HAWK: a post-mortem

Daniël van Gent.

Universiteit
Leiden
The Netherlands

CWI
Centrum Wiskunde & Informatica

Public Service Announcement

- HAWK is a lattice-based digital signature scheme
- HAWK reached round 3 of NIST standardization

- HAWK is subject of 3 attacks that reduce security by a factor $\in \{.5, .75\}$:
- Straznickas–Weis • Luo et al • Mureau–Pellet-Mary
- Some were reached with AI-assistance: we will make no further mention of this

(Disclaimer: none of these attacks are mine)

Our task: Digest these attacks; learn new constraints for future schemes.

Preliminaries

Lattice = quadratic form

Two equivalent definitions:

Definition

A *lattice* is a discrete subgroup of $\mathbb{R}^n$ for some $n \geq 0$.

Definition

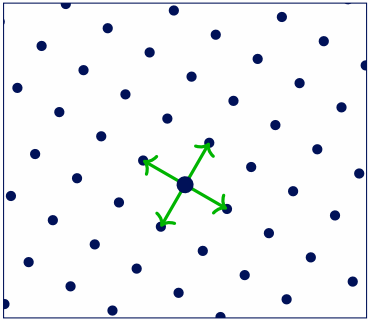
A *quadratic form* is a symmetric bilinear map $\langle -, - \rangle : \mathbb{Z}^n \times \mathbb{Z}^n \to \mathbb{R}$ for some n such that $\langle x, x \rangle \geq 0$, with equality only for $x = 0$.

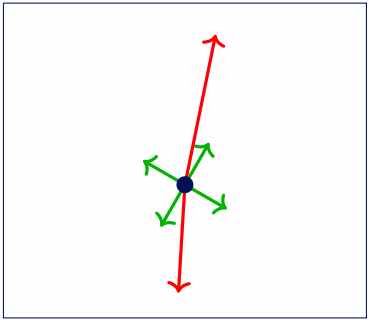
Matrix representation: lattice by basis B, quadratic form by positive definite Q.

Distinction: Hexagonal lattice has rational quadratic form.

$$B = \begin{pmatrix} 2 & 1 \\ 0 & \sqrt{3} \end{pmatrix} \quad \text{versus} \quad Q = B^T B = \begin{pmatrix} 4 & 2 \\ 2 & 4 \end{pmatrix}.$$

Shortest Vector Problem (SVP)



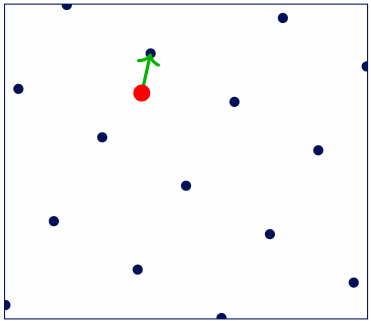


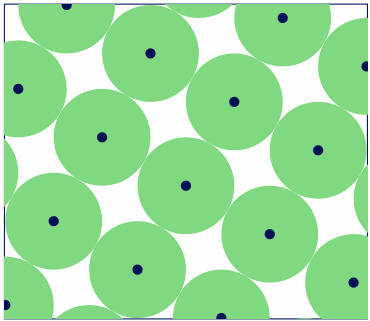
Heuristic

Solving SVP for $\mathbf{\Lambda}$ is hard if $\mathrm{gap}(\mathbf{\Lambda}) := \mathrm{gh}(\mathbf{\Lambda})/\lambda_1(\mathbf{\Lambda}) \leq n^{o(1)}$, where

$$\mathrm{gh}(\mathbf{\Lambda}) := \pi^{-1/2} \cdot \Gamma(1 + n/2)^{1/n} \cdot \det(\mathbf{\Lambda})^{1/n}.$$

Closest Vector Problem (CVP)





