

Cryptographie post quantique : TP3 - Schémas sur les réseaux structurés

1 Réseaux Structurés et Module-LWE

1.1 Rappels sur les anneaux et les idéaux

Définition 1 (Idéal). On dit que $\mathcal{I}$ est un idéal d'un anneau $\mathcal{R}$, s'il satisfait les deux conditions suivantes :

- Pour tout $\alpha, \beta \in \mathcal{I}, \alpha + \beta \in \mathcal{I}$ (sous-groupe additif),
- Pour tout $\alpha \in \mathcal{I}, \beta \in \mathcal{R}, \alpha\beta \in \mathcal{I}$ (stabilité par multiplication).

Exemple: $2\mathbb{Z}$ est un idéal de $\mathbb{Z}$, car il est stable par addition et par multiplication par les éléments de $\mathbb{Z}$.

- La somme de nombres pairs est un nombre pair (sous-groupe additif),
- La multiplication d'un nombre pair par un nombre entier est un nombre pair (stabilité par multiplication).

Définition 2 (Anneau cyclotomique). Soit d une puissance de 2. On définit le polynôme cyclotomique d'ordre $2d$ comme étant $X^d + 1$. On définit $\mathcal{I} = \langle X^d + 1 \rangle$, l'idéal engendré par $X^d + 1$ dans l'anneau $\mathbb{Z}[X]$. On définit l'anneau cyclotomique à l'ordre $2d$ par $\mathcal{R} = \mathbb{Z}[X]/\mathcal{I}$, c'est-à-dire l'ensemble des polynômes de degré strictement inférieur à d avec des coefficients dans $\mathbb{Z}$.

Remarque: Si $d \neq 2^k$, alors $X^d + 1$ n'est pas cyclotomique, et $\mathcal{R}$ n'est pas un anneau intègre. C'est pour cela que l'on choisit d comme une puissance de 2.

Exemple: Considérons $d = 4$. Alors, l'anneau cyclotomique $\mathcal{R} = \mathbb{Z}[X]/\langle X^4 + 1 \rangle$ est l'ensemble des polynômes de degré strictement inférieur à 4 avec des coefficients dans $\mathbb{Z}$, c'est-à-dire les polynômes de la forme $a_0 + a_1X + a_2X^2 + a_3X^3$ avec $a_i \in \mathbb{Z}$.

On étend même la définition à des anneaux cyclotomiques modulo un entier premier q , en définissant $\mathcal{R}_q = \mathbb{Z}_q[X]/\langle X^d + 1 \rangle$.

1.2 Le cas des réseaux euclidiens

L'intérêt principal de la structuration par anneau cyclotomique est, in fine, de réduire la taille des clés et des messages, tout en conservant la sécurité, tout en améliorant la complexité. La première étape est de s'assurer que cela préserve une structure de réseau.

Si on considère $a_0 + a_1X + a_2X^2 + a_3X^3 \in \mathcal{R}$ avec $a_i \in \mathbb{Z}$, et $b_0 + b_1X + b_2X^2 + b_3X^3 \in \mathcal{R}$ avec $b_i \in \mathbb{Z}$, alors on peut définir la somme $\mathcal{R}$, comme somme des coefficients par coefficients.

$$a(X) + b(X) = (a_0 + b_0) + (a_1 + b_1)X + (a_2 + b_2)X^2 + (a_3 + b_3)X^3$$

D'un point de vue coefficients, on a :

$$\text{Coeffs}(a(X) + b(X)) = \begin{bmatrix} a_0 + b_0 \\ a_1 + b_1 \\ a_2 + b_2 \\ a_3 + b_3 \end{bmatrix} = \text{Coeffs}(a(X)) + \text{Coeffs}(b(X))$$

On peut également définir le produit de ces deux polynômes dans $\mathcal{R}$, en utilisant la relation $X^4 = -1$ pour réduire les polynômes modulo $X^4 + 1$. Pour cela, on peut utiliser la forme matricielle de $\text{Rot}(a(X))$ définie ci-dessous, pour calculer le produit de polynômes.

$$\text{Rot}(a(X)) = \begin{bmatrix} a_0 & -a_3 & -a_2 & -a_1 \\ a_1 & a_0 & -a_3 & -a_2 \\ a_2 & a_1 & a_0 & -a_3 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix}, \text{ donnant } \text{Coeffs}(a(X) \cdot b(X)) = \text{Rot}(a(X)) \cdot \text{Coeffs}(b(X))$$

Définition 3 (Réseaux Idéaux). Soit d une puissance de 2 et $\mathcal{R} = \mathbb{Z}[X]/\langle X^d + 1 \rangle$. Un réseau idéal est un réseau $\Lambda \subseteq \mathcal{R}$ qui est un idéal de l'anneau $\mathcal{R}$. On peut également définir un réseau idéal dans $\mathcal{R}_q = \mathbb{Z}_q[X]/\langle X^d + 1 \rangle$.

