Méthodes algébriques appliquées à la recherche d'isométries de réseaux structurés

Guilhem Mureau (IMB/Inria, Bordeaux)

Journées C2, Pornichet

3 Avril 2025

Un peu de contexte...

$\rightarrow$ En 2021, première utilisation du Problème de l'Isomorphisme de Réseaux (LIP) en cryptographie ([1] Ducas, van Woerden).

Un peu de contexte...

$\rightarrow$ En 2021, première utilisation du Problème de l'Isomorphisme de Réseaux (LIP) en cryptographie ([1] Ducas, van Woerden).

$\rightarrow$ En 2022, une variante algébrique de LIP (module-LIP) et un schéma de signature, HAWK, basé sur ce problème ([2] Ducas, Postlethwaite, Pulles, van Woerden).

Un peu de contexte...

$\rightarrow$ En 2021, première utilisation du Problème de l'Isomorphisme de Réseaux (LIP) en cryptographie ([1] Ducas, van Woerden).

$\rightarrow$ En 2022, une variante algébrique de LIP (module-LIP) et un schéma de signature, HAWK, basé sur ce problème ([2] Ducas, Postlethwaite, Pulles, van Woerden).

$\rightarrow$ En 2023 et 2024, de premiers résultats de cryptanalyse sur module-LIP [3] et [4].

Un peu de contexte...

$\rightarrow$ En 2021, première utilisation du Problème de l'Isomorphisme de Réseaux (LIP) en cryptographie ([1] Ducas, van Woerden).

$\rightarrow$ En 2022, une variante algébrique de LIP (module-LIP) et un schéma de signature, HAWK, basé sur ce problème ([2] Ducas, Postlethwaite, Pulles, van Woerden).

$\rightarrow$ En 2023 et 2024, de premiers résultats de cryptanalyse sur module-LIP [3] et [4].

1. LIP et module-LIP

2. Résultats et Perspectives

LIP et module-LIP

LIP et module-LIP

$\rightarrow$ Un réseau dans $\mathbb{R}^n$ est l'ensemble des combinaisons entières de n vecteurs linéairement indépendants $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^n$:

$$\mathcal{L} = \mathbb{Z}\mathbf{b}_1 + \cdots + \mathbb{Z}\mathbf{b}_n = \left\{ \sum_{i=1}^{n} x_i \mathbf{b}_i \mid x_i \in \mathbb{Z} \right\}.$$

On dit que $(\mathbf{b}_1 | \cdots | \mathbf{b}_n) \in \mathbf{GL}_n(\mathbb{R})$ est une base de $\mathcal{L}$.

LIP et module-LIP

$\rightarrow$ Un réseau dans $\mathbb{R}^n$ est l'ensemble des combinaisons entières de n vecteurs linéairement indépendants $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^n$:

$$\mathcal{L} = \mathbb{Z}\mathbf{b}_1 + \cdots + \mathbb{Z}\mathbf{b}_n = \left\{ \sum_{i=1}^{n} x_i \mathbf{b}_i \mid x_i \in \mathbb{Z} \right\}.$$

