Apprentissage avec erreurs

Schéma de chiffrement

- $p < q$ des puissances de deux et $\Delta = q/p$
- Clé secrète: $s \xleftarrow{R} \{0,1\}^n$
- Avec $a \xleftarrow{R} \mathbb{Z}_q^n$ appelé le masque et l'erreur $e \xleftarrow{\phi} \mathbb{Z}_q$

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

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

- On a $Dec_s(Enc_s(m)) = m$ tant que $e < \Delta$

Apprentissage avec erreurs

Généralisation aux anneaux

- Rappel chiffrement d'un scalaire
- Avec $a \xleftarrow{R} \mathbb{Z}_q^n$ appelé le masque et l'erreur $e \xleftarrow{\chi} \mathbb{Z}_q$

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

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