

Survol de TFHE

Évaluation aveugle

$$\cancel{RWE} \times \cancel{RLWE} \rightarrow LWE$$

- Obtenir un chiffré de $f(x)$ étant donné un chiffré de x
- On peut encoder n'importe quelle fonction f en un polynôme LUT

m_0	m_1	m_2	m_3
$f(0)$	$f(1)$	$f(2)$	$f(3)$

- Une rotation aveugle de x place $f(x)$ en première position

$$Eval = SampleExtract \circ BlindRotate$$

Survol de TFHE

Évaluation aveugle

$$RLWE \times LWE \rightarrow LWE$$

- Obtenir un chiffré de $f(x)$ étant donné un chiffré de x
- On peut encoder n'importe quelle fonction f en un polynôme LUT

m_0	m_1	m_2	m_3
$f(0)$	$f(1)$	$f(2)$	$f(3)$

- Une rotation aveugle de x place $f(x)$ en première position

$$Eval = SampleExtract \circ BlindRotate$$