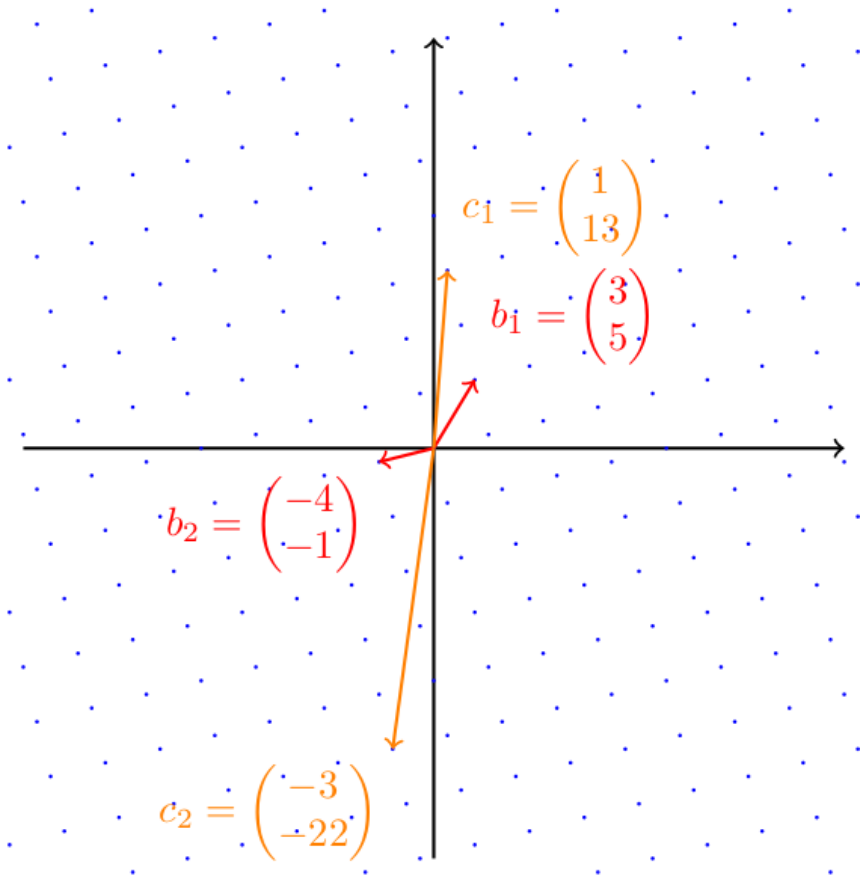
On dit que $(\mathbf{b}_1 | \cdots | \mathbf{b}_n) \in \mathbf{GL}_n(\mathbb{R})$ est une base de $\mathcal{L}$.

$\rightarrow$ On sait caractériser les bases d'un même réseau :

$\mathbf{B}, \mathbf{C} \in \mathbf{GL}_n(\mathbb{R})$ engendrent le même réseau $\iff \exists\, \mathbf{U} \in \mathbf{GL}_n(\mathbb{Z})$ (unimodulaire) telle que

$$\mathbf{C} = \mathbf{BU}.$$

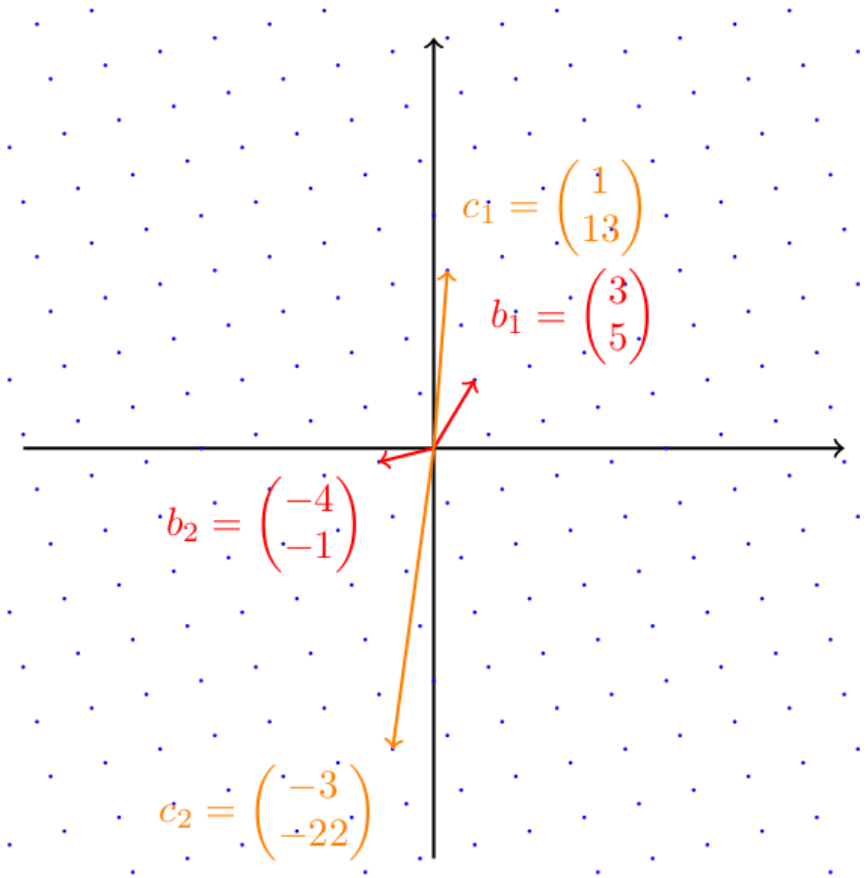
LIP et module-LIP



$\rightarrow$ Un exemple avec $\mathbf{B} = \begin{pmatrix} 3 & -4 \\ 5 & -1 \end{pmatrix}$ et

$\mathbf{C} = \begin{pmatrix} 1 & -3 \\ 13 & -22 \end{pmatrix}$.

