

# Survol de TFHE

## Rotation aveugle

$$LWE \times RLWE \rightarrow RLWE$$

- Soit un indice de rotation chiffré  $\pi$  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  $\frac{2X^i + \dots + 2X^{i+\Delta}}{2}$
- La rotation est **négacyclique** à gauche de  $\pi$  positions

$$m_{\pi} + m_{\pi+1}X + \dots + m_{N-1}X^{N-\pi-1} - m_0X^{N-\pi} - \dots - m_{\pi-1}X^{N-1}$$

# Survol de TFHE

## Rotation aveugle

$$LWE \times RLWE \rightarrow RLWE$$

- Soit un indice de rotation chiffré  $\pi$  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 boites de redondance  $\frac{2X^i + \dots + 2X^{i+\Delta}}{2}$
- La rotation est **négacyclique** à gauche de  $\pi$  positions

$$m_{\pi} + m_{\pi+1}X + \dots + m_{N-1}X^{N-\pi-1} - m_0X^{N-\pi} - \dots - m_{\pi-1}X^{N-1}$$

