Survol de TFHE

Évaluation aveugle

$$LWE \times RLWE \rightarrow LWE$$

- Obtenir un chiffré de $f(x)$ étant donné un chiffré de x

Survol de TFHE

Évaluation aveugle

$$LWE \times RLWE \rightarrow LWE$$

- 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