

Étude du problème MP-LWE

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

Résumé

Insérer abstract ici

Table des matières

1	Introduction	2
2	Préliminaires	2
2.1	Problème LWE et difficulté	2
2.2	Variantes structurées	3
3	Étude de la réduction	4
3.1	Principe de la réduction	5
3.2	Effets géométriques	6
4	Schéma de chiffrement	6
4.1	Preuve de correction	6
	Références	7

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.

Le problème LWE est privilégié dans la construction de schémas de chiffrement car il été prouvé [Reg09] que résoudre une instance aléatoire de LWE est aussi dur que résoudre la pire instance d'un problème dur (cf suite). On dit que LWE bénéficie d'une réduction *pire-cas moyen-cas*.

Cependant, si l'on utilise la version standard de LWE pour construire des protocoles, ces derniers auront une efficacité très réduite à cause d'opérations faisant intervenir de grandes matrices aléatoires. La variante *Polynomial Learning With Errors*, proposée par Stehlé *et al.* [SSTX09], résout ce problème en utilisant des réseaux structurés : les calculs matriciels correspondent alors à des produits de polynômes, calculables très efficacement. Cependant, ce gain d'efficacité se fait au détriment de garanties de sécurité : les polynômes sont manipulés dans $\mathbb{Z}_p[X]/f$ et la complexité de la variante est directement liée au f choisi.

Afin de se débarrasser de cette dépendance, Roşca *et al.* introduisent le *Middle-Product Learning With Errors problem* (MP-LWE) [RSSS17] dont l'intérêt est d'être aussi dur que des classes exponentiellement grandes de problèmes PLWE(f) (dont on espère qu'elles contiennent au moins une instance difficile), tout en conservant l'efficacité des réseaux structurés.

Durant mon stage, j'ai donc travaillé sur la variante MP-LWE du problème de Regev, et plus particulièrement sur les effets de la réduction de PLWE vers MP-LWE proposée par [RSSS17].

2 Préliminaires

Définition 2.1 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 :

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

Dans ce qui suit, on note \mathbb{Z}_q (resp. \mathbb{R}_q) le quotient $\mathbb{Z}/q\mathbb{Z}$ (resp. $\mathbb{R}/q\mathbb{Z}$), et $\|\cdot\|$ désigne la norme euclidienne.

2.1 Problème LWE et difficulté

Définition 2.2 (Distribution LWE) Soient $q \geq 2$, $m \geq 1$, χ une distribution de probabilité sur \mathbb{Z} . À partir de $s \in \mathbb{Z}_q^m$, on définit $\mathcal{D}_{q,\chi,m}$ la distribution sur $\mathbb{Z}_q^m \times \mathbb{Z}_q$ obtenue en choisissant $a \leftarrow \mathcal{U}(\mathbb{Z}_q^m)$, $e \leftarrow \chi$, et qui renvoie $(a, b) := (a, \langle a, s \rangle + e \bmod q)$.

Définition 2.3 (Problèmes LWE) Soient $q \geq 2$, $m \geq 1$, χ . Muni de la distribution $\mathcal{D}_{q,\chi,m}$ précédente, on peut alors définir deux problèmes :

- **LWE-Décisionnel** consiste à distinguer un nombre arbitraire d'échantillons de $\mathcal{D}_{q,\chi,m}$ et le même nombre d'échantillons de $\mathcal{U}(\mathbb{Z}_q^m) \times \mathcal{U}(\mathbb{Z}_q)$.
- **LWE-Calculatoire** consiste à retrouver le secret s à partir d'un nombre fixé d'échantillons indépendants.

En notant A la matrice dont les lignes sont formées des $(a_i)_{i \leq t}$, $e := (e_i)_{i \leq t}$ et $b := (b_i)_{i \leq t}$ (t représente le nombre d'échantillons), on a : $b = As + e \bmod q$.

Définition 2.4 Dans un réseau Λ , on note $\lambda_i := \inf\{r, \dim(\text{Vect}(\Lambda \cap \mathcal{B}(0, r))) = i\}$ le i -ème minimum du réseau. En particulier, on a $\lambda_1 = \inf\{\|v\|, v \in \mathcal{L}(B) \setminus \{0\}\}$ qui est le plus court vecteur non nul du réseau.