Heuristic

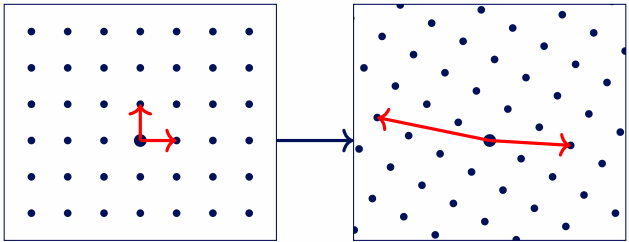
Solving CVP for $\mathbf{\Lambda}$ is hard if $\mathrm{gap}(\mathbf{\Lambda}) := \mathrm{gh}(\mathbf{\Lambda})/\lambda_1(\mathbf{\Lambda}) \leq n^{o(1)}$, where

$$\mathrm{gh}(\mathbf{\Lambda}) := \pi^{-1/2} \cdot \Gamma(1 + n/2)^{1/n} \cdot \det(\mathbf{\Lambda})^{1/n}.$$

Lattice Isomorphism Problem (LIP)

The Lattice Isomorphism Problem

Given two lattices $\mathbf{\Lambda_1}, \mathbf{\Lambda_2} \subseteq \mathbb{R}^n$, compute an orthonormal matrix $\boldsymbol{T} \in \mathrm{O}_n(\mathbb{R})$ such that $\boldsymbol{T}\mathbf{\Lambda_1} = \mathbf{\Lambda_2}$, an *isomorphism between* $\mathbf{\Lambda_1}$ *and* $\mathbf{\Lambda_2}$, or decide that it does not exist.



Heuristic

Even when $\mathbf{\Lambda_1}$ is fixed, LIP is considered to be at least as hard as SVP on $\mathbf{\Lambda_2}$.

Lattice Isomorphism Problem (LIP)

Two equivalent problems:

The Lattice Isomorphism Problem (for lattices)

Given two lattices $\boldsymbol{B_1}, \boldsymbol{B_2} \in \mathrm{GL}_{\boldsymbol{n}}(\mathbb{R})$, compute an orthonormal matrix $\boldsymbol{O} \in \mathrm{O}_{\boldsymbol{n}}(\mathbb{R})$ such that $\boldsymbol{O}\boldsymbol{B_1}\mathbb{Z}^{\boldsymbol{n}} = \boldsymbol{B_2}\mathbb{Z}^{\boldsymbol{n}}$ or decide that it does not exist.

The Lattice Isomorphism Problem (for quadratic forms)

Given two quadratic forms $\boldsymbol{Q_1}, \boldsymbol{Q_2} \in \mathrm{GL}_{\boldsymbol{n}}(\mathbb{R})$, compute a unimodular matrix $\boldsymbol{T} \in \mathrm{GL}_{\boldsymbol{n}}(\mathbb{Z})$ such that $\boldsymbol{T}^\top \boldsymbol{Q_1} \boldsymbol{T} = \boldsymbol{Q_2}$ or decide that it does not exist.

Distinction: $\boldsymbol{T}$ is integral, $\boldsymbol{O}$ very much not. ← why LIP-schemes use quadratic forms

Best known LIP-algorithms

Heuristic

Even when $\mathbf{\Lambda_1}$ is fixed, LIP is considered to be at least as hard as SVP on $\mathbf{\Lambda_2}$.

In theory:

Theorem (Haviv–Regev)

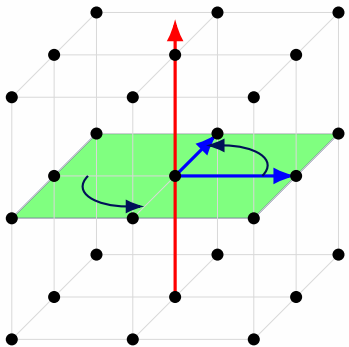
There is an algorithm to solve LIP in time $2^{O(n \log n)}$, where n is the rank.

In practice:

- Construct graph on shortest vectors.
- Compute graph isomorphism. (easy in practice + graphs quite small)
- Worst case $2^{O(n^2)}$ complexity.

Automorphisms

- Λ is a lattice of rank n.
- $\sigma : \Lambda \to \Lambda$ is an *automorphism* (isomorphism from an object to itself)
- f the minimal polynomial of σ



Example

- $\Lambda = \mathbb{Z} \perp \mathbb{Z} \perp \mathbb{Z}$.
- $\sigma =$ quarter turn around vertical axis.
- $f = (X - 1)(X^2 + 1)$.
- Eigenspace $\ker(\sigma - 1)$ is vertical axis.
- Eigenspace $\ker(\sigma^2 + 1)$ is horizontal plane.

