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

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

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

Conclusion

Résumé et ouverture

- Réseaux Euclidiens pas directement utilisés dans les schémas
- Mais la sécurité dépend de la difficulté du SVP
- Il existe plusieurs autres schémas basés sur LWE (et donc SVP)
  - Chiffrement asymétrique (encryptions de zéro comme clé publique)
  - Échange de clés (schéma RLWE-KEX)
  - Signatures basées sur $RLWE$ (schéma GLYPH)
  - Chiffrement complètement homomorphe (schéma TFHE)