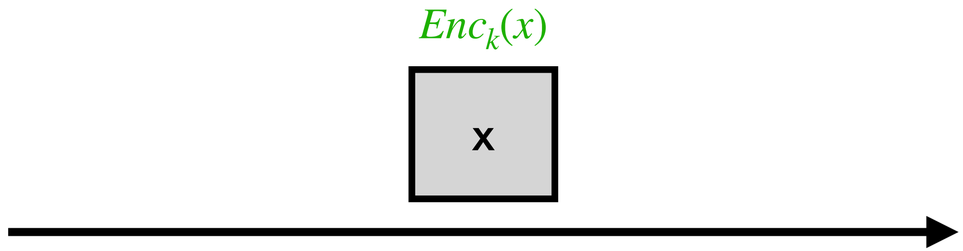
Introduction

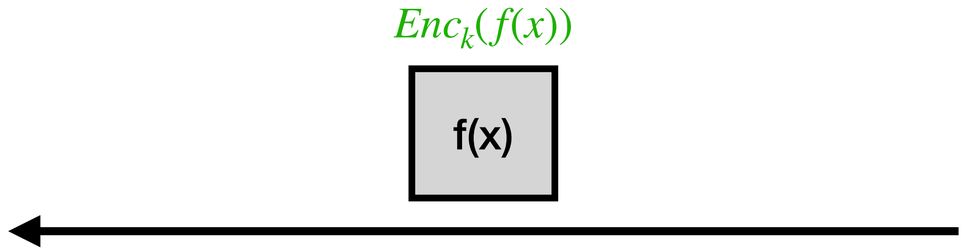
Calcul par un tiers (actuellement)

- 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

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.