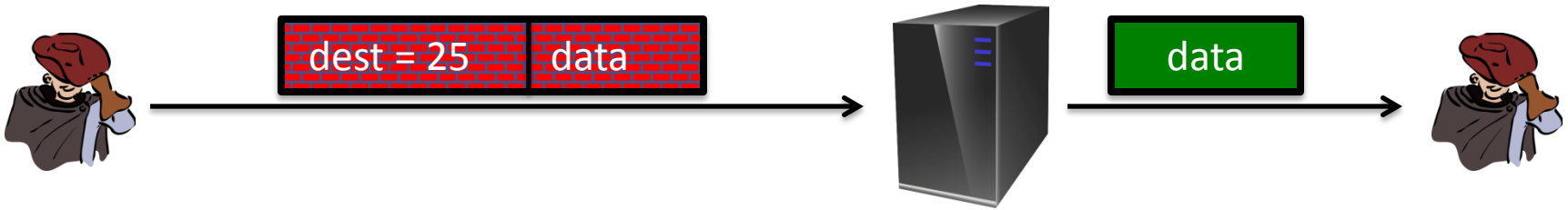

# Authenticated Encryption

## Chosen ciphertext attacks

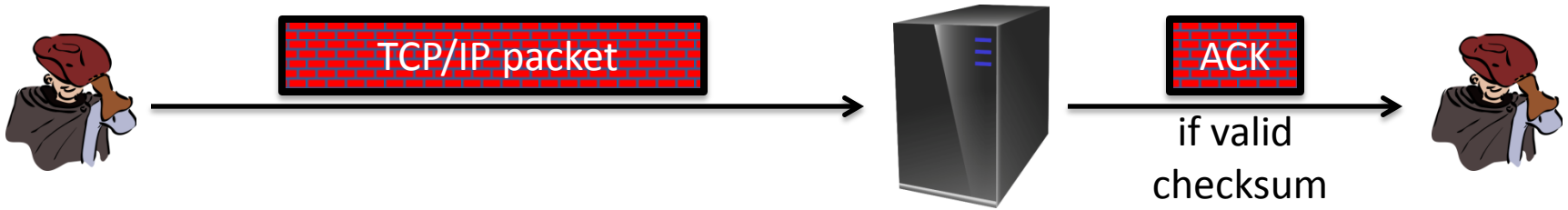
# Example chosen ciphertext attacks

Adversary has ciphertext c that it wants to decrypt

- Often, adv. can fool server into decrypting **certain** ciphertexts (not c)




