclotomic fields**
- efficient and compact

2023: Heuristic poly-time algorithm solving module-LIP over **totally real** fields (M., Pellet-Mary, Pliatsok, Wallet, [4] at Eurocrypt 2024). Does **not** break Hawk!

This talk: Poly-time reduction from **rank-2** module-LIP over **CM** fields (includes Hawk) to a problem on **ideals** in a **quaternion algebra** [1].

A bit of context...

2022: module-LIP and **Hawk** (Ducas, Postlethwaite, Pulles, van Woerden, [2]).

- NIST candidate (additional call for signatures)
- based on module-LIP over **cyclotomic fields**
- efficient and compact

2023: Heuristic poly-time algorithm solving module-LIP over **totally real** fields (M., Pellet-Mary, Pliatsok, Wallet, [4] at Eurocrypt 2024). Does **not** break Hawk!

This talk: Poly-time reduction from **rank-2** module-LIP over **CM** fields (includes Hawk) to a problem on **ideals** in a **quaternion algebra** [1]. Does **not** break Hawk!

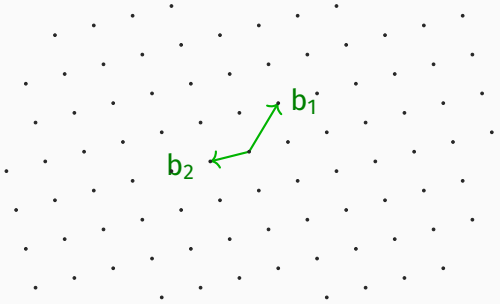
The module-Lattice Isomorphism Problem (module-LIP)

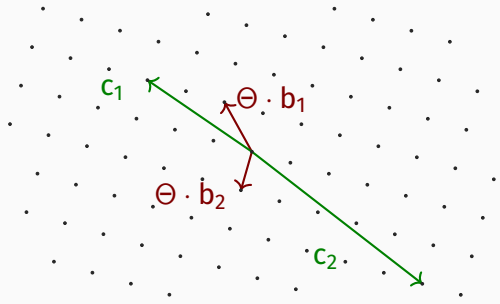
The module-Lattice Isomorphism Problem

The **Lattice Isomorphism Problem** (LIP) asks to compute an isometry between isomorphic lattices: $\mathcal{L}$ and $\mathcal{L}' = \Theta \cdot \mathcal{L}$, where Θ is orthogonal (*i.e.*, $\Theta^T\Theta = \mathrm{Id}$).

The module-Lattice Isomorphism Problem

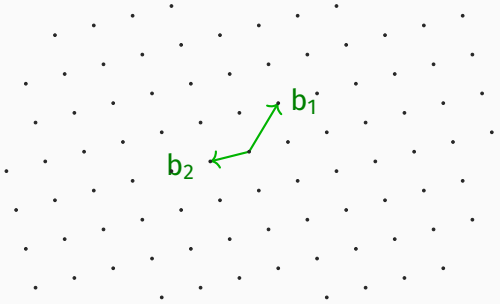
The **Lattice Isomorphism Problem** (LIP) asks to compute an isometry between isomorphic lattices: $\mathcal{L}$ and $\mathcal{L}' = \Theta \cdot \mathcal{L}$, where Θ is orthogonal (*i.e.*, $\Theta^T\Theta = \mathrm{Id}$).

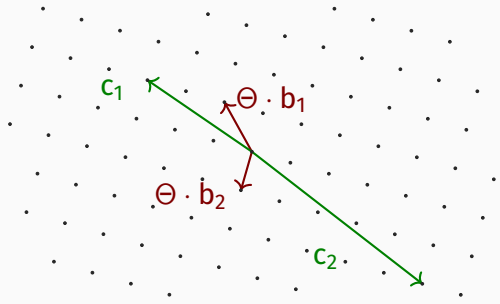




The module-Lattice Isomorphism Problem

The **Lattice Isomorphism Problem** (LIP) asks to compute an isometry between isomorphic lattices: $\mathcal{L}$ and $\mathcal{L}' = \Theta \cdot \mathcal{L}$, where Θ is orthogonal (*i.e.*, $\Theta^T\Theta = \mathrm{Id}$).





Input: Bases **B** and **C**

Goal: Compute Θ orthogonal or $\mathbf{U} \in \mathbf{GL}_n(\mathbb{Z})$ such that $\mathbf{C} = \Theta\mathbf{B}\mathbf{U}$.

