Special Genera of Hermitian Lattices and Applications to HAWK

Lattice Coding & Crypto Meeting, London King's College

Guilhem Mureau

Inria de Bordeaux, IMB, France

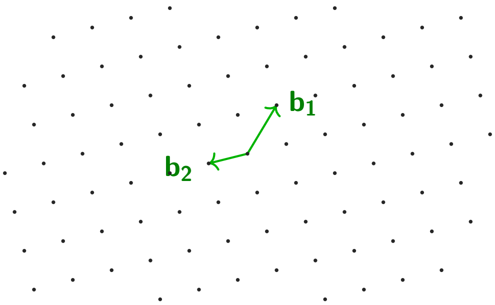
December 15th

The Lattice Isomorphism Problem (LIP)

Let $\mathbf{b_1}, \ldots, \mathbf{b_n} \in \mathbb{R}^n$ which are $\mathbb{R}$-linearly independant.
$\mathcal{L} := \{\sum_i x_i \mathbf{b_i} \,|\, x_i \in \mathbb{Z}\}$ is a **lattice** in $\mathbb{R}^n$ and $\mathbf{B} = (\mathbf{b_1}| \cdots |\mathbf{b_n})$ is a **basis** of $\mathcal{L}$.

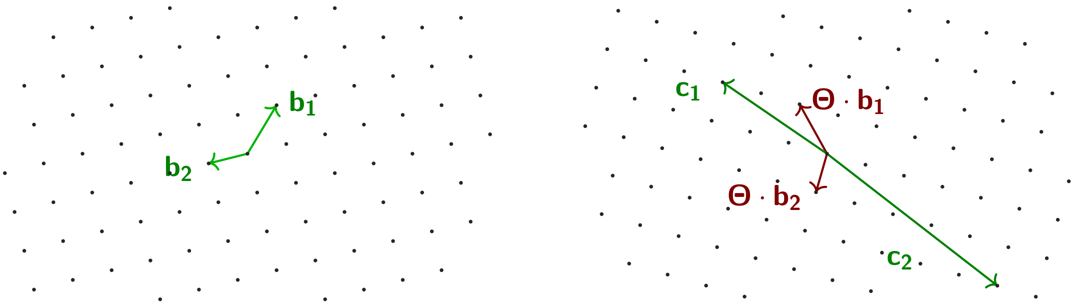
The Lattice Isomorphism Problem (LIP)

Let $\mathbf{b_1}, \ldots, \mathbf{b_n} \in \mathbb{R}^n$ which are $\mathbb{R}$-linearly independant.
$\mathcal{L} := \{\sum_i x_i \mathbf{b_i} \,|\, x_i \in \mathbb{Z}\}$ is a **lattice** in $\mathbb{R}^n$ and $\mathbf{B} = (\mathbf{b_1}|\cdots|\mathbf{b_n})$ is a **basis** of $\mathcal{L}$.



The Lattice Isomorphism Problem (LIP)

Let $\mathbf{b_1}, \ldots, \mathbf{b_n} \in \mathbb{R}^n$ which are $\mathbb{R}$-linearly independant.
$\mathcal{L} := \{\sum_i x_i \mathbf{b_i} \mid x_i \in \mathbb{Z}\}$ is a **lattice** in $\mathbb{R}^n$ and $\mathbf{B} = (\mathbf{b_1}|\cdots|\mathbf{b_n})$ is a **basis** of $\mathcal{L}$.



Lattices $\mathcal{L}_1$ and $\mathcal{L}_2$ are **isomorphic** if $\mathcal{L}_2 = \mathbf{\Theta}(\mathcal{L}_1)$ for some $\mathbf{\Theta} \in \mathcal{O}_n(\mathbb{R})$ orthogonal.

The Lattice Isomorphism Problem (LIP)

Given bases $\mathbf{B}$ and $\mathbf{C}$ of $\mathcal{L}_1$ and $\mathcal{L}_2$ resp., define:

search LIP: Assume $\mathcal{L}_1$ and $\mathcal{L}_2$ are isomorphic. Compute $\mathbf{\Theta} \in \mathcal{O}_n(\mathbb{R})$.

The Lattice Isomorphism Problem (LIP)

Given bases $\mathbf{B}$ and $\mathbf{C}$ of $\mathcal{L}_1$ and $\mathcal{L}_2$ resp., define:

search LIP: Assume $\mathcal{L}_1$ and $\mathcal{L}_2$ are isomorphic. Compute $\mathbf{\Theta} \in \mathcal{O}_n(\mathbb{R})$.

decision LIP: Decide whether $\mathcal{L}_1$ and $\mathcal{L}_2$ are isomorphic or not.

The Lattice Isomorphism Problem (LIP)

Given bases $\mathbf{B}$ and $\mathbf{C}$ of $\mathcal{L}_1$ and $\mathcal{L}_2$ resp., define:

search LIP: Assume $\mathcal{L}_1$ and $\mathcal{L}_2$ are isomorphic. Compute $\mathbf{\Theta} \in \mathcal{O}_n(\mathbb{R})$.

decision LIP: Decide whether $\mathcal{L}_1$ and $\mathcal{L}_2$ are isomorphic or not.

Remark: Can state LIP with **quadratic forms** instead.

$$\mathcal{L}_1 \simeq_{\text{iso}} \mathcal{L}_2 \iff \exists\, \mathbf{\Theta} \in \mathcal{O}_n(\mathbb{R}) \text{ and } \mathbf{U} \in \mathbf{GL}_n(\mathbb{Z})\ s.t.\ \mathbf{C} = \mathbf{\Theta}\,\mathbf{B}\,\mathbf{U}.$$

The Lattice Isomorphism Problem (LIP)

Given bases $\mathbf{B}$ and $\mathbf{C}$ of $\mathcal{L}_1$ and $\mathcal{L}_2$ resp., define:

search LIP: Assume $\mathcal{L}_1$ and $\mathcal{L}_2$ are isomorphic. Compute $\mathbf{\Theta} \in \mathcal{O}_n(\mathbb{R})$.

decision LIP: Decide whether $\mathcal{L}_1$ and $\mathcal{L}_2$ are isomorphic or not.

Remark: Can state LIP with **quadratic forms** instead.

$$\mathcal{L}_1 \simeq_{\text{iso}} \mathcal{L}_2 \iff \exists\, \mathbf{\Theta} \in \mathcal{O}_n(\mathbb{R}) \text{ and } \mathbf{U} \in \mathbf{GL}_n(\mathbb{Z}) \ s.t.\ \mathbf{C} = \mathbf{\Theta}\,\mathbf{B}\,\mathbf{U}.$$

Then the **Gram matrices** $\mathbf{G} := \mathbf{B}^T\mathbf{B}$ and $\mathbf{H} := \mathbf{C}^T\mathbf{C}$ are **congruent**:

$$\mathbf{H} = \mathbf{U}^T\mathbf{G}\mathbf{U}.$$

The Lattice Isomorphism Problem (LIP)

Given bases $\mathbf{B}$ and $\mathbf{C}$ of $\mathcal{L}_1$ and $\mathcal{L}_2$ resp., define:

search LIP: Assume $\mathcal{L}_1$ and $\mathcal{L}_2$ are isomorphic. Compute $\mathbf{\Theta} \in \mathcal{O}_n(\mathbb{R})$.

decision LIP: Decide whether $\mathcal{L}_1$ and $\mathcal{L}_2$ are isomorphic or not.

Remark: Can state LIP with **quadratic forms** instead.

$$\mathcal{L}_1 \simeq_{\textbf{iso}} \mathcal{L}_2 \iff \exists\, \mathbf{\Theta} \in \mathcal{O}_n(\mathbb{R}) \text{ and } \mathbf{U} \in \mathbf{GL}_n(\mathbb{Z}) \; s.t.\; \mathbf{C} = \mathbf{\Theta}\,\mathbf{B}\,\mathbf{U}.$$

Then the **Gram matrices** $\mathbf{G} := \mathbf{B}^T\mathbf{B}$ and $\mathbf{H} := \mathbf{C}^T\mathbf{C}$ are **congruent**:

$$\mathbf{H} = \mathbf{U}^T\mathbf{G}\mathbf{U}.$$

Two point of views, truly equivalent (Cholesky factorization over $\mathbb{R}$).
In practice we prefer quadratic forms. In this talk: keep lattice bases.

The Lattice Isomorphism Problem (LIP)

Very old questions (Gauss, classification of binary integral quadratic forms).

The Lattice Isomorphism Problem (LIP)

Very old questions (Gauss, classification of binary integral quadratic forms).

Hard algorithmic problems in high dimension: Plesken & Souvignier (1997), Haviv & Regev (2013). Best algorithms require to compute short vectors.

The Lattice Isomorphism Problem (LIP)

Very old questions (Gauss, classification of binary integral quadratic forms).

Hard algorithmic problems in high dimension: Plesken & Souvignier (1997), Haviv & Regev (2013). Best algorithms require to compute short vectors.

