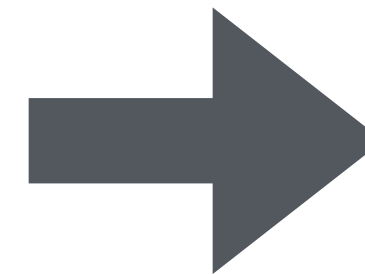


# Survol de TFHE

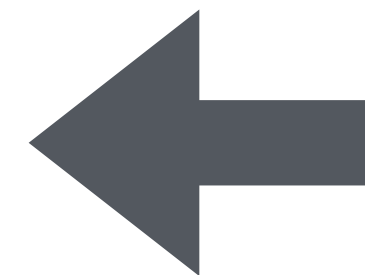
Chiffrement GLWE (LWE ou RLWE)

**LWE:** Chiffré de scalaire

2



Key Switching (Slow)



Sample Extract (Fast)

**RLWE:** Chiffré de polynôme

0	1	2	3
0	1	2	3

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

# Survol de TFHE

Chiffrement GLWE (LWE ou RLWE)

**LWE:** Chiffré de scalaire

2

$GLWE + GLWE$

Key Switching (Slow)

Sample Extract (Fast)

$GLWE + CLEAR$

**RLWE:** Chiffré de polynôme

0	1	2	3
0	1	2	3

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

$GLWE \times CLEAR$