IND-CPA$^{\mathrm{D}}$ (Li and Micciancio, 2020)

IND-CPA with (restricted) Decryption oracle, not quite CCA

- **IND-CPA$^{\mathrm{D}}$** is a game against an adversary $\mathscr{A}$ having access to an oracle $\mathscr{O}$ (for random $k \in \mathscr{K}$, $b \in \mathbb{B}$)
    1. $\mathscr{A}$ gets $c_i \leftarrow Enc_k(m_{i,b})$ from $\mathscr{O}$ for messages $m_{i,0}, m_{i,1} \in \mathscr{P}$ of their choosing
        1. $\mathscr{O}$ keeps track of $(m_{i,0}, m_{i,1}, c_i)$
    2. $\mathscr{A}$ gets $c \leftarrow c_i \circ c_j$ from $\mathscr{O}$ for a binary operation $\circ$ and valid indices i, j of their choosing
        1. $\mathscr{O}$ keeps track of $(m_{i,0} \circ m_{j,0}, m_{i,1} \circ m_{j,1}, c)$
    3. $\mathscr{A}$ gets $m_i \leftarrow Dec_k(c_i)$ from $\mathscr{O}$ for ciphertexts $c_i \in \mathscr{C}$ (iff $m_{i,0} = m_{i,1}$) for valid index i of their choosingp
    4. $\mathscr{A}$ guesses $b' \in \mathbb{B}$ and wins if and only if $b = b'$
- A cryptosystem is **CPA$^{\mathrm{D}}$ secure** if no adversary wins this game more than half the time

$$CPA \subset CPA^D \subset CCA$$

A new notion for FHE schemes