



Stream ciphers

Semantic security

Goal: secure PRG \Rightarrow “secure” stream cipher

What is a secure cipher?

Attacker's abilities: **obtains one ciphertext** (for now)

Possible security requirements:

attempt #1: **attacker cannot recover secret key**

$$E(k, m) = m$$

attempt #2: **attacker cannot recover all of plaintext**

$$E(k, m_0 \| m_1) = m_0 \| m_1 \oplus k$$

Recall Shannon's idea:

CT should reveal no "info" about PT

Recall Shannon's perfect secrecy

Let (E,D) be a cipher over (K,M,C)

(E,D) has perfect secrecy if $\forall m_0, m_1 \in M \quad (|m_0| = |m_1|)$

$$\{ E(k, m_0) \} = \{ E(k, m_1) \} \quad \text{where } k \leftarrow K$$

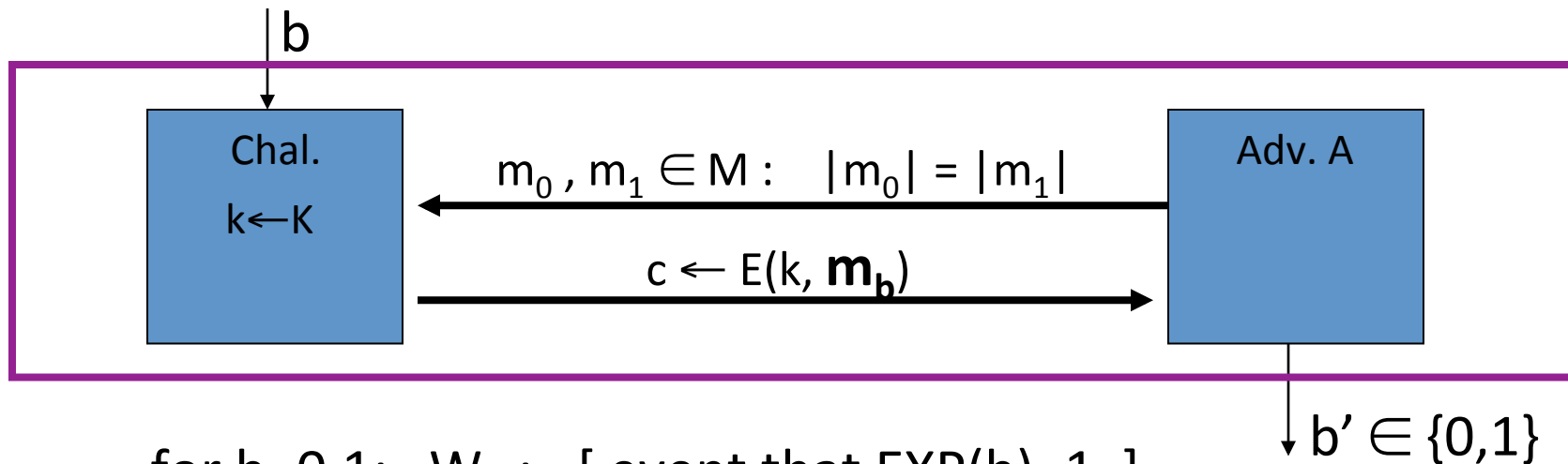
(E,D) has perfect secrecy if $\forall m_0, m_1 \in M \quad (|m_0| = |m_1|)$

$$\{ E(k, m_0) \} \approx_p \{ E(k, m_1) \} \quad \text{where } k \leftarrow K$$

... but also need adversary to exhibit $m_0, m_1 \in M$ explicitly

Semantic Security (one-time key)

For $b=0,1$ define experiments $\text{EXP}(0)$ and $\text{EXP}(1)$ as:



for $b=0,1$: $W_b := [\text{event that } \text{EXP}(b)=1]$

$$\text{Adv}_{\text{SS}}[A,E] := \left| \Pr[W_0] - \Pr[W_1] \right| \in [0,1]$$

Semantic Security (one-time key)