The module-Lattice Isomorphism Problem

For efficiency and compactness, we use **module-lattices.** That is, we consider

$$\mathcal{L} = \mathbf{b_1}\mathbb{Z}_K + \cdots + \mathbf{b_n}\mathbb{Z}_K,$$

where K is a **number field**, $\mathbb{Z}_K$ its **ring of integers** and $\mathbf{b_1}, \ldots, \mathbf{b_n} \in K^n$ are K-linearly independent. $\mathbf{B} = (\mathbf{b_1}|\cdots|\mathbf{b_n})$ is a **basis** of $\mathcal{L}$.

The module-Lattice Isomorphism Problem

For efficiency and compactness, we use **module-lattices.** That is, we consider

$$\mathcal{L} = \mathbf{b_1}\mathbb{Z}_K + \cdots + \mathbf{b_n}\mathbb{Z}_K,$$

where K is a **number field**, $\mathbb{Z}_K$ its **ring of integers** and $\mathbf{b_1}, \ldots, \mathbf{b_n} \in K^n$ are K-linearly independent. $\mathbf{B} = (\mathbf{b_1}|\cdots|\mathbf{b_n})$ is a **basis** of $\mathcal{L}$.

Example: $K = \mathbb{Q}[X]/(X^{2^m} + 1)$ and $\mathbb{Z}_K = \mathbb{Z}[X]/(X^{2^m} + 1)$ a **power-of-two cyclotomic** number field. It is equipped with an automorphism $a \mapsto \overline{a}$ "complex conjugation".

The module-Lattice Isomorphism Problem

For efficiency and compactness, we use **module-lattices.** That is, we consider

$$\mathcal{L} = \mathbf{b_1}\mathbb{Z}_K + \cdots + \mathbf{b_n}\mathbb{Z}_K,$$

where K is a **number field**, $\mathbb{Z}_K$ its **ring of integers** and $\mathbf{b_1}, \ldots, \mathbf{b_n} \in K^n$ are K-linearly independent. $\mathbf{B} = (\mathbf{b_1}|\cdots|\mathbf{b_n})$ is a **basis** of $\mathcal{L}$.

Example: $K = \mathbb{Q}[X]/(X^{2^m}+1)$ and $\mathbb{Z}_K = \mathbb{Z}[X]/(X^{2^m}+1)$ a **power-of-two cyclotomic** number field. It is equipped with an automorphism $a \mapsto \overline{a}$ "complex conjugation".

Remark: Consider only power-of-two cyclotomic fields in the talk. Everything works for a larger family of fields (**CM** number fields).

The module-Lattice Isomorphism Problem

The **module-Lattice Isomorphism Problem** (module-LIP) asks for a "K-isometry" between isomorphic module-lattices: $\mathbf{C} = \Theta\mathbf{B}\mathbf{U}$, where $\mathbf{U} \in \mathbf{GL}_n(\mathbb{Z}_K)$ and $\Theta^*\Theta = \mathrm{Id}$.

The module-Lattice Isomorphism Problem

The **module-Lattice Isomorphism Problem** (module-LIP) asks for a "K-isometry" between isomorphic module-lattices: $\mathbf{C} = \Theta\mathbf{B}\mathbf{U}$, where $\mathbf{U} \in \mathbf{GL}_n(\mathbb{Z}_K)$ and $\Theta^*\Theta = \mathrm{Id}$.

Example: With the module-lattice $\mathcal{H} = \binom{1}{0}\mathbb{Z}_K + \binom{0}{1}\mathbb{Z}_K$ as in Hawk and $\mathbf{B} = \mathrm{Id}_2$.

The module-Lattice Isomorphism Problem

The **module-Lattice Isomorphism Problem** (module-LIP) asks for a "K-isometry" between isomorphic module-lattices: $\mathbf{C} = \Theta\mathbf{B}\mathbf{U}$, where $\mathbf{U} \in \mathbf{GL}_n(\mathbb{Z}_K)$ and $\Theta^*\Theta = \mathrm{Id}$.

Example: With the module-lattice $\mathcal{H} = \binom{1}{0}\mathbb{Z}_K + \binom{0}{1}\mathbb{Z}_K$ as in Hawk and $\mathbf{B} = \mathrm{Id}_2$.
An input of module-LIP is a basis $\mathbf{C}$ of a module-lattice $\mathcal{L} \simeq \mathcal{H}$.

