

On Module Lattices with Galois-Symmetries: what you see is not what you get

Ronald Cramer, **Daniël van Gent**, Andrea Lesavourey, and Alice Pellet-Mary.



Universiteit
Leiden
The Netherlands



Centrum Wiskunde & Informatica

Lattices

Definition

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

Represent lattice by a basis $B \in \mathbf{GL}_n(\mathbb{R})$.

Lattices

Definition

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

Represent lattice by a basis $B \in \mathbf{GL}_n(\mathbb{R})$.

Lattices are used for cryptography.

Example

Fix a good lattice basis $B \in \mathbf{GL}_n(\mathbb{R})$.

Secret key: Basis transformation $T \in \mathbf{GL}_n(\mathbb{Z})$.

Public key: Gram matrix $(BT)^T(BT)$ with respect to bad basis.

Lattices

Definition

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

Represent lattice by a basis $B \in \text{GL}_n(\mathbb{R})$.

Lattices are used for cryptography.

Example

Fix a good lattice basis $B \in \text{GL}_n(\mathbb{R})$.

Secret key: Basis transformation $T \in \text{GL}_n(\mathbb{Z})$.

Public key: Gram matrix $(BT)^T(BT)$ with respect to bad basis.

Issue

Keys require $\Theta(n^2)$ integers/reals to specify.[†]

Key compression

Idea: impose (public) structure to reduce entropy.

Example

Consider the *circulant matrices*

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

If we choose $\mathbf{T} \in \mathcal{C}$, then we require only $\Theta(n)$ integers to specify it.

Key compression

Idea: impose (public) structure to reduce entropy.

Example

Consider the *circulant matrices*

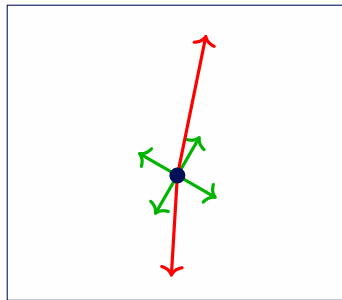
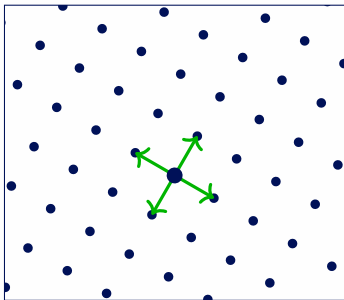
$$\mathcal{C} := \left\{ \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a_n & a_1 & a_2 & \dots & a_{n-1} \\ \vdots & & & & \vdots \\ a_2 & a_3 & a_4 & \dots & a_1 \end{pmatrix} \mid a_1, \dots, a_n \in \mathbb{Z} \right\}.$$

If we choose $\mathbf{T} \in \mathcal{C}$, then we require only $\Theta(n)$ integers to specify it.

Issue

Invertible elements of $\mathcal{C}$ preserve $\pm(1, 1, \dots, 1)^\top$.

Shortest Vector Problem (SVP)



Heuristic

Solving SVP for lattice Λ with 'bad basis' is hard if

$$\lambda_1(\Lambda) \approx \det(\Lambda)^{1/n}$$

Approximate SVP

We want SVP approximation to be hard as well:

Definition

Let $\gamma \geq 1$. The γ -approximate Shortest Vector Problem (γ -SVP) asks to compute $\mathbf{v} \in \Lambda \setminus \{\mathbf{0}\}$ such that $\|\mathbf{v}\| \leq \gamma \cdot \lambda_1(\Lambda)$.

Approximate SVP

We want SVP approximation to be hard as well:

Definition

Let $\gamma \geq 1$. The γ -approximate Shortest Vector Problem (γ -SVP) asks to compute $\mathbf{v} \in \Lambda \setminus \{0\}$ such that $\|\mathbf{v}\| \leq \gamma \cdot \lambda_1(\Lambda)$.