LIP et module-LIP

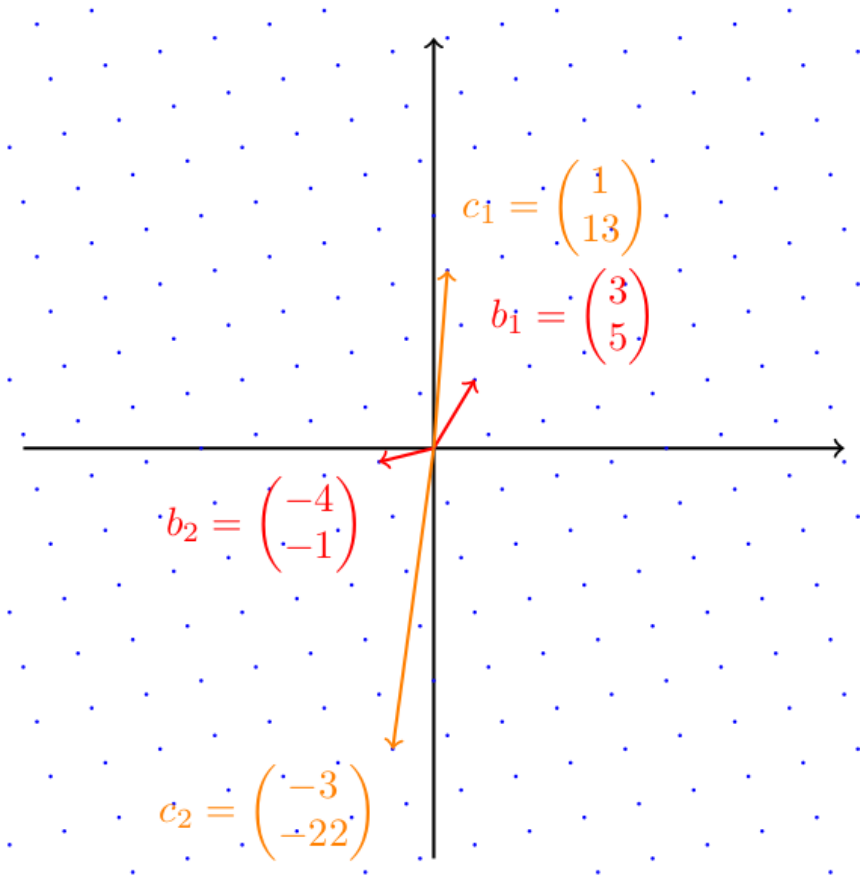


$\rightarrow$ Un exemple avec $\mathbf{B} = \begin{pmatrix} 3 & -4 \\ 5 & -1 \end{pmatrix}$ et $\mathbf{C} = \begin{pmatrix} 1 & -3 \\ 13 & -22 \end{pmatrix}$. On vérifie alors

$$\mathbf{C} = \mathbf{B}\mathbf{U},$$

avec $\mathbf{U} = \begin{pmatrix} 3 & -5 \\ 2 & -3 \end{pmatrix} \in \mathbf{GL}_2(\mathbb{Z})$.

LIP et module-LIP



$\rightarrow$ Un exemple avec $\mathbf{B} = \begin{pmatrix} 3 & -4 \\ 5 & -1 \end{pmatrix}$ et $\mathbf{C} = \begin{pmatrix} 1 & -3 \\ 13 & -22 \end{pmatrix}$. On vérifie alors

$$\mathbf{C} = \mathbf{BU},$$

avec $\mathbf{U} = \begin{pmatrix} 3 & -5 \\ 2 & -3 \end{pmatrix} \in \mathbf{GL}_2(\mathbb{Z})$.