Rq : λ_i s'interprète comme le rayon de la plus petite boule centrée à l'origine qui contient i vecteurs indépendants du réseau.

Le calcul effectif de ces minimums semble très dur : les meilleurs algorithmes polynomiaux connus calculant λ_1 ont un facteur d'approximation exponentiel.

On peut alors considérer le problème algorithmique suivant, qui apparaît lors de l'étude des réseaux reliés aux protocoles utilisant LWE :

Définition 2.5 (BDD) Soit B une base d'un réseau de dimension n , et $\gamma \in \mathbb{R}^+$. 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 $\|e\| \leq \lambda_1/\gamma$. Le problème consiste à retrouver x (ou e) à partir de t .

En revenant au problème LWE-Décisionnel, on constate que ce dernier se réduit à une instance de BDD dans le réseau engendré par les colonnes de $[A, qI_t]$.

Conjecture 2.1 Dans un réseau de dimension n , pour γ polynomial en n , le problème BDD est conjecturé exponentiellement (en n) dur à résoudre, même sur des ordinateurs quantiques.

2.2 Variantes structurées

On considère la variante polynomiale du problème LWE :

Définition 2.6 (Distribution PLWE) Soient $q \geq 2$, $m > 0$, f polynôme de degré m , χ une distribution sur $\mathbb{R}_q[X]/f$. À partir de $s \in \mathbb{Z}_q[X]/f$, on définit la distribution $P_{q,\chi}^{(f)}(s)$ sur $\mathbb{Z}_q[X]/f \times \mathbb{R}_q[X]/f$ obtenue en tirant $a \leftarrow \mathcal{U}(\mathbb{Z}_q[X]/f)$, $e \leftarrow \chi$ et qui renvoie $(a, b = a \cdot s + e)$.

Ensuite, on définit un nouveau produit sur les polynômes :

Définition 2.7 (Middle-Product) Soient $d_a, d_b, d, k \in \mathbb{N}$ tels que $d_a + d_b - 1 = d + 2k$. Alors le *middle-product* $\odot_d : \mathbb{R}^{<d_a}[X] \times \mathbb{R}^{<d_b}[X] \rightarrow \mathbb{R}^{<d}[X]$ est la fonction :

$$(a, b) \mapsto a \odot_d b = \left\lfloor \frac{(a \cdot b) \bmod x^{k+d}}{x^k} \right\rfloor$$

On construit alors une distribution plus générale utilisant le produit précédent :

Définition 2.8 (Distribution MP-LWE) Soient $n, d > 0$, $q \geq 2$ et χ une distribution sur $\mathbb{R}_q^{<d}[X]$. Pour $s \in \mathbb{Z}^{n+d-1}$, on définit la distribution $\text{MP}_{q,n,d,\chi}(s)$ sur $\mathbb{Z}_q^{<n}[X] \times \mathbb{R}_q^{<d}$ obtenu en tirant $a \leftarrow \mathcal{U}(\mathbb{Z}_q^{<n}[X])$, $e \leftarrow \chi$ et qui renvoie $(a, b = a \odot_d s + e)$.

Les problèmes décisionnels $\text{PLWE}_{q,\chi}^{(f)}$ et $\text{MP-LWE}_{q,n,d,\chi}$ associés peuvent se définir ensuite de manière parfaitement analogue au cas LWE classique.

Définition 2.9 Soit $\sigma > 0$ et $m \in \mathbb{N}$

- On note D_σ la gaussienne en dimension n dont la matrice de covariance est $\sigma^2 \text{Id}_n$.
- Soit $f \in \mathbb{Z}[X]$ de degré m . On définit le *facteur d'expansion* de f par

$$EF(f) := \max_{\substack{g \in \mathbb{Z}^{2m-1}[X] \\ g \neq 0}} \left(\frac{\|g \bmod f\|_\infty}{\|g\|_\infty} \right)$$

Théorème 2.1 Soient $n, d > 0$, $q \geq 2$, et $\alpha \in (0, 1)$. Pour $S > 0$, on note $\mathcal{F}(S, d, n)$ les polynômes de $\mathbb{Z}[X]$ unitaires, dont le coefficient constant est inversible dans \mathbb{Z}_q , de degré m vérifiant $d \leq m \leq n$, et tels que $EF(f) \leq S$. Il existe une réduction *ppt* depuis $\text{PLWE}_{q,D_{\alpha q}}^{(f)}$ pour tout $f \in \mathcal{F}(S, d, n)$ vers $\text{MP-LWE}_{q,n,d,D_{\alpha' q}}$, où $\alpha' = \alpha d S$.

