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 $e \xleftarrow{\chi} \mathbb{Z}_q$

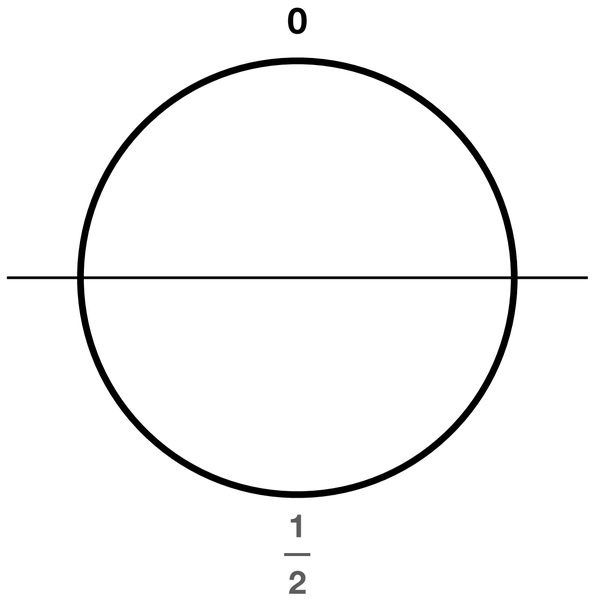
$$Enc_s : \mathbb{Z}_p \to (\mathbb{Z}_q^n \times \mathbb{Z}_q) \qquad Dec_s : (\mathbb{Z}_q^n \times \mathbb{Z}_q) \to \mathbb{Z}_p$$

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

Apprentissage avec erreurs

Schéma de Regev (clé publique)

- Clé privée: $sk = s \xleftarrow{R} \mathbb{Z}_q^n$
- Clé publique: $pk = (a_i, b_i = (a_i \cdot s)/q + e_i)_{i=1}^m \in (\mathbb{Z}_q^n \times \mathbb{T})^m$
  - Avec $a_1, \ldots, a_m \xleftarrow{R} \mathbb{Z}_q^n$ et $e_1, \ldots, e_m \xleftarrow{\chi} \mathbb{T}$
- Chiffrement: pour un $S \subseteq [m]$ aléatoire, $x \in \{0,1\}$



$$Enc_{pk}\colon \{0,1\} \to (\mathbb{Z}_q^n \times \mathbb{T})$$

$$Enc_{pk}(x) = \left(\sum_{i \in S} a_i, \frac{x}{2} + \sum_{i \in S} b_i \right)$$

$$Dec_{sk}\colon (\mathbb{Z}_q^n \times \mathbb{T}) \to \{0,1\}$$

$$Dec_{sk}(a,b) = \begin{cases} 0 \text{ si } \lfloor b - as \rceil_{\frac{1}{2}} = 0 \\ 1 \text{ sinon} \end{cases}$$