

TFHE

Fast Fully Homomorphic Encryption over the Torus

- Schéma de chiffrement complètement homomorphe
- Implémenté par la librairie TFHE-rs 🦀
- Primitives cryptographiques:
 - Blind Arithmetic
 - Blind Comparison
 - Blind Function Evaluation

RevoLUT

LookUp Table avec rotation aveugle

- Une LUT est un tableau de taille fixe de n chiffrés d'entiers modulo n
- Primitives supplémentaires de RevoLUT
 - Blind Rotation
 - Blind Array Access
 - Blind Matrix Access
 - Blind Permutation