$\rightarrow$ $\mathbf{B}$ est une "bonne" base (vecteurs courts et presque orthogonaux) alors que $\mathbf{C}$ est une "mauvaise" base.

LIP et module-LIP

$\rightarrow$ Deux réseaux $\mathcal{L}$ et $\mathcal{M}$ dans $\mathbb{R}^n$ sont isomorphes s'il existe $\Theta \in \mathrm{O}_n(\mathbb{R})$ telle que

$$\mathcal{M} = \Theta \cdot \mathcal{L} := \{\Theta \cdot \mathbf{v} \,|\, \mathbf{v} \in \mathcal{L}\}.$$

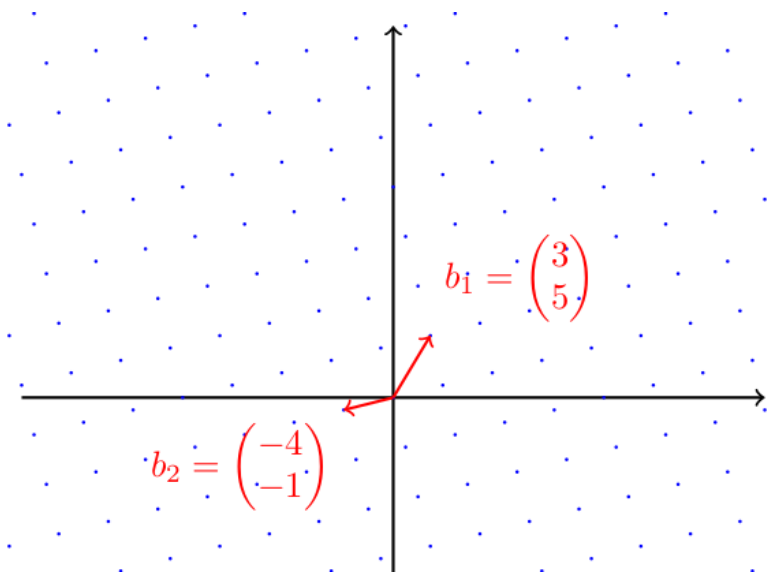
Moralement, "$\mathcal{M}$ est une rotation et/ou symétrie de $\mathcal{L}$".

LIP et module-LIP

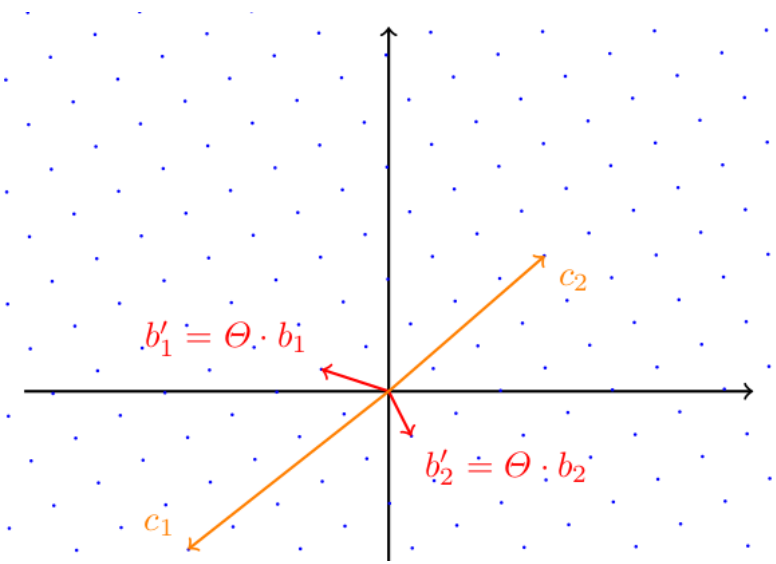
$\rightarrow$ Deux réseaux $\mathcal{L}$ et $\mathcal{M}$ dans $\mathbb{R}^n$ sont isomorphes s'il existe $\Theta \in \mathrm{O}_n(\mathbb{R})$ telle que

$$\mathcal{M} = \Theta \cdot \mathcal{L} := \{\Theta \cdot \mathbf{v} \,|\, \mathbf{v} \in \mathcal{L}\}.$$

Moralement, "$\mathcal{M}$ est une rotation et/ou symétrie de $\mathcal{L}$".