The module-Lattice Isomorphism Problem

The **module-Lattice Isomorphism Problem** (module-LIP) asks for a "K-isometry" between isomorphic module-lattices: $\mathbf{C} = \Theta\mathbf{B}\mathbf{U}$, where $\mathbf{U} \in \mathbf{GL}_n(\mathbb{Z}_K)$ and $\Theta^*\Theta = \mathrm{Id}$.

Example: With the module-lattice $\mathcal{H} = \binom{1}{0}\mathbb{Z}_K + \binom{0}{1}\mathbb{Z}_K$ as in Hawk and $\mathbf{B} = \mathrm{Id}_2$.
An input of module-LIP is a basis $\mathbf{C}$ of a module-lattice $\mathcal{L} \simeq \mathcal{H}$.

Remark: The security of Hawk is related to the hardness of module-LIP on $\mathcal{H}$.
$\longrightarrow$ In the following, we focus on the module-lattice $\mathcal{H}$.

A reduction from Hawk to nrdPIP

A reduction from Hawk to nrdPIP

- K power-of-two cyclo, **B** = Id_2 basis of $\mathcal{H} = \binom{1}{0}\mathbb{Z}_K + \binom{0}{1}\mathbb{Z}_K$ and **C** = Θ**BU**.

A reduction from Hawk to nrdPIP

- K power-of-two cyclo, $\mathbf{B} = \mathrm{Id}_2$ basis of $\mathcal{H} = \binom{1}{0}\mathbb{Z}_K + \binom{0}{1}\mathbb{Z}_K$ and $\mathbf{C} = \Theta\mathbf{B}\mathbf{U}$.
- Bases $\mathbf{B}$ and $\mathbf{C}$ are **public**, Θ orthogonal and $\mathbf{U} \in \mathbf{GL}_2(\mathbb{Z}_K)$ are **secret**.

A reduction from Hawk to nrdPIP

- K power-of-two cyclo, $\mathbf{B} = \mathrm{Id}_2$ basis of $\mathcal{H} = \binom{1}{0}\mathbb{Z}_K + \binom{0}{1}\mathbb{Z}_K$ and $\mathbf{C} = \Theta\mathbf{B}\mathbf{U}$.
- Bases $\mathbf{B}$ and $\mathbf{C}$ are **public**, Θ orthogonal and $\mathbf{U} \in \mathbf{GL}_2(\mathbb{Z}_K)$ are **secret**.

Idea: Get information on $\mathbf{U}$ from the Gram matrix $\mathbf{H} = \mathbf{C}^*\mathbf{C}$.

A reduction from Hawk to nrdPIP

- K power-of-two cyclo, $\mathbf{B} = \mathrm{Id}_2$ basis of $\mathcal{H} = \binom{1}{0}\mathbb{Z}_K + \binom{0}{1}\mathbb{Z}_K$ and $\mathbf{C} = \Theta\mathbf{B}\mathbf{U}$.
- Bases $\mathbf{B}$ and $\mathbf{C}$ are **public**, Θ orthogonal and $\mathbf{U} \in \mathbf{GL}_2(\mathbb{Z}_K)$ are **secret**.

Idea: Get information on $\mathbf{U}$ from the Gram matrix $\mathbf{H} = \mathbf{C}^*\mathbf{C}$. One has:

$$\mathbf{H} = \mathbf{U}^* \underbrace{(\Theta^*\Theta)}_{=\mathrm{Id}} \mathbf{U} = \mathbf{U}^*\mathbf{U} = \begin{pmatrix} \bar{x} & \bar{y} \\ \bar{z} & \bar{t} \end{pmatrix} \begin{pmatrix} x & z \\ y & t \end{pmatrix} = \begin{pmatrix} x\bar{x} + y\bar{y} & \bar{x}z + \bar{y}t \\ x\bar{z} + y\bar{t} & z\bar{z} + t\bar{t} \end{pmatrix}.$$

A reduction from Hawk to nrdPIP

- K power-of-two cyclo, $\mathbf{B} = \mathrm{Id}_2$ basis of $\mathcal{H} = \binom{1}{0}\mathbb{Z}_K + \binom{0}{1}\mathbb{Z}_K$ and $\mathbf{C} = \Theta\mathbf{B}\mathbf{U}$.
- Bases $\mathbf{B}$ and $\mathbf{C}$ are **public**, Θ orthogonal and $\mathbf{U} \in \mathbf{GL}_2(\mathbb{Z}_K)$ are **secret**.

