Cryptographie post quantique : TP3 - Schémas sur les réseaux structurés

1 Implémentation de variantes structurées

(StructRegevFR) **Exercice 1.** *Chiffrement de Regev structuré*

Ici, l'objectif est de modifier le chiffrement de 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).

1. Modifier vos différentes fonctions afin de définir un schéma de chiffrement de Regev exploitant des réseaux structurés.

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

(StructDualRegevFR) **(Facultatif) Exercice 2.** *Chiffrement Dual-Regev structuré*

1. Modifier vos différentes fonctions afin de définir un schéma de chiffrement Dual-Regev exploitant des réseaux structurés.

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

(StructGPVFR) **Exercice 3.** *Signature GPV structuré*

1. Modifier votre échantillonneur gaussien afin qu'il génère et retourne des matrices et trappes de réseaux structurés.

2. Modifier le schéma de signature GPV afin de prendre en compte la structuration du réseau associé (et des matrices).

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

2 Implémentation du standard ML-KEM

(KEMFR) **Exercice 4.** *ML-KEM*

Récemment, le standard ML-KEM (pour Méchanisme 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/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.

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 remarquez 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 1, 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.