In cryptography :

1. Ducas & van Woerden (2021): primitives based on decision LIP.
2. Ducas *et. al.* (2022): signature scheme **HAWK**, related to search **module**-LIP.

The module-Lattice Isomorphism Problem (module-LIP)

Module lattices (or Hermitian lattices) are lattices with additional algebraic structure (symmetries). They admit a compact representation: good candidates for crypto!

The module-Lattice Isomorphism Problem (module-LIP)

Module lattices (or Hermitian lattices) are lattices with additional algebraic structure (symmetries). They admit a compact representation: good candidates for crypto!

module-LIP is LIP restricted to module lattices (and where the isomorphism must preserve the structure). As before, search module-LIP and decision module-LIP.

So far: several attempts to break **search** module-LIP. HAWK is still safe.

The module-Lattice Isomorphism Problem (module-LIP)

Module lattices (or Hermitian lattices) are lattices with additional algebraic structure (symmetries). They admit a compact representation: good candidates for crypto!

module-LIP is LIP restricted to module lattices (and where the isomorphism must preserve the structure). As before, search module-LIP and decision module-LIP.

So far: several attempts to break **search** module-LIP. HAWK is still safe.

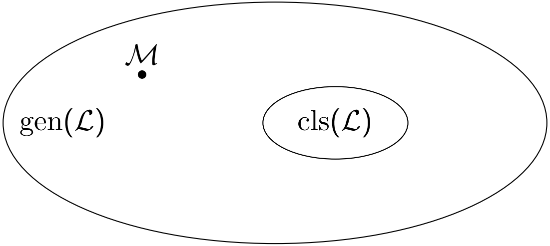
van Gent & van Woerden (2025): reduce search module-LIP to **decision** module-LIP.
$\rightsquigarrow$ HAWK reduces to several instances of decision module-LIP.

The important slide (don't blink)

We target **decision module-LIP**: are $\mathcal{L}$ and $\mathcal{M}$ isomorphic as module lattices?

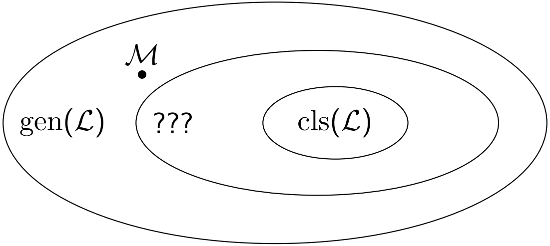
The important slide (don't blink)

We target **decision module-LIP**: are $\mathcal{L}$ and $\mathcal{M}$ isomorphic as module lattices?
So far: test efficiently if $\mathcal{L}$, $\mathcal{M}$ are in the same **genus** (necessary but not sufficient!).



The important slide (don't blink)

We target **decision module-LIP**: are $\mathcal{L}$ and $\mathcal{M}$ isomorphic as module lattices?
So far: test efficiently if $\mathcal{L}$, $\mathcal{M}$ are in the same **genus** (necessary but not sufficient!).



Our goal: Find an equivalence relation $\sim$ on gen($\mathcal{L}$) s.t. the equivalence class of $\mathcal{L}$ is between gen($\mathcal{L}$) and cls($\mathcal{L}$). Also we want $\mathcal{M} \sim \mathcal{L}$ to be **efficiently testable**.

This one is actually important too

Ling, Liu and Mendelsohn (Asiacrypt 24') considered the **spinor genus**. It is defined for a lattice in a **quadratic** space over $\mathbb{Q}$ (*e.g*, $(\mathbb{Q}^\ell, \Phi)$, where $\Phi(\mathbf{v}, \mathbf{w}) = \sum_i v_i w_i$).

This one is actually important too

Ling, Liu and Mendelsohn (Asiacrypt 24') considered the **spinor genus**. It is defined for a lattice in a **quadratic** space over $\mathbb{Q}$ (*e.g*, $(\mathbb{Q}^\ell, \Phi)$), where $\Phi(\mathbf{v}, \mathbf{w}) = \sum_i v_i w_i$).

This applies to (binary) **quadratic** module lattices over a number field K. Under assumptions on $\mathbb{Z}_K$, $\exists$ a poly-time (quantum) algorithm to distinguish spinor genera.

This one is actually important too

Ling, Liu and Mendelsohn (Asiacrypt 24') considered the **spinor genus**. It is defined for a lattice in a **quadratic** space over $\mathbb{Q}$ (*e.g*, $(\mathbb{Q}^\ell, \Phi)$, where $\Phi(\mathbf{v}, \mathbf{w}) = \sum_i v_i w_i$).

This applies to (binary) **quadratic** module lattices over a number field K. Under assumptions on $\mathbb{Z}_K$, $\exists$ a poly-time (quantum) algorithm to distinguish spinor genera.

Issue: HAWK considers (binary) **Hermitian** module lattices (with $\Phi(\mathbf{v}, \mathbf{w}) = \sum_i v_i \overline{w_i}$). Moreover $\mathbb{Z}_K$ doesn't satisfy the assumption

This one is actually important too

Ling, Liu and Mendelsohn (Asiacrypt 24') considered the **spinor genus**. It is defined for a lattice in a **quadratic** space over $\mathbb{Q}$ (*e.g*, $(\mathbb{Q}^\ell, \Phi)$, where $\Phi(\mathbf{v}, \mathbf{w}) = \sum_i v_i w_i$).

This applies to (binary) **quadratic** module lattices over a number field K. Under assumptions on $\mathbb{Z}_K$, $\exists$ a poly-time (quantum) algorithm to distinguish spinor genera.

Issue: HAWK considers (binary) **Hermitian** module lattices (with $\Phi(\mathbf{v}, \mathbf{w}) = \sum_i v_i \overline{w_i}$). Moreover $\mathbb{Z}_K$ doesn't satisfy the assumption $\rightarrow$ no impact on HAWK.

This one is actually important too

Ling, Liu and Mendelsohn (Asiacrypt 24') considered the **spinor genus**. It is defined for a lattice in a **quadratic** space over $\mathbb{Q}$ (*e.g*, $(\mathbb{Q}^\ell, \Phi)$, where $\Phi(\mathbf{v}, \mathbf{w}) = \sum_i v_i w_i$).

This applies to (binary) **quadratic** module lattices over a number field K. Under assumptions on $\mathbb{Z}_K$, $\exists$ a poly-time (quantum) algorithm to distinguish spinor genera.

Issue: HAWK considers (binary) **Hermitian** module lattices (with $\Phi(\mathbf{v}, \mathbf{w}) = \sum_i v_i \overline{w_i}$). Moreover $\mathbb{Z}_K$ doesn't satisfy the assumption $\to$ no impact on HAWK.

This talk: Shimura (1964) introduced the **special genus**. An avatar of the spinor genus for **Hermitian** lattices. It is efficiently computable for several module lattices. We discuss the impact on HAWK.

Background on Hermitian lattices

Background on number theory (1)

Let $n = 2^r$ and $K = \mathbb{Q}[X]/(X^n + 1)$ is a (power-of-two) **cyclotomic number field**.
Its **ring of integers** is $\mathbb{Z}_K = \mathbb{Z}[X]/(X^n + 1)$. $\exists$ a **complex conjugation** $a \mapsto \overline{a}$ on K.

Background on number theory (1)

Let $n = 2^r$ and $K = \mathbb{Q}[X]/(X^n + 1)$ is a (power-of-two) **cyclotomic number field**.
Its **ring of integers** is $\mathbb{Z}_K = \mathbb{Z}[X]/(X^n + 1)$. $\exists$ a **complex conjugation** $a \mapsto \overline{a}$ on K.

More generally: We can consider any CM number field K.

Background on number theory (1)

Let $n = 2^r$ and $K = \mathbb{Q}[X]/(X^n + 1)$ is a (power-of-two) **cyclotomic number field**.
Its **ring of integers** is $\mathbb{Z}_K = \mathbb{Z}[X]/(X^n + 1)$. $\exists$ a **complex conjugation** $a \mapsto \overline{a}$ on K.

More generally: We can consider any CM number field K.

An **ideal** of $\mathbb{Z}_K$ is a subgroup $\mathfrak{a} \subseteq \mathbb{Z}_K$ s.t. $\mathbb{Z}_K \cdot \mathfrak{a} \subseteq \mathfrak{a}$.

Background on number theory (1)

Let $n = 2^r$ and $K = \mathbb{Q}[X]/(X^n + 1)$ is a (power-of-two) **cyclotomic number field**.
Its **ring of integers** is $\mathbb{Z}_K = \mathbb{Z}[X]/(X^n + 1)$. $\exists$ a **complex conjugation** $a \mapsto \overline{a}$ on K.

More generally: We can consider any CM number field K.

An **ideal** of $\mathbb{Z}_K$ is a subgroup $\mathfrak{a} \subseteq \mathbb{Z}_K$ s.t. $\mathbb{Z}_K \cdot \mathfrak{a} \subseteq \mathfrak{a}$. If for all $x, y \in \mathbb{Z}_K$,

$$xy \in \mathfrak{a} \Rightarrow x \in \mathfrak{a} \text{ or } y \in \mathfrak{a},$$

it is a **prime ideal** (denote $\mathfrak{p} = \mathfrak{a}$).

