Chiffrement homomorphe approximatif CKKS

Arithmétique aveugle

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

- La fonction de chiffrement est un homomorphisme $\mathscr{R} \to \mathscr{R}^2$:
  - 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

Encodage en vecteurs complexes

Paradigme Single Instruction Multiple Data (SIMD)

$$\mathcal{R} = \mathbb{Z}_q[X]/(X^N + 1)$$
$$\Phi_M(X) = X^N + 1$$
$$M = 2N$$

- Un polynôme $a(x) \in \mathbb{C}[X]/\Phi_M(X)$ peut être plongé dans $\mathbb{C}^N$

$$\sigma : \mathbb{C}[X]/\Phi_M(X) \to \mathbb{C}^N$$

$$a(x) \overset{\sigma}{\mapsto} \left(a(\zeta_M^k)\right)_{k \in \mathbb{Z}_M^\times}$$

- Avec ζ_M^k les N puissances impaires des racines M-ième de l'unité

$$\sigma(a_1 + a_2) = \sigma(a_1) + \sigma(a_2)$$

Polynômes Vecteurs

$$\sigma(a_1 \cdot a_2) = \sigma(a_1) \odot \sigma(a_2)$$