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 :

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

On peut alors considérer le problème algorithmique suivant, qui apparait lors de l'étude des réseaux sur lesquels se basent les protocoles utilisant LWE :

Definition 1.2 Soit B une base d'un réseau de dimension n, et $\delta \in \mathbb{R}^+$. Une instance du problème *Bounded Distance Decoding* est un vecteur $t \in \mathbb{R}^m$ de la forme $t = x + e$, où $x \in \mathcal{L}(B)$ et $e \leq \delta$. Le problème consiste à retrouver x (ou e) à partir de t.

Conjecture 1.1 Dans des réseaux de dimension n, pour δ polynomial en n, le problème BDD est conjecturé exponentiellement (en n) dur à résoudre, même sur des ordinateurs quantiques.

2 Développements

2.1 Preuve de correction

On se propose tout d'abord de détailler la preuve de correction du schéma de chiffrement proposé dans [RSSS17] :

On rappelle le cadre de la preuve : $s \hookleftarrow \mathcal{U}(\mathbb{Z}^{n+d+k-1}[X])$, pour $i \leq t$ on a $a_i \hookleftarrow \mathcal{U}(\mathbb{Z}^n[X])$; $e_i \hookleftarrow \lfloor D_{\alpha q} \rceil [X]^{<k+d}$ et finalement $r_i \hookleftarrow \mathcal{U}(\{0,1\}^{<k+1}[X])$. On note $e_i(j)$ le j-ème coefficient de e_i. Le but est d'avoir avec bonne probabilité que :

$$\|\mu + 2 \sum_{i \leq t} r_i \odot_d e_i\|_\infty < q/2$$

où μ est le message à chiffrer.

Theorem 2.1 Si $\alpha \leq \frac{1}{64(k+1)t\sqrt{\lambda}}$ et $t(k+d) \leq e^{\lambda}$, alors tout texte μ, avec une probabilité $\geq 1-2^{-\Omega(\lambda)}$ sur `(sk,pk)` $\hookleftarrow$ `KeyGen`, on a `Decrypt(sk,Encrypt(pk,mu))= mu`

Preuve : On commence par donner une borne classique sur la distribution gaussienne :

$$\begin{aligned}
\mathbb{P}_{X\hookleftarrow\mathcal{N}(\sigma^2)}(|X| \geq M) &= \frac{2}{\sigma\sqrt{2\pi}}\int_M^{\infty} e^{-\frac{t^2}{2\sigma^2}}\,\mathrm{d}t \\
&\leq \frac{2\sigma^2}{\sigma\sqrt{2\pi}}\int_M^{\infty}\frac{t}{\sigma^2 M}e^{-\frac{t^2}{2\sigma^2}}\,\mathrm{d}t \\
&\leq \frac{2\sigma}{M\sqrt{2\pi}}[-e^{-\frac{t^2}{2\sigma^2}}]_M^{\infty} \\
&\leq \frac{2\sigma}{M\sqrt{2\pi}}e^{-\frac{M^2}{2\sigma^2}}
\end{aligned}$$

De plus, si on note $E := \max_{i,j}|e_i(j)|$, on a que :

$$\begin{aligned}
|(r_i \odot_d e_i)_{l\text{-eme}}| &= |(r_i \times e_i)_{l+k\text{-eme}}| \\
&= |\sum_{j=0}^{k+l} r_i(j)e_i(k+l-j)| \\
&\leq (k+1)E
\end{aligned}$$

Donc $|(\sum_{i\leq t} r_i \odot_d e_i)_{l\text{-eme}}| \leq t(k+1)E$.

Alors, on obtient que :

$$\begin{aligned}
\mathbb{P}(\|\mu + 2\sum_{i\leq t} r_i \odot_d e_i\|_{\infty} \geq q/2) &\leq \mathbb{P}(E \geq \frac{q}{4t(k+1)}) \\
&\leq \mathbb{P}(\bigcup_{i,j}|e_i(j)| \geq \frac{q}{4t(k+1)}) \\
&\leq (k+d)t\ \mathbb{P}_{X\hookleftarrow\mathcal{N}(\alpha^2q^2)}(X \geq \frac{q}{4t(k+1)}) \\
&\leq \frac{8t^2(k+1)(k+d)\alpha q}{q\sqrt{2\pi}}e^{-\frac{q^2}{32(\alpha q(k+1)t)^2}} \\
&\leq \frac{8t^2(k+1)(k+d)\alpha}{\sqrt{2\pi}}e^{-\frac{1}{32(\alpha(k+1)t)^2}}
\end{aligned}$$

En appliquant les hypothèses sur les paramètres de sécurité, on obtient finalement :

$$\begin{aligned}
\mathbb{P}(\|\mu + 2\sum_{i\leq t} r_i \odot_d e_i\|_{\infty} \geq q/2) &\leq \frac{t(k+d)}{8\sqrt{2\pi\lambda}}e^{-2\lambda} \\
&\leq e^{-\lambda-\log(8\sqrt{2\pi\lambda})} \\
&\leq 2^{-\Omega(\lambda)}
\end{aligned}$$

□

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.