Exemple: Considérons $d = 4$ et $q = 17$ c'est-à-dire $\mathcal{R}_q = \mathbb{Z}_{17}[X]/\langle X^4 + 1 \rangle$. On définit un réseau par $\Lambda_1 = \langle 3 + 2X + 5X^2 + 4X^3 \rangle$. Λ_1 est un réseau idéal de $\mathcal{R}_q$, il est stable par addition et par multiplication par les éléments de $\mathcal{R}_q$. Les éléments de Λ_1 sont de la forme $(3 + 2X + 5X^2 + 4X^3) \cdot (a_0 + a_1X + a_2X^2 + a_3X^3)$ avec $a_i \in \mathbb{Z}_{17}$.

Dans ce cas là, on peut voir on voit que Λ_1 le réseau défini par la base:

$$\mathbf{B}_1 = \text{Rot}(3 + 2X + 5X^2 + 4X^3) = \begin{bmatrix} 3 & -4 & -5 & -2 \\ 2 & 3 & -4 & -5 \\ 5 & 2 & 3 & -4 \\ 4 & 5 & 2 & 3 \end{bmatrix}.$$

(IdéauxFR) Exercice 1.

Initiation aux Réseaux Idéaux

Considérer $q = 17$ et $d = 4$. On considèrera ensuite l'anneau cyclotomique $\mathcal{R}_q := \mathbb{Z}_q[X]/\langle X^d + 1 \rangle$.

Rappel: Dans $\mathcal{R}_q$, on a $X^d = -1$. Ainsi, tous les polynômes de $\mathcal{R}_q$ sont de la forme $a_0 + a_1X + \dots + a_{d-1}X^{d-1}$ avec $a_i \in \mathbb{Z}_q$.

Considérer $a(X) = 3 + 2X + 5X^2 + 4X^3$ et $b(X) = 1 + 3X + 2X^2 + 6X^3$. Calculer dans $\mathcal{R}_q$:

1. $a(X) + b(X)$.
2. $a(X) - b(X)$.
3. $a(X) \cdot b(X)$.

Aide: Passer par la forme matricielle de $\text{Rot}(a(X))$ pour le produit de polynômes.

Définition 4 (Réseaux Modules). Soit d une puissance de 2, q un entier premier, et $\mathcal{R}_q = \mathbb{Z}_q[X]/\langle X^d + 1 \rangle$. Un réseau module est un sous-ensemble $\Lambda \subseteq \mathcal{R}_q^k$ qui est stable par addition et par multiplication par les éléments de $\mathcal{R}_q$.

On définit un réseau module par $\Lambda_2 = \begin{bmatrix} 3 + 2X + 5X^2 + 4X^3 & X + 12X^2 \\ 4 + 2X^2 + 3X^3 & 7 + X^3 \end{bmatrix}$ de $\mathcal{R}_q$.

Dans ce cas là, on peut voir que Λ_2 le réseau défini par la base

$$\mathbf{B}_2 = \begin{bmatrix} \text{Rot}(3 + 2X + 5X^2 + 4X^3) & \text{Rot}(X + 12X^2) \\ \text{Rot}(4 + 2X^2 + 3X^3) & \text{Rot}(7 + X^3) \end{bmatrix} = \begin{bmatrix} 3 & -4 & -5 & -2 & 0 & 0 & -12 & -1 \\ 2 & 3 & -4 & -5 & 1 & 0 & 0 & -12 \\ 5 & 2 & 3 & -4 & 12 & 1 & 0 & 0 \\ 4 & 5 & 2 & 3 & 0 & 12 & 1 & 0 \\ 4 & -3 & -2 & 0 & 7 & -1 & 0 & 0 \\ 0 & 4 & -3 & -2 & 0 & 7 & -1 & 0 \\ 2 & 0 & 4 & -3 & 0 & 0 & 7 & -1 \\ 3 & 2 & 0 & 4 & 1 & 0 & 0 & 7 \end{bmatrix}.$$

Definition 5 (Module-LWE $_{q,d,n,m,\sigma_e}$). Soit d une puissance de 2, q un entier premier, et $\mathcal{R}_q = \mathbb{Z}_q[X] / \langle X^d + 1 \rangle$. Le problème Module-LWE (MLWE) est défini comme suit : étant donné un ensemble de paires $(\mathbf{A}, \mathbf{b})$ où $\mathbf{A} \in \mathcal{R}_q^{m \times n}$ est une matrice aléatoire et $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$ pour un vecteur secret aléatoire de $\mathbf{s} \in \mathcal{R}_q^n$ et un vecteur d'erreur $\mathbf{e} \in \mathcal{R}_q^m$ où chaque coefficient suit une distribution gaussienne discrète $\mathcal{D}_{\sigma_e}$, le but est de retrouver le vecteur secret $\mathbf{s}$.

Definition 6 (Module-SIS $_{q,d,n,m,\beta}$). Soit d une puissance de 2, q un entier premier, et $\mathcal{R}_q = \mathbb{Z}_q[X] / \langle X^d + 1 \rangle$. Le problème Module-SIS (MSIS) est défini comme suit : étant donnée $\mathbf{A} \in \mathcal{R}_q^{n \times m}$. Trouver un vecteur $\mathbf{x} \in \mathcal{R}_q^m$ non nul tel que $\mathbf{A}\mathbf{x} = 0$ et $\|\mathbf{x}\| \leq \beta$ pour un certain paramètre β .

