Historique

Chiffrement homomorphe

- Pre-FHE: Sous-ensemble des circuits arithmétiques (RSA, ElGamal, Paillier)
- FHE 1st gen: Tout circuit arithmétiques grâce au **bootstrapping** [Gentry09], [DGHV11]
- FHE 2nd gen: Début des schémas basés sur (R)-LWE, parallélisme SIMD [BGV11], [BFV12]
- FHE 3rd gen: Bootstrapping rapide et **programmable** (pas SIMD) [GSW13], [DM14], [CGGI16]
- FHE 4th gen: Chiffrement approximatif, parallélisme SIMD [CKKS17]

Historique

Chiffrement homomorphe

- Pre-FHE: Sous-ensemble des circuits arithmétiques (RSA, ElGamal, Paillier)
- FHE 1st gen: Tout circuit arithmétiques grâce au **bootstrapping** [Gentry09], [DGHV11]
- FHE 2nd gen: Début des schémas basés sur (R)-LWE, parallélisme SIMD [BGV11], [BFV12]
- FHE 3rd gen: Bootstrapping rapide et **programmable** (pas SIMD) [GSW13], [DM14], [CGGI16]
- FHE 4th gen: Chiffrement approximatif, parallélisme SIMD [CKKS17]

[AKP25] introduit un bootstrapping programmable dans CKKS