Problème du tri aveugle

Introduction

- Étant donné un tableau de valeurs chiffrées
- On cherche à trier le tableau sans déchiffrer les entrées

- **Motivation**: performance de calcul confidentiel (recherche, apprentissage automatique…)

Problème du tri aveugle

Chiffrement homomorphe

- Fonction de chiffrement préserve les opérations de calcul

$$Enc(a + b) \equiv Enc(a) + Enc(b)$$

$$Enc(a \times b) \equiv Enc(a) \times Enc(b)$$

- LookUp Tables (LUT) permet d'évaluer en aveugle $f(x)$ pour un x chiffré