Background on number theory (1)

Let $n = 2^r$ and $K = \mathbb{Q}[X]/(X^n + 1)$ is a (power-of-two) **cyclotomic number field**.
Its **ring of integers** is $\mathbb{Z}_K = \mathbb{Z}[X]/(X^n + 1)$. $\exists$ a **complex conjugation** $a \mapsto \overline{a}$ on K.

More generally: We can consider any CM number field K.

An **ideal** of $\mathbb{Z}_K$ is a subgroup $\mathfrak{a} \subseteq \mathbb{Z}_K$ s.t. $\mathbb{Z}_K \cdot \mathfrak{a} \subseteq \mathfrak{a}$. If for all $x, y \in \mathbb{Z}_K$,

$$xy \in \mathfrak{a} \Rightarrow x \in \mathfrak{a} \text{ or } y \in \mathfrak{a},$$

it is a **prime ideal** (denote $\mathfrak{p} = \mathfrak{a}$). **Example:** $K = \mathbb{Q}$, $\mathbb{Z}_K = \mathbb{Z}$ and $\mathfrak{p} = 2\mathbb{Z}$.

Background on number theory (1)

Let $n = 2^r$ and $K = \mathbb{Q}[X]/(X^n + 1)$ is a (power-of-two) **cyclotomic number field**. Its **ring of integers** is $\mathbb{Z}_K = \mathbb{Z}[X]/(X^n + 1)$. $\exists$ a **complex conjugation** $a \mapsto \overline{a}$ on K.

More generally: We can consider any CM number field K.

An **ideal** of $\mathbb{Z}_K$ is a subgroup $\mathfrak{a} \subseteq \mathbb{Z}_K$ s.t. $\mathbb{Z}_K \cdot \mathfrak{a} \subseteq \mathfrak{a}$. If for all $x, y \in \mathbb{Z}_K$,

$$xy \in \mathfrak{a} \Rightarrow x \in \mathfrak{a} \text{ or } y \in \mathfrak{a},$$

it is a **prime ideal** (denote $\mathfrak{p} = \mathfrak{a}$). **Example:** $K = \mathbb{Q}$, $\mathbb{Z}_K = \mathbb{Z}$ and $\mathfrak{p} = 2\mathbb{Z}$.

K **embeds** into larger fields. Two types of embeddings:

1. **Complex**: $K \hookrightarrow \mathbb{C}$, by sending X to a root of $X^n + 1$ in $\mathbb{C}$.
2. **Local**: $K \hookrightarrow K_{\mathfrak{p}}$, for any prime ideal $\mathfrak{p}$.

Background on number theory (2)

Let $\ell \in \mathbb{Z}_{>0}$. Hermitian space $V = (K^\ell, \Phi)$ with the standard form $\Phi(\mathbf{v}, \mathbf{w}) = \sum_i v_i \overline{w_i}$.

Background on number theory (2)

Let $\ell \in \mathbb{Z}_{>0}$. Hermitian space $V = (K^\ell, \Phi)$ with the standard form $\Phi(\mathbf{v}, \mathbf{w}) = \sum_i v_i \overline{w_i}$.
A (full rank) **Hermitian lattice** in V is of the form:

$$\mathcal{L} = \mathfrak{a}_1 \mathbf{b_1} + \cdots + \mathfrak{a}_\ell \mathbf{b}_\ell,$$

where $B = (\mathbf{b_1} | \cdots | \mathbf{b}_\ell) \in \mathbf{GL}_\ell(K)$, and $\mathfrak{a}_1, \ldots, \mathfrak{a}_\ell \subseteq \mathbb{Z}_K$ are ideals.

Background on number theory (2)

Let $\ell \in \mathbb{Z}_{>0}$. Hermitian space $V = (K^\ell, \Phi)$ with the standard form $\Phi(\mathbf{v}, \mathbf{w}) = \sum_i v_i \overline{w_i}$.
A (full rank) **Hermitian lattice** in V is of the form:

$$\mathcal{L} = \mathfrak{a}_1 \mathbf{b_1} + \cdots + \mathfrak{a}_\ell \mathbf{b}_\ell,$$

where $B = (\mathbf{b_1} | \cdots | \mathbf{b}_\ell) \in \mathbf{GL}_\ell(K)$, and $\mathfrak{a}_1, \ldots, \mathfrak{a}_\ell \subseteq \mathbb{Z}_K$ are ideals.
We say $\mathbf{B} = (B, \{\mathfrak{a}_i\}_{1 \le i \le \ell})$ is a **pseudo-basis** of $\mathcal{L}$.

Background on number theory (2)

Let $\ell \in \mathbb{Z}_{>0}$. Hermitian space $V = (K^\ell, \Phi)$ with the standard form $\Phi(\mathbf{v}, \mathbf{w}) = \sum_i v_i \overline{w_i}$.
A (full rank) **Hermitian lattice** in V is of the form:

$$\mathcal{L} = \mathfrak{a}_1 \mathbf{b_1} + \cdots + \mathfrak{a}_\ell \mathbf{b}_\ell,$$

where $B = (\mathbf{b_1}|\cdots|\mathbf{b}_\ell) \in \mathbf{GL}_\ell(K)$, and $\mathfrak{a}_1, \ldots, \mathfrak{a}_\ell \subseteq \mathbb{Z}_K$ are ideals.
We say $\mathbf{B} = (B, \{\mathfrak{a}_i\}_{1 \leq i \leq \ell})$ is a **pseudo-basis** of $\mathcal{L}$. $\mathbf{C} = (C, \{\mathfrak{b}_i\}_{1 \leq i \leq \ell})$ is another pseudo-basis of $\mathcal{L}$ **iff** $\exists\, U = (u_{i,j}) \in \mathbf{GL}_\ell(K)$ s.t.

1. $C = BU$
2. $u_{i,j} \in \mathfrak{a}_i \mathfrak{b}_j^{-1}$
3. $\mathfrak{a}_1 \cdots \mathfrak{a}_\ell = (\det U) \mathfrak{b}_1 \cdots \mathfrak{b}_\ell$.

Background on number theory (2)

Let $\ell \in \mathbb{Z}_{>0}$. Hermitian space $V = (K^\ell, \Phi)$ with the standard form $\Phi(\mathbf{v}, \mathbf{w}) = \sum_i v_i \overline{w_i}$.
A (full rank) **Hermitian lattice** in V is of the form:

$$\mathcal{L} = \mathfrak{a}_1 \mathbf{b_1} + \cdots + \mathfrak{a}_\ell \mathbf{b}_\ell,$$

where $B = (\mathbf{b_1} | \cdots | \mathbf{b}_\ell) \in \mathbf{GL}_\ell(K)$, and $\mathfrak{a}_1, \ldots, \mathfrak{a}_\ell \subseteq \mathbb{Z}_K$ are ideals.
We say $\mathbf{B} = (B, \{\mathfrak{a}_i\}_{1 \leq i \leq \ell})$ is a **pseudo-basis** of $\mathcal{L}$. $\mathbf{C} = (C, \{\mathfrak{b}_i\}_{1 \leq i \leq \ell})$ is another pseudo-basis of $\mathcal{L}$ **iff** $\exists\, U = (u_{i,j}) \in \mathbf{GL}_\ell(K)$ s.t.

1. $C = BU$
2. $u_{i,j} \in \mathfrak{a}_i \mathfrak{b}_j^{-1}$
3. $\mathfrak{a}_1 \cdots \mathfrak{a}_\ell = (\det U) \mathfrak{b}_1 \cdots \mathfrak{b}_\ell$.

Example: $\mathcal{L} = \mathbb{Z}_K \binom{1}{0} + \mathbb{Z}_K \binom{0}{1}$ as in **HAWK**, $\{(\text{pseudo-})\text{bases of } \mathcal{L}\} \supseteq \mathbf{GL}_2(\mathbb{Z}_K)$.

Background on number theory (3)

Let $\mathcal{L}$, $\mathcal{M} \subset V$ with pseudo-bases $(B, \{\mathfrak{a}_i\}_{1 \leq i \leq \ell})$ and $(C, \{\mathfrak{b}_i\}_{1 \leq i \leq \ell})$ resp.

Background on number theory (3)

Let $\mathcal{L}$, $\mathcal{M} \subset V$ with pseudo-bases $(B, \{\mathfrak{a}_i\}_{1\leq i\leq \ell})$ and $(C, \{\mathfrak{b}_i\}_{1\leq i\leq \ell})$ resp.

The **module index** of $\mathcal{M}$ in $\mathcal{L}$ is:

$$[\mathcal{L} : \mathcal{M}] := \det(B^{-1}C) \cdot \mathfrak{a}_1\mathfrak{b}_1^{-1} \cdots \mathfrak{a}_\ell\mathfrak{b}_\ell^{-1}.$$

Doesn't depend on the choice of pseudo-bases. Behaves as the "covolume of $\mathcal{M}$ in $\mathcal{L}$".