Automorphisms

- Λ is a lattice of rank n.
- $\sigma : \Lambda \to \Lambda$ is an *automorphism* (isomorphism from an object to itself)
- f the minimal polynomial of σ

Lemma (cf. [GP25])

If given σ with f reducible in $\mathbb{Q}[X]$, then can in poly-time compute $\Lambda' \subseteq \Lambda$ with

$$\mathbf{rk}\ \Lambda' \leq \tfrac{1}{2}\mathbf{rk}\ \Lambda \qquad \text{and} \qquad \lambda_1(\Lambda') \leq \sqrt{n} \cdot \lambda_1(\Lambda)$$

Sketch: Reduce to case $f = X^p - 1$. Then $p\Lambda \subseteq \mathbf{im}(\sigma - 1) + \mathbf{ker}(\sigma - 1)$.

'reducible' automorphism $\Rightarrow$ enormous progress on approximate SVP

LIP-based cryptography

Naive Encryption LIP-Scheme

- Globally fix quadratic form $\boldsymbol{Q_1}$

Receiver:

- Private key: horrible change of basis $\boldsymbol{T} \in \mathrm{GL}_{\boldsymbol{n}}(\mathbb{Z})$
- Public key: corresponding quadratic form $\boldsymbol{Q_2} = \boldsymbol{T}^\top \boldsymbol{Q_1} \boldsymbol{T}$

Sender:

- Generate error $\boldsymbol{e} \in \mathbb{R}^{\boldsymbol{n}}$ that is small in $\boldsymbol{Q_2}$
- Embed message $\boldsymbol{m}$ in $\mathbb{Z}^{\boldsymbol{n}}$ and publish $\boldsymbol{s} = \boldsymbol{m} + \boldsymbol{e}$

Receiver:

- Translate $\boldsymbol{s}$ to $\boldsymbol{Q_1}$ using $\boldsymbol{T}$
- Recover $\boldsymbol{m}$ with decoding algorithm

Some observations

- Private key is isomorphism $\boldsymbol{T}$ $\longrightarrow$ key recovery is LIP-instance
- Cyphertext is point $\boldsymbol{s}$ close to lattice $\longrightarrow$ eavesdropping is CVP-instance
- Better decoder $\Rightarrow$ larger errors $\boldsymbol{e}$ $\Rightarrow$ less precision $\Rightarrow$ shorter cyphertexts

Main benefit of LIP-cryptography
May globally fix $\boldsymbol{\Lambda_1}$. Optimize for

- hard SVP, CVP, LIP instances
- efficient decoder
- other scheme dependent properties

HAWK is not an encryption scheme
However, attacks target common LIP-component

Key compression

Issue

Private key $\boldsymbol{T}$ and public key $\boldsymbol{Q_2}$ are in $\mathrm{GL}_n(\mathbb{Z})$: size is $\Theta(n^2)$ integers.

Idea: impose (public) structure to reduce entropy.

Example (Circulant matrices)

$$\mathcal{C} := \left\{ \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a_n & a_1 & a_2 & \dots & a_{n-1} \\ \vdots & & & & \vdots \\ a_2 & a_3 & a_4 & \dots & a_1 \end{pmatrix} \middle| \, a_1, \dots, a_n \in \mathbb{Z} \right\}.$$

Impose $\boldsymbol{Q_1}, \boldsymbol{Q_2}, \boldsymbol{T} \in \mathcal{C}$.
Now $\boldsymbol{T}, \boldsymbol{Q_2}$ require only $\Theta(n)$ integers to specify.

Understanding Key Compression

Definition

A *module* generalizes a vector space: scalars need not form a field, just a ring.

Unstructured case:

$\mathbb{Z}^n$ is a $\mathbb{Z}$-module and $T \in \mathrm{GL}_n(\mathbb{Z}) = \mathrm{Aut}_{\mathbb{Z}}(\mathbb{Z}^n)$ is a $\mathbb{Z}$-module automorphism.

