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

Chiffrement homomorphe

Learning With Errors in TFHE

Soient $p, q, n \in \mathbb{N}$ tels que $p < q$ des puissances de 2, et une distribution $\chi_\sigma \sim N(\mu = 0, \sigma)$

Le chiffre LWE, avec une clé secrète $\vec{s} \in \{0,1\}^n$ est défini par:

$$Enc_{\vec{s}} : \mathbb{Z}_p \to \mathbb{Z}_q^n \times \mathbb{Z}_q \qquad Dec_{\vec{s}} : \mathbb{Z}_q^n \times \mathbb{Z}_q \to \mathbb{Z}_p$$

$$m \mapsto (\vec{a}, \vec{a} \cdot \vec{s} + \Delta m + e) \qquad (\vec{a}, b) \mapsto (b - \vec{a} \cdot \vec{s})/\Delta$$

Où $\vec{a} \in_R \mathbb{Z}_{q'}^n$ $e \in_{\chi_\sigma} \mathbb{Z}_q$ et $\Delta = \frac{p}{q}$