Computer Security

Block ciphers
(Semantic security)

Hyoungshick Kim

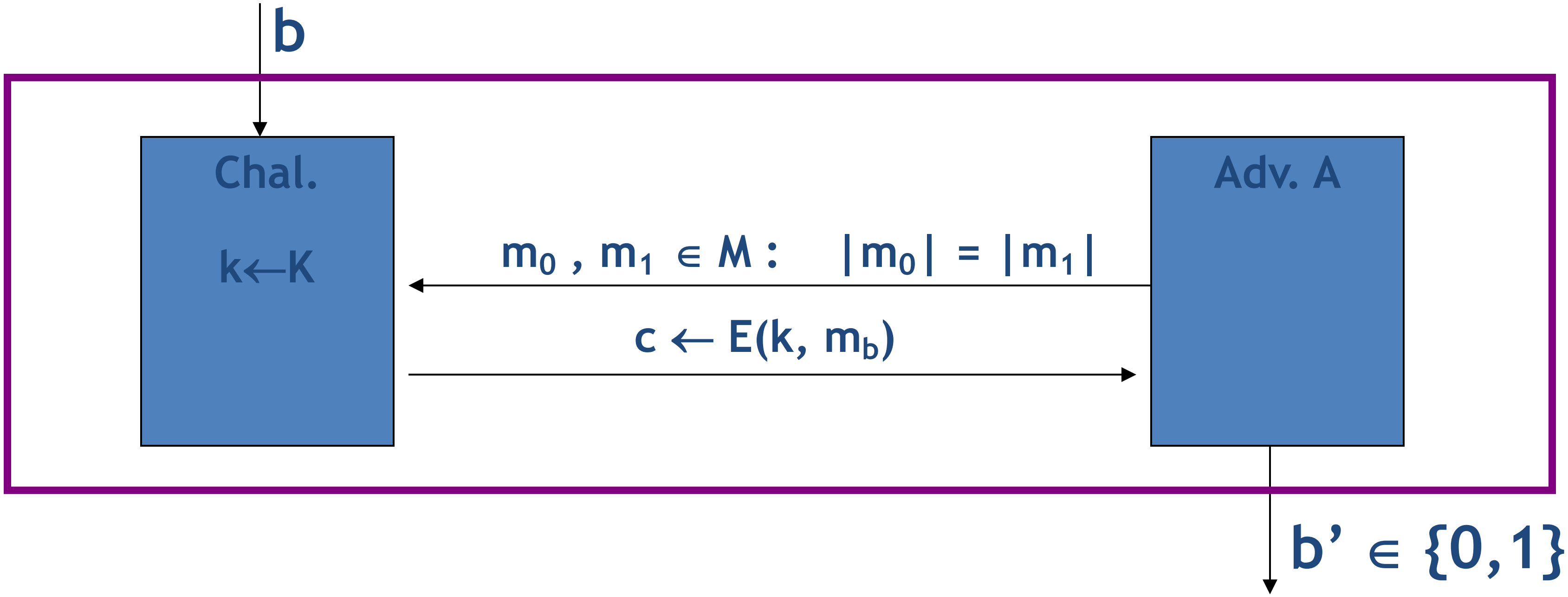
Department of Software

College of Software

Sungkyunkwan University

Semantic security for one-time key

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



- Def: $\mathbb{E}$ is semantically secure for one-time key if for all "efficient" A:

$$\text{Adv}_{SS}[A,\mathbb{E}] = \left|\Pr[\text{EXP}(0)=1] - \Pr[\text{EXP}(1)=1]\right|$$

