Étude du problème MP-LWE

Sacha Ben-Arous, sous la direction d'Alice Pellet-Mary

Résumé

Insérer abstract ici

Table des matières

1 Introduction

Les réseaux euclidiens sont une construction algébrique permettant entre autres de définir des problèmes mathématiques dont la résolution algorithmique est conjecturée difficile, même pour des ordinateurs quantiques. Cela les rend donc particulièrement intéressants pour construire des protocoles sûrs en cryptographie post-quantique.
Deux exemples fondamentaux de problèmes sur les réseaux sont le *Small Integer Solutions problem* (SIS) introduit par Ajtai en 1996, et le *Learning With Errors problem* (LWE), découvert par Regev en 2005.
Durant mon stage, j'ai travaillé sur la variante *Middle-Product Learning With Errors* (MP-LWE) du problème de Regev, initialement présenté par Roşca *et al.* [RSSS17]

Definition 1.1 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.

En notant $B := [b_1, \dots, b_n]$ la matrice dont les colonnes sont formées par les $(b_i)_{1 \leq i \leq n}$, on considérera de manière équivalente :

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

Définition : Soit B une base d'un réseau de dimension n, et $\delta \in \mathbb{R}^+$. Une instance du problème *Bounded Distance Decoding*

Références

[RSSS17] Miruna Roşca, Amin Sakzad, Damien Stehlé et Ron Steinfeld. "Middle-Product Learning With Errors". In : *Annual International Cryptology Conference* (2017), p. 283-297.