

Bootstrapping CKKS

Original bootstrapping [CHKKS18]

- [CKKS17] Permet d'évaluer des circuits arithmétiques finis
 - Chaque multiplication consomme un “niveau”

Bootstrapping CKKS

Original bootstrapping [CHKKS18]

- [CKKS17] Permet d'évaluer des circuits arithmétiques finis
 - Chaque multiplication consomme un “niveau”
- [CKKS18] Permet l'évaluation de circuits arithmétiques quelconques
 - Évaluation de la fonction de déchiffrement en aveugle
 - Approximation polynomiale de la fonction de réduction de module
 - Rafraîchit le nombre de “niveau” et PAS le bruit des cryptogrammes (y contribue)