Chiffrement homomorphe

Objectif: calcul privé

- Alice possède des données privées
- Elle chiffre ses données et envoi le chiffré à Bob
- Bob effectue un calcul sur les données chiffrées et renvoi le chiffré résultant à Alice
- Alice déchiffre le résultat du calcul (fait en aveugle par Bob)

Chiffrement homomorphe

Définition

- Un schéma de chiffrement (Enc, Dec) est dit (complètement) **homomorphe** si pour tous messages x, y on a:

$$Enc(x + y) \equiv_{Dec} Enc(x) \oplus Enc(y)$$

$$Enc(x \times y) \equiv_{Dec} Enc(x) \otimes Enc(y)$$

- Similaire à la notion de morphisme en algèbre
- Permet le calcul privé