Theorem

For fixed γ , best known algorithm solves γ -SVP in time $\exp(O(n))$ up to polynomial factors, where n is the rank of Λ .

Approximate SVP

We want SVP approximation to be hard as well:

Definition

Let $\gamma \geq 1$. The γ -approximate Shortest Vector Problem (γ -SVP) asks to compute $\mathbf{v} \in \Lambda \setminus \{\mathbf{0}\}$ such that $\|\mathbf{v}\| \leq \gamma \cdot \lambda_1(\Lambda)$.

Theorem

For fixed γ , best known algorithm solves γ -SVP in time $\exp(O(n))$ up to polynomial factors, where n is the rank of Λ .

Issue (cont.)

If $\Lambda = \mathbb{Z}^n$ and $\mathbf{T}$ is circulant, then $(1, 1, \dots, 1)$ is a public vector of length $\sqrt{n}$. Solves approximate SVP in polytime; Could impact security if based around SVP.

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 $T \in GL_n(\mathbb{Z}) = \text{Aut}_{\mathbb{Z}}(\mathbb{Z}^n)$ is a $\mathbb{Z}$ -module automorphism.

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 $T \in GL_n(\mathbb{Z}) = \text{Aut}_{\mathbb{Z}}(\mathbb{Z}^n)$ 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

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

Then $T \in GL_n(\mathbb{Z})$ circulant $\Leftrightarrow T \in \text{Aut}_R(\mathbb{Z}^n)$.

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 $T \in \text{GL}_n(\mathbb{Z}) = \text{Aut}_{\mathbb{Z}}(\mathbb{Z}^n)$ 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

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

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

Issue (cont.)

Multiplication by X is a public automorphism with reducible minimal polynomial

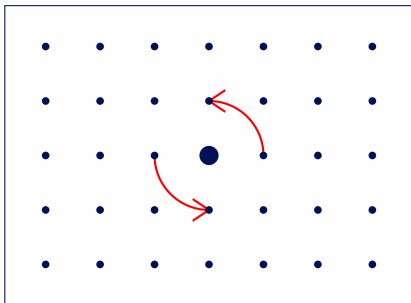
$$X^n - 1 = (X - 1)(X^{n-1} + \dots + 1), \quad \text{and} \quad (1, \dots, 1) \in \ker(X - 1).$$

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

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

Suppose:

- we apply the same compression to the public key (quadratic form)
- all matrices are rational for simplicity

Module lattices

Suppose:

- we apply the same compression to the public key (quadratic form)
- all matrices are rational for simplicity

Definition

Let K be a number field and $\mathcal{O}$ its ring of integers.

An $\mathcal{O}$ -module lattice is a finitely generated $\mathcal{O}$ -submodule of K^n for some $n \geq 0$.

We may interpret it as a lattice by taking quadratic form

$$(x, y) \in K^n \times K^n \mapsto \sum_{f: K \rightarrow \mathbb{C}} \sum_{i=1}^n \overline{f(x_i)} f(y_i) \approx \text{Tr}_{K/\mathbb{Q}}(x^* \cdot y).$$

Main question of module lattice cryptography:

Are structured lattices secure[†]?

(†) Do hard problems (SVP/LIP/etc) become significantly easier given this structure?

Main question of module lattice cryptography:

Are structured lattices secure[†]?

([†]) Do hard problems (SVP/LIP/etc) become significantly easier given this structure?

Warning (Gentry–Szydło)

Can solve module Lattice Isomorphism Problem (mLIP) in poly-time when $\Lambda \subseteq K$.

Security

Main question of module lattice cryptography:

Are structured lattices secure[†]?

(†) Do hard problems (SVP/LIP/etc) become significantly easier given this structure?

Warning (Gentry–Szydlo)

Can solve module Lattice Isomorphism Problem (mLIP) in poly-time when $\Lambda \subseteq K$.

Warning (Straznickas–Weis)

mLIP on NIST candidate HAWK's lattice reduces to SVP in half-dimensional lattice.