Structured (circulant) case:

Consider $R = \mathbb{Z}[X]/(X^n - 1)$. Then $\mathbb{Z}^n$ is an R-module, where X acts as

$$(a_1, \ldots, a_n) \mapsto (a_n, a_1, a_2, \ldots, a_{n-1}).$$

Then $T \in \mathrm{GL}_n(\mathbb{Z})$ circulant $\Leftrightarrow$ $T \in \mathrm{Aut}_R(\mathbb{Z}^n)$.

Issue (see NTRU Composite)

Multiplication by X is a public automorphism with reducible minimal polynomial

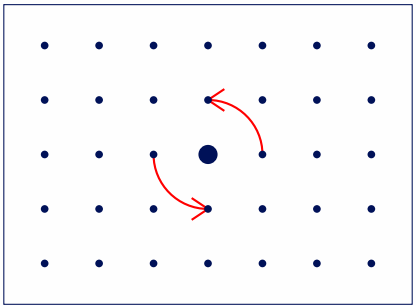
$$X^n - 1 = (X - 1)(X^{n-1} + \cdots + 1)$$

Number fields

Want:

- R acts on a lattice
- R is commutative (negotiable, see quaternions)
- R is a domain

$\Rightarrow$ R is an order in a number field



Example

- $\Lambda = \mathbb{Z} \perp \mathbb{Z}$.
- $R = \mathbb{Z}[X]/(X^2 + 1)$
  $=$ Gaussian integers
- $X = (a, b) \mapsto (-b, a)$
  $=$ quarter turn

Module lattices

- K is a complex multiplication (aka CM) field of degree d.
- $\mathcal{O}$ is the maximal order (aka ring of integers) of K.

Example: $\mathcal{O}$ has a natural quadratic form $(x, y) \mapsto \mathrm{Tr}_{K/\mathbb{Q}}(\bar{x}y)$.

Definition

An $\mathcal{O}$-module quadratic form is a map $\langle -, - \rangle : \mathcal{O}^m \times \mathcal{O}^m \to K$ such that for all $x, y, z \in \mathcal{O}^m$ and $\alpha \in \mathcal{O}$

- $\langle x, \alpha y + z \rangle = \alpha \langle x, y \rangle + \langle x, z \rangle$.
- $\langle x, y \rangle = \overline{\langle y, x \rangle}$.
- $(x, y) \mapsto \mathrm{Tr}_{K/\mathbb{Q}}(\langle x, y \rangle)$ is positive definite.

(we are ignoring the class group in this simplified definition)

Are module lattices secure?

Warning (Gentry–Szydlo)

Rank-1 module lattices are not secure (e.g., $\Lambda = \mathcal{O}$).

It is easy to avoid the rank-1 case:

- Increase rank: e.g. $\Lambda \perp \Lambda$ over $\mathcal{O}$ instead of Λ over $\mathcal{O}$.
- Decrease field: Λ over $\mathcal{O} \cap F$ for a subfield $F \subseteq K$.

Warning (Allombert–Pellet-Mary–Woerden)

Rank-2 module lattices are not secure if K has a real embedding.

HAWK predates this result, 'got lucky'

HAWK

The HAWK lattice

- ζ_ℓ is a primitive ℓ-th root of unity.
- $K = \mathbb{Q}(\zeta_{2^k})$ is a cyclotomic number field of degree $d = 2^{k-1}$.
- $\mathcal{O} = \mathbb{Z}[\zeta_{2^k}]$ is the maximal order of K.

