

# **Chiffrement complètement homomorphe**

**Une introduction au bootstrapping**

**Félix Larose-Gervais, Mars 2024**

# 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

$\implies$  Schéma complètement homomorphe