

Cleaning error in CKKS

BLEACH: Via polynomial approximation [DMPS24]

$$b \in \{0,1\} \iff b + \epsilon \in \mathbb{R}$$

For small ϵ

$$b_1 \wedge b_2 = b_1 \cdot b_2$$

$$b_1 \vee b_2 = b_1 + b_2 - b_1 \cdot b_2$$

$$b_1 \oplus b_2 = (b_1 - b_2)^2$$

Cleaning error in CKKS

BLEACH: Via polynomial approximation [DMPS24]

$$b \in \{0,1\} \iff b + \epsilon \in \mathbb{R}$$

For small ϵ

$$b_1 \wedge b_2 = b_1 \cdot b_2$$

$$b_1 \vee b_2 = b_1 + b_2 - b_1 \cdot b_2$$

$$b_1 \oplus b_2 = (b_1 - b_2)^2$$

On sait évaluer des polynômes en aveugle