Conclusion: This is a very valid question.

Our results consider the hardness of SVP

Galois invariant lattices

- $K \subseteq L$ is an extension of number fields
- $G = \{\sigma \in \text{Aut}(L) \mid (\forall x \in K) \sigma(x) = x\}$ is the group of L/K
- $\Lambda \subseteq L^n$ a $\mathcal{O}_L$ -module lattice

Definition

Let $\sigma \in G$ act on L^n coordinate-wise. Then Λ is

- *setwise G -invariant* if $\sigma(\Lambda) = \Lambda$ for all $\sigma \in G$.
- *pointwise G -invariant* if $\Lambda^G := \{x \in \Lambda \mid (\forall \sigma \in G) \sigma(x) = x\}$ equals Λ .

Galois invariant lattices

- $K \subseteq L$ is an extension of number fields
- $G = \{\sigma \in \text{Aut}(L) \mid (\forall x \in K) \sigma(x) = x\}$ is the group of L/K
- $\Lambda \subseteq L^n$ a $\mathcal{O}_L$ -module lattice

Definition

Let $\sigma \in G$ act on L^n coordinate-wise. Then Λ is

- *setwise G -invariant* if $\sigma(\Lambda) = \Lambda$ for all $\sigma \in G$.
- *pointwise G -invariant* if $\Lambda^G := \{x \in \Lambda \mid (\forall \sigma \in G) \sigma(x) = x\}$ equals Λ .

(Note: Λ pointwise G -invariant implies $\Lambda = 0$ or $G = 1$)

Warning (Boudgoust–Gachon–Pellet–Mary)

Setwise G -invariant lattices are not secure when $n = 1$ and $G \neq 1$.

Example

- $K = \mathbb{Q}$ and $L = \mathbb{Q}(i)$
- $G = \{1, \tau\} = \{\text{id}, \text{complex conjugation}\}$ is the group of L/K
- $\Lambda = \mathfrak{p} = (1 + i) \cdot \mathbb{Z}[i]$ a $\mathbb{Z}[i]$ -module lattice

Example

(setwise G -invariance) $\tau(1 + i) = 1 - i = (1 + i) \cdot (-i) \Rightarrow \tau(\Lambda) \subseteq \Lambda.$

(pointwise G -invariants) $\Lambda^G = \Lambda \cap K = 2 \cdot \mathbb{Z}.$

Example

- $K = \mathbb{Q}$ and $L = \mathbb{Q}(i)$
- $G = \{1, \tau\} = \{\text{id}, \text{complex conjugation}\}$ is the group of L/K
- $\Lambda = \mathfrak{p} = (1 + i) \cdot \mathbb{Z}[i]$ a $\mathbb{Z}[i]$ -module lattice

Example

(setwise G -invariance) $\tau(1 + i) = 1 - i = (1 + i) \cdot (-i) \Rightarrow \tau(\Lambda) \subseteq \Lambda.$

(pointwise G -invariants) $\Lambda^G = \Lambda \cap K = 2 \cdot \mathbb{Z}.$

Comparison:

	Λ	Λ^G
$\mathbb{Z}$ -rank	2	1
shortest vector	$1 + i$	2
λ_1	$\sqrt{2}$	2
$\lambda_1 \cdot \det^{-1/n}$	1	1

At cost of losing factor $\sqrt{2}$ in λ_1 , we may halve lattice dimension for approximate SVP.

Definition

For $\gamma \geq 1$ and lattice Λ , the γ -approximate Hermite Shortest Vector Problem (γ -HSVP) asks to compute $\mathbf{v} \in \Lambda \setminus \{\mathbf{0}\}$ such that $\|\mathbf{v}\| \leq \gamma \cdot \det(\Lambda)^{1/\text{rk } \Lambda}$.

