

Survol de TFHE

Rotation aveugle

$$LWE \times RLWE \rightarrow RLWE$$

- Soit un indice de rotation chiffré π et un polynôme chiffré $M = m_0 + m_1X + \dots + m_{N-1}X^{N-1}$
- La rotation aveugle permet de calculer $M \cdot X^{-\pi} \pmod{X^N - 1}$

Survol de TFHE

Rotation aveugle

$$LWE \times RLWE \rightarrow RLWE$$

- Soit un indice de rotation chiffré π et un polynôme chiffré $M = m_0 + m_1X + \dots + m_{N-1}X^{N-1}$
- La rotation aveugle permet de calculer $M \cdot X^{-\pi} \pmod{X^N - 1}$
- La rotation est **bruitée**, donc on encode en boîtes de redondance

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