Introduction

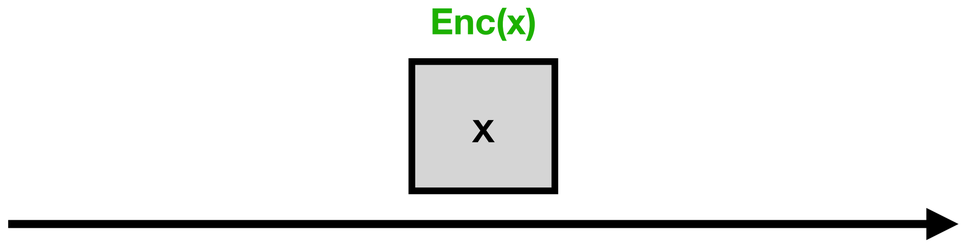
Calcul en aveugle

- **Chiffrement homomorphe**: Il s'agit d'un schéma permettant d'effectuer du calcul sur des données chiffrées sans avoir à les déchiffrer.
- On appelle **partiellement** homomorphe un schéma permettant cela pour certains calculs ou avec certaines limitations. (Par exemple RSA)
- On appelle **complètement** homomorphe un schéma permettant cela pour des calculs arbitraires.

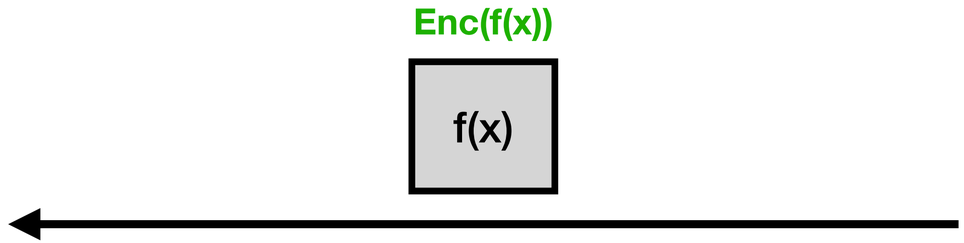
Introduction

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)



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