Rank 1: As $\mathbb{Z}$-module lattices we have

$$\mathcal{O} = (\mathbb{Z} \cdot \zeta_{2^k}^0) \perp (\mathbb{Z} \cdot \zeta_{2^k}^1) \perp \cdots \perp (\mathbb{Z} \cdot \zeta_{2^k}^{d-1}) \cong_{\mathbb{Z}} \mathbb{Z}^{\perp d}$$

Rank 2: The HAWK lattice is

$$\Lambda_1 = \mathcal{O} \perp \mathcal{O} \cong_{\mathbb{Z}} \mathbb{Z}^{\perp 2d}, \quad \text{equivalently} \quad Q_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(K)$$

(Un)structured automorphisms

Unstructured: The $\mathbb{Z}$-lattice automorphisms of $\mathbb{Z}^{\perp n} \cong_{\mathbb{Z}} \mathcal{O} \perp \mathcal{O}$ are

$$(x_1, x_2, \ldots, x_n) \mapsto (s_1 x_{\tau(1)}, s_2 x_{\tau(2)}, \ldots, s_n x_{\tau(n)})$$

for $(s_1, \ldots, s_n, \tau) \in \{\pm 1\}^n \rtimes \mathbf{Sym}_n$.

Structured: The $\mathcal{O}$-lattice automorphisms of $\mathcal{O} \perp \mathcal{O}$ are

$$(x_1, x_2) \mapsto (s_1 x_{\tau(1)}, s_2 x_{\tau(2)})$$

for $(s_1, s_2, \tau) \in \mu^2 \rtimes \mathbf{Sym}_2$, where $\mu = \{\zeta^0, \zeta^1, \ldots\}$ are the roots of unity.

$$\#\text{unstructured} = 2^n \cdot (n!) \qquad \textbf{vs} \qquad \#\text{structured} = 2n^2$$

Public automorphisms

- For an arbitrary $\mathbb{Z}$-lattice, we can only expect to compute the automorphisms

$$\boldsymbol{v} \mapsto \boldsymbol{v} \qquad \text{and} \qquad \boldsymbol{v} \mapsto -\boldsymbol{v}.$$

- For an arbitrary $\mathcal{O}$-lattice, we can only expect to compute the automorphisms

$$\boldsymbol{v} \mapsto \boldsymbol{s}\boldsymbol{v} \quad \text{for} \quad \boldsymbol{s} \in \boldsymbol{\mu}.$$

  Namely, $\langle \zeta \boldsymbol{v}, \zeta \boldsymbol{w} \rangle = \zeta \overline{\zeta} \langle \boldsymbol{v}, \boldsymbol{w} \rangle = \langle \boldsymbol{v}, \boldsymbol{w} \rangle$.

Warning (Luo–Jiang–Pan–Wang)

Can compute in poly-time the $\mathcal{O}^+$-automorphism $\omega : (\boldsymbol{x}, \boldsymbol{y}) \mapsto (\overline{\boldsymbol{y}}, -\overline{\boldsymbol{x}})$ on public $\boldsymbol{Q}_2$.

Sketch: $\omega = \boldsymbol{Q}_2^{-1} \cdot \left(\begin{smallmatrix} 0 & +1 \\ -1 & 0 \end{smallmatrix} \right) \circ \gamma$, where γ is complex conjugation.

Luckily, ω has irreducible minimal polynomial $\boldsymbol{X}^2 + \boldsymbol{1}$.

Reductions to automorphisms

- $\omega : \mathcal{O}^2 \to \mathcal{O}^2$ is given by $(x, y) \mapsto (\overline{y}, -\overline{x})$.

Still, ω opens an avenue for attacks:

Observe: $\mathcal{O} \perp \mathcal{O}$ is a rank-1 module over quaternion algebra $\mathcal{O}[\omega]$.

Warning (Chevignard–Mureau–Espitau–Pellet-Mary–Pliatsok–Wallet)

LIP for HAWK reduces to reduced-norm Principal Ideal Problem on $\mathcal{O}[\omega]$.

Warning (G.–Pulles)

Given any public HAWK $\mathbb{Z}$-automorphism not in $\mu \cup \omega\mu$, the security halves.

The First Attack: Straznickas–Weis

Galois action

- τ is a Galois automorphism of order 2 of $K = \mathbb{Q}(\zeta_e)$. (e.g. $x \mapsto \overline{x}$)
- $Q = B^* B$ with Q the public quadratic form and B the private isomorphism.

