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

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

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

Apprentissage avec erreurs

Généralisation aux anneaux

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

$$Enc_s: \mathscr{R}_p \to (\mathscr{R}_q \times \mathscr{R}_q) \qquad Dec_s: (\mathscr{R}_q \times \mathscr{R}_q) \to \mathscr{R}_p$$

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