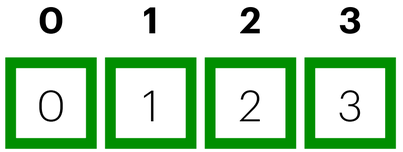
Survol de TFHE

Chiffrement GLWE (LWE ou RLWE)

LWE: Chiffré de scalaire

RLWE: Chiffré de polynôme

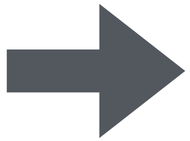


$$0 + 1 + 2x^2 + 3x^3$$

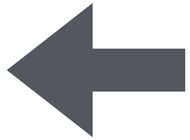
Survol de TFHE

Chiffrement GLWE (LWE ou RLWE)

LWE: Chiffré de scalaire

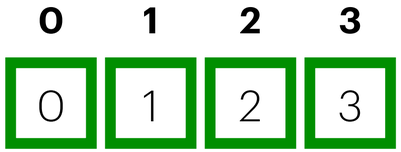


Key Switching (Slow)



Sample Extract (Fast)

RLWE: Chiffré de polynôme



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