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: $T = AS + E$

Apprentissage avec erreurs (Anneaux)

Schéma de signature: GLYPH

- Pour signer des bits m
  - Générer $Y_1, Y_2 \in \mathcal{R}_q$ petits
  - Calcule $W = AY_1 + Y_2$ (Mapping to bits ω)
  - $C = H(\omega \,|\, m)$
  - $Z_1 = SC + Y_1$ et $Z_2 = EC + Y_2$
- Répète tant que Z_1 ou Z_2 trop grand
- Signature de m est (C, Z_1, Z_2)