Odds and ends

Deterministic Encryption

The need for det. Encryption (no nonce)

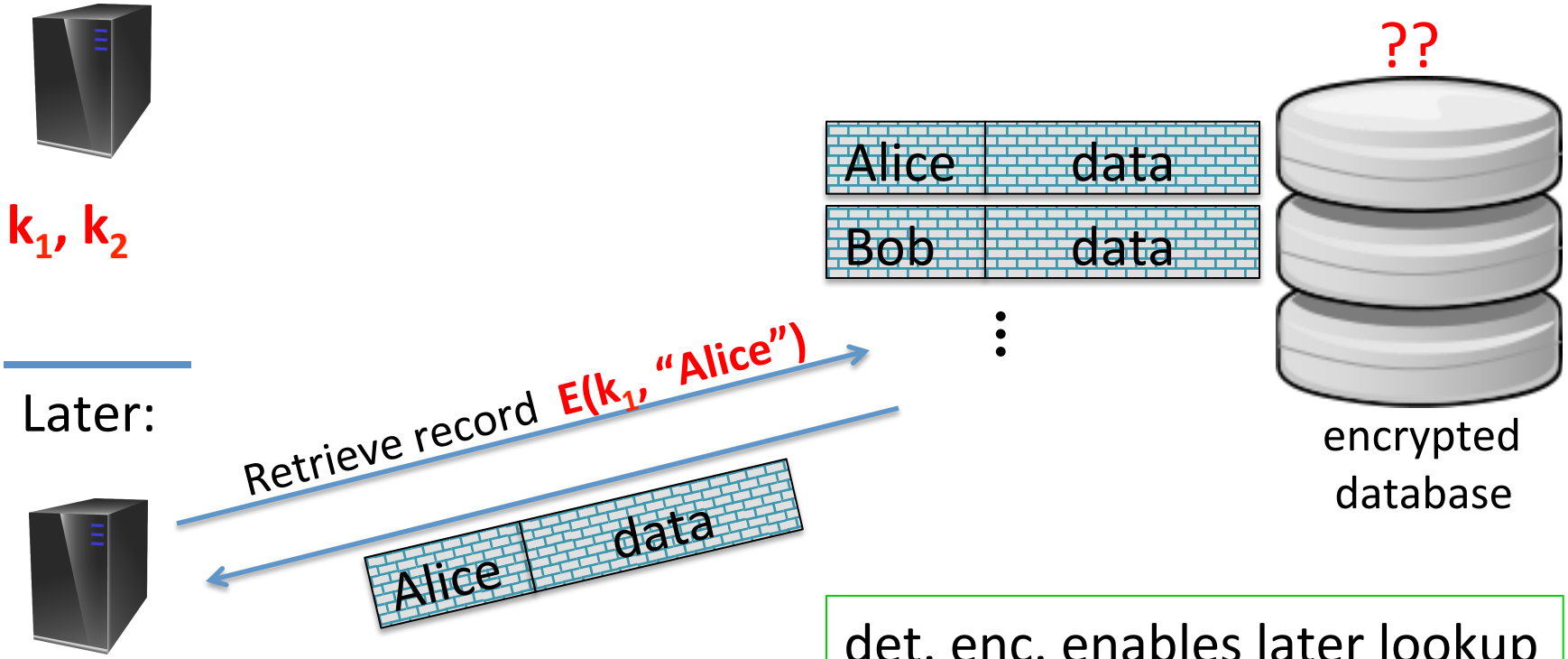
Alice | data

k_1, k_2

Bob | data

encrypted database

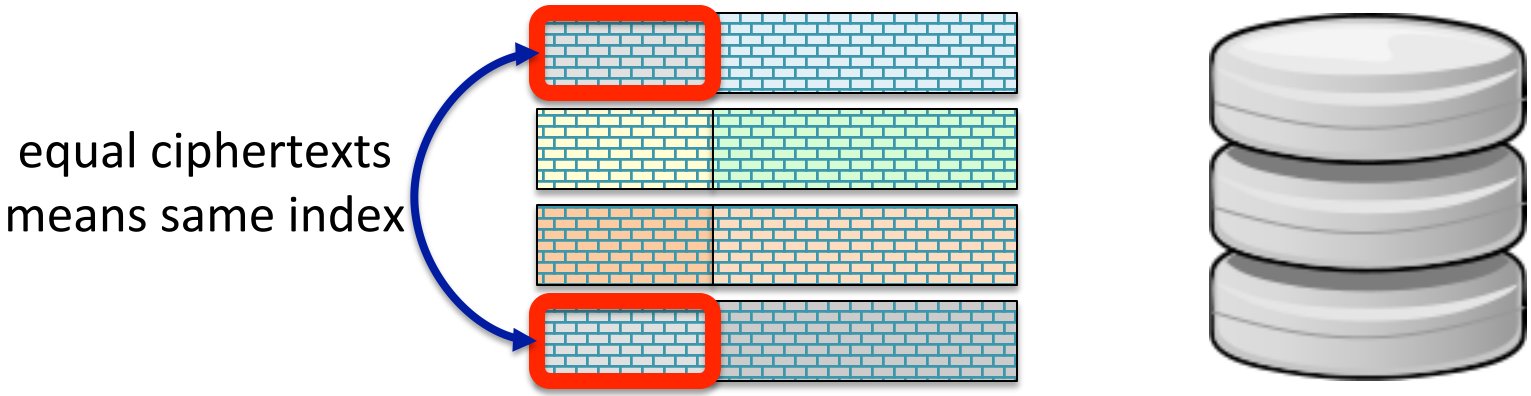
The need for det. Encryption (no nonce)



