

## Réduction Recherche-Décision LWE

On rappelle la définition de la distribution LWE :  $D_{n,q,\alpha}^{LWE}(\mathbf{s})$  est la distribution discrète sur  $\mathbb{Z}_q^{n+1}$  obtenue par :

1.  $\mathbf{a} \leftarrow U(\mathbb{Z}_q^n)$
2.  $e \leftarrow D_{\mathbb{Z}^\ell, \alpha}$ , ie  $e$  est un vecteur court dans  $\mathbb{Z}^\ell$ .
3. Renvoyer  $(\mathbf{a}, (\mathbf{a} \cdot \mathbf{s}) + e \bmod q)$

On rappelle que le problème de **recherche** est de trouver  $\mathbf{s}$  à partir de tirages LWE, et que le problème de **décision** est de distinguer entre des tirages LWE et  $U(\mathbb{Z}_q^n \times \mathbb{Z}_q)$  avec probabilité  $1/2 + \text{constante}$  (disons  $3/4$ ).

Nous allons montrer :

**Lemma 1.** *Lorsque  $q$  est polynomial en  $n$ , Recherche-LWE et Décision-LWE sont équivalents en termes de complexité computationnelle.*

**Question 1.** *Montrer la réduction de Décision à Recherche : étant donné un algorithme  $\mathcal{A}$  qui résout le problème de Recherche, en déduire un algorithme pour résoudre le problème de Décision.*

**Question 2.** *Montrer que si l'on a un algorithme pour Décision-LWE qui fonctionne sur une entrée  $\mathbf{s}$  uniformément aléatoire (ce qui est l'hypothèse de départ), on peut contruire un algorithme fonctionnant sur une entrée  $\mathbf{s}$  quelconque fixée.*

**Question 3.** *Montrer que si l'on a un algorithme pour Décision-LWE, on peut construire un algorithme qui teste si  $s_0 = k$  pour un  $k \in \mathbb{Z}_q$  donné, où  $s_0$  est la première coordonnée de  $\mathbf{s}$ . En déduire que Recherche-LWE peut être réduit à Décision-LWE.*

## Chiffrement de Regev

On rappelle la définition du chiffrement de Regev.

### LWE PKE

KeyGen :

- Clé privée :  $\mathbf{s} \in \mathbb{Z}_q^n$  aléatoire
- Clé publique :  $(\mathbf{A}, \mathbf{b} := \mathbf{A}\mathbf{s} + e)$  où  $\mathbf{A}$  est une matrice aléatoire  $\mathbf{A} \in \mathbb{Z}_q^{\ell \times n}$ , et  $e \in \mathbb{Z}_q^\ell$  est échantillonné en utilisant la distribution d'erreurs "petites" (i.e., Gaussienne discrète)

Enc  $m \in \{0, 1\}$  :

- Choisir un vecteur aléatoire  $\mathbf{r} \in \{0, 1\}^\ell$
- Retourner  $\mathbf{c}_1, c_2 := \mathbf{r}\mathbf{A}, (\text{Decompress}(m) + \mathbf{r} \cdot \mathbf{b})$

Dec  $c = (\mathbf{c}_1, c_2) \in \mathbb{Z}_q^{n+1}$  :

- $m = \text{Compress}(c_2 - \mathbf{c}_1 \cdot \mathbf{s})$

**Question 4.** *Montrer que le chiffrement de Regev est additivement homomorph.*

**Question 5.** *En déduire qu'il n'est pas IND-CCA.*