Plan de l'exposé

Implémentation de BlindSort dans RevoLUT

1. Chiffrement homomorphe
    1.1. (Generalized) Learning With Errors in TFHE
    1.2. Boite à outils RevoLUT
2. Blind Sort
    2.1. Première implémentation
    2.2. Deuxième implémentation

Chiffrement homomorphe

Objectif: calcul privé

- Alice possède des données privées
- Elle chiffre ses données et envoi le chiffré à Bob
- Bob effectue un calcul sur les données chiffrées et renvoi le chiffré résultant à Alice
- Alice déchiffre le résultat du calcul (fait en aveugle par Bob)