Definition

For $\gamma \geq 1$ and lattice Λ , the γ -approximate Hermite Shortest Vector Problem (γ -HSVP) asks to compute $\mathbf{v} \in \Lambda \setminus \{\mathbf{0}\}$ such that $\|\mathbf{v}\| \leq \gamma \cdot \mathbf{det}(\Lambda)^{1/\text{rk } \Lambda}$.

Theorem

There is a polynomial-time algorithm that on input

- $\mathcal{O}_K$ for some number field K
- an $\mathcal{O}_K$ -module lattice Λ of $\mathcal{O}_K$ -rank $n > 0$ and with unramified discriminant computes
- $G = \{\sigma \in \text{Aut}(K) \mid \sigma(\Lambda) = \Lambda\}$ and K^G
- a reduction from γ -HSVP on Λ to γ -HSVP on some rank $n \cdot [K^G : \mathbb{Q}]$ lattice.

Why ramification?

We use the auxillary result:

Theorem

Let L/K be Galois with group G and $M \subseteq \mathcal{O}_L^n$ with unramified discriminant. The following are equivalent:

- M is setwise G -stable
- $\mathcal{O}_L \cdot (M \cap K^n) = M$
- there exist setwise G -stable rank-1 submodules $M_1, \dots, M_n \subseteq M$ such that $M = M_1 \oplus \dots \oplus M_n$.

Why ramification?

We use the auxillary result:

Theorem

Let L/K be Galois with group G and $M \subseteq \mathcal{O}_L^n$ with unramified discriminant. The following are equivalent:

- M is setwise G -stable
- $\mathcal{O}_L \cdot (M \cap K^n) = M$
- there exist setwise G -stable rank-1 submodules $M_1, \dots, M_n \subseteq M$ such that $M = M_1 \oplus \dots \oplus M_n$.

It fails in the ramified case:

Example

Let $L = \mathbb{Q}(i)$ and $K = \mathbb{Q}$. Then $M = \mathcal{O}_L \cdot (1, i) \oplus \mathcal{O}_L \cdot (1, -i)$ is not the sum of two G -stable rank-1 submodules.

Return of the module

- $K \subseteq L$ is an extension of number fields
- $G = \{\sigma \in \text{Aut}(L) \mid (\forall x \in K) \sigma(x) = x\}$ is the group of L/K
- $\Lambda \subseteq L^n$ a $\mathcal{O}_L$ -module lattice

Let $L\langle G \rangle$ be the L -vector space with basis G and ring structure extending

$$(a\sigma) \cdot (b\tau) = (a\sigma(b)) \cdot (\sigma\tau) \quad (\forall a, b \in L, \forall \sigma, \tau \in G)$$

This is the *twisted group ring* of L and G . Similarly define $\mathcal{O}_L\langle G \rangle \subseteq L\langle G \rangle$.

Return of the module

- $K \subseteq L$ is an extension of number fields
- $G = \{\sigma \in \text{Aut}(L) \mid (\forall x \in K) \sigma(x) = x\}$ is the group of L/K
- $\Lambda \subseteq L^n$ a $\mathcal{O}_L$ -module lattice

Let $L\langle G \rangle$ be the L -vector space with basis G and ring structure extending

$$(a\sigma) \cdot (b\tau) = (a\sigma(b)) \cdot (\sigma\tau) \quad (\forall a, b \in L, \forall \sigma, \tau \in G)$$

This is the *twisted group ring of L and G* . Similarly define $\mathcal{O}_L\langle G \rangle \subseteq L\langle G \rangle$.

Lemma

If Λ is setwise G -stable, then Λ is an $\mathcal{O}_L\langle G \rangle$ -module.

Issue

$\mathcal{O}_L\langle G \rangle$ has zero-divisors: $(1 - \sigma) \cdot \sum_{\tau \in G} \tau = 0$. (cf. circulant case)

Conclusion

- Describing public lattice structure in terms of modules helps cryptanalysis.
- For security, the ring should have no zero-divisors.
- In particular, public Galois action is insecure.

Thank you for your attention