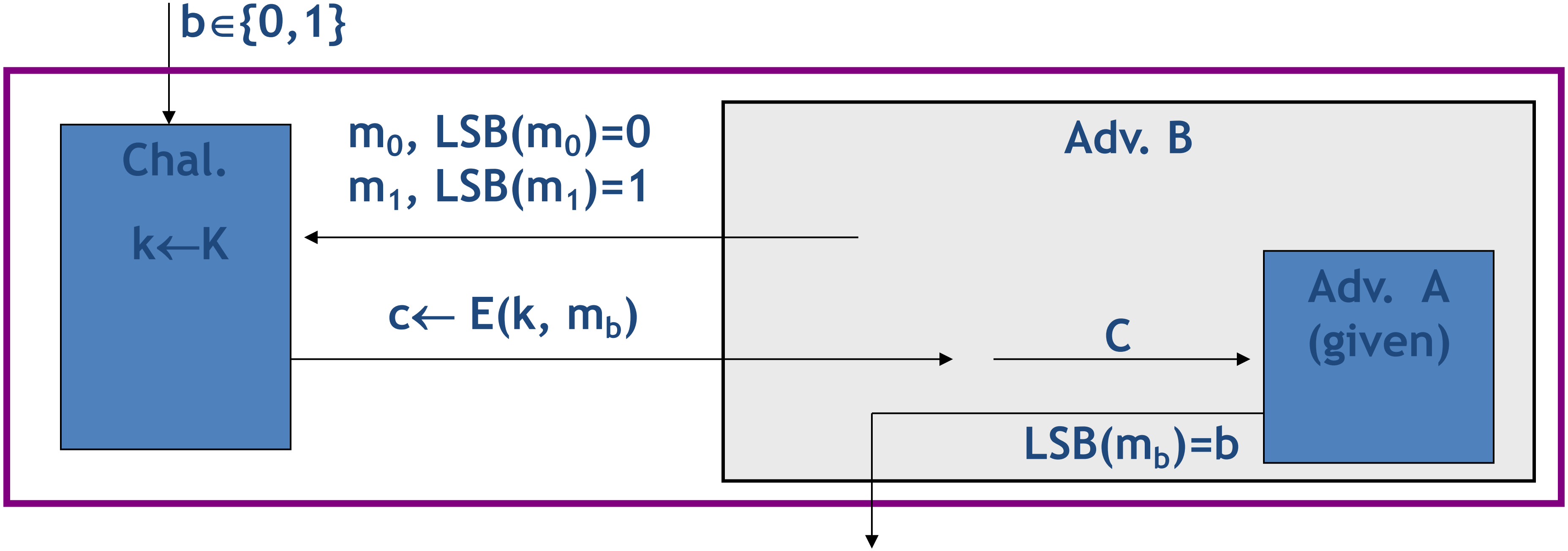
is "negligible."

Semantic security

Semantically Secure ⇒ no "efficient" adversary learns information about plaintext from a **single** ciphertext.

Example: Suppose efficient A can deduce LSB of plaintext from ciphertext.

Then $\mathbb{E}$ = (E,D) is not semantically secure.