Example

τ induces a $\mathbb{Z}$-automorphism $(x_1, x_2) \mapsto (\tau(x_1), \tau(x_2))$ of $\mathcal{O} \perp \mathcal{O}$ on **private** basis:

$$\mathrm{Tr}(\langle \tau(\vec{x}), \tau(\vec{y}) \rangle) = \mathrm{Tr}(\tau(\overline{x_1} y_1 + \overline{x_2} y_2)) = \mathrm{Tr}(\langle \vec{x}, \vec{y} \rangle).$$

Its minimal polynomial is $(X - 1)(X + 1)$.

Corresponding automorphism on **public** Q is

$$B^{-1} \circ \tau \circ B = V \circ \tau \quad \text{where} \quad V = B^{-1} \tau(B).$$

Goal: Compute V from public data.

Linear constraints on automorphisms

- τ is a Galois automorphism of order 2 of $K = \mathbb{Q}(\zeta_e)$. (e.g. $x \mapsto \overline{x}$)
- $Q = B^* B$ with Q the public quadratic form and B the private isomorphism.
- $V = B^{-1}\tau(B)$ is our target.

Note: For 2×2-matrices of fixed determinant, inversion is linear operation:

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \Rightarrow \quad M^{-1} = \frac{\mathbf{adj}(M)}{\det(M)} \quad \text{where} \quad \mathbf{adj}(M) = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Constraint 1 (τ has order 2)

From $V \cdot \tau(V) = B^{-1} \cdot \tau(B) \cdot \tau(B)^{-1} \cdot \tau^2(B) = 1$ we obtain

$$\boxed{V = \mathbf{adj}(\tau(V))}$$

a K^τ-linear constraint.

Linear constraints on automorphisms

- τ is a Galois automorphism of order 2 of $K = \mathbb{Q}(\zeta_e)$. (e.g. $x \mapsto \overline{x}$)
- $Q = B^* B$ with Q the public quadratic form and B the private isomorphism.
- $V = B^{-1}\tau(B)$ is our target satisfying $V = \mathbf{adj}(\tau(V))$.

Constraint 2 (τ is an automorphism)

From

$$V^* Q V = \tau(B)^* \cdot B^{-*} \cdot B^* \cdot B \cdot B^{-1} \cdot \tau(B) = \tau(B)^* \tau(B) = \tau(Q)$$

we obtain

$$\boxed{V = Q^{-1} \cdot \mathbf{adj}(V^*) \cdot \tau(Q)}$$

a K^γ-linear constraint for fixed Q, where γ is complex conjugation.

Lattice of matrices

- τ is a Galois automorphism of order 2 of $K = \mathbb{Q}(\zeta_e)$. (e.g. $x \mapsto \overline{x}$)
- $Q = B^* B$ with Q the public quadratic form and B the private isomorphism.
- $V = B^{-1}\tau(B)$ is our target satisfying $V = \mathbf{adj}(\tau(V)) = Q^{-1} \cdot \mathbf{adj}(V^*) \cdot \tau(Q)$.
- $F = K^{\tau,\gamma}$, where γ is complex conjugation.

Suppose n is the $\mathbb{Z}$-rank of $\mathcal{O} \perp \mathcal{O}$ and $\tau \neq \gamma$.

The attack:

- Constraints on V define a $\mathcal{O}_F$-submodule $\mathcal{M} \subseteq \mathrm{Mat}_2(\mathcal{O})$ of $\mathbb{Z}$-rank $n/2$.
- $\langle M, N \rangle := \det(M+N) - \det(M) - \det(N)$ defines a $\mathcal{O}_F$-quadratic form on $\mathcal{M}$.
- V is a shortest vector of $\mathcal{M}$.
- Solve SVP on $\mathcal{M}$ to obtain automorphism τ of Q.
- Solve LIP on Q by reducing to SVP on in rank $n/2$ using τ.

Lessons

What have we learnt from Straznickas–Weis:

- Galois automorphisms of order $\mathbf{2}$ are subject to linear constraints.
- The $\mathcal{O}$-rank of $\mathrm{Mat}_{\mathbf{2}}(\mathcal{O})$ is not too large compared to $\mathcal{O}^{\mathbf{2}}$.
- Subspace of $\mathrm{Mat}_{\mathbf{2}}(\mathcal{O})$ has a natural quadratic form.