Background on number theory (3)

Let $\mathcal{L}$, $\mathcal{M} \subset V$ with pseudo-bases $(B, \{\mathfrak{a}_i\}_{1 \leq i \leq \ell})$ and $(C, \{\mathfrak{b}_i\}_{1 \leq i \leq \ell})$ resp.

The **module index** of $\mathcal{M}$ in $\mathcal{L}$ is:

$$[\mathcal{L} : \mathcal{M}] := \det(B^{-1}C) \cdot \mathfrak{a}_1 \mathfrak{b}_1^{-1} \cdots \mathfrak{a}_\ell \mathfrak{b}_\ell^{-1}.$$

Doesn't depend on the choice of pseudo-bases. Behaves as the "covolume of $\mathcal{M}$ in $\mathcal{L}$".

Example: if $K = \mathbb{Q}(i)$ and $\mathcal{L} = \mathbb{Z}[i] + \mathbb{Z}[i]$, $\mathcal{M} = \mathbb{Z}[i] + 2\mathbb{Z}[i]$, then $[\mathcal{L} : \mathcal{M}] = 2\mathbb{Z}[i]$.

Background on number theory (3)

Let $\mathcal{L}$, $\mathcal{M} \subset V$ with pseudo-bases $(B, \{\mathfrak{a}_i\}_{1\le i\le \ell})$ and $(C, \{\mathfrak{b}_i\}_{1\le i\le \ell})$ resp.

The **module index** of $\mathcal{M}$ in $\mathcal{L}$ is:

$$[\mathcal{L} : \mathcal{M}] := \det(B^{-1}C) \cdot \mathfrak{a}_1\mathfrak{b}_1^{-1} \cdots \mathfrak{a}_\ell\mathfrak{b}_\ell^{-1}.$$

Doesn't depend on the choice of pseudo-bases. Behaves as the "covolume of $\mathcal{M}$ in $\mathcal{L}$".

Example: if $K = \mathbb{Q}(i)$ and $\mathcal{L} = \mathbb{Z}[i] + \mathbb{Z}[i]$, $\mathcal{M} = \mathbb{Z}[i] + 2\mathbb{Z}[i]$, then $[\mathcal{L} : \mathcal{M}] = 2\mathbb{Z}[i]$.

Remark: $[\mathcal{L} : \mathcal{M}]$ well defined even if there is no inclusion.

Genus and special genus

(Locally) isometric Hermitian lattices

The group of **unitary transformations** of V is $\mathcal{U}(V) := \{\Theta \in \mathbf{GL}_\ell(K) \,|\, \Theta^*\Theta = \mathrm{Id}\}$.[1]

[1]Where $\Theta^* := \overline{\Theta^T}$.

(Locally) isometric Hermitian lattices

The group of **unitary transformations** of V is $\mathcal{U}(V) := \{\Theta \in \mathbf{GL}_\ell(K) \mid \Theta^*\Theta = \mathrm{Id}\}$.[1]
Hermitian lattices $\mathcal{L}$, $\mathcal{M} \subset V$ are **isomorphic** (we write $\mathcal{M} \in \mathsf{cls}(\mathcal{L})$) if:

$$\exists\, \Theta \in \mathcal{U}(V) \text{ s.t. } \mathcal{M} = \Theta(\mathcal{L}).$$

[1] Where $\Theta^* := \overline{\Theta^T}$.

(Locally) isometric Hermitian lattices

The group of **unitary transformations** of V is $\mathcal{U}(V) := \{\Theta \in \mathbf{GL}_\ell(K) \mid \Theta^*\Theta = \mathrm{Id}\}$.[1]
Hermitian lattices $\mathcal{L}$, $\mathcal{M} \subset V$ are **isomorphic** (we write $\mathcal{M} \in \mathrm{cls}(\mathcal{L})$) if:

$$\exists\, \Theta \in \mathcal{U}(V) \text{ s.t. } \mathcal{M} = \Theta(\mathcal{L}).$$

Fix $\mathfrak{p} \subset \mathbb{Z}_K$; the map $K \hookrightarrow K_\mathfrak{p}$ extends to $V \hookrightarrow V_\mathfrak{p}$.
Images of $\mathcal{L}$, $\mathcal{M}$ are denoted by $\mathcal{L}_\mathfrak{p}$, $\mathcal{M}_\mathfrak{p}$. They are "local" Hermitian lattices.

[1] Where $\Theta^* := \overline{\Theta^T}$.

(Locally) isometric Hermitian lattices

The group of **unitary transformations** of V is $\mathcal{U}(V) := \{\Theta \in \mathbf{GL}_\ell(K) \,|\, \Theta^*\Theta = \mathrm{Id}\}$.[1]
Hermitian lattices $\mathcal{L}$, $\mathcal{M} \subset V$ are **isomorphic** (we write $\mathcal{M} \in \mathsf{cls}(\mathcal{L})$) if:

$$\exists\,\Theta \in \mathcal{U}(V) \text{ s.t. } \mathcal{M} = \Theta(\mathcal{L}).$$

Fix $\mathfrak{p} \subset \mathbb{Z}_K$; the map $K \hookrightarrow K_\mathfrak{p}$ extends to $V \hookrightarrow V_\mathfrak{p}$.
Images of $\mathcal{L}$, $\mathcal{M}$ are denoted by $\mathcal{L}_\mathfrak{p}$, $\mathcal{M}_\mathfrak{p}$. They are "local" Hermitian lattices.

It is **computationally easy** to test if $\mathcal{L}$, $\mathcal{M}$ are locally isomorphic at $\mathfrak{p}$, *i.e.*, if

$$\exists\,\Theta_\mathfrak{p} \in \mathcal{U}(V_\mathfrak{p}) \text{ s.t. } \mathcal{M}_\mathfrak{p} = \Theta_\mathfrak{p}(\mathcal{L}_\mathfrak{p}).$$

---

[1] Where $\Theta^* := \overline{\Theta^T}$.

Genus of a Hermitian lattice

$\mathcal{L}, \mathcal{M} \subset V$ belong to the same **genus** if they are locally isomorphic at any $\mathfrak{p}$,

Genus of a Hermitian lattice

$\mathcal{L}, \mathcal{M} \subset V$ belong to the same **genus** if they are locally isomorphic at any $\mathfrak{p}$, *i.e.*, if

$$\forall\,\mathfrak{p}, \exists\,\Theta_\mathfrak{p} \in \mathcal{U}(V_\mathfrak{p}) \text{ s.t. } \mathcal{M}_\mathfrak{p} = \Theta_\mathfrak{p}(\mathcal{L}_\mathfrak{p}).$$

Genus of a Hermitian lattice

$\mathcal{L}$, $\mathcal{M} \subset V$ belong to the same **genus** if they are locally isomorphic at any $\mathfrak{p}$, *i.e.*, if

$$\forall \mathfrak{p}, \exists \Theta_\mathfrak{p} \in \mathcal{U}(V_\mathfrak{p}) \text{ s.t. } \mathcal{M}_\mathfrak{p} = \Theta_\mathfrak{p}(\mathcal{L}_\mathfrak{p}).$$

Fact: $\mathcal{L}$ and $\mathcal{M}$ are trivially locally isomorphic at $\mathfrak{p}$, for all but finitely many $\mathfrak{p}$.

$\rightarrow$ poly-time algo to test if $\mathcal{L}$, $\mathcal{M}$ are in the same genus (we write $\mathcal{M} \in \mathrm{gen}(\mathcal{L})$).

Genus of a Hermitian lattice

$\mathcal{L}$, $\mathcal{M} \subset V$ belong to the same **genus** if they are locally isomorphic at any $\mathfrak{p}$, *i.e.*, if

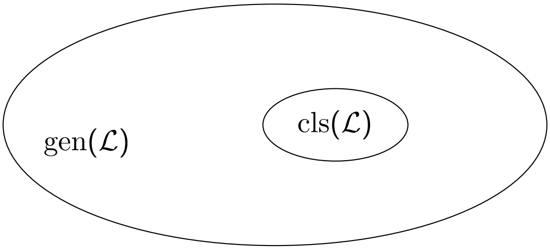
$$\forall\, \mathfrak{p}, \exists\, \Theta_\mathfrak{p} \in \mathcal{U}(V_\mathfrak{p}) \text{ s.t. } \mathcal{M}_\mathfrak{p} = \Theta_\mathfrak{p}(\mathcal{L}_\mathfrak{p}).$$

Fact: $\mathcal{L}$ and $\mathcal{M}$ are trivially locally isomorphic at $\mathfrak{p}$, for all but finitely many $\mathfrak{p}$.

$\to$ poly-time algo to test if $\mathcal{L}$, $\mathcal{M}$ are in the same genus (we write $\mathcal{M} \in \text{gen}(\mathcal{L})$).

The genus of $\mathcal{L}$ contains its isomorphism class, $\text{cls}(\mathcal{L})$.