Problem: det. enc. cannot be CPA secure

The problem: attacker can tell when two ciphertexts encrypt the same message ⇒ leaks information

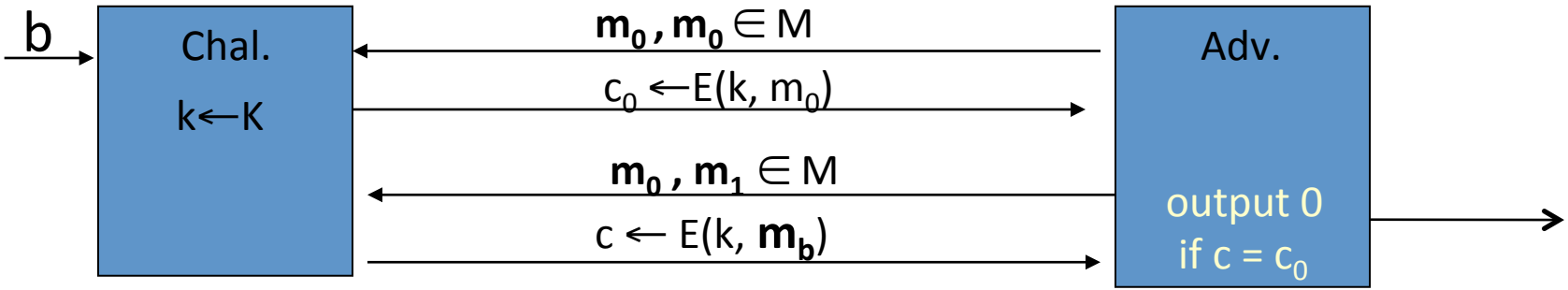
Leads to significant attacks when message space M is small.



Problem: det. enc. cannot be CPA secure

The problem: attacker can tell when two ciphertexts encrypt the same message ⇒ leaks information

Attacker wins CPA game:



A solution: the case of unique messages

Suppose encryptor **never** encrypts same message twice:

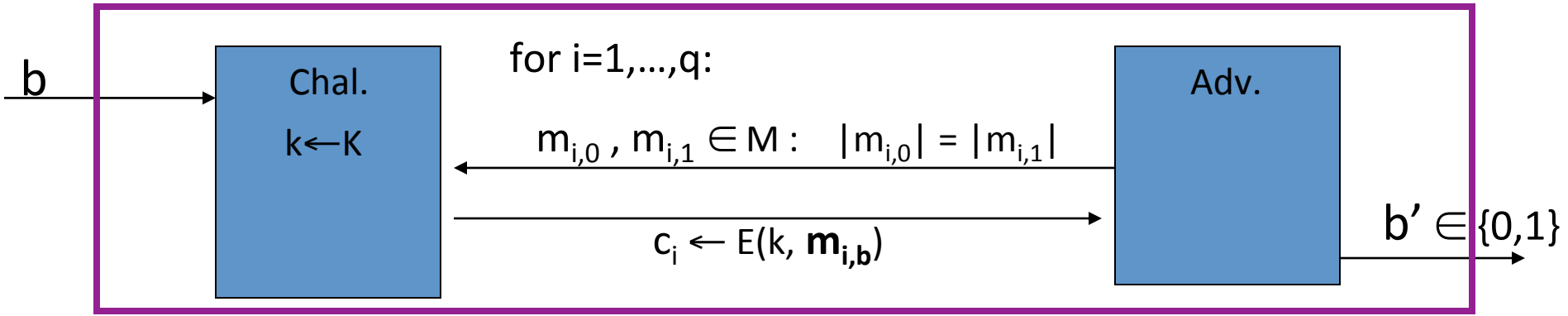
the pair (k , m) never repeats

This happens when encryptor:

- Chooses messages at random from a large msg space (e.g. keys)
- Message structure ensures uniqueness (e.g. unique user ID)

Deterministic CPA security

$E = (E,D)$ a cipher defined over (K,M,C). For $b=0,1$ define EXP(b) as:



where $m_{1,0}, \ldots, m_{q,0}$ are distinct and $m_{1,1}, \ldots, m_{q,1}$ are distinct

