



TLwe( $\mathbf{b}$ )

$\mathbb{T}[X]$

$$c_b = z + (\mathbf{0}, b)$$

TGsw( $\mathbf{A}$ )

$\mathbb{Z}[X]$

$$\mathbf{C}_{\mathbf{A}} = \mathbf{Z} + \mathbf{A} \cdot \mathbf{h}$$

New external

$$\mathbf{C}_{\mathbf{A}} \boxdot c_b = \text{Decomp}_{\mathbf{h}}(c_b) \cdot \mathbf{C}_{\mathbf{A}}$$

is a TLwe ciphertext of  $A \cdot b$

Classical internal

$$\mathbf{C}_{\mathbf{A}} \boxtimes \mathbf{C}_{\mathbf{B}} = \text{Decomp}_{\mathbf{h}}(\mathbf{C}_{\mathbf{B}}) \cdot \mathbf{C}_{\mathbf{A}}$$

is a TGsw ciphertext of  $A \cdot B$