Une bonne base **B** de $\mathcal{L}$.



Une bonne base Θ**B** et une mauvaise base **C** d'un réseau isomorphe $\mathcal{M}$.

LIP et module-LIP

Lattice Isomophism Problem

Étant données $\mathbf{B}$ et $\mathbf{C}$ comme avant, trouver $\Theta \in \mathrm{O}_n(\mathbb{R})$ et/ou $\mathbf{U} \in \mathbf{GL}_n(\mathbb{Z})$ telles que

$$\mathbf{C} = \Theta\mathbf{B}\mathbf{U}. \tag{1}$$

LIP et module-LIP

Lattice Isomophism Problem

Étant données $\mathbf{B}$ et $\mathbf{C}$ comme avant, trouver $\Theta \in \mathrm{O}_n(\mathbb{R})$ et/ou $\mathbf{U} \in \mathbf{GL}_n(\mathbb{Z})$ telles que

$$\mathbf{C} = \Theta \mathbf{B} \mathbf{U}. \tag{1}$$

LIP (variante décisionnelle)

Étant données des (bases de) réseaux $\mathcal{L}$ et $\mathcal{M}$, décider si les réseaux sont isomorphes.
De façon équivalente, décider s'il existe une relation (1).

LIP et module-LIP

Lattice Isomophism Problem

Étant données $\mathbf{B}$ et $\mathbf{C}$ comme avant, trouver $\Theta \in \mathrm{O}_n(\mathbb{R})$ et/ou $\mathbf{U} \in \mathbf{GL}_n(\mathbb{Z})$ telles que

$$\mathbf{C} = \Theta \mathbf{B} \mathbf{U}. \tag{1}$$

LIP (variante décisionnelle)

Étant données des (bases de) réseaux $\mathcal{L}$ et $\mathcal{M}$, décider si les réseaux sont isomorphes.
De façon équivalente, décider s'il existe une relation (1).

$\rightarrow$ En se basant sur la variante décisionelle, Ducas et van Woerden construisent un schéma d'identification et un KEM.

LIP et module-LIP

Lattice Isomophism Problem

Étant données $\mathbf{B}$ et $\mathbf{C}$ comme avant, trouver $\Theta \in \mathrm{O}_n(\mathbb{R})$ et/ou $\mathbf{U} \in \mathbf{GL}_n(\mathbb{Z})$ telles que

$$\mathbf{C} = \Theta \mathbf{B} \mathbf{U}. \tag{1}$$

LIP (variante décisionnelle)

Étant données des (bases de) réseaux $\mathcal{L}$ et $\mathcal{M}$, décider si les réseaux sont isomorphes.
De façon équivalente, décider s'il existe une relation (1).

$\rightarrow$ En se basant sur la variante décisionelle, Ducas et van Woerden construisent un schéma d'identification et un KEM.

$\rightarrow$ État de l'art ? Des algorithmes peu efficaces : besoin de calculer des vecteurs courts (Plesken-Souvignier, Haviv-Regev, van Woerden).

LIP et module-LIP

$\rightarrow$ LIP avec des réseaux de grandes dimensions et avec une représentation compacte ?

LIP et module-LIP

$\rightarrow$ LIP avec des réseaux de grandes dimensions et avec une représentation compacte ?

$\rightarrow$ K un corps de nombres (une extension finie de $\mathbb{Q}$) et $\mathbb{Z}_K$ son anneau d'entiers.
Par exemple, $K = \mathbb{Q}[X]/(X^{2^r} + 1)$ et $\mathbb{Z}_K = \mathbb{Z}[X]/(X^{2^r} + 1)$, ou même $K = \mathbb{Q}$ et $\mathbb{Z}_K = \mathbb{Z}$.

LIP et module-LIP

$\rightarrow$ LIP avec des réseaux de grandes dimensions et avec une représentation compacte ?

$\rightarrow$ K un corps de nombres (une extension finie de $\mathbb{Q}$) et $\mathbb{Z}_K$ son anneau d'entiers.
Par exemple, $K = \mathbb{Q}[X]/(X^{2^r} + 1)$ et $\mathbb{Z}_K = \mathbb{Z}[X]/(X^{2^r} + 1)$, ou même $K = \mathbb{Q}$ et $\mathbb{Z}_K = \mathbb{Z}$.

