

Bootstrapping fonctionnel de CKKS discret [AKP25]

Théorie de l'approximation pour le calcul exact

Plan de la présentation

Interpolation et Évaluation de polynôme dans CKKS

- Rappels du schéma CKKS
- Algorithme de bootstrapping fonctionnel
- Évaluation de polynôme de Paterson-Stockmeyer (minimiser les multiplications coûteuses)
- Interpolation de Vandermonde (algèbre linéaire) / Lagrange (algorithme efficace)
- Interpolation Tchebychev (minimiser l'erreur d'interpolation)
- Interpolation d'Hermite (contraindre les dérivées pour nettoyer le bruit)