Fact: $\text{gen}(\mathcal{L})$ is the disjoint union of **finitely many** isomorphism classes.



Special genus of a Hermitian lattice

$\mathcal{L}$, $\mathcal{M} \subset V$ belong to the same **special genus** if:

$$(\exists\, \Sigma \in \mathcal{U}(V), \forall\, \mathfrak{p}, \exists\, \Theta_{\mathfrak{p}} \in \mathcal{U}(V_{\mathfrak{p}}) \text{ with } \det \Theta_{\mathfrak{p}} = 1) \text{ s.t. } \mathcal{M}_{\mathfrak{p}} = \Sigma \circ \Theta_{\mathfrak{p}}(\mathcal{L}_{\mathfrak{p}}).$$

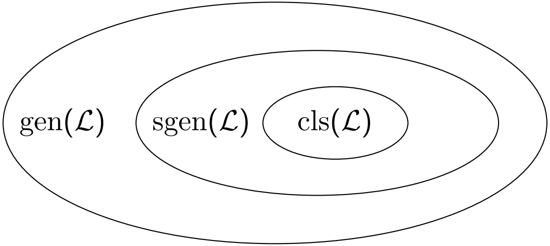
Special genus of a Hermitian lattice

$\mathcal{L}$, $\mathcal{M} \subset V$ belong to the same **special genus** if:

$$(\exists\, \Sigma \in \mathcal{U}(V), \forall\, \mathfrak{p}, \exists\, \Theta_{\mathfrak{p}} \in \mathcal{U}(V_{\mathfrak{p}}) \text{ with } \det \Theta_{\mathfrak{p}} = 1) \text{ s.t. } \mathcal{M}_{\mathfrak{p}} = \Sigma \circ \Theta_{\mathfrak{p}}(\mathcal{L}_{\mathfrak{p}}).$$

Equivalence relation $\sim$ on $\mathrm{gen}(\mathcal{L})$.
Denote the class of $\mathcal{L}$ by **sgen**$(\mathcal{L})$.

Gives an **intermediate classification** between $\mathrm{gen}(\mathcal{L})$ and $\mathrm{cls}(\mathcal{L})$.



How to distinguish special genera?

Main theoretic result: Shimura's theorem

Shimura studied how gen($\mathcal{L}$) splits into special genera.

Main theoretic result: Shimura's theorem

Shimura studied how gen($\mathcal{L}$) splits into special genera. For simplicity, $\mathcal{L}_0 = \mathbb{Z}_K^2$.

Main theoretic result: Shimura's theorem

Shimura studied how gen($\mathcal{L}$) splits into special genera. For simplicity, $\mathcal{L}_0 = \mathbb{Z}_K^2$.

$$J = \{(\text{fractional})\text{ ideals } \mathfrak{a} \text{ of } K \mid \mathfrak{a} \cdot \overline{\mathfrak{a}} = \mathbb{Z}_K\},$$
$$J_0 = \{g \cdot \mathbb{Z}_K \mid g \in K^\times \text{ and } g\overline{g} = 1\}.$$

J_0 is a subgroup of J (principal ideals).

Main theoretic result: Shimura's theorem

Shimura studied how $\text{gen}(\mathcal{L})$ splits into special genera. For simplicity, $\mathcal{L}_0 = \mathbb{Z}_K^2$.

$$J = \{(\text{fractional}) \text{ ideals } \mathfrak{a} \text{ of } K \mid \mathfrak{a} \cdot \overline{\mathfrak{a}} = \mathbb{Z}_K\},$$
$$J_0 = \{g \cdot \mathbb{Z}_K \mid g \in K^\times \text{ and } g\overline{g} = 1\}.$$

J_0 is a subgroup of J (principal ideals). Then, the map

$$\begin{aligned} \text{gen}(\mathcal{L}) &\longrightarrow J \\ \mathcal{M} &\longmapsto [\mathcal{L}_0 : \mathcal{M}] \end{aligned}$$

is well-defined and induces a **bijection** between $\text{gen}(\mathcal{L})/\sim$ and J/J_0.

Main theoretic result: Shimura's theorem

Shimura studied how $\text{gen}(\mathcal{L})$ splits into special genera. For simplicity, $\mathcal{L}_0 = \mathbb{Z}_K^2$.

$$J = \{(\text{fractional) ideals } \mathfrak{a} \text{ of } K \mid \mathfrak{a} \cdot \overline{\mathfrak{a}} = \mathbb{Z}_K\},$$
$$J_0 = \{g \cdot \mathbb{Z}_K \mid g \in K^\times \text{ and } g\overline{g} = 1\}.$$

J_0 is a subgroup of J (principal ideals). Then, the map

$$\begin{aligned} \text{gen}(\mathcal{L}) &\longrightarrow J \\ \mathcal{M} &\longmapsto [\mathcal{L}_0 : \mathcal{M}] \end{aligned}$$

is well-defined and induces a **bijection** between $\text{gen}(\mathcal{L})/\sim$ and J/J_0.

Corollary.

Let $\mathcal{M} \in \text{gen}(\mathcal{L}_0)$. $\mathcal{M} \in \text{sgen}(\mathcal{L}_0)$ **iff** $[\mathcal{L}_0 : \mathcal{M}]$ has the form $g \cdot \mathbb{Z}_K$ with $g\overline{g} = 1$.

Main algorithmic tool: Lenstra-Silverberg's algorithm

Testing if an ideal $\mathfrak{a}$ is principal is a **hard problem** for (classical) computers. Moreover if $\mathfrak{a}$ is principal, two generators g, h have $g\overline{g} \neq h\overline{h}$ in general.

Main algorithmic tool: Lenstra-Silverberg's algorithm

Testing if an ideal $\mathfrak{a}$ is principal is a **hard problem** for (classical) computers. Moreover if $\mathfrak{a}$ is principal, two generators g, h have $g\overline{g} \neq h\overline{h}$ in general. Luckily we have:

Lenstra-Silverberg's algorithm

There is a (classical) **poly-time** algorithm that given a (fractional) ideal $\mathfrak{a} \subset K$ and $q \in K$ s.t. $\mathfrak{a} \cdot \overline{\mathfrak{a}} = q \cdot \mathbb{Z}_K$, computes $g \in K$ s.t. $\mathfrak{a} = g \cdot \mathbb{Z}_K$ and $g\overline{g} = q$ (if one exists).

Main algorithmic tool: Lenstra-Silverberg's algorithm

Testing if an ideal $\mathfrak{a}$ is principal is a **hard problem** for (classical) computers. Moreover if $\mathfrak{a}$ is principal, two generators g, h have $g\overline{g} \neq h\overline{h}$ in general. Luckily we have:

Lenstra-Silverberg's algorithm

There is a (classical) **poly-time** algorithm that given a (fractional) ideal $\mathfrak{a} \subset K$ and $q \in K$ s.t. $\mathfrak{a} \cdot \overline{\mathfrak{a}} = q \cdot \mathbb{Z}_K$, computes $g \in K$ s.t. $\mathfrak{a} = g \cdot \mathbb{Z}_K$ and $g\overline{g} = q$ (if one exists).

1. Originally due to Gentry and Szydlo.

Main algorithmic tool: Lenstra-Silverberg's algorithm

Testing if an ideal $\mathfrak{a}$ is principal is a **hard problem** for (classical) computers. Moreover if $\mathfrak{a}$ is principal, two generators g, h have $g\overline{g} \neq h\overline{h}$ in general. Luckily we have:

Lenstra-Silverberg's algorithm

There is a (classical) **poly-time** algorithm that given a (fractional) ideal $\mathfrak{a} \subset K$ and $q \in K$ s.t. $\mathfrak{a} \cdot \overline{\mathfrak{a}} = q \cdot \mathbb{Z}_K$, computes $g \in K$ s.t. $\mathfrak{a} = g \cdot \mathbb{Z}_K$ and $g\overline{g} = q$ (if one exists).

1. Originally due to Gentry and Szydlo.
2. **Fundamental tool** for the cryptanalysis of (rank-2) module-LIP.

Main algorithmic tool: Lenstra-Silverberg's algorithm

Testing if an ideal $\mathfrak{a}$ is principal is a **hard problem** for (classical) computers. Moreover if $\mathfrak{a}$ is principal, two generators g, h have $g\overline{g} \neq h\overline{h}$ in general. Luckily we have:

Lenstra-Silverberg's algorithm

There is a (classical) **poly-time** algorithm that given a (fractional) ideal $\mathfrak{a} \subset K$ and $q \in K$ s.t. $\mathfrak{a} \cdot \overline{\mathfrak{a}} = q \cdot \mathbb{Z}_K$, computes $g \in K$ s.t. $\mathfrak{a} = g \cdot \mathbb{Z}_K$ and $g\overline{g} = q$ (if one exists).

1. Originally due to Gentry and Szydlo.
2. **Fundamental tool** for the cryptanalysis of (rank-2) module-LIP.
3. An generalization to **quaternionic** ideals would break HAWK.

