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 $b_1, \ldots, b_n$, 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.

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 $B := [b_1, \ldots, b_n]$ la matrice dont les colonnes sont formées par les $(b_i)_{1 \leq i \leq n}$, 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

$$(a_i, b_i) := (a_i, \langle a_i, s \rangle + e_i \bmod p)$$

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

Learning With Errors

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

$$(a_i, b_i) := (a_i, \langle a_i, s \rangle + e_i \bmod p)$$

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

Rq : 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 de la résolution algorithmique de ce problème est relié au facteur $\gamma = \frac{\lambda_1}{\|e\|}$, où λ_1 est la norme du plus court vecteur non nul du réseau engendré par A'.

Difficulté de LWE

La difficulté de la résolution algorithmique de ce problème est relié au facteur $\gamma = \frac{\lambda_1}{\|e\|}$, où λ_1 est la norme du plus court vecteur non nul du réseau engendré par A'.

Plus γ est petit, plus le problème est dur, et inversement.

Difficulté de LWE

La difficulté de la résolution algorithmique de ce problème est relié au facteur $\gamma = \frac{\lambda_1}{\|e\|}$, où λ_1 est la norme du plus court vecteur non nul du réseau engendré par A'.

Plus γ est petit, plus le problème est dur, et inversement.

Pour γ polynomial en n, ce problème est conjecturé exponentiellement dur à résoudre, même sur un ordinateur quantique.

Variantes structurées

Si on utilise LWE tel quel pour construire un protocole, ce dernier aura une efficacité très moyenne, étant donné que les calculs mis en jeu sont des produits de grandes matrices aléatoires.

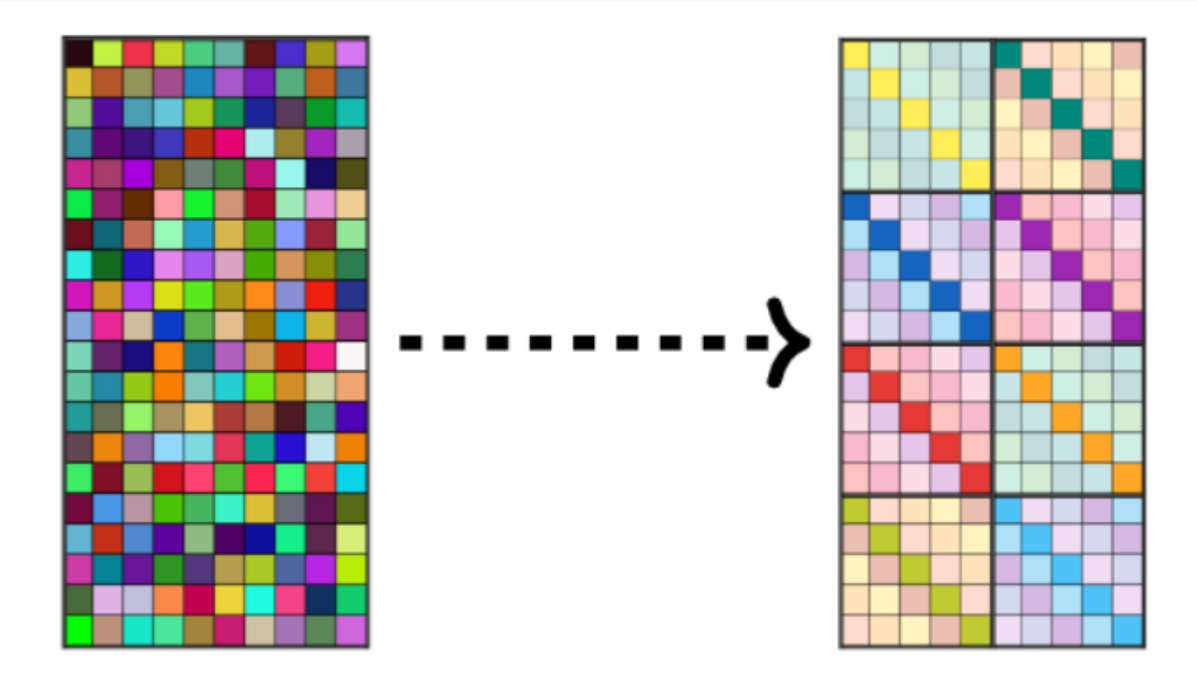
Variantes structurées

Si on utilise LWE tel quel pour construire un protocole, ce dernier aura une efficacité très moyenne, étant donné que les calculs mis en jeu sont des produits de grandes matrices aléatoires.

Stehlé *et al.* [SSTX09], résout ce problème en utilisant des réseaux structurés : les calculs matriciels correspondent alors à des produits de polynômes, calculables plus rapidement. C'est la variante P-LWE

Illustration

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



Variantes structurées

Cependant, cette variante souffre encore d'un défaut : un nouveau paramètre $f \in \mathbb{Z}_p^m[X]$ est utilisé, et la complexité de P-LWE(f) est directement liée au f choisi.

Variantes structurées

Cependant, cette variante souffre encore d'un défaut : un nouveau paramètre $f \in \mathbb{Z}_p^m[X]$ est utilisé, et la complexité de P-LWE(f) est directement liée au f choisi.

Roșca *et al.* introduisent ainsi une nouvelle variante structurée, Middle-Product Learning With Errors, et prouve que des classes exponentiellement grandes de problèmes P-LWE s'y réduisent, afin de se débarasser de la dépendance en f.

Représentation matricielle de la réduction

Pour $f \in \mathbb{Z}_p^m[X]$ et $a \in \mathbb{Z}_p^n[X]$, on note $\mathrm{Rot}_f(a) \in \mathbb{R}^{m \times m}$ la matrice dont la i-ème ligne est constituée des coefficients de $a \cdot x^{i-1} \bmod f$.

Représentation matricielle de la réduction

Pour $f \in \mathbb{Z}_p^m[X]$ et $a \in \mathbb{Z}_p^n[X]$, on note $\mathsf{Rot}_f(a) \in \mathbb{R}^{m \times m}$ la matrice dont la i-ème ligne est constituée des coefficients de $a \cdot x^{i-1}$ mod f.

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

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