# Plan de l’exposé

## Fully homomorphic encryption using ideal lattices (Gentry, 2009)

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

# 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.