Soient $n \in \mathbb{N}_{>0}$ et $\mathbf{b_1}, \ldots, \mathbf{b_n} \in K^n$ des vecteurs K-linéairement indépendants. Alors,

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

est un $\mathbb{Z}_K$-réseau de K^n. Si $\dim_{\mathbb{Q}}(K) = d$, on peut voir $\mathcal{L}$ comme un réseau dans $\mathbb{R}^{dn}$.

LIP et module-LIP

module-Lattice Isomorphism Problem

module-LIP $=$ restriction de LIP aux $\mathbb{Z}_K$-réseaux, avec les contraintes $\Theta \in \mathrm{O}_n(K)$ et $\mathbf{U} \in \mathbf{GL}_n(\mathbb{Z}_K)$.

De même, une variante de recherche et une décisionelle.

LIP et module-LIP

module-Lattice Isomorphism Problem

module-LIP = restriction de LIP aux $\mathbb{Z}_K$-réseaux, avec les contraintes $\Theta \in \mathrm{O}_n(K)$ et $\mathbf{U} \in \mathbf{GL}_n(\mathbb{Z}_K)$.
De même, une variante de recherche et une décisionelle.

$\rightarrow$ Un exemple d'intérêt en cryptographie :

$$K = \mathbb{Q}[X]/(X^{2^r}+1) \quad \text{et} \quad \mathcal{H} = \mathbb{Z}_K \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \mathbb{Z}_K \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

La securité de HAWK est liée à la difficulté de module-LIP avec le $\mathbb{Z}_K$-réseau $\mathcal{H}$.

LIP et module-LIP

module-Lattice Isomorphism Problem

module-LIP = restriction de LIP aux $\mathbb{Z}_K$-réseaux, avec les contraintes $\Theta \in \mathrm{O}_n(K)$ et $\mathbf{U} \in \mathbf{GL}_n(\mathbb{Z}_K)$.
De même, une variante de recherche et une décisionelle.

$\rightarrow$ Un exemple d'intérêt en cryptographie :

$$K = \mathbb{Q}[X]/(X^{2^r}+1) \quad \text{et} \quad \mathcal{H} = \mathbb{Z}_K \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \mathbb{Z}_K \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

La securité de HAWK est liée à la difficulté de module-LIP avec le $\mathbb{Z}_K$-réseau $\mathcal{H}$.

$\rightarrow$ Les $\mathbb{Z}_K$-réseaux sont davantages structurés (symétries, propriétés arithmétiques, etc).

Question : Peut-on utiliser cette structure pour résoudre module-LIP plus efficacement ?

Résultats et Perspectives

Résultats et Perspectives

$\rightarrow$ Dans HAWK, on considère $\mathcal{H} = \mathbb{Z}_K \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \mathbb{Z}_K \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ et $\mathbf{B} = \mathbf{Id}$ une (bonne) base de $\mathcal{H}$ et $\mathbf{C} = \Theta\mathbf{B}\mathbf{U} = \Theta\mathbf{U}$ une (mauvaise) base d'un $\mathbb{Z}_K$-réseau isomorphe.[1]

[1] Rappel : $\Theta \in \mathrm{O}_2(K)$ et $\mathbf{U} \in \mathbf{GL}_2(\mathbb{Z}_K)$.

Résultats et Perspectives

$\rightarrow$ Dans HAWK, on considère $\mathcal{H} = \mathbb{Z}_K \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \mathbb{Z}_K \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ et $\mathbf{B} = \mathbf{Id}$ une (bonne) base de $\mathcal{H}$ et $\mathbf{C} = \Theta\mathbf{B}\mathbf{U} = \Theta\mathbf{U}$ une (mauvaise) base d'un $\mathbb{Z}_K$-réseau isomorphe.[1]

$\rightarrow$ On récupère des informations sur $\mathbf{U}$ en prenant la matrice de Gram associée à $\mathbf{C}$:

$$\mathbf{G} := \mathbf{C}^*\mathbf{C}, \quad \text{où } \mathbf{C}^* \text{ est la transposée-conjuguée de } \mathbf{C}.$$

[1] Rappel : $\Theta \in \mathrm{O}_2(K)$ et $\mathbf{U} \in \mathbf{GL}_2(\mathbb{Z}_K)$.

