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 $\mathscr{A}$ can

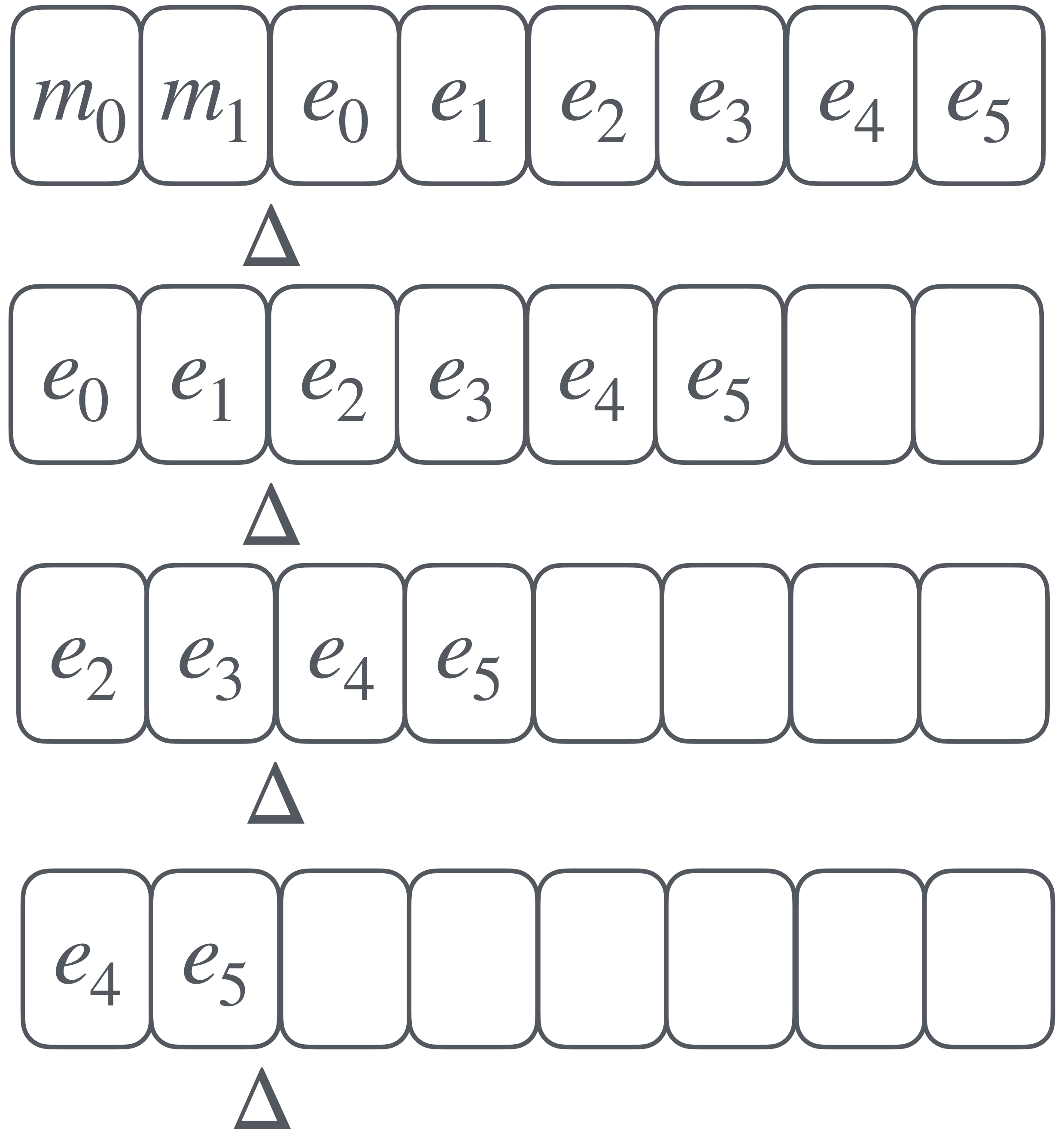
1. Query $\mathcal{O}$ for $(\overrightarrow{a_i}, b_i)$ the encryptions of m_i and $\tilde{m}_i$ the decryptions of $(\overrightarrow{a_i}, b_i)$
2. Solve $As = b - \tilde{m}$ for s to recover the secret key

IND-CPA^D (Cheon et al, 2024)

Attacks against exact FHE schemes

- Showed that it's not a flaw of approximate FHE

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



Loop $\frac{\log_2 \Delta}{\log_2 p}$ times:

    Loop $\log_2 p$ times:

        $c \leftarrow c + c$ // shift left 1 bit

    Leak $\log_2 p$ bits of noise from $\mathcal{O}$