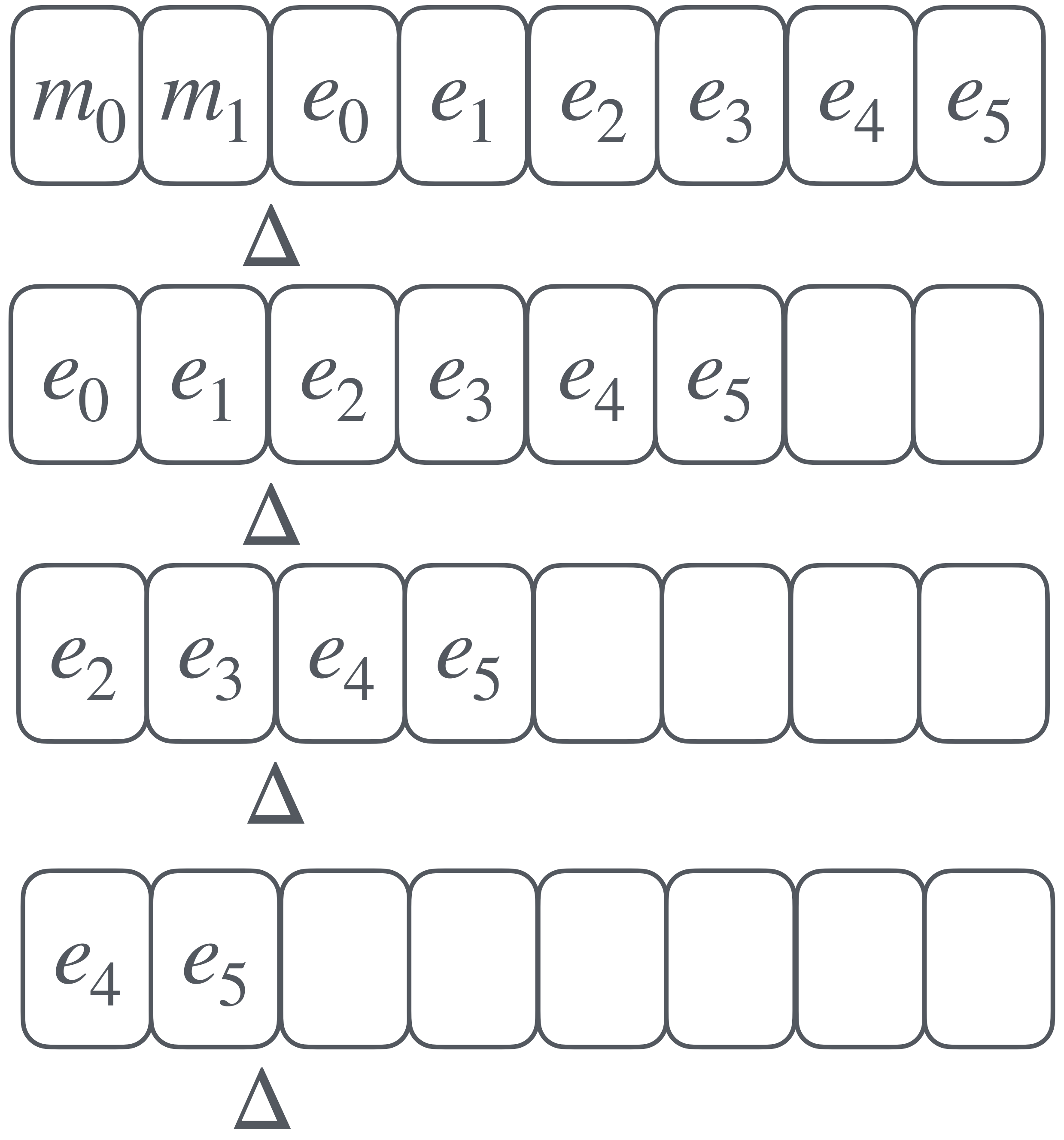
IND-CPA^D (Cheon et al, 2024)

Attacks against exact FHE schemes

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

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



m_0 m_1 e_0 e_1 e_2 e_3 e_4 e_5

Δ

e_0 e_1 e_2 e_3 e_4 e_5

Δ

e_2 e_3 e_4 e_5

Δ

e_4 e_5

Δ

```
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 $\mathcal{O}$
```

Conclusion

Food for thought

- Traditional security notions don’t necessarily apply as-is to FHE
  - Usually giving out decryptions gives the adversary no advantage in IND-CPA
  - But it can on LWE-based schemes
- Attacks against the real cryptosystems (BGV, BFV, TFHE, CKKS, …) are more nuanced
  - Details in the respective papers