Idea: Get information on $\mathbf{U}$ from the Gram matrix $\mathbf{H} = \mathbf{C}^*\mathbf{C}$. One has:

$$\mathbf{H} = \mathbf{U}^* \underbrace{(\Theta^*\Theta)}_{=\mathrm{Id}} \mathbf{U} = \mathbf{U}^*\mathbf{U} = \begin{pmatrix} \bar{x} & \bar{y} \\ \bar{z} & \bar{t} \end{pmatrix} \begin{pmatrix} x & z \\ y & t \end{pmatrix} = \begin{pmatrix} x\bar{x} + y\bar{y} & \bar{x}z + \bar{y}t \\ x\bar{z} + y\bar{t} & z\bar{z} + t\bar{t} \end{pmatrix}.$$

Diagonal coefficients of $\mathbf{H}$ are invariant under complex conjugation. They belong to the **totally real subfield** F of K (think of $K = \mathbb{Q}(i)$ with $i^2 = -1$, then $F = \mathbb{Q}$).

A reduction from Hawk to nrdPIP

- K power-of-two cyclo, $\mathbf{B} = \mathrm{Id}_2$ basis of $\mathcal{H} = \binom{1}{0}\mathbb{Z}_K + \binom{0}{1}\mathbb{Z}_K$ and $\mathbf{C} = \Theta\mathbf{B}\mathbf{U}$.
- Bases $\mathbf{B}$ and $\mathbf{C}$ are **public**, Θ orthogonal and $\mathbf{U} \in \mathbf{GL}_2(\mathbb{Z}_K)$ are **secret**.

Idea: Get information on $\mathbf{U}$ from the Gram matrix $\mathbf{H} = \mathbf{C}^*\mathbf{C}$. One has:

$$\mathbf{H} = \mathbf{U}^* \underbrace{(\Theta^*\Theta)}_{=\mathrm{Id}} \mathbf{U} = \mathbf{U}^*\mathbf{U} = \begin{pmatrix} \bar{x} & \bar{y} \\ \bar{z} & \bar{t} \end{pmatrix} \begin{pmatrix} x & z \\ y & t \end{pmatrix} = \begin{pmatrix} x\bar{x} + y\bar{y} & \bar{x}z + \bar{y}t \\ x\bar{z} + y\bar{t} & z\bar{z} + t\bar{t} \end{pmatrix}.$$

Diagonal coefficients of $\mathbf{H}$ are invariant under complex conjugation. They belong to the **totally real subfield** F of K (think of $K = \mathbb{Q}(i)$ with $i^2 = -1$, then $F = \mathbb{Q}$).

Fact: $K = F + F \cdot i$ and $\mathbb{Z}_K = \mathbb{Z}_F + \mathbb{Z}_F \cdot i$, where $i^2 = -1$.

A reduction from Hawk to nrdPIP

- K power-of-two cyclo, $\mathbf{B} = \mathrm{Id}_2$ basis of $\mathcal{H} = \binom{1}{0}\mathbb{Z}_K + \binom{0}{1}\mathbb{Z}_K$ and $\mathbf{C} = \Theta\mathbf{B}\mathbf{U}$.
- Bases $\mathbf{B}$ and $\mathbf{C}$ are **public**, Θ orthogonal and $\mathbf{U} \in \mathbf{GL}_2(\mathbb{Z}_K)$ are **secret**.

Idea: Get information on $\mathbf{U}$ from the Gram matrix $\mathbf{H} = \mathbf{C}^*\mathbf{C}$. One has:

$$\mathbf{H} = \mathbf{U}^* \underbrace{(\Theta^*\Theta)}_{=\mathrm{Id}} \mathbf{U} = \mathbf{U}^*\mathbf{U} = \begin{pmatrix} \bar{x} & \bar{y} \\ \bar{z} & \bar{t} \end{pmatrix} \begin{pmatrix} x & z \\ y & t \end{pmatrix} = \begin{pmatrix} x\bar{x} + y\bar{y} & \bar{x}z + \bar{y}t \\ x\bar{z} + y\bar{t} & z\bar{z} + t\bar{t} \end{pmatrix}.$$

Diagonal coefficients of $\mathbf{H}$ are invariant under complex conjugation. They belong to the **totally real subfield** F of K (think of $K = \mathbb{Q}(i)$ with $i^2 = -1$, then $F = \mathbb{Q}$).