Résultats et Perspectives

$\rightarrow$ Dans HAWK, on considère $\mathcal{H} = \mathbb{Z}_K \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \mathbb{Z}_K \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ et $\mathbf{B} = \mathbf{Id}$ une (bonne) base de $\mathcal{H}$ et $\mathbf{C} = \Theta\mathbf{B}\mathbf{U} = \Theta\mathbf{U}$ une (mauvaise) base d'un $\mathbb{Z}_K$-réseau isomorphe.[1]

$\rightarrow$ On récupère des informations sur $\mathbf{U}$ en prenant la matrice de Gram associée à $\mathbf{C}$:

$$\mathbf{G} := \mathbf{C}^*\mathbf{C}, \quad \text{où } \mathbf{C}^* \text{ est la transposée-conjuguée de } \mathbf{C}.$$

Puisque $\Theta^*\Theta = \mathbf{Id}$, on a en fait

$$\mathbf{G} = \mathbf{U}^*\mathbf{U} = \begin{pmatrix} \overline{u_1} & \overline{u_2} \\ \overline{u_3} & \overline{u_4} \end{pmatrix} \begin{pmatrix} u_1 & u_3 \\ u_2 & u_4 \end{pmatrix} = \begin{pmatrix} u_1\overline{u_1} + u_2\overline{u_2} & \overline{u_1}u_3 + \overline{u_2}u_4 \\ u_1\overline{u_3} + u_2\overline{u_4} & u_3\overline{u_3} + u_4\overline{u_4} \end{pmatrix}.$$

[1] Rappel : $\Theta \in \mathrm{O}_2(K)$ et $\mathbf{U} \in \mathbf{GL}_2(\mathbb{Z}_K)$.

Résultats et Perspectives

$\rightarrow$ Lorsque K est un corps de nombres totalement réel (exemple $K = \mathbb{Q}$), les coefficients diagonaux de $\mathbf{G}$ sont des sommes de deux carrés dans $\mathbb{Z}_K$: $u_1^2 + u_2^2$ et $u_3^2 + u_4^2$.

Résultats et Perspectives

$\rightarrow$ Lorsque K est un corps de nombres totalement réel (exemple $K = \mathbb{Q}$), les coefficients diagonaux de $\mathbf{G}$ sont des sommes de deux carrés dans $\mathbb{Z}_K$: $u_1^2 + u_2^2$ et $u_3^2 + u_4^2$.

On sait retrouver efficacement les coefficients de $\mathbf{U}$ en résolvant des équations de norme.
Outils : arithmétique des idéaux et un algorithme de Gentry et Szydlo pour calculer des générateurs d'idéaux principaux. Ne **casse pas** HAWK.

Travail avec A. Pellet–Mary, H. Pliatsok et A. Wallet (Eurocrypt 2024) [3].

Résultats et Perspectives

$\rightarrow$ À l'inverse quand K est totalement complexe (comme dans HAWK), les coefficients diagonaux de $\mathbf{G}$ sont des sommes de quatre carrés dans $\mathbb{Z}_F$.[2]

[2] Où F est un sous-corps de K. Penser à $K = \mathbb{Q}[X]/(X^2+1)$ et $F = \mathbb{Q}$

Résultats et Perspectives

$\rightarrow$ À l'inverse quand K est totalement complexe (comme dans HAWK), les coefficients diagonaux de $\mathbf{G}$ sont des sommes de quatre carrés dans $\mathbb{Z}_F$.[2]

On voit ces coefficients comme des normes de quaternions sur F. On obtient une réduction de module-LIP vers un problème d'arithmétique sur des quaternions.
Les outils précédents ne s'appliquent pas. Ne **casse pas** HAWK.

Travail avec C. Chevignard, P-A. Fouque, A. Pellet–Mary, A. Wallet (Eurocrypt 2025) [4].

[2] Où F est un sous-corps de K. Penser à $K = \mathbb{Q}[X]/(X^2+1)$ et $F = \mathbb{Q}$

Résultats et Perspectives

$\rightarrow$ Le problème sur les quaternions semble difficile mais il pourrait y avoir une astuce similaire à celle de Gentry et Szydlo. Toute avancée sur ce problème impacterait HAWK.

