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 $\Delta = \dfrac{p}{q}$

Chiffrement homomorphe

Ring Learning With Errors in TFHE

Soit $\mathcal{R}_q = \mathbb{Z}_q[X]/\langle X^N + 1\rangle$ l'anneau des polynômes sur $\mathbb{Z}_q$ de degré inférieur à N

On défini le chiffre RLWE, à clé secrète $S \in \mathcal{R}_q$ avec $s_i \in \{0,1\}$ par:

$$Enc_S \colon \mathcal{R}_p \to \mathcal{R}_q \times \mathcal{R}_q \qquad\qquad Dec_S : \mathcal{R}_q \times \mathcal{R}_q \to \mathcal{R}_p$$

$$M \mapsto (A, A \cdot S + \Delta M + E) \qquad\qquad (A, B) \mapsto (B - A \cdot S)/\Delta$$

Où $A \in_R \mathcal{R}_{q'}$ $E \in_{\chi_\sigma} \mathcal{R}_q$ et $\Delta = \dfrac{p}{q}$