Fact: $K = F + F \cdot i$ and $\mathbb{Z}_K = \mathbb{Z}_F + \mathbb{Z}_F \cdot i$, where $i^2 = -1$.
Put $x = \mathbf{x}_1 + \mathbf{i}\mathbf{x}_2$, $y = \mathbf{y}_1 + \mathbf{i}\mathbf{y}_2$, first coefficient of $\mathbf{H}$ is a **sum of four squares** in $\mathbb{Z}_F$:

$$x\bar{x} + y\bar{y} = \mathbf{x}_1^2 + \mathbf{x}_2^2 + \mathbf{y}_1^2 + \mathbf{y}_2^2.$$

A reduction from Hawk to nrdPIP

Introduce the **quaternion algebra**

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

with basis $\{1, i, j, ij\}$ and rules $i^2 = j^2 = -1$, $ji = -ij$.

A reduction from Hawk to nrdPIP

Introduce the **quaternion algebra**

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

with basis $\{1, i, j, ij\}$ and rules $i^2 = j^2 = -1$, $ji = -ij$.

- Non-commutative F-algebra containing $K = F + F \cdot i$.
- Has complex conjugation $\alpha \mapsto \overline{\alpha}$ extending the one on K.
- The **reduced norm** of $\alpha = x + yi + zj + tij$ is $\mathrm{nrd}(\alpha) := \alpha\overline{\alpha} = x^2 + y^2 + z^2 + t^2$.

A reduction from Hawk to nrdPIP

Introduce the **quaternion algebra**

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

with basis $\{1, i, j, ij\}$ and rules $i^2 = j^2 = -1$, $ji = -ij$.

- Non-commutative F-algebra containing $K = F + F \cdot i$.
- Has complex conjugation $\alpha \mapsto \overline{\alpha}$ extending the one on K.
- The **reduced norm** of $\alpha = x + yi + zj + tij$ is $\mathrm{nrd}(\alpha) := \alpha\overline{\alpha} = x^2 + y^2 + z^2 + t^2$.

See the column $\binom{x}{y} \in \mathbb{Z}_K^2$ of the secret matrix **U** as a quaternion $\alpha = x + y \cdot j \in \mathcal{A}$.
Its reduced norm is $\mathrm{nrd}(\alpha) = x_1^2 + x_2^2 + y_1^2 + y_2^2$, the first coefficient of **H**.

A reduction from Hawk to nrdPIP

Introduce the **quaternion algebra**

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

with basis $\{1, i, j, ij\}$ and rules $i^2 = j^2 = -1$, $ji = -ij$.

- Non-commutative F-algebra containing $K = F + F \cdot i$.
- Has complex conjugation $\alpha \mapsto \overline{\alpha}$ extending the one on K.
- The **reduced norm** of $\alpha = x + yi + zj + tij$ is $\mathrm{nrd}(\alpha) := \alpha\overline{\alpha} = x^2 + y^2 + z^2 + t^2$.

See the column $\binom{x}{y} \in \mathbb{Z}_K^2$ of the secret matrix **U** as a quaternion $\alpha = x + y \cdot j \in \mathcal{A}$.
Its reduced norm is $\mathrm{nrd}(\alpha) = x_1^2 + x_2^2 + y_1^2 + y_2^2$, the first coefficient of **H**.

$\longrightarrow$ Compute **all** solutions $\alpha \in \mathbb{Z}_K + \mathbb{Z}_K \cdot j$ to $\mathrm{nrd}(\alpha) = q$ to recover **U**.

A reduction from Hawk to nrdPIP

Remark: In a previous work [4], for rank-2 module-LIP over a totally real field (when $\mathcal{L}, \mathcal{L}' \subset F^2$), we solved $\mathrm{nrd}(\alpha) = q$ with $\alpha \in \mathbb{Z}_K = \mathbb{Z}_F + \mathbb{Z}_F \cdot i$.

A reduction from Hawk to nrdPIP

Remark: In a previous work [4], for rank-2 module-LIP over a totally real field (when $\mathcal{L}, \mathcal{L}' \subset F^2$), we solved $\mathrm{nrd}(\alpha) = q$ with $\alpha \in \mathbb{Z}_K = \mathbb{Z}_F + \mathbb{Z}_F \cdot i$.

Issue: Equations $\mathrm{nrd}(\alpha) = q$ have too many solutions in $\mathbb{Z}_K + \mathbb{Z}_K \cdot j$ to enumerate them all + we don't know how to compute them...

