Introduction

Fully homomorphic encryption using ideal lattices (Gentry, 2009)

- 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

Plan de l’exposé

Résumé de l’article de Gentry

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