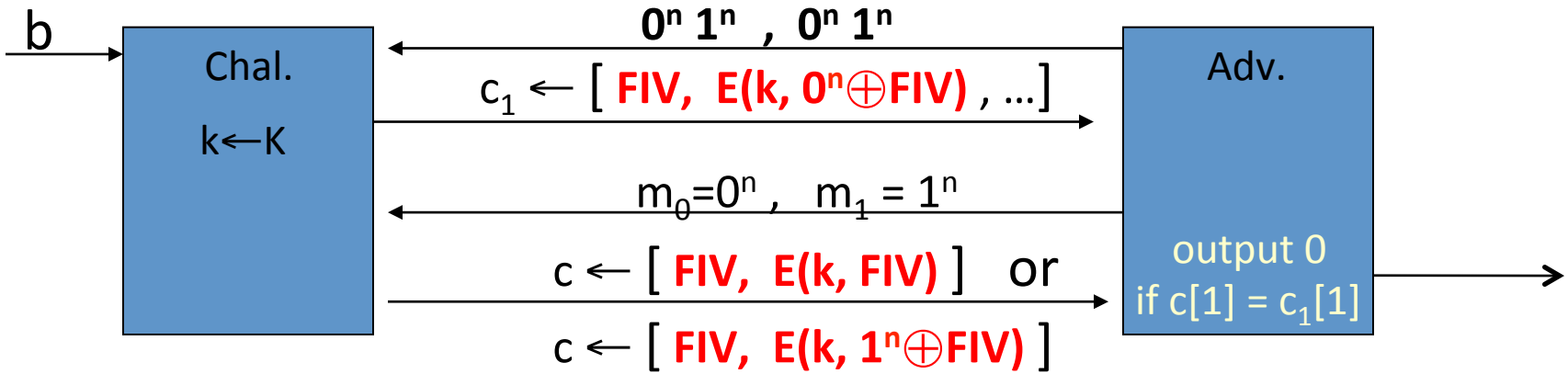
Def: E is **sem. sec. under det. CPA** if for all efficient A:

$$Adv_{dCPA}[A,E] = \left| Pr[EXP(0)=1] - Pr[EXP(1)=1] \right|$$ is negligible.

A Common Mistake

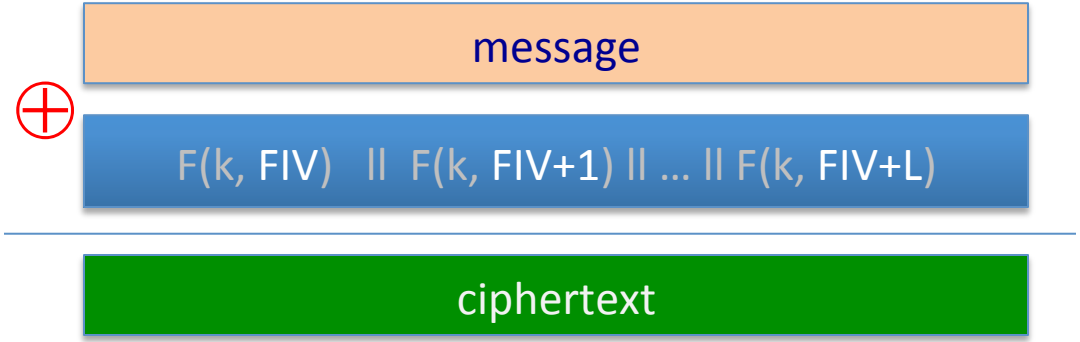
CBC with fixed IV is not det. CPA secure.

Let $E: K \times \{0,1\}^n \longrightarrow \{0,1\}^n$ be a secure PRP used in CBC

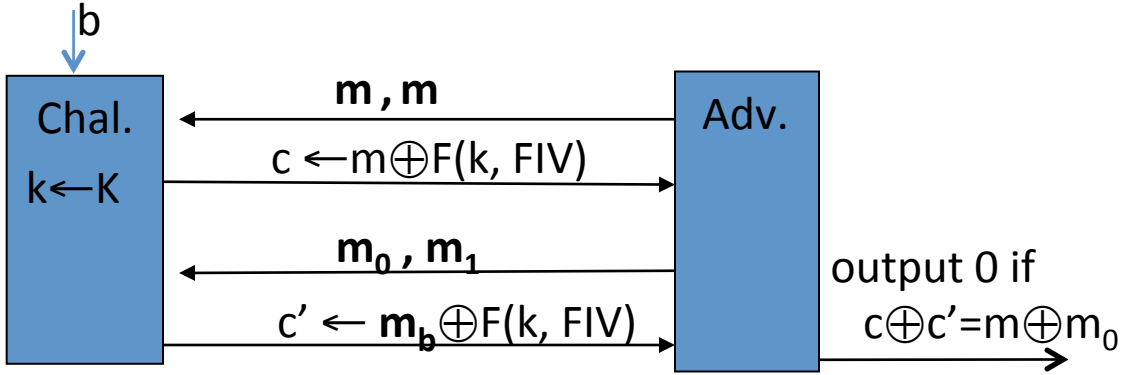


Leads to significant attacks in practice.

Is counter mode with a fixed IV det. CPA secure?



- ○ Yes
- ○ No
- ○ It depends
- ○



End of Segment