These combine to reduce LIP from $\mathcal{O}^{\mathbf{2}}$ to a lattice in $\mathrm{Mat}_{\mathbf{2}}(\mathcal{O})$ of $\mathbf{1/2}$ the dimension.

Question: Is increasing the rank to **3** or **4** sufficient mitigation?

The Second Attack: Luo et al

Brief overview (Luo et al)

- Constructs similar 'matrix lattice' as Straznickas–Weis.
- Identifies 'matrix lattice' with symmetric square $\mathbf{Sym}^2(\mathcal{O}^2)$.
- Automorphism is $\mathcal{O}$-module automorphism $(x, y) \mapsto (\zeta y, \overline{\zeta} x)$ of order 2.

Comparison

	Straznickas–Weis	**Luo et al**
Automorphism	Galois of order 2	$\mathcal{O}$-module of order $\mathbf{2}$
Matrix lattice rank	$\mathbf{1/2}$ or $\mathbf{3/4}$	$\mathbf{3/4}$
Find automorphism	SVP in matrix lattice	SVP in matrix lattice
Find isomorphism	SVP in automorphism eigenspace rank $\mathbf{1/2}$ [GP25]	poly-time directly from eigenspace [LJJPW25]

Least common generalization

Definition

Let $\mathbf{\Lambda}$ be an $\mathcal{O}$-module lattice. A *semilinear automorphism* of $\mathbf{\Lambda}$ is a map $f : \mathbf{\Lambda} \to \mathbf{\Lambda}$ for which there exists a $\tau \in \mathbf{Aut}(\mathcal{O})$ such that $(\forall x \in \mathcal{O},\ v, w \in \mathbf{\Lambda})$

$$f(xv + w) = \tau(x)f(v) + f(w) \quad \text{and} \quad \langle f(v), f(w)\rangle = \tau(\langle v, w\rangle)$$

(E.g: $\tau =$ complex conjugation. $\tau = \mathbf{id}$ gives normal automorphism)

Attack:

If $\mathbf{\Lambda}$ of $\mathcal{O}$-rank $\mathbf{2}$ has order-$\mathbf{2}$ semilinear automorphism, then computable with

$$\text{security reduction factor} = \begin{cases} \mathbf{3/4} & \text{if } \tau = \mathbf{id}\text{, complex conjugation} \\ \mathbf{1/2} & \text{otherwise} \end{cases}$$

Rank 4

- $\boldsymbol{L}$ is $\mathcal{O}$-module lattice of rank $\mathbf{4}$.
- $\boldsymbol{\Lambda := L \wedge L}$ has $\mathcal{O}$-module rank $\binom{4}{2} = \mathbf{6}$.
- Subspace of tensor product defines module quadratic form structure:

$$\boldsymbol{\Lambda} \hookrightarrow \operatorname{span}\{\boldsymbol{a \otimes b - b \otimes a} \mid \boldsymbol{a, b \in L}\} \subseteq \boldsymbol{L \otimes L}$$

- Wedge defines a symmetric bilinear form:

$$\boldsymbol{H : \Lambda \times \Lambda \to \bigwedge^4 L \hookrightarrow K}$$

$$\boldsymbol{(a \wedge b), (c \wedge d) \mapsto a \wedge b \wedge c \wedge d = \det(a, b, c, d)}$$

Automorphism: Their 'difference' $\boldsymbol{\Delta}$, defined by $\boldsymbol{H(\Delta x, y) = \langle x, y \rangle \quad (\forall x, y)}$.

Dimension reduction: Factor $\mathbf{3/4}$.

Question: Can we get factor $\mathbf{1/2}$ by using semilinearity?

The Third Attack: Mureau–Pellet-Mary

Brief overview (Mureau–Pellet-Mary)

- $\omega : \mathcal{O}^2 \to \mathcal{O}^2$ is given by $(x, y) \mapsto (\overline{y}, -\overline{x})$.