Main algorithmic tool: Lenstra-Silverberg's algorithm

Testing if an ideal $\mathfrak{a}$ is principal is a **hard problem** for (classical) computers. Moreover if $\mathfrak{a}$ is principal, two generators g, h have $g\overline{g} \neq h\overline{h}$ in general. Luckily we have:

Lenstra-Silverberg's algorithm

There is a (classical) **poly-time** algorithm that given a (fractional) ideal $\mathfrak{a} \subset K$ and $q \in K$ s.t. $\mathfrak{a} \cdot \overline{\mathfrak{a}} = q \cdot \mathbb{Z}_K$, computes $g \in K$ s.t. $\mathfrak{a} = g \cdot \mathbb{Z}_K$ and $g\overline{g} = q$ (if one exists).

1. Originally due to Gentry and Szydlo.
2. **Fundamental tool** for the cryptanalysis of (rank-2) module-LIP.
3. An generalization to **quaternionic** ideals would break HAWK.

$\Longrightarrow$ We obtain a (classical) poly-time algo to test if $\mathcal{M} \in \text{sgen}(\mathcal{L}_0)$.

Pseudo-code for $\mathcal{L}_0 = \mathbb{Z}_K^2$

Algorithm: Test if $\mathcal{M} \in \mathrm{sgen}(\mathcal{L}_0)$

Input: A pseudo-basis $\mathbf{C} = (C, \mathfrak{b}_1, \mathfrak{b}_2)$ of $\mathcal{M} \in \mathrm{gen}(\mathcal{L}_0)$
Output: 1 if $\mathcal{M} \in \mathrm{sgen}(\mathcal{L}_0)$ and 0 otherwise

Compute $\mathfrak{a} = [\mathcal{L}_0 : \mathcal{M}]$ using $\mathbf{C}$;

Run `LenstraSilverberg` on input $\mathfrak{a}$ and 1;

if *it outputs g with $g\overline{g} = 1$* **then**

  Return 1

else

  Return 0

Pseudo-code for $\mathcal{L}_0 = \mathbb{Z}_K^2$

Algorithm: Test if $\mathcal{M} \in \mathrm{sgen}(\mathcal{L}_0)$

Input: A pseudo-basis $\mathbf{C} = (C, \mathfrak{b}_1, \mathfrak{b}_2)$ of $\mathcal{M} \in \mathrm{gen}(\mathcal{L}_0)$
Output: 1 if $\mathcal{M} \in \mathrm{sgen}(\mathcal{L}_0)$ and 0 otherwise

Compute $\mathfrak{a} = [\mathcal{L}_0 : \mathcal{M}]$ using $\mathbf{C}$;

Run `LenstraSilverberg` on input $\mathfrak{a}$ and 1;
if *it outputs* g *with* $g\overline{g} = 1$ **then**
    Return 1
else
    Return 0

Remark: In HAWK we have $\mathbf{G} = (G, \mathfrak{b}_1, \mathfrak{b}_2)$ instead of $\mathbf{C}$, where $G = C^*C$.

Pseudo-code for $\mathcal{L}_0 = \mathbb{Z}_K^2$

Algorithm: Test if $\mathcal{M} \in \mathrm{sgen}(\mathcal{L}_0)$

Input: A pseudo-basis $\mathbf{C} = (C, \mathfrak{b}_1, \mathfrak{b}_2)$ of $\mathcal{M} \in \mathrm{gen}(\mathcal{L}_0)$
Output: 1 if $\mathcal{M} \in \mathrm{sgen}(\mathcal{L}_0)$ and 0 otherwise

Compute $\mathfrak{a} = [\mathcal{L}_0 : \mathcal{M}]$ using $\mathbf{C}$;

Run `LenstraSilverberg` on input $\mathfrak{a}$ and 1;
if *it outputs* g *with* $g\overline{g} = 1$ **then**
    Return 1
else
    Return 0

Remark: In HAWK we have $\mathbf{G} = (G, \mathfrak{b}_1, \mathfrak{b}_2)$ instead of $\mathbf{C}$, where $G = C^* C$.
Can't compute a Cholesky factorization **over** K $\rightsquigarrow$ don't have a basis for $\mathfrak{a} = [\mathcal{L}_0 : \mathcal{M}]$.

Pseudo-code for $\mathcal{L}_0 = \mathbb{Z}_K^2$

Algorithm: Test if $\mathcal{M} \in \mathrm{sgen}(\mathcal{L}_0)$

Input: A pseudo-basis $\mathbf{C} = (C, \mathfrak{b}_1, \mathfrak{b}_2)$ of $\mathcal{M} \in \mathrm{gen}(\mathcal{L}_0)$
Output: 1 if $\mathcal{M} \in \mathrm{sgen}(\mathcal{L}_0)$ and 0 otherwise

Compute $\mathfrak{a} = [\mathcal{L}_0 : \mathcal{M}]$ using $\mathbf{C}$;

Run `LenstraSilverberg` on input $\mathfrak{a}$ and 1;
if *it outputs* g *with* $g\overline{g} = 1$ **then**
  Return 1
else
  Return 0

Remark: In HAWK we have $\mathbf{G} = (G, \mathfrak{b}_1, \mathfrak{b}_2)$ instead of $\mathbf{C}$, where $G = C^*C$.
Can't compute a Cholesky factorization **over** $K \rightsquigarrow$ don't have a basis for $\mathfrak{a} = [\mathcal{L}_0 : \mathcal{M}]$.
But we can still check if $\mathfrak{a}$ has a generator with $g\overline{g} = 1$.

Remarks on the general algorithm

Previous algorithm is extended to any $\mathcal{L} \subset K^\ell$ and $\mathcal{M} \in \text{gen}(\mathcal{L})$.

Remarks on the general algorithm

Previous algorithm is extended to any $\mathcal{L} \subset K^\ell$ and $\mathcal{M} \in \mathrm{gen}(\mathcal{L})$. In general:

1. Check if $[\mathcal{L} : \mathcal{M}] = g \cdot \mathbb{Z}_K$ with $g\overline{g} = 1$.

Remarks on the general algorithm

Previous algorithm is extended to any $\mathcal{L} \subset K^\ell$ and $\mathcal{M} \in \mathrm{gen}(\mathcal{L})$. In general:

1. Check if $[\mathcal{L} : \mathcal{M}] = g \cdot \mathbb{Z}_K$ with $g\overline{g} = 1$.
2. Check local conditions for a small set of primes $\mathfrak{p}$ (depends on $\mathcal{L}$).
   $\to$ Need to compute $\det(\Theta_\mathfrak{p})$ with good enough precision.

Remarks on the general algorithm

Previous algorithm is extended to any $\mathcal{L} \subset K^\ell$ and $\mathcal{M} \in \text{gen}(\mathcal{L})$. In general:

1. Check if $[\mathcal{L} : \mathcal{M}] = g \cdot \mathbb{Z}_K$ with $g\overline{g} = 1$.
2. Check local conditions for a small set of primes $\mathfrak{p}$ (depends on $\mathcal{L}$).
   $\rightarrow$ Need to compute $\det(\Theta_\mathfrak{p})$ with good enough precision.

Second item is hard to analyze. I don't have a complexity result for general case :(

Remarks on the general algorithm

Previous algorithm is extended to any $\mathcal{L} \subset K^\ell$ and $\mathcal{M} \in \text{gen}(\mathcal{L})$. In general:

1. Check if $[\mathcal{L} : \mathcal{M}] = g \cdot \mathbb{Z}_K$ with $g\overline{g} = 1$.
2. Check local conditions for a small set of primes $\mathfrak{p}$ (depends on $\mathcal{L}$).
   $\rightarrow$ Need to compute $\det(\Theta_\mathfrak{p})$ with good enough precision.

Second item is hard to analyze. I don't have a complexity result for general case :(

Remark: For several Hermitian lattices (including HAWK), there are no local conditions to check! :)

Impact on HAWK

Impact on HAWK (1)

Recall: $\mathcal{L}_0 = \mathbb{Z}_K^2$, and fix $m = 512$. We are able to distinguish $\mathrm{sgen}(\mathcal{L}_0) \subseteq \mathrm{gen}(\mathcal{L}_0)$.

Impact on HAWK (1)

Recall: $\mathcal{L}_0 = \mathbb{Z}_K^2$, and fix $m = 512$. We are able to distinguish $\mathrm{sgen}(\mathcal{L}_0) \subseteq \mathrm{gen}(\mathcal{L}_0)$.

Question: Can we quantify the gain? What is the impact on HAWK?

Impact on HAWK (1)

Recall: $\mathcal{L}_0 = \mathbb{Z}_K^2$, and fix $m = 512$. We are able to distinguish $\mathrm{sgen}(\mathcal{L}_0) \subseteq \mathrm{gen}(\mathcal{L}_0)$.

Question: Can we quantify the gain? What is the impact on HAWK?

$\rightsquigarrow$ How many classes in $\mathrm{gen}(\mathcal{L}_0)$? in $\mathrm{sgen}(\mathcal{L}_0)$?

