Survol de TFHE

Rotation aveugle

$$LWE \times RLWE \rightarrow RLWE$$

- Soit un indice de rotation chiffré π et un polynôme chiffré $M = m_0 + m_1 X + \ldots + m_{N-1} X^{N-1}$
- La rotation aveugle permet de calculer $M \cdot X^{-\pi} \pmod{X^N - 1}$
- La rotation est **bruitée**, donc on encode en boites de redondance

$$\underbrace{2X^i + \ldots + 2X^{i+\Delta}}_{2}$$

Survol de TFHE

Rotation aveugle

$$LWE \times RLWE \rightarrow RLWE$$

- Soit un indice de rotation chiffré π et un polynôme chiffré $M = m_0 + m_1 X + \ldots + m_{N-1} X^{N-1}$
- La rotation aveugle permet de calculer $M \cdot X^{-\pi} \pmod{X^N - 1}$
- La rotation est **bruitée**, donc on encode en boites de redondance $\underbrace{2X^i + \ldots + 2X^{i+\Delta}}_{2}$
- La rotation est **négacyclique** à gauche de π positions

$$m_\pi + m_{\pi+1} X + \ldots + m_{N-1} X^{N-\pi-1} - m_0 X^{N-\pi} - \ldots - m_{\pi-1} X^{N-1}$$