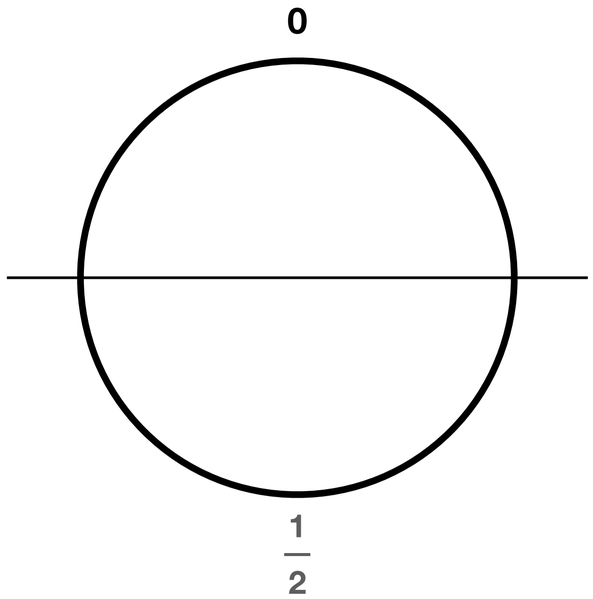
Apprentissage avec erreurs

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, $x \in \{0,1\}$



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

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

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

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

Apprentissage avec erreurs

Nécessité du bruit

- Clé privée: $s \xleftarrow{R} \mathbb{Z}_q^n$
- Clé publique: $(a_i, b_i = (a_i \cdot s)/q)_{i=1}^m$ avec $a_1, \ldots, a_m \xleftarrow{R} \mathbb{Z}_q^n$

$$\begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix} \times \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} \equiv_q q \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$