Impact on HAWK (1)

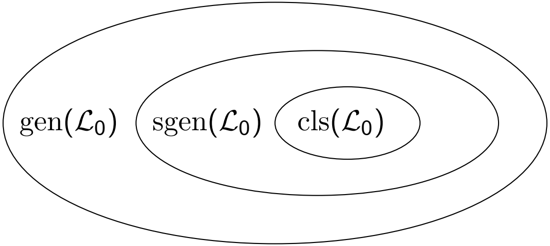
Recall: $\mathcal{L}_0 = \mathbb{Z}_K^2$, and fix $m = 512$. We are able to distinguish $\mathrm{sgen}(\mathcal{L}_0) \subseteq \mathrm{gen}(\mathcal{L}_0)$.

Question: Can we quantify the gain? What is the impact on HAWK?

$\rightsquigarrow$ How many classes in $\mathrm{gen}(\mathcal{L}_0)$? in $\mathrm{sgen}(\mathcal{L}_0)$?
We will approximate:

$$\#\{\text{iso. classes in } \mathrm{sgen}(\mathcal{L}_0)\}$$

$$\approx \frac{\#\{\text{iso. classes in } \mathrm{gen}(\mathcal{L}_0)\}}{\#\{\text{special genera in } \mathrm{gen}(\mathcal{L}_0)\}}$$



Impact on HAWK (2)

First we compute the **class number** $h(\mathcal{L}_0) := \#\{\text{iso. classes in gen}(\mathcal{L}_0)\}$.

Impact on HAWK (2)

First we compute the **class number** $h(\mathcal{L}_0) := \#\{\text{iso. classes in gen}(\mathcal{L}_0)\}$.

The **mass** of $\mathcal{L}_0$ is $\text{Mass}(\mathcal{L}_0) := \sum_{\mathcal{L}'} \frac{1}{\#\text{Aut}(\mathcal{L}')}$, where $\mathcal{L}' \in$ set of representatives.

Siegel's mass formula gives a way to compute the mass (van Gent):

$$\text{Mass}(\mathcal{L}_0) = \frac{1}{2^{\frac{m}{2}-1}} \cdot \prod_{\mathfrak{p}} \lambda(\mathcal{L}_{0\mathfrak{p}}) \cdot \left| \frac{\zeta_K}{\zeta_F}(0) \right| \cdot |\zeta_F(-1)|$$

Impact on HAWK (2)

First we compute the **class number** $h(\mathcal{L}_0) := \#\{\text{iso. classes in gen}(\mathcal{L}_0)\}$.

The **mass** of $\mathcal{L}_0$ is $\text{Mass}(\mathcal{L}_0) := \sum_{\mathcal{L}'} \frac{1}{\#\text{Aut}(\mathcal{L}')}$, where $\mathcal{L}' \in$ set of representatives.

Siegel's mass formula gives a way to compute the mass (van Gent):

$$\text{Mass}(\mathcal{L}_0) = \frac{1}{2^{\frac{m}{2}-1}} \cdot \prod_{\mathfrak{p}} \lambda(\mathcal{L}_{0\mathfrak{p}}) \cdot \left| \frac{\zeta_K}{\zeta_F}(0) \right| \cdot |\zeta_F(-1)|$$

We have upper and lower bounds on $\text{Aut}(\mathcal{L}')$. Overall for $m = 512$,

Impact on HAWK (2)

First we compute the **class number** $h(\mathcal{L}_0) := \#\{\text{iso. classes in gen}(\mathcal{L}_0)\}$.

The **mass** of $\mathcal{L}_0$ is $\text{Mass}(\mathcal{L}_0) := \sum_{\mathcal{L}'} \frac{1}{\#\text{Aut}(\mathcal{L}')}$, where $\mathcal{L}' \in$ set of representatives.

Siegel's mass formula gives a way to compute the mass (van Gent):

$$\text{Mass}(\mathcal{L}_0) = \frac{1}{2^{\frac{m}{2}-1}} \cdot \prod_{\mathfrak{p}} \lambda(\mathcal{L}_{0\mathfrak{p}}) \cdot \left| \frac{\zeta_K}{\zeta_F}(0) \right| \cdot |\zeta_F(-1)|$$

We have upper and lower bounds on $\text{Aut}(\mathcal{L}')$. Overall for $m = 512$,

$$h(\mathcal{L}_0) \approx 2^{1000}.$$

Impact on HAWK (3)

Next we compute the **special class number** $sh(\mathcal{L}_0) := \#\{\text{special genera in gen}(\mathcal{L}_0)\}$.

Impact on HAWK (3)

Next we compute the **special class number** $sh(\mathcal{L}_0) := \#\{\text{special genera in gen}(\mathcal{L}_0)\}$.

$$J = \{\text{(fractional) ideals } \mathfrak{a} \text{ of } K \mid \mathfrak{a} \cdot \overline{\mathfrak{a}} = \mathbb{Z}_K\}$$
$$J_0 = \{g \cdot \mathbb{Z}_K \mid g \in K^\times \text{ and } g\overline{g} = 1\},$$

and recall $\{\text{special genera in gen}(\mathcal{L}_0)\} \simeq J/J_0$.

Impact on HAWK (3)

Next we compute the **special class number** $sh(\mathcal{L}_0) := \#\{\text{special genera in gen}(\mathcal{L}_0)\}$.

$$J = \{\text{(fractional) ideals } \mathfrak{a} \text{ of } K \mid \mathfrak{a} \cdot \overline{\mathfrak{a}} = \mathbb{Z}_K\}$$
$$J_0 = \{g \cdot \mathbb{Z}_K \mid g \in K^\times \text{ and } g\overline{g} = 1\},$$

and recall $\{\text{special genera in gen}(\mathcal{L}_0)\} \simeq J/J_0$. In particular, $sh(\mathcal{L}_0) = |J/J_0|$.

Impact on HAWK (3)

Next we compute the **special class number** $sh(\mathcal{L}_0) := \#\{\text{special genera in gen}(\mathcal{L}_0)\}$.

$$J = \{(\text{fractional) ideals } \mathfrak{a} \text{ of } K \mid \mathfrak{a} \cdot \overline{\mathfrak{a}} = \mathbb{Z}_K\}$$
$$J_0 = \{g \cdot \mathbb{Z}_K \mid g \in K^\times \text{ and } g\overline{g} = 1\},$$

and recall $\{\text{special genera in gen}(\mathcal{L}_0)\} \simeq J/J_0$. In particular, $sh(\mathcal{L}_0) = |J/J_0|$.

J/J_0 is closely related to the **class group** of K: we have $|J/J_0| = h_K/h_F$.

Impact on HAWK (3)

Next we compute the **special class number** $sh(\mathcal{L}_0) := \#\{\text{special genera in gen}(\mathcal{L}_0)\}$.

$$J = \{\text{(fractional) ideals } \mathfrak{a} \text{ of } K \mid \mathfrak{a} \cdot \overline{\mathfrak{a}} = \mathbb{Z}_K\}$$
$$J_0 = \{g \cdot \mathbb{Z}_K \mid g \in K^\times \text{ and } g\overline{g} = 1\},$$

and recall $\{\text{special genera in gen}(\mathcal{L}_0)\} \simeq J/J_0$. In particular, $sh(\mathcal{L}_0) = |J/J_0|$.

J/J_0 is closely related to the **class group** of K: we have $|J/J_0| = h_K/h_F$.

Moreover for $m = 512$, and under GRH, $h_F = 1$.

Impact on HAWK (3)

Next we compute the **special class number** $sh(\mathcal{L}_0) := \#\{\text{special genera in gen}(\mathcal{L}_0)\}$.

$$J = \{(\text{fractional}) \text{ ideals } \mathfrak{a} \text{ of } K \mid \mathfrak{a} \cdot \overline{\mathfrak{a}} = \mathbb{Z}_K\}$$
$$J_0 = \{g \cdot \mathbb{Z}_K \mid g \in K^\times \text{ and } g\overline{g} = 1\},$$

and recall $\{\text{special genera in gen}(\mathcal{L}_0)\} \simeq J/J_0$. In particular, $sh(\mathcal{L}_0) = |J/J_0|$.

J/J_0 is closely related to the **class group** of K: we have $|J/J_0| = h_K/h_F$.