  - Identifies the 'matrix lattice' with

    $$\Lambda^0 = \{\text{trace-}0 \text{ elements of quaternion algebra } \mathcal{O}[\omega]\}.$$

  - Reduces to isomorphism of Λ^0
    (more structure than just a lattice, so should be easier)
  - However, solves Λ^0 isomorphism with the plain reduction to SVP.
  - Reduces dimension by factor $3/4$.

Endomorphisms

Why consider the algebraic structure of 'matrix lattice'.

Example

Let $\mathbf{\Lambda}$ be defined by $\mathcal{O} = \mathbb{Z}$, $B = \begin{pmatrix} 11 & 5+\sqrt{3} \\ 11 & 5-\sqrt{3} \end{pmatrix}$, $Q = B^*B = \begin{pmatrix} 242 & 110 \\ 110 & 56 \end{pmatrix}$.

Then $\mathbf{Aut}(\mathbf{\Lambda}) = \{\pm 1\}$. However, $\mathbf{\Lambda}$ has *endomorphism*

$$\alpha = \begin{pmatrix} \sqrt{3} & 0 \\ 0 & -\sqrt{3} \end{pmatrix}, \quad \text{namely} \quad \|\alpha \boldsymbol{v}\| = \sqrt{3} \cdot \|\boldsymbol{v}\| \quad \text{and} \quad \alpha\mathbf{\Lambda} \subseteq \mathbf{\Lambda}.$$

Thus $\mathbf{\Lambda}$ is rank-1 $\mathbb{Z}[\sqrt{3}]$-lattice. Given α, LIP solved with Gentry–Szydlo.

- If α has reducible minpoly, then eigenspace attack.
- We should understand and bound endomorphism ring of lattice.

Future

Rank 3

Attack vector

$\boldsymbol{\Lambda}$ has module-rank **2** or **4**.

Idea 1: Use $\boldsymbol{\Lambda} = \mathcal{O}^{\perp 3}$ instead of $\mathcal{O}^{\perp 2}$.

Question 1: Can module-rank **4** attack achieve $\mathbf{1/2}$ rank reduction?

Can publicly embed $\boldsymbol{\Lambda} \hookrightarrow \boldsymbol{\Lambda} \perp \mathcal{O}$ into rank **4**.
If yes, then $\mathbf{2/3}$ rank reduction in rank **3** for free.

Idea 2: Additionally, choose $\boldsymbol{K}$ without order-2 Galois.

E.g.:
- For $\boldsymbol{p \equiv 3 \pmod 4}$ prime, $\mathbb{Q}(\zeta_p)^+$ has no order-2 Galois.
- $\mathbb{Z}^{\perp 3(p-1)/2}$ is rank-3 $\mathbb{Q}(\zeta_p)^+$-lattice.

Question 2: Is rank-3 real case susceptible to poly-time attack (cf. [APW25])?

Rank 2

Attack vector

$\mathbf{\Lambda}$ has semi-linear automorphism of order **2**.

Idea 3: Choose $\mathbf{\Lambda}$ without such automorphisms.

Note: $\mathbf{\Lambda} = \mathfrak{a} \perp \mathfrak{b}$ has $(x, y) \mapsto (-x, y)$.

Question 3a: Are such $\mathcal{O}$-lattices $\mathbf{\Lambda}$ as secure as corresponding $\mathbb{Z}$-lattice $\mathbf{\Lambda}$?

Question 3b: Can such $\mathbf{\Lambda}$ have geometry suitable for an efficient scheme?

Attack vector (?)

$\mathbf{\Lambda}$ has additional endomorphisms.

Idea 4: Choose $\mathbf{\Lambda}$ with $\mathbf{End}(\mathbf{\Lambda}) = \mathcal{O}$.

Note: true for random lattices

Conclusion

Straznickas–Weis:	Best security reduction: factor $\mathbf{1/2}$
Luo et al:	Dimension 4 generalization
Mureau–Pellet-Mary:	Additional algebraic structure that could be exploited

These results probably combine

Question: What's next?

- Rank-3 module lattices over a totally real field of odd degree?
- Rank-2 module lattices without semilinear automorphisms of order 2?

Conjecture: Rank **2** cryptography is possible, once we figure out required constraints.

Thank you for your attention