Définitions

Chiffrement homomorphe

- Un schéma est homomorphe si sa fonction de chiffrement est un homomorphisme
- Par exemple le chiffrement RSA $(Enc(m) = m^e \pmod N)$ est un morphisme multiplicatif

$$
\begin{aligned}
Enc(m_1) \times Enc(m_2) &= m_1^e m_2^e \pmod N \\
&= m_1 \cdots m_1 m_2 \cdots m_2 \pmod N \\
&= (m_1 m_2) \cdots (m_1 m_2) \pmod N \\
&= (m_1 m_2)^e \pmod N \\
&= Enc(m_1 m_2)
\end{aligned}
$$

- Permet d'évaluer la multiplication en **aveugle** (privacy homomorphism [RAD78])

Historique

Chiffrement homomorphe

- Pre-FHE: Sous-ensemble des circuits arithmétiques (RSA, ElGamal, Paillier)