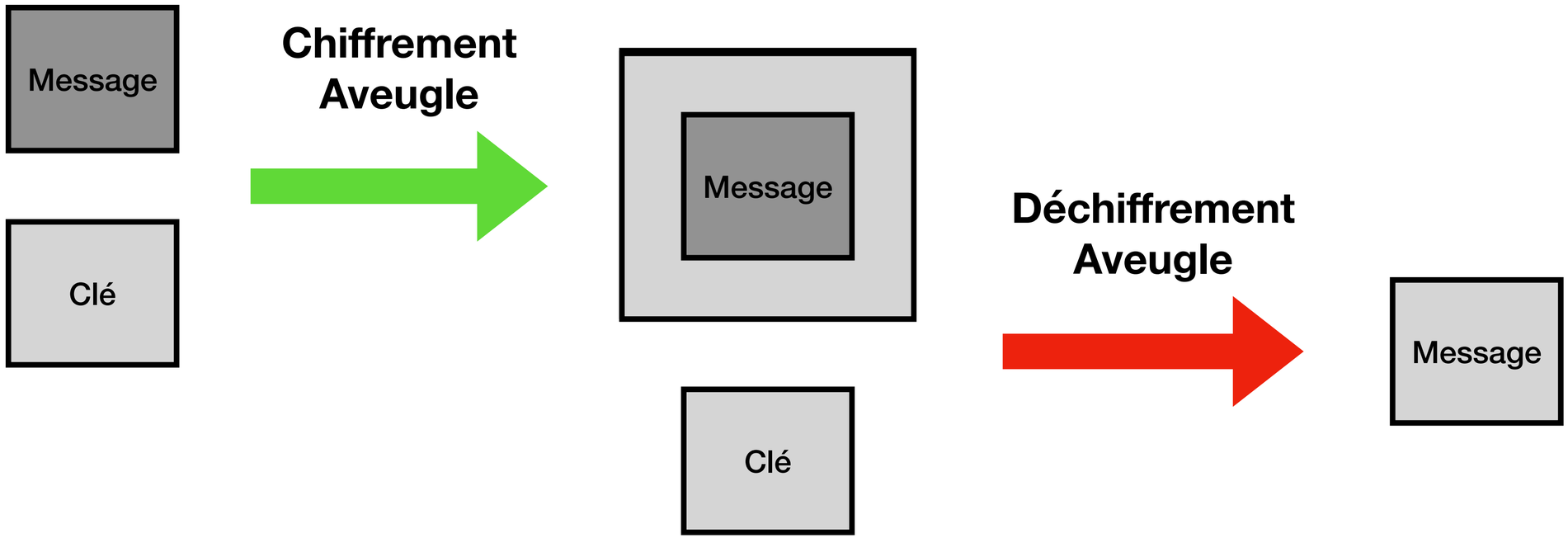
Bootstrapping

Conceptuellement [Gentry09]



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]