Étude du problème MP-LWE

Sacha Ben-Arous

31 Août 2023

ENS Paris-Saclay

Plan

Introduction aux réseaux

Définition

Un **réseau euclidien** de $\mathbb{R}^m$ est l'ensemble des combinaisons à coefficients entiers de vecteurs linéairements indépendants $b_1, \ldots, b_n$, que l'on note :

$$\mathcal{L}(b_1, \ldots, b_n) := \left\{ \sum_{i=1}^{n} x_i b_i, x_i \in \mathbb{Z} \right\}$$

Définition

Un **réseau euclidien** de $\mathbb{R}^m$ est l'ensemble des combinaisons à coefficients entiers de vecteurs linéairements indépendants $b_1, \dots, b_n$, que l'on note :

$$\mathcal{L}(b_1, \dots, b_n) := \left\{ \sum_{i=1}^{n} x_i b_i, x_i \in \mathbb{Z} \right\}$$

Le réseau est alors de *dimension* n, et la famille des $(b_i)_{1 \leq i \leq n}$ est appelée **base** de ce réseau.

Définition

Un **réseau euclidien** de $\mathbb{R}^m$ est l'ensemble des combinaisons à coefficients entiers de vecteurs linéairements indépendants $b_1, \ldots, b_n$, que l'on note :

$$\mathcal{L}(b_1, \ldots, b_n) := \left\{ \sum_{i=1}^{n} x_i b_i, x_i \in \mathbb{Z} \right\}$$

Le réseau est alors de *dimension* n, et la famille des $(b_i)_{1 \leq i \leq n}$ est appelée **base** de ce réseau.

En notant $B := [b_1, \ldots, b_n]$, on considérera de manière équivalente :

$$\mathcal{L}(B) := \{Bx, x \in \mathbb{Z}^n\}$$

Exemples

Insérer des illustrations svp (si possible dimension 2 et 3 et q-ary et plusieurs bases pour un même réseau)

Learning With Errors

Learning With Errors Problem :

On fixe des entiers n et t, un nombre premier p et une distribution de bruit χ. On tire un secret $s \hookleftarrow \mathcal{U}(\mathbb{Z}_p^n)$.

Learning With Errors

Learning With Errors Problem :

On fixe des entiers n et t, un nombre premier p et une distribution de bruit χ. On tire un secret $s \hookleftarrow \mathcal{U}(\mathbb{Z}_p^n)$.

Le problème est le suivant : à partir de t échantillons

$$(a_i, b_i) := (a_i, \langle a_i, s \rangle + e_i \text{ mod } p)$$

où $a_i \hookleftarrow \mathcal{U}(\mathbb{Z}_p^n)$ et $e_i \hookleftarrow \chi$, on souhaite retrouver le secret s.

Learning With Errors Problem :

On fixe des entiers n et t, un nombre premier p et une distribution de bruit χ. On tire un secret $s \hookleftarrow \mathcal{U}(\mathbb{Z}_p^n)$.

Le problème est le suivant : à partir de t échantillons

$$(a_i, b_i) := (a_i, \langle a_i, s\rangle + e_i \text{ mod } p)$$

où $a_i \hookleftarrow \mathcal{U}(\mathbb{Z}_p^n)$ et $e_i \hookleftarrow \chi$, on souhaite retrouver le secret s.

<u>Rq</u> : Sans bruit, le problème est facile à résoudre.

Lien avec les réseaux

Cela revient à chercher le point le plus proche de $A \cdot s + e$ dans le réseau engendré par

$$A' := \left[\begin{array}{c|ccc} a_1 & q & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_t & 0 & \cdots & q \end{array}\right] \in \mathbb{Z}^{t \times (n+t)}$$

Difficulté de LWE

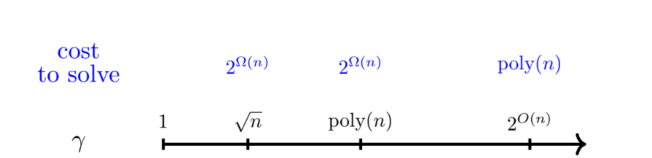
- La difficulté est relié au facteur $\gamma = \frac{\lambda_1}{\|e\|}$

Difficulté de LWE

- La difficulté est relié au facteur $\gamma = \frac{\lambda_1}{||e||}$
- Plus γ est petit, plus le problème est dur

Difficulté de LWE

- La difficulté est relié au facteur $\gamma = \frac{\lambda_1}{||e||}$
- Plus γ est petit, plus le problème est dur
- Si $\gamma = poly(n)$, ce problème est conjecturé exponentiellement dur à résoudre, même sur un ordinateur quantique



Variantes structurées

Problème : LWE tel quel est peu efficace à cause des grandes matrices aléatoires.

