

Chiffrement partiellement homomorphe

Problème du bruit dans Learning With Errors (LWE)

- Un schéma basé sur le problème LWE introduit du **bruit** dans le cryptogramme, et les opérations homomorphes accumulent le bruit jusqu'à **corrompre le cryptogramme**.
- Le **bootstrapping** permet de régler ce problème en maintenant le niveau de bruit sous un seuil acceptable.

Chiffrement partiellement homomorphe

Accumulation de bruit