Il s'agit du résultat principal de [RSSS17]. Durant mon stage, j'ai étudié comment la réduction explicitée dans la preuve du théorème agit géométriquement sur les réseaux sous-jacents aux problèmes de manière à en augmenter la complexité.

3 Étude de la réduction

Afin de manipuler les réseaux sous-jacents à ces variantes, il est nécessaire de définir les objets suivants :

Définition 3.1 Soient $f, a \in \mathbb{R}_d[X]$ de degré m et n , et $d \in \mathbb{N}$

- On note $\text{Rot}_f^d(a) \in \mathbb{R}^{d \times m}$ la matrice dont la i -ème ligne est constituée des coefficients de $a \cdot x^{i-1} \bmod f$. On écrira $\text{Rot}_f(a)$ pour $\text{Rot}_f^m(a)$
- On note $\text{Toep}^{d,n}(a) \in \mathbb{R}^{d \times (n+d-1)}$ la matrice dont la i -ème ligne est constituée des coefficients de $a \cdot x^{i-1}$.
- On note $\text{M}_f^d \in \mathbb{R}^{d \times m}$ la matrice dont l'entrée (i, j) est le coefficient constant de $x^{i+j-2} \bmod f$. On écrira M_f pour M_f^m .

Dans la suite, on notera de manière identique un polynôme et le vecteur de ses coefficients. De plus, pour un vecteur a , on notera \bar{a} ce vecteur renversé.

Lemme 3.1 Soient $d, k > 0$, et $a \in \mathbb{R}^{<k+1}[X]$, $b \in \mathbb{R}^{<k+d}[X]$ et $f \in \mathbb{R}[X]$ de degré m , alors :

- (1) $\text{Rot}_f^d(a) = \text{Toep}^{d,k+1}(a) \cdot \text{Rot}_f^{k+d}(1)$
- (2) $a \odot_d b = \overline{\text{Toep}^{d,k+1}(a)} \cdot \bar{b}$
- (3) $\text{Rot}_f^d(a \cdot b) = \text{Rot}_f^d(a) \cdot \text{Rot}_f^d(b)$
- (4) Si $\deg(a) < m$, $\text{Rot}_f(a) \cdot (1, 0, \dots, 0)^\top = \text{M}_f \cdot a$

Les preuves calculatoires sont fournies dans [RSSS17].

3.1 Principe de la réduction

Soient $q \geq 2$, $\alpha \in (0, 1)$, f polynôme vérifiant les hypothèses du Théorème 2.1, dont on gardera les notations.

À partir de $s \in \mathbb{Z}_q[X]/f$, on se donne initialement un nombre t d'échantillons $(a_i, b_i)_{i \leq t}$ de $P_{q, D_{\alpha q}}^{(f)}(s)$. Le but est de construire t échantillons $(a'_i, b'_i)_{i \leq t}$ de $MP_{q, n, d, D_{\alpha' q}}(s)$. Dans un premier temps, on va "prolonger" les a_i dans un espace de polynômes de plus grand degré. Ensuite grâce au Lemme 3.1 on passera du produit usuel dans l'espace quotient au middle-product. Il faudra alors re-randomiser le secret, et éliminer la dernière dépendance en f dans la distribution de la nouvelle erreur.

Tout d'abord, on tire $(r_i)_{i \leq t} \leftarrow \mathcal{U}(\mathbb{Z}_q^{<n-m}[X])$, et on définit $a'_i := a_i + f \cdot r_i \in \mathbb{Z}_q^{<n}[X]$. On a alors que, les a_i et r_i étant uniformes, les a'_i le sont aussi. Moralement, on rajoute la partie des a_i qui a été oubliée en passant au quotient. La preuve formelle consitue le Lemme 2.1 de [Lyu16]. Elle se fait par récurrence, en utilisant de manière cruciale que f est unitaire.