A reduction from Hawk to nrdPIP

Remark: In a previous work [4], for rank-2 module-LIP over a totally real field (when $\mathcal{L}, \mathcal{L}' \subset F^2$), we solved $\mathrm{nrd}(\alpha) = q$ with $\alpha \in \mathbb{Z}_K = \mathbb{Z}_F + \mathbb{Z}_F \cdot i$.

Issue: Equations $\mathrm{nrd}(\alpha) = q$ have too many solutions in $\mathbb{Z}_K + \mathbb{Z}_K \cdot j$ to enumerate them all + we don't know how to compute them...

$\longrightarrow$ Use extra information on $\mathbf{H}$ to **reduce the solution space**.

A reduction from Hawk to nrdPIP

Denote $\mathbf{H} = \begin{pmatrix} q_1 & q_2 \\ \overline{q_2} & q_3 \end{pmatrix}$ and $\mathbf{U} = \begin{pmatrix} x & z \\ y & t \end{pmatrix}$. Set $\alpha = x + y \cdot j$ and $\beta = z + t \cdot j \in \mathcal{A}$.

A reduction from Hawk to nrdPIP

Denote $\mathsf{H} = \begin{pmatrix} q_1 & q_2 \\ \overline{q_2} & q_3 \end{pmatrix}$ and $\mathsf{U} = \begin{pmatrix} x & z \\ y & t \end{pmatrix}$. Set $\alpha = x + y \cdot j$ and $\beta = z + t \cdot j \in \mathcal{A}$.

$$\text{We prove:} \quad \mathsf{U}^*\mathsf{U} = \mathsf{H} \iff \begin{cases} \mathrm{nrd}(\alpha) = q_1 \\ \alpha\beta^{-1} = q_3^{-1}(\overline{q_2} - j) \end{cases}$$

A reduction from Hawk to nrdPIP

Denote $\mathbf{H} = \begin{pmatrix} q_1 & q_2 \\ \overline{q_2} & q_3 \end{pmatrix}$ and $\mathbf{U} = \begin{pmatrix} x & z \\ y & t \end{pmatrix}$. Set $\alpha = x + y \cdot j$ and $\beta = z + t \cdot j \in \mathcal{A}$.

$$\text{We prove:} \quad \mathbf{U}^*\mathbf{U} = \mathbf{H} \iff \begin{cases} \mathrm{nrd}(\alpha) = q_1 \\ \alpha\beta^{-1} = q_3^{-1}(\overline{q_2} - j) \end{cases}$$

- Proof is direct computation.
- From $\mathbf{H}$ (public), can compute $\alpha\beta^{-1}$ (α and β fully determine a solution).
- Only need to compute $\alpha \in \mathbb{Z}_K + \mathbb{Z}_K \cdot j$.

A reduction from Hawk to nrdPIP

Denote $\mathbf{H} = \begin{pmatrix} q_1 & q_2 \\ \overline{q_2} & q_3 \end{pmatrix}$ and $\mathbf{U} = \begin{pmatrix} x & z \\ y & t \end{pmatrix}$. Set $\alpha = x + y \cdot j$ and $\beta = z + t \cdot j \in \mathcal{A}$.

$$\text{We prove:} \quad \mathbf{U}^*\mathbf{U} = \mathbf{H} \iff \begin{cases} \mathrm{nrd}(\alpha) = q_1 \\ \alpha\beta^{-1} = q_3^{-1}(\overline{q_2} - j) \end{cases}$$

- Proof is direct computation.
- From $\mathbf{H}$ (public), can compute $\alpha\beta^{-1}$ (α and β fully determine a solution).
- Only need to compute $\alpha \in \mathbb{Z}_K + \mathbb{Z}_K \cdot j$.

Question: Can we retrieve α from $\alpha\beta^{-1}$?

A reduction from Hawk to nrdPIP

Example: Let $a, b \in \mathbb{Z}$, $b \neq 0$. Suppose $\gcd(a, b) = 1$. Can we get a from $\frac{a}{b}$?

[1] Precisely, take a **maximal order** containing it.

A reduction from Hawk to nrdPIP

Example: Let $a, b \in \mathbb{Z}$, $b \neq 0$. Suppose $\gcd(a, b) = 1$. Can we get a from $\frac{a}{b}$? Build the **ideal** of $\mathbb{Z}$:

$$\mathcal{I} = \frac{a}{b}\mathbb{Z} \cap \mathbb{Z} = a\mathbb{Z},$$

and then take a generator $\rightarrow$ get a up to sign.

[1] Precisely, take a **maximal order** containing it.

