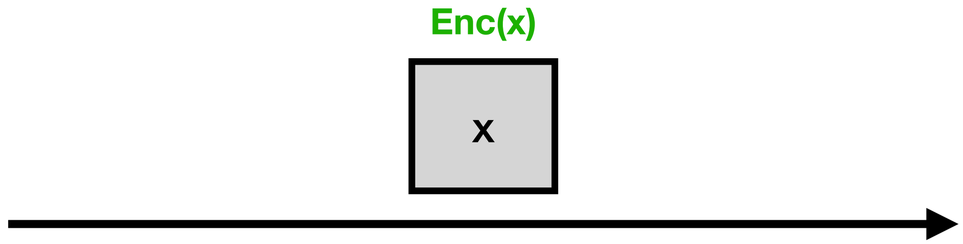
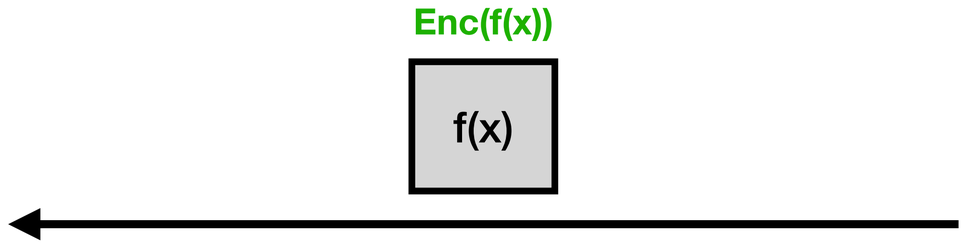
Introduction

Calcul en aveugle

- Alice souhaite faire faire le calcul **f(x)** à Bob sans révéler **x**.
- Alice chiffre **x** à l'aide d'un chiffrement complètement homomorphe Enc



- Bob calcule f en aveugle sur le chiffré de x pour produire le chiffré de f(x)



$$f(Enc(x)) = Enc(f(x))$$

Chiffrement partiellement homomorphe

Problème du bruit dans le schéma de Gentry

- La construction initiale de Gentry 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.