- Often, adversary can learn partial information about plaintext



# Chosen ciphertext security

**Adversary's power**: both CPA and CCA

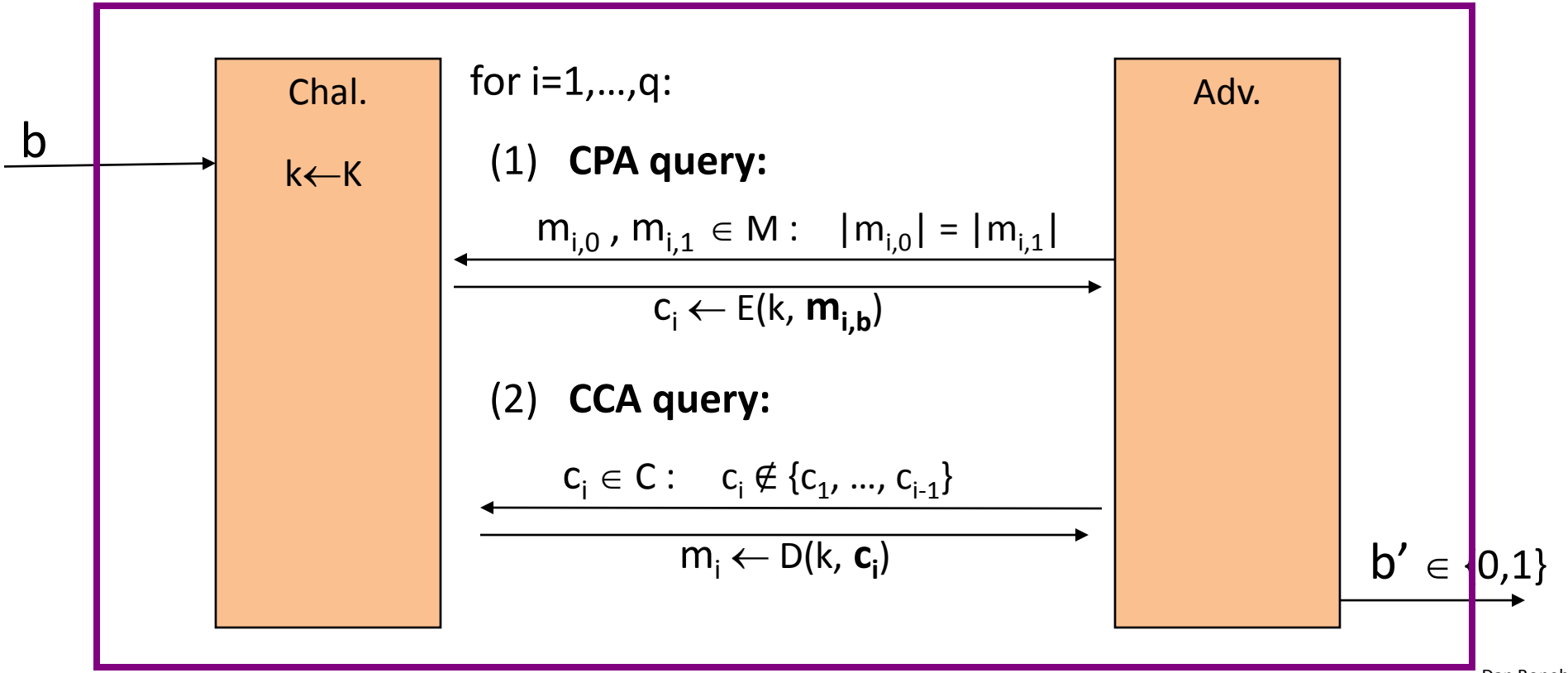
- Can obtain the encryption of arbitrary messages of his choice
- Can decrypt any ciphertext of his choice, other than challenge

(conservative modeling of real life)

**Adversary's goal**: Break sematic security

# Chosen ciphertext security: definition

$\mathbb{E}$ = (E,D) cipher defined over (K,M,C). For b=0,1 define EXP(b):

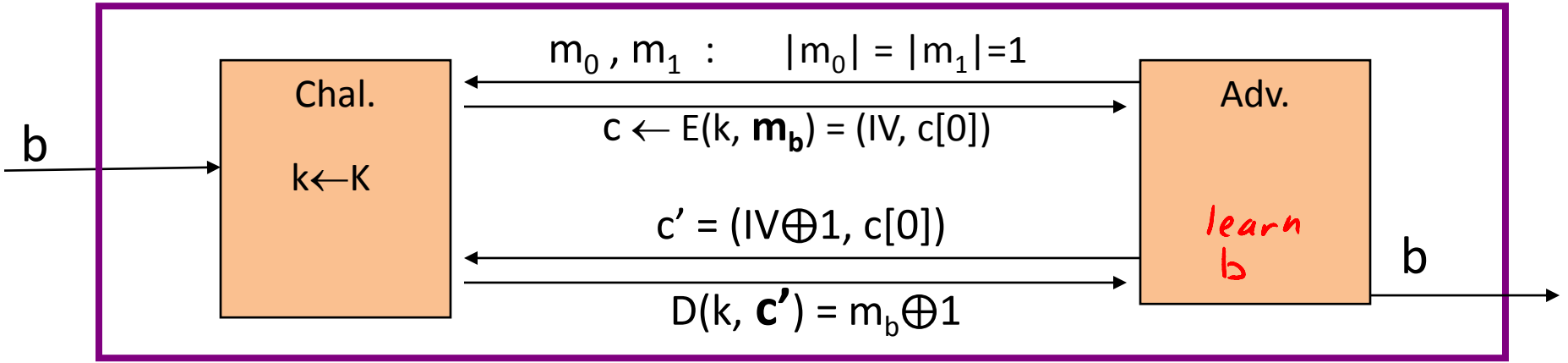


# Chosen ciphertext security: definition

$\mathbb{E}$ is CCA secure if for all "efficient" A:

