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 $E \xleftarrow{\chi} \mathscr{R}_q$

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

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

Apprentissage avec erreurs (Anneaux)

Schéma de signature: GLYPH

- Soit $A \xleftarrow{R} \mathscr{R}_q$
- $H : \{0,1\}^n \to \mathscr{R}_q$ tel que les coefficients sont nuls sauf k qui sont $< b$
- Clé privée: $S, E \in \mathscr{R}_q$ petits
- Clé publique: $T = AS + E$