Résultats et Perspectives

$\rightarrow$ Le problème sur les quaternions semble difficile mais il pourrait y avoir une astuce similaire à celle de Gentry et Szydlo. Toute avancée sur ce problème impacterait HAWK.

$\rightarrow$ Et pour la variante décisionnelle de module-LIP ?

Résultats et Perspectives

$\rightarrow$ Le problème sur les quaternions semble difficile mais il pourrait y avoir une astuce similaire à celle de Gentry et Szydlo. Toute avancée sur ce problème impacterait HAWK.

$\rightarrow$ Et pour la variante décisionnelle de module-LIP ?

On sait tester efficacement si deux $\mathbb{Z}_K$-réseaux sont dans le même genre. Deux réseaux isomorphes sont dans le même genre, mais la réciproque n'est en général pas vraie.

Résultats et Perspectives

$\rightarrow$ Le problème sur les quaternions semble difficile mais il pourrait y avoir une astuce similaire à celle de Gentry et Szydlo. Toute avancée sur ce problème impacterait HAWK.

$\rightarrow$ Et pour la variante décisionnelle de module-LIP ?

On sait tester efficacement si deux $\mathbb{Z}_K$-réseaux sont dans le même genre. Deux réseaux isomorphes sont dans le même genre, mais la réciproque n'est en général pas vraie.

Comment parcourir les classes d'isomorphismes dans un genre ? Calculer des invariants plus fins que le genre peut permettre de décider (genre spinoriel, genre spécial).

Work in progress...

Résumé

$\rightarrow$ Un problème récent en cryptographie, nécessite davantage de cryptanalyse pour comprendre sa difficulté.

Résumé

$\rightarrow$ Un problème récent en cryptographie, nécessite davantage de cryptanalyse pour comprendre sa difficulté.

$\rightarrow$ Des attaques algébriques cassent la variante de recherche pour certains paramètres (modules de rang 2 sur un corps totalement réel).

Résumé

$\rightarrow$ Un problème récent en cryptographie, nécessite davantage de cryptanalyse pour comprendre sa difficulté.

$\rightarrow$ Des attaques algébriques cassent la variante de recherche pour certains paramètres (modules de rang 2 sur un corps totalement réel).

$\rightarrow$ Pour les modules de rang 2 sur un totalement complexe : une connexion avec les algèbres de quaternions et un angle d'attaque possible.

Résumé

$\rightarrow$ Un problème récent en cryptographie, nécessite davantage de cryptanalyse pour comprendre sa difficulté.

$\rightarrow$ Des attaques algébriques cassent la variante de recherche pour certains paramètres (modules de rang 2 sur un corps totalement réel).

$\rightarrow$ Pour les modules de rang 2 sur un totalement complexe : une connexion avec les algèbres de quaternions et un angle d'attaque possible.

$\rightarrow$ De nombreuses questions ouvertes (variante de recherche en rang ≥ 3? réduction pire cas / moyen cas dans un genre pour la variante décisionelle?, etc).

Résumé

$\rightarrow$ Un problème récent en cryptographie, nécessite davantage de cryptanalyse pour comprendre sa difficulté.

$\rightarrow$ Des attaques algébriques cassent la variante de recherche pour certains paramètres (modules de rang 2 sur un corps totalement réel).

$\rightarrow$ Pour les modules de rang 2 sur un totalement complexe : une connexion avec les algèbres de quaternions et un angle d'attaque possible.

$\rightarrow$ De nombreuses questions ouvertes (variante de recherche en rang ≥ 3? réduction pire cas / moyen cas dans un genre pour la variante décisionelle?, etc).

Merci de votre attention !

Références

Léo Ducas and Wessel van Woerden.
On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography.
In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 643–673. Springer, 2022.

Léo Ducas, Eamonn W Postlethwaite, Ludo N Pulles, and Wessel van 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.

Guilhem Mureau, Alice Pellet-Mary, Georgii Pliatsok, and Alexandre 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.

Clémence Chevignard, Guilhem Mureau, Thomas Espitau, Alice Pellet-Mary, Heorhii Pliatsok, and Alexandre Wallet.
A reduction from hawk to the principal ideal problem in a quaternion algebra.
Cryptology ePrint Archive, 2025.