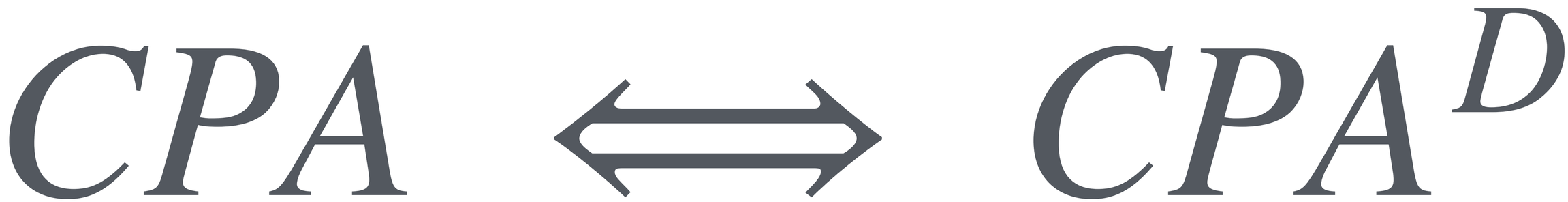

For traditional cryptosystems

IND-CPA^D (Li and Micciancio, 2020)

Why is that important?

- Approximate FHE schemes (like CKKS) leak the noise

$$\begin{cases} Enc_s(m) = (\vec{a}, \langle \vec{a}, \vec{s} \rangle + m + e) \\ Dec_s(\vec{a}, b) = b - \langle \vec{a}, \vec{s} \rangle \end{cases}$$

Toy approximate scheme

- Since we have $Dec_s(Enc_s(m)) = m + e$, then $\mathcal{A}$ can

1. Query $\mathcal{O}$ for $(\overrightarrow{a_i}, b_i)$ the encryptions of m_i and $\tilde{m}_i$ the decryptions of $(\overrightarrow{a_i}, b_i)$

2. Solve $As = b - \tilde{m}$ for s to recover the secret key