Def: E is **semantically secure** if for all efficient A

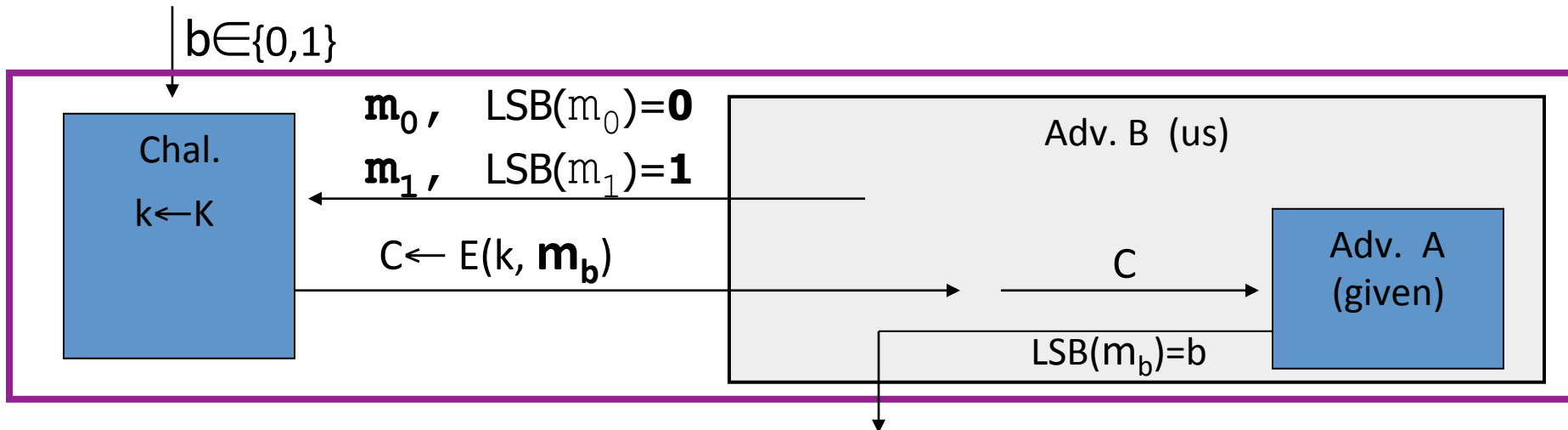
$\text{Adv}_{SS}[A, E]$ is negligible.

\Rightarrow for all explicit $m_0, m_1 \in M$: $\{ E(k, m_0) \} \approx_p \{ E(k, m_1) \}$

Examples

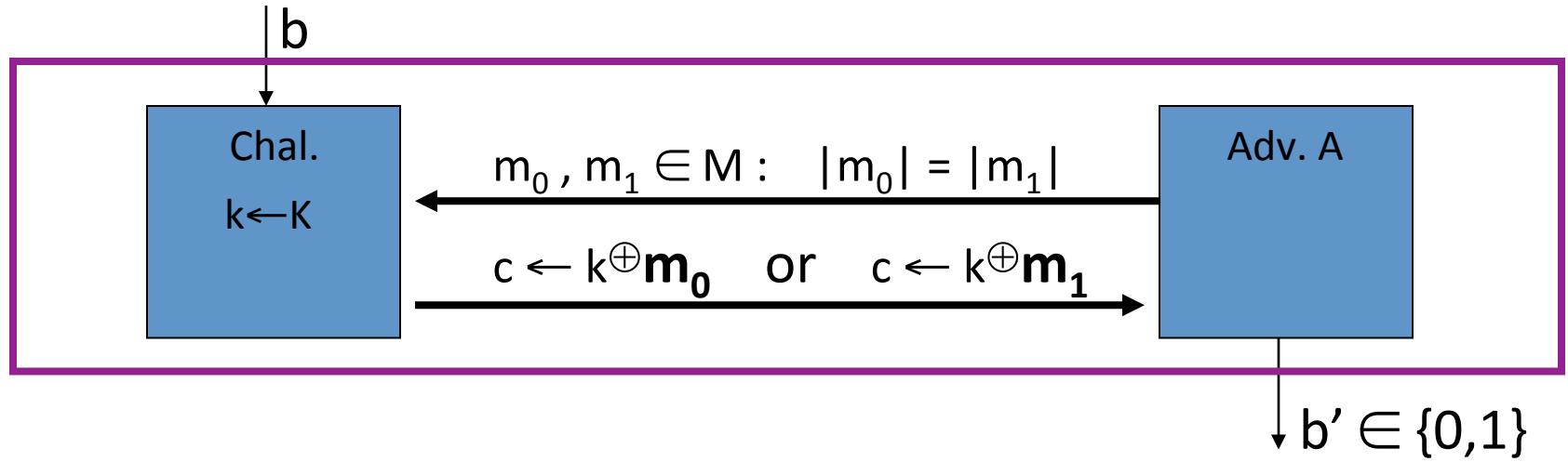
Suppose efficient A can always deduce LSB of PT from CT.

\Rightarrow $E = (E, D)$ is not semantically secure.



Then $\text{Adv}_{ss}[B, E] = \left| \Pr[\mathbf{EXP}(0)=1] - \Pr[\mathbf{EXP}(1)=1] \right| =$

OTP is semantically secure



For all A : $\text{Adv}_{ss}[A, \text{OTP}] = \left| \Pr[A(k \oplus \mathbf{m}_0) = 1] - \Pr[A(k \oplus \mathbf{m}_1) = 1] \right| = 0$

End of Segment