Crypto refresher

IND-CCA: Indistinguishability under Chosen Ciphertext Attack

- **IND-CCA** is a game against an adversary $\mathscr{A}$ having access to an oracle $\mathcal{O}$

  1. Game chooses $k \in \mathcal{K}$, $b \in \mathbb{B}$ and $m_0, m_1 \in \mathcal{P}$ and sends $c \leftarrow Enc_k(m_b)$ to $\mathscr{A}$
  2. $\mathscr{A}$ gets $c_i \leftarrow Enc_k(m_i)$ from $\mathcal{O}$ for messages $m_i \in \mathcal{P}$ of their choosing
  3. $\mathscr{A}$ gets $\tilde{m}_i \leftarrow Dec_k(c_i)$ from $\mathcal{O}$ for ciphertext $c_i \in \mathcal{C}$ of their choosing (except c)
  4. $\mathscr{A}$ guesses $b' \in \mathbb{B}$ and wins if and only if $b = b'$

- A cryptosystem is **CCA secure** if no adversary wins this game more than half the time

$$CPA \subset CCA$$

FHE schemes are malleable and by definition not CCA secure