A reduction from Hawk to nrdPIP

Example: Let $a, b \in \mathbb{Z}$, $b \neq 0$. Suppose $\gcd(a, b) = 1$. Can we get a from $\frac{a}{b}$? Build the **ideal** of $\mathbb{Z}$:

$$\mathcal{I} = \frac{a}{b}\mathbb{Z} \cap \mathbb{Z} = a\mathbb{Z},$$

and then take a generator $\rightarrow$ get a up to sign.

The **same works with quaternions**! Put $\mathcal{O} = \mathbb{Z}_K + \mathbb{Z}_K \cdot j$,[1]

[1] Precisely, take a **maximal order** containing it.

A reduction from Hawk to nrdPIP

Example: Let $a, b \in \mathbb{Z}$, $b \neq 0$. Suppose $\gcd(a, b) = 1$. Can we get a from $\frac{a}{b}$? Build the **ideal** of $\mathbb{Z}$:

$$\mathcal{I} = \frac{a}{b}\mathbb{Z} \cap \mathbb{Z} = a\mathbb{Z},$$

and then take a generator $\rightarrow$ get a up to sign.

The **same works with quaternions**! Put $\mathcal{O} = \mathbb{Z}_K + \mathbb{Z}_K \cdot j$,[1] then one can build the **ideal** of $\mathcal{O}$:

$$\mathcal{I} = \alpha\beta^{-1}\mathcal{O} \cap \mathcal{O} = \alpha\mathcal{O}.$$

[1] Precisely, take a **maximal order** containing it.

A reduction from Hawk to nrdPIP

Example: Let $a, b \in \mathbb{Z}$, $b \neq 0$. Suppose $\gcd(a, b) = 1$. Can we get a from $\frac{a}{b}$? Build the **ideal** of $\mathbb{Z}$:

$$\mathcal{I} = \frac{a}{b}\mathbb{Z} \cap \mathbb{Z} = a\mathbb{Z},$$

and then take a generator $\rightarrow$ get a up to sign.

The **same works with quaternions**! Put $\mathcal{O} = \mathbb{Z}_K + \mathbb{Z}_K \cdot j$,[1] then one can build the **ideal** of $\mathcal{O}$:

$$\mathcal{I} = \alpha\beta^{-1}\mathcal{O} \cap \mathcal{O} = \alpha\mathcal{O}.$$

The "gcd" of α and β is 1, morally because $\alpha \leftrightarrow \binom{x}{y}$ and $\beta \leftrightarrow \binom{z}{t}$ generate $\mathbb{Z}_K^2$.

[1] Precisely, take a **maximal order** containing it.

A reduction from Hawk to nrdPIP

Sum-up:

- Columns of the secret matrix $\mathbf{U} \leftrightarrow$ secret quaternions $\alpha, \beta \in \mathcal{A}$.

A reduction from Hawk to nrdPIP

Sum-up:

- Columns of the secret matrix **U** $\leftrightarrow$ secret quaternions $\alpha, \beta \in \mathcal{A}$.
- From the public Gram matrix **H**, compute $\alpha\beta^{-1}$.

A reduction from Hawk to nrdPIP

Sum-up:

- Columns of the secret matrix **U** $\leftrightarrow$ secret quaternions $\alpha, \beta \in \mathcal{A}$.
- From the public Gram matrix **H**, compute $\alpha\beta^{-1}$.
- Use $\alpha\beta^{-1}$ to build the **principal ideal** $\mathcal{I} = \alpha\mathcal{O}$.

A reduction from Hawk to nrdPIP

Sum-up:

- Columns of the secret matrix **U** $\leftrightarrow$ secret quaternions $\alpha, \beta \in \mathcal{A}$.
- From the public Gram matrix **H**, compute $\alpha\beta^{-1}$.
- Use $\alpha\beta^{-1}$ to build the **principal ideal** $\mathcal{I} = \alpha\mathcal{O}$.

We have reduced to the reduced norm Principal Ideal Problem (**nrdPIP**):

Input: A (right) $\mathcal{O}$-ideal $\mathcal{I}$ of $\mathcal{A}$ and $q \in F$.

Goal: A (left) generator α of $\mathcal{I}$ with $\mathrm{nrd}(\alpha) = q$, if it exists.

A reduction from Hawk to nrdPIP

Sum-up:

- Columns of the secret matrix **U** $\leftrightarrow$ secret quaternions $\alpha, \beta \in \mathcal{A}$.
- From the public Gram matrix **H**, compute $\alpha\beta^{-1}$.
- Use $\alpha\beta^{-1}$ to build the **principal ideal** $\mathcal{I} = \alpha\mathcal{O}$.