Ensuite, en utilisant le Lemme 3.1 et la définition des $(b_i)_{i \leq t}$, on a

$$\text{Rot}_f(b_i) = \text{Rot}_f(a_i) \cdot \text{Rot}_f(s) + \text{Rot}_f(e_i)$$

Ce qui donne, en conservant la première colonne (i.e en multipliant par $(1, 0, \dots, 0)^\top$) et les d premières lignes :

$$\begin{aligned} M_f^d \cdot b_i &= \text{Rot}_f^d(a_i) \cdot M_f^d \cdot s + M_f^d \cdot e_i \\ &= \text{Rot}_f^d(a'_i) \cdot M_f^d \cdot s + M_f^d \cdot e_i \\ &= \text{Toep}^{d, n}(a'_i) \cdot \text{Rot}_f^{d+n-1}(1) \cdot M_f^d \cdot s + M_f^d \cdot e_i \\ \overline{b'_i} &= \text{Toep}^{d, n}(a'_i) \cdot \overline{s'} + \overline{e'_i} \end{aligned}$$

$$\text{où on a noté } \begin{cases} b'_i = \overline{M_f^d \cdot b_i} \\ s' = \overline{\text{Rot}_f^{d+n-1}(1) \cdot M_f^d \cdot s} \\ e'_i = \overline{M_f^d \cdot e_i} \end{cases}$$

Alors on a, toujours en utilisant le Lemme 3.1, que $b'_i = a'_i \odot_d s' + e'_i$

On obtient que b'_i est uniformément distribué car b_i l'est, et que M_f est inversible modulo q . Cette dernière affirmation repose sur l'hypothèse que le coefficient constant de f est inversible modulo q .

Ensuite, on constate que le nouveau secret est encore fortement lié au secret de l'ancien réseau. Pour régler ce problème, on prend $s'' \leftarrow \mathcal{U}(\mathbb{Z}_q^{n+d-1}[X])$ et on en sortie, on ajoute à chaque (a'_i, b'_i) le couple $(0, a'_i \odot_d s'')$, de manière à re-randomiser le secret, i.e : le nouveau secret $\tilde{s} = s' + s''$ est maintenant uniforme dans le nouveau réseau.

On a de plus que, en notant $J \in \mathbb{R}^{d \times d}$ la matrice qui a des 1 sur son anti-diagonale et des 0 ailleurs, la nouvelle distribution de l'erreur est $J \cdot M_f^d \cdot D_{\alpha q}$. Pour obtenir à nouveau une gaussienne dont la matrice de covariance est diagonale, il suffit alors de majorer les valeurs singulières de la nouvelle distribution, et de choisir le majorant comme variance de la gaussienne diagonale. Or dans notre cas, on a clairement $\|J\| = 1$ et $\|M_f\| \leq d\text{EF}(f) = dS$, d'où $\alpha' = \alpha dS$, comme annoncé dans le Théorème 2.1.

3.2 Effets géométriques

Afin d'étudier les effets de cette réduction, on remarque que 3 réseaux distincts apparaissent :

- Le réseau initial $\mathcal{L}_0 = \{[(\text{Rot}_f(a_i))_{i \leq t}] \cdot x \bmod q, x \in \mathbb{Z}^m\}$
- Le réseau intermédiaire $\mathcal{L}_1 = \{[(\text{Rot}_f^d(a_i))_{i \leq t}] \cdot x \bmod q, x \in \mathbb{Z}^d\}$ qui correspond au projeté en dimension d du réseau initial
- Le réseau final $\mathcal{L}_2 = \{[(\text{Toep}^{d,n}(a'_i))_{i \leq t}] \cdot x \bmod q, x \in \mathbb{Z}^d\}$

4 Schéma de chiffrement

4.1 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 : $s \leftarrow \mathcal{U}(\mathbb{Z}^{n+d+k-1}[X])$, pour $i \leq t$ on a $a_i \leftarrow \mathcal{U}(\mathbb{Z}^n[X])$; $e_i \leftarrow [D_{\alpha q}][X]^{<k+d}$ et finalement $r_i \leftarrow \mathcal{U}(\{0,1\}^{<k+1}[X])$. 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.

