Survol de TFHE

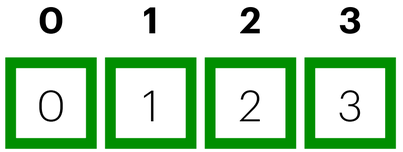
Chiffrement GLWE (LWE ou RLWE)

LWE: Chiffré de scalaire

Key Switching (Slow)

Sample Extract (Fast)

RLWE: Chiffré de polynôme



$$0 + 1 + 2x^2 + 3x^3$$

$$GLWE + GLWE \qquad GLWE + CLEAR \qquad GLWE \times CLEAR$$

Survol de TFHE

Rotation aveugle

$$LWE \times RLWE \rightarrow RLWE$$