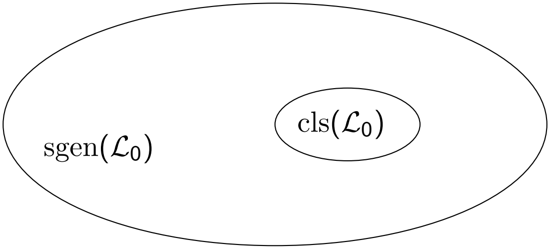
Moreover for $m = 512$, and under GRH, $h_F = 1$. Overall:

$$sh(\mathcal{L}_0) = h_K \approx 2^{200}.$$

Impact on HAWK (4)

For $\mathcal{L}_0$ and $m = 512$ as in HAWK,

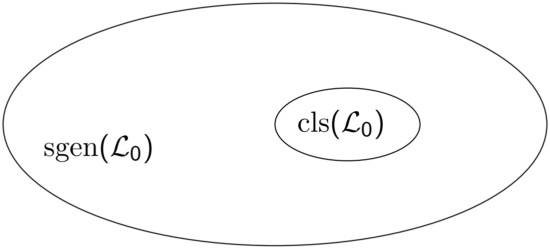
$\#\{\text{iso. classes in sgen}(\mathcal{L}_0)\} \approx 2^{800}$



Impact on HAWK (4)

For $\mathcal{L}_0$ and $m = 512$ as in HAWK,

$\#\{\text{iso. classes in sgen}(\mathcal{L}_0)\} \approx 2^{800}$



Recall: Have a reduction from HAWK to (several instances) of decision module-LIP.
(Unfortunately) lattices involved are all in sgen($\mathcal{L}_0$) $\rightsquigarrow$ **No impact on HAWK!**

Takeaway and perspectives

- The special genus is a finer invariant than the genus. To make a hard instance of decision module-LIP, lattices must be chosen inside the same special genus.

Takeaway and perspectives

- The special genus is a finer invariant than the genus. To make a hard instance of decision module-LIP, lattices must be chosen inside the same special genus.
- Have a (classical) algo to test $\mathcal{M} \in \mathrm{sgen}(\mathcal{L}_0)$. Run in poly-time for $\mathcal{L}_0 = \mathbb{Z}_K^2$.

Takeaway and perspectives

- The special genus is a finer invariant than the genus. To make a hard instance of decision module-LIP, lattices must be chosen inside the same special genus.

- Have a (classical) algo to test $\mathcal{M} \in \mathrm{sgen}(\mathcal{L}_0)$. Run in poly-time for $\mathcal{L}_0 = \mathbb{Z}_K^2$.

- Despite exponential gain, still exponential number of classes in $\mathrm{sgen}(\mathcal{L}_0)$.

Takeaway and perspectives

- The special genus is a finer invariant than the genus. To make a hard instance of decision module-LIP, lattices must be chosen inside the same special genus.
- Have a (classical) algo to test $\mathcal{M} \in \mathrm{sgen}(\mathcal{L}_0)$. Run in poly-time for $\mathcal{L}_0 = \mathbb{Z}_K^2$.
- Despite exponential gain, still exponential number of classes in $\mathrm{sgen}(\mathcal{L}_0)$.
- No concrete impact on the security of HAWK.

Takeaway and perspectives

- The special genus is a finer invariant than the genus. To make a hard instance of decision module-LIP, lattices must be chosen inside the same special genus.
- Have a (classical) algo to test $\mathcal{M} \in \mathrm{sgen}(\mathcal{L}_0)$. Run in poly-time for $\mathcal{L}_0 = \mathbb{Z}_K^2$.
- Despite exponential gain, still exponential number of classes in $\mathrm{sgen}(\mathcal{L}_0)$.
- No concrete impact on the security of HAWK.
- **Open:** $\mathcal{L}_0$ can be seen as a **quadratic** lattices (of rank 4!). Spinor genus? How does it compare with the special genus?

Takeaway and perspectives

- The special genus is a finer invariant than the genus. To make a hard instance of decision module-LIP, lattices must be chosen inside the same special genus.
- Have a (classical) algo to test $\mathcal{M} \in \mathrm{sgen}(\mathcal{L}_0)$. Run in poly-time for $\mathcal{L}_0 = \mathbb{Z}_K^2$.
- Despite exponential gain, still exponential number of classes in $\mathrm{sgen}(\mathcal{L}_0)$.
- No concrete impact on the security of HAWK.
- **Open:** $\mathcal{L}_0$ can be seen as a **quadratic** lattices (of rank 4!). Spinor genus? How does it compare with the special genus?
- **More generally:** Other computable invariants for $\mathcal{L}_0$?

Takeaway and perspectives

- The special genus is a finer invariant than the genus. To make a hard instance of decision module-LIP, lattices must be chosen inside the same special genus.
- Have a (classical) algo to test $\mathcal{M} \in \mathrm{sgen}(\mathcal{L}_0)$. Run in poly-time for $\mathcal{L}_0 = \mathbb{Z}_K^2$.
- Despite exponential gain, still exponential number of classes in $\mathrm{sgen}(\mathcal{L}_0)$.
- No concrete impact on the security of HAWK.
- **Open:** $\mathcal{L}_0$ can be seen as a **quadratic** lattices (of rank 4!). Spinor genus? How does it compare with the special genus?
- **More generally:** Other computable invariants for $\mathcal{L}_0$?

Thank you for your attention!

Bonus: Gentry-Szydlo's algorithm (1)

Let $K = \mathbb{Q}[X]/(X^m + 1)$ with $m = 2^r$. Fix $g \in \mathbb{Z}_K$

Bonus: Gentry-Szydlo's algorithm (1)

Let $K = \mathbb{Q}[X]/(X^m + 1)$ with $m = 2^r$. Fix $g \in \mathbb{Z}_K$

`GentrySzydlo`

Input: A basis of $g \cdot \mathbb{Z}_K$ and $g\overline{g}$
Output: g (up to a root of unity of K)

Bonus: Gentry-Szydlo's algorithm (1)

Let $K = \mathbb{Q}[X]/(X^m + 1)$ with $m = 2^r$. Fix $g \in \mathbb{Z}_K$

`GentrySzydlo`

Input: A basis of $g \cdot \mathbb{Z}_K$ and $g\overline{g}$
Output: g (up to a root of unity of K)

1. Find a prime number $p = 1 \pmod{m}$, so that $\mathbb{Z}_K/(p) \simeq (\mathbb{F}_p)^{m/2}$
2. Compute a LLL-reduced basis of $(g \cdot \mathbb{Z}_K)^{p-1} = g^{p-1} \cdot \mathbb{Z}_K$
   At each step, divide the basis by $g\overline{g}$ to avoid coefficient blow-up

Bonus: Gentry-Szydlo's algorithm (1)

Let $K = \mathbb{Q}[X]/(X^m + 1)$ with $m = 2^r$. Fix $g \in \mathbb{Z}_K$

GentrySzydlo

Input: A basis of $g \cdot \mathbb{Z}_K$ and $g\overline{g}$
Output: g (up to a root of unity of K)

1. Find a prime number $p = 1 \pmod{m}$, so that $\mathbb{Z}_K/(p) \simeq (\mathbb{F}_p)^{m/2}$
2. Compute a LLL-reduced basis of $(g \cdot \mathbb{Z}_K)^{p-1} = g^{p-1} \cdot \mathbb{Z}_K$
   At each step, divide the basis by $g\overline{g}$ to avoid coefficient blow-up
3. The first basis vector is $g^{p-1} \cdot v$ with v **short**. Reduce it modulo p

Bonus: Gentry-Szydlo's algorithm (2)

4. By Fermat's theorem, $g^{p-1} = 1 \pmod{p}$, so we have $v \pmod{p}$

Bonus: Gentry-Szydlo's algorithm (2)

4. By Fermat's theorem, $g^{p-1} = 1 \pmod{p}$, so we have $v \pmod{p}$
5. If p is **big enough**, obtain v exactly and deduce g^{p-1}

Bonus: Gentry-Szydlo's algorithm (2)

4. By Fermat's theorem, $g^{p-1} = 1 \pmod{p}$, so we have $v \pmod{p}$
5. If p is **big enough**, obtain v exactly and deduce g^{p-1}
6. With some trick, reduce the exponent and obtain g^m

Bonus: Gentry-Szydlo's algorithm (2)

4. By Fermat's theorem, $g^{p-1} = 1 \pmod{p}$, so we have $v \pmod{p}$
5. If p is **big enough**, obtain v exactly and deduce g^{p-1}
6. With some trick, reduce the exponent and obtain g^m
7. Compute a m-th root and get g, up to a root of unity

Bonus: Gentry-Szydlo's algorithm (2)

4. By Fermat's theorem, $g^{p-1} = 1 \pmod{p}$, so we have $v \pmod{p}$
5. If p is **big enough**, obtain v exactly and deduce g^{p-1}
6. With some trick, reduce the exponent and obtain g^m
7. Compute a m-th root and get g, up to a root of unity

$\rightarrow$ We have an implementation in `SageMath`!

References

Léo Ducas, Eamonn W Postlethwaite, Ludo N Pulles, and Wessel van Woerden. Hawk: Module lip makes lattice signatures fast, compact and simple. 2022.

Léo Ducas and Wessel van Woerden. On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography. 2022.

Hendrik W Lenstra Jr and Alice Silverberg. Testing isomorphism of lattices over cmorders. 2019.

Cong Ling, Jingbo Liu, and Andrew Mendelsohn. On the Spinor Genus and the Distinguishing Lattice Isomorphism Problem. 2024.

Goro Shimura. Arithmetic of unitary groups. 1964.

Daniel M. H. van Gent. A note on the genus of the HAWK lattice. 2025.