Théorème 4.1 Si $\alpha \leq \frac{1}{16(k+1)t\sqrt{\lambda}}$ et $12td(k+1) \leq qd \leq e^\lambda$, alors pour tout texte μ , avec probabilité $\geq 1 - 2^{-\Omega(\lambda)}$ sur $(\text{sk}, \text{pk}) \leftarrow \text{KeyGen}$, on a $\text{Decrypt}(\text{sk}, \text{Encrypt}(\text{pk}, \mu)) = \mu$

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

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

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

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

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

Alors, on obtient que :

$$\begin{aligned}
\mathbb{P}(\|\mu + 2 \sum_{i \leq t} r_i \odot_d e_i\|_\infty \geq q/2) &\leq \mathbb{P}(1 + 2E \geq \frac{q}{2t(k+1)}) \\
&\leq \mathbb{P}(\bigcup_{i,j} |e_i(j)| \geq \frac{q}{4t(k+1)} - \frac{1}{2}) \\
&\leq (k+d)t \mathbb{P}_{X \leftarrow \mathcal{N}(\alpha^2 q^2)}(|X| \geq \frac{q}{4t(k+1)} - \frac{3}{2}) \\
&\leq \frac{8t^2(k+1)(k+d)\alpha q}{q - 6t(k+1)} e^{-\frac{1}{2(\alpha q)^2} (\frac{q}{4t(k+1)} - \frac{3}{2})^2}
\end{aligned}$$

En appliquant les hypothèses sur les paramètres de sécurité, on obtient l'inégalité suivante sur l'exposant :

$$\frac{1}{2(\alpha q)^2} (\frac{q}{4t(k+1)} - \frac{3}{2})^2 \geq \frac{16^2 \lambda t^2 (k+1)^2}{2q^2} (\frac{q}{4t(k+1)} - \frac{3}{2})^2 \geq \frac{\lambda}{2} (4 - \frac{24t(k+1)}{q})^2 \geq 2\lambda$$

On majore de même le facteur pré-exponentiel :

$$\frac{8t^2(k+1)(k+d)\alpha q}{q - 6t(k+1)} \leq \frac{8t^2(k+1)(k+d)\alpha q}{6t(k+1)} \leq \frac{4t(k+d)q}{3} \frac{1}{16(k+1)t\sqrt{\lambda}} \leq \frac{(k+d)q}{12(k+1)\sqrt{\lambda}} \leq \frac{qd}{12\sqrt{\lambda}}$$

Finalement on obtient la borne voulue :

$$\begin{aligned}
\mathbb{P}(\|\mu + 2 \sum_{i \leq t} r_i \odot_d e_i\|_\infty \geq q/2) &\leq \frac{qd}{12\sqrt{\lambda}} e^{-2\lambda} \\
&\leq e^{-\lambda - \log(12\sqrt{\lambda})} \\
&\leq 2^{-\Omega(\lambda)}
\end{aligned}$$

□

Références

- [Reg09] Oded REGEV. “On lattices, learning with errors, random linear codes, and cryptography”. In : *Journal of the ACM* (2009), p. 1-40.
- [SSTX09] Damien STEHLÉ, Ron STEINFELD, Keisuke TANAKA et Keita XAGAWA. “Efficient public key encryption based on ideal lattices”. In : *International Conference on the Theory and Application of Cryptology and Information Security* (2009), p. 617-635.
- [Lyu16] Vadim LYUBASHEVSKY. “Digital signatures based on the hardness of ideal lattice problems in all rings”. In : *International Conference on the Theory and Application of Cryptology and Information Security* (2016), p. 196-214.
- [RSSS17] Miruna ROȘCA, Amin SAKZAD, Damien STEHLÉ et Ron STEINFELD. “Middle-Product Learning With Errors”. In : *Annual International Cryptology Conference* (2017), p. 283-297.