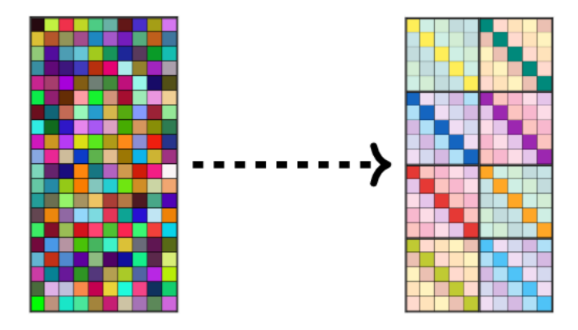
Variantes structurées

Problème : LWE tel quel est peu efficace à cause des grandes matrices aléatoires.

Solution : Rajouter de la structure : polynômes (Stehlé *et al.* [SSTX09])

Illustration

Concrètement, cela consiste à représenter matriciellement le produit de polynômes, et donc à mettre des blocs structurés dans A



Variantes structurées

Défaut : nouveau paramètre $f \in \mathbb{Z}_p^m[X]$ qui régit la complexité.

Ex : $x^n + 1$ et $x^n - 1$

Variantes structurées

Défaut : nouveau paramètre $f \in \mathbb{Z}_p^m[X]$ qui régit la complexité.

<u>Ex</u> : $x^n + 1$ et $x^n - 1$

Roşca *et al.* [RSSS17] introduisent une nouvelle variante structurée, et y réduisent des classes exponentiellement grandes de problèmes P-LWE.

Étude de la réduction

Objectif

- Comprendre le fonctionnement de la réduction, et son impact sur les paramètres de difficulté.

Objectif

- Comprendre le fonctionnement de la réduction, et son impact sur les paramètres de difficulté.

- Établir des propriétés sur le nouveau réseau d'arrivée

Représentation matricielle de la réduction

On défini $\mathrm{Rot}_f(a)$ pour qu'elle vérifie $\mathrm{Rot}_f(a) \cdot b = (a \times b \mod f)$

Représentation matricielle de la réduction

On défini $\mathsf{Rot}_f(a)$ pour qu'elle vérifie $\mathsf{Rot}_f(a) \cdot b = (a \times b \mod f)$

<u>Ex</u> : Si $f = x^4 + 1$ et $a = \sum_{0 \leq i < 4} a_i x^i$, alors :

$$\mathsf{Rot}_f(a) = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ -a_3 & a_0 & a_1 & a_2 \\ -a_2 & -a_3 & a_0 & a_1 \\ -a_1 & -a_2 & -a_3 & a_0 \end{pmatrix}$$

Représentation matricielle de la réduction

De même pour $\mathsf{Toep}_d(a)$, choisie pour avoir $\mathsf{Toep}_d(a) \cdot b = (a \odot b)$

Représentation matricielle de la réduction

De même pour $\mathsf{Toep}_d(a)$, choisie pour avoir $\mathsf{Toep}_d(a) \cdot b = (a \odot b)$

<u>Ex</u> : Si $d = 3$ et $a = \sum_{0 \leq i < 4} a_i x^i$, alors :

$$\mathsf{Toep}(a) = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 & 0 & 0 & 0 \\ 0 & a_0 & a_1 & a_2 & a_3 & 0 & 0 \\ 0 & 0 & a_0 & a_1 & a_2 & a_3 & 0 \\ 0 & 0 & 0 & a_0 & a_1 & a_2 & a_3 \end{pmatrix}$$

Représentation matricielle de la réduction

La réduction va donc de $\mathcal{L}_1 = \begin{bmatrix} \mathsf{Rot}_f(a_1) \\ \vdots \\ \mathsf{Rot}_f(a_t) \end{bmatrix}$ vers $\mathcal{L}_2 = \begin{bmatrix} \mathsf{Toep}_d(a_1) \\ \vdots \\ \mathsf{Toep}_d(a_t) \end{bmatrix}$

Annexe

Références