Chiffrement homomorphe approximatif CKKS

Ring Learning With Errors (RLWE)

- On note $\mathscr{R} = \mathbb{Z}_q[X]/(X^N + 1)$ les polynômes de degré N à coefficients entiers modulo q
- Le chiffrement d'un message $m \in \mathscr{R}$ sous la clé $s \in \mathscr{R}$ avec aléas $a, e \xleftarrow{\$} \mathscr{R}$ est

$$Enc_s(m) = (-as + m + e, a) \in \mathscr{R}^2$$

$$Dec_s(b, a) = b + as = m + e \approx m$$

Chiffrement homomorphe approximatif CKKS

Arithmétique aveugle

$\mathcal{R} = \mathbb{Z}_q[X]/(X^N + 1)$

- La fonction de chiffrement est un homomorphisme $\mathcal{R} \to \mathcal{R}^2$:
  - Additif: $Enc_s(m_1) + Enc_s(m_2) = Enc_s(m_1 + m_2)$
  - Linéaire: $\alpha \cdot Enc_s(m) + \beta = Enc_s(\alpha \cdot m + \beta)$
  - Multiplicatif: $Enc_s(m_1) \cdot Enc_s(m_2) = Enc_s(m_1 \cdot m_2)$
    - (Nécessite relinéarisation, clé d'évaluation)
- Permet d'évaluer des expressions arithmétique ou des polynômes sur les chiffrés