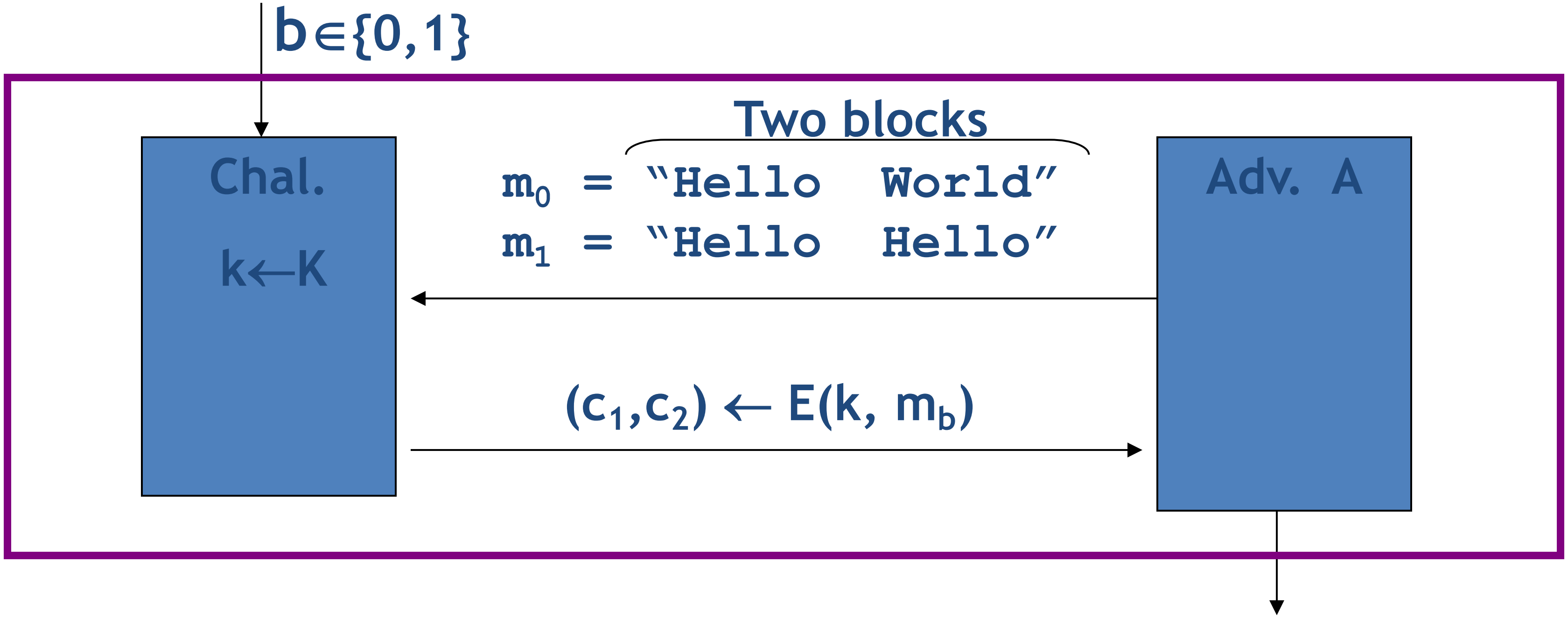


Then $\mathrm{Adv}_{SS}[B, \mathbb{E}] = 1$ ⇒ $\mathbb{E}$ is not semantically secure

ECB is not Semantically Secure

Electronic Code Book (ECB):

- Not semantically secure for messages that contain more than one block.



$b \in \{0,1\}$

Chal.

$k \leftarrow K$

$$\overbrace{}^{\text{Two blocks}}$$

m_0 = “Hello World”

m_1 = “Hello Hello”

$(c_1, c_2) \leftarrow E(k, m_b)$

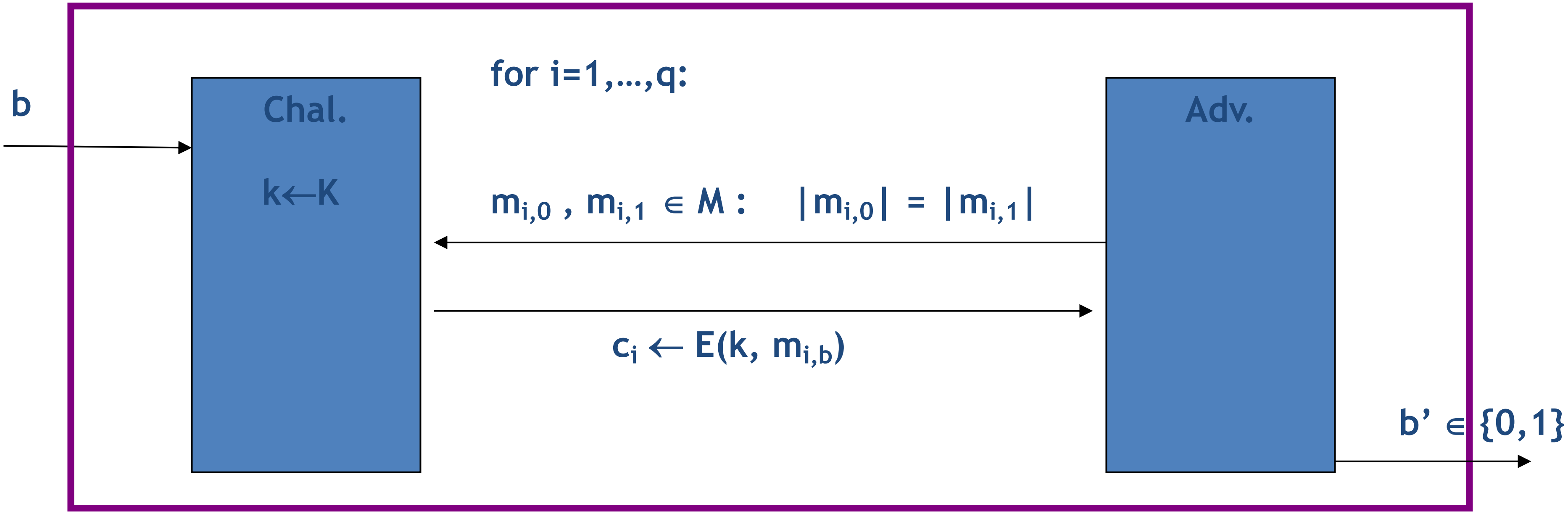
Adv. A

If $c_1 = c_2$ output 1, else output 0

Then $\text{Adv}_{SS}[A, \text{ECB}] = 1$

Semantic security for many-time key (CPA security)

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


b
Chal.
k←K
for i=1,…,q:
$m_{i,0}$, $m_{i,1}$ ∈ M : $|m_{i,0}| = |m_{i,1}|$
$c_i \leftarrow E(k, m_{i,b})$
Adv.
b' ∈ {0,1}

- Def: $\mathbb{E}$ is semantically secure under CPA if for all "efficient" A:

