

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

$$Enc_s: \mathbb{Z}_p \rightarrow (\mathbb{Z}_q^n \times \mathbb{Z}_q)$$

$$Dec_s: (\mathbb{Z}_q^n \times \mathbb{Z}_q) \rightarrow \mathbb{Z}_p$$

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

# Apprentissage avec erreurs

## Généralisation aux anneaux

- Soit  $\mathcal{R}_q = \mathbb{Z}_q[x]/(x^n + 1)$
- Avec  $A \xleftarrow{R} \mathcal{R}_q$  appelé le masque et l'erreur  $E \xleftarrow{\chi} \mathcal{R}_q$

$$Enc_s: \mathcal{R}_p \rightarrow (\mathcal{R}_q \times \mathcal{R}_q)$$

$$Dec_s: (\mathcal{R}_q \times \mathcal{R}_q) \rightarrow \mathcal{R}_p$$

$$Enc_s(M) = (A, A \cdot S + \Delta M + E) \quad Dec_s(A, B) = (B - A \cdot S) / \Delta$$