(ModulesFR) **Exercice 2.**

Initiation aux Réseaux Modules

Considérer $q = 17$ et $d = 4$. On considérera ensuite l'anneau cyclotomique $\mathcal{R}_q := \mathbb{Z}_q[X] / \langle X^d + 1 \rangle$.

Rappel: Dans $\mathcal{R}_q$, on a $X^d = -1$. Ainsi, tous les polynômes de $\mathcal{R}_q$ sont de la forme $a_0 + a_1X + \dots + a_{d-1}X^{d-1}$ avec $a_i \in \mathbb{Z}_q$.

$$\text{Considérer } \mathbf{A} = \begin{bmatrix} 3 + 2X + 5X^2 + 4X^3 & X + 12X^2 \\ 16 + 16X + 2X^3 & 7 + X^3 \\ 14 + 15X + 12X^2 + 13X^3 & 8X + 15X^2 + 16X^3 \end{bmatrix} \text{ et } \mathbf{s} = \begin{bmatrix} 1 + 3X + 2X^2 + 6X^3 \\ 3 + 8X^2 + 16X^3 \end{bmatrix}.$$

1. Calculer $\mathbf{A} \cdot \mathbf{s}$ dans $\mathcal{R}_q$.

Aide: Les opérations sur les coefficients des polynômes se font dans $\mathbb{Z}_q$, dans certains cas, il peut être avantageux de réduire les coefficients modulo q , et de les voir dans $\{-\frac{q-1}{2}, \dots, \frac{q-1}{2}\}$.

2 Implémentation de variantes structurées

Ici, l'objectif est de modifier le chiffrement Regev implémenté avant en remplaçant la structure d'entier $\mathbb{Z}_q$ par la structure d'anneaux cyclotomiques de polynômes $\mathbb{Z}_q[X] / \langle X^d + 1 \rangle$ (où d est une puissance de 2).

(StructRegevFR) **Exercice 3.**

Chiffrement Regev structuré

1. Modifier vos différentes fonctions afin de définir un schéma de chiffrement de Regev exploitant des réseaux structurés. Prenez en compte la chiffrement/déchiffrement de messages binaires $m \in \{0, 1\}^\ell$ où $\ell \leq d$.

Aide: Vous pouvez vous inspirer de vos fonctions du TP1/2, mais il faudra adapter les fonctions pour prendre en compte la structure des réseaux, la taille des matrices et des polynômes, ainsi que les opérations sur les coefficients des polynômes dans $\mathbb{Z}_q$.

2. Réutiliser le LWE Estimator pour évaluer la robustesse de votre nouveau schéma. (Vous pouvez réutiliser vos fonctions du TP1/2)

Aide: Il existe peu d'attaques exploitant la structure sous-jacentes des réseaux et elle ne sont pas encore bien comprises. Ainsi, pour évaluer la robustesse de votre schéma, considérer simplement les attaques classiques comme s'il n'y avait pas de structure (mais attention aux tailles des matrices et des degrés des polynômes).

3. Comparer l'efficacité de votre nouveau schéma avec vos précédentes constructions non structurées. (Temps + Taille)

3 Implémentation du standard ML-KEM

Récemment, le standard ML-KEM (pour Mécanisme d'encapsulation de clé) a été adopté par le NIST en Août 2024. Dans un contexte professionnel, vous serez potentiellement amené à l'implémenter, l'utiliser ou identifier les potentiels points de pression cybersensibles. Pour s'assurer de l'efficacité et de l'optimalité du schéma, les paramètres ont donc été définis par le NIST lui-même.

(KEMFR) Exercice 4.

ML-KEM

1. Aller chercher dans la [documentation officielle](#) et modifier vos fonctions afin de prendre en compte les paramètres clairement définis.

Le standard ML-KEM exploite la structure du chiffrement de Regev mais vous avez montré lors du TP1 que le schéma n'est pas IND-CCA (seulement IND-CPA). Il existe un paradigme de transformation cryptographique transformant n'importe quel schéma IND-CPA en schéma IND-CCA, appelé Transformation de Fujisaki-Okamoto.

2. Renseignez-vous puis expliquez la transformation FO, en utilisant la [sous-section 4.8](#).
3. Si vous avez été attentif, vous remarquerez que le NIST n'a pas standardisé un schéma de chiffrement mais une méthode d'encapsulation de clé: pourquoi selon vous ?
4. En utilisant les nouvelles fonctions de l'exercice 3, construire de nouvelles fonctions permettant de prendre en compte cette transformation. Faites dans un premier temps par vous même en essayant de comprendre la transformation, ensuite seulement corrigez-vous avec la représentation des fonctions définies dans la [\[Figure 4\]](#).

Bravo ! Vous venez d'implémenter votre premier schéma post-quantique.