We have reduced to the reduced norm Principal Ideal Problem (**nrdPIP**):

Input: A (right) $\mathcal{O}$-ideal $\mathcal{I}$ of $\mathcal{A}$ and $q \in F$.

Goal: A (left) generator α of $\mathcal{I}$ with $\mathrm{nrd}(\alpha) = q$, if it exists.

$\longrightarrow$ We obtain a polynomial-time reduction from module-LIP on $\mathcal{H}$ to nrdPIP in $\mathcal{O}$.

$\longrightarrow$ Can be adapted to any rank-2 module $\mathcal{M} \subset K^2$.

A reduction from Hawk to nrdPIP

About nrdPIP:

- State-of-the-art: compute a shortest vector in $\mathcal{I}$ (rank-$2\dim_{\mathbb{Q}}(K)$ lattice) [3].

A reduction from Hawk to nrdPIP

About nrdPIP:

- State-of-the-art: compute a shortest vector in $\mathcal{I}$ (rank-$2\dim_{\mathbb{Q}}(K)$ lattice) [3].
- When $\mathcal{I}$ is an ideal of K (commutative) and $q \in F$, $\exists$ poly-time algorithm (Gentry & Szydlo) to compute $g \in K$ such that $\mathcal{I} = g\mathbb{Z}_K$ and $g\overline{g} = q$ (if it exists).

A reduction from Hawk to nrdPIP

About nrdPIP:

- State-of-the-art: compute a shortest vector in $\mathcal{I}$ (rank-$2\dim_{\mathbb{Q}}(K)$ lattice) [3].
- When $\mathcal{I}$ is an ideal of K (commutative) and $q \in F$, $\exists$ poly-time algorithm (Gentry & Szydlo) to compute $g \in K$ such that $\mathcal{I} = g\mathbb{Z}_K$ and $g\overline{g} = q$ (if it exists).
- Open question: is there a "Gentry & Szydlo algorithm" for quaternions?

A reduction from Hawk to nrdPIP

About nrdPIP:

- State-of-the-art: compute a shortest vector in $\mathcal{I}$ (rank-$2\dim_{\mathbb{Q}}(K)$ lattice) [3].
- When $\mathcal{I}$ is an ideal of K (commutative) and $q \in F$, $\exists$ poly-time algorithm (Gentry & Szydlo) to compute $g \in K$ such that $\mathcal{I} = g\mathbb{Z}_K$ and $g\overline{g} = q$ (if it exists).
- Open question: is there a "Gentry & Szydlo algorithm" for quaternions?

Conclusion:

- New angle of attack on module-LIP and Hawk.
- Connection between a lattice problem and the world of quaternions.
- A lot to do on nrdPIP. Any improvements would impact Hawk.

A reduction from Hawk to nrdPIP

About nrdPIP:

- State-of-the-art: compute a shortest vector in $\mathcal{I}$ (rank-$2\dim_{\mathbb{Q}}(K)$ lattice) [3].
- When $\mathcal{I}$ is an ideal of K (commutative) and $q \in F$, $\exists$ poly-time algorithm (Gentry & Szydlo) to compute $g \in K$ such that $\mathcal{I} = g\mathbb{Z}_K$ and $g\overline{g} = q$ (if it exists).
- Open question: is there a "Gentry & Szydlo algorithm" for quaternions?

Conclusion:

- New angle of attack on module-LIP and Hawk.
- Connection between a lattice problem and the world of quaternions.
- A lot to do on nrdPIP. Any improvements would impact Hawk.

Thanks a lot! Any questions?

References i

C. Chevignard, P.-A. Fouque, G. Mureau, A. Pellet-Mary, and A. Wallet.
A reduction from hawk to the principal ideal problem in a quaternion algebra.
Cryptology ePrint Archive, 2024.

L. Ducas, E. W. Postlethwaite, L. N. Pulles, and W. v. Woerden.
Hawk: Module lip makes lattice signatures fast, compact and simple.
In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 65–94. Springer, 2022.

M. Kirschmer and J. Voight.
Algorithmic enumeration of ideal classes for quaternion orders.
SIAM Journal on Computing, 39(5), 1714-1747, 2010.


G. Mureau, A. Pellet-Mary, G. Pliatsok, and A. Wallet.
Cryptanalysis of rank-2 module-lip in totally real number fields.
In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 226–255. Springer, 2024.