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

Présentation de l'article de Gentry

- Gentry propose un premier schéma complètement homomorphe.
- Son schéma se base sur une nouvelle technique appelée "**bootstrapping**".

Schéma capable d'évaluer son propre algorithme en aveugle

$\Longrightarrow$ Schéma complètement homomorphe