Plan de l’exposé

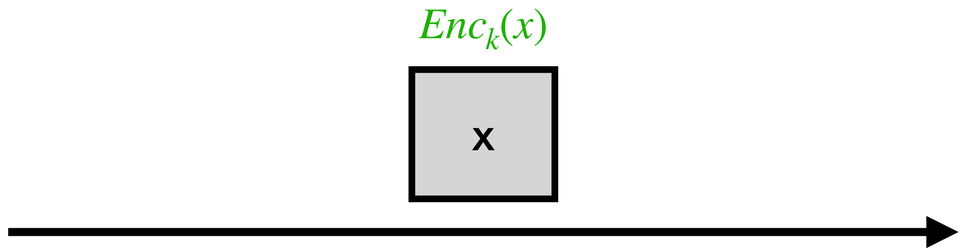
Résumé de l’article de Gentry

- Introduction au calcul privé
- Chiffrement partiellement homomorphe
- Chiffrement complètement homomorphe
- Bootstrapping

Introduction

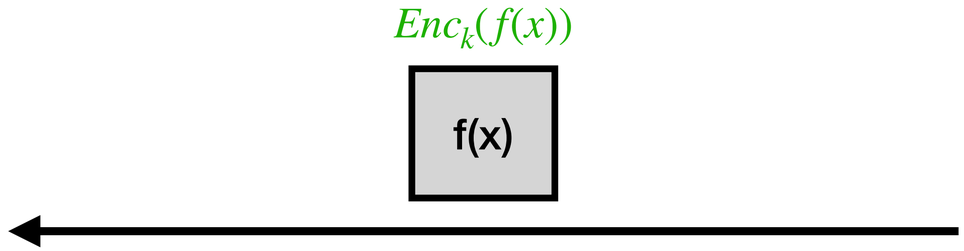
Calcul par un tiers (actuellement)

- Alice souhaite faire faire le calcul **f(x)** à Bob, et doit lui révéler **x**.
- Alice chiffre **x** à l'aide d'un secret partagé avec Bob.



Protection contre l'espionnage

- Bob déchiffre **x**, calcule **f(x)**, re-chiffre le résultat et le renvoie à Alice.



Pas contre un Bob un peu trop curieux