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

**Example**: CBC with rand. IV is not CCA-secure



# Authenticated enc. ⇒ CCA security

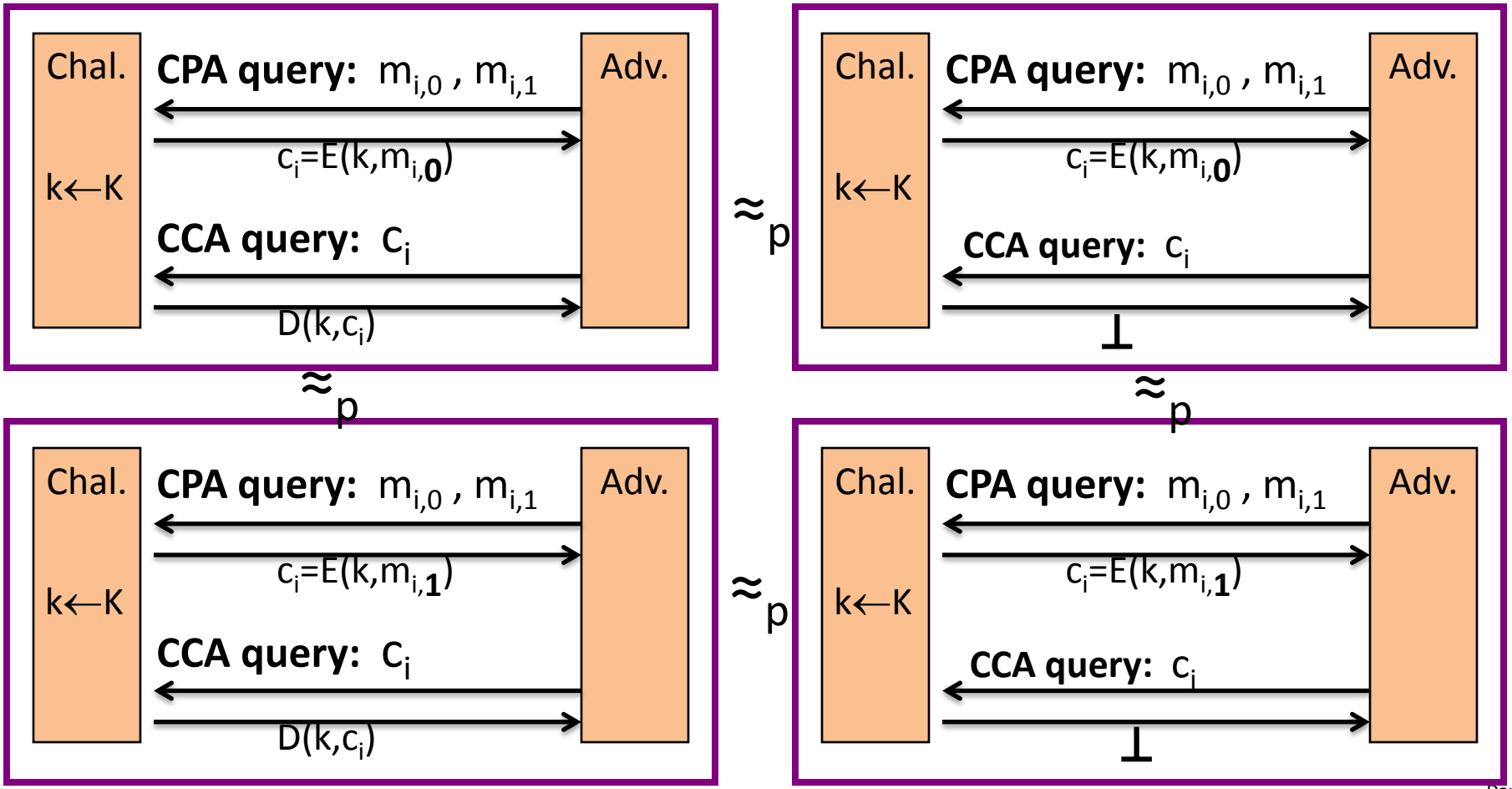
**Thm**: Let (E,D) be a cipher that provides AE.

Then (E,D) is CCA secure !

In particular, for any q-query eff. A there exist eff. $B_1$, $B_2$ s.t.

$$Adv_{CCA}[A,E] \le 2q \cdot Adv_{CI}[B_1,E] + Adv_{CPA}[B_2,E]$$

# Proof by pictures



# So what?

Authenticated encryption:

- ensures confidentiality against an active adversary that can decrypt some ciphertexts

Limitations:

- does not prevent replay attacks
- does not account for side channels (timing)

# End of Segment