Apprentissage avec erreurs

Définition du problème

- Soit $\mathbb{T} \cong \mathbb{R}/\mathbb{Z} \cong [0,1)$, étant donné $s \in \mathbb{Z}_q^n$, et ϕ une distribution sur $\mathbb{T}$
- On note $A_{s,\phi}$ la distribution sur $\mathbb{Z}_q^n \times \mathbb{T}$ telle que
  - On choisi $a \in \mathbb{Z}_q^n$ uniformément et $e \in \mathbb{T}$ par ϕ
  - On calcule $(a, (a \cdot s)/q + e)$
- Le problème $LWE_{q,\phi}$ demande à trouver $s \in \mathbb{Z}_q^n$ étant donné un nombre polynomial d'échantillons de $A_{s,\phi}$

Apprentissage avec erreurs
Schéma TFHE (clé secrète)

- $q > p$ des puissances de deux et $\Delta = q/p$
- χ une distribution Gaussienne centrée sur $\mathbb{Z}_q$
- $Gen(1^n) = s \xleftarrow{R} \{0,1\}^n$
- Avec $a \xleftarrow{R} \mathbb{Z}_q^n$ appelé le masque et l'erreur $e \xleftarrow{\chi} \mathbb{Z}_q$

$$Enc_s : \mathbb{Z}_p \to (\mathbb{Z}_q^n \times \mathbb{Z}_q) \qquad Dec_s : (\mathbb{Z}_q^n \times \mathbb{Z}_q) \to \mathbb{Z}_p$$

$$Enc_s(m) = (a, a \cdot s + \Delta m + e) \quad Dec_s(a, b) = (b - a \cdot s)/\Delta$$