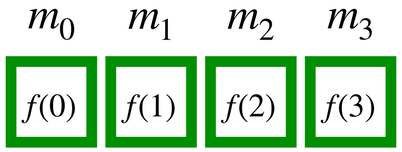
Survol de TFHE

Évaluation aveugle

$$RLWE \times LWE \rightarrow LWE$$

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



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

$$Eval = SampleExtract \circ BlindRotate$$

Survol de TFHE

Évaluation aveugle multi-variée (TreePBS) [Guimarães, 21]

$$f(x, y, z) : \mathbb{Z}_p^3 \to \mathbb{Z}_p$$

- Posons $p = 4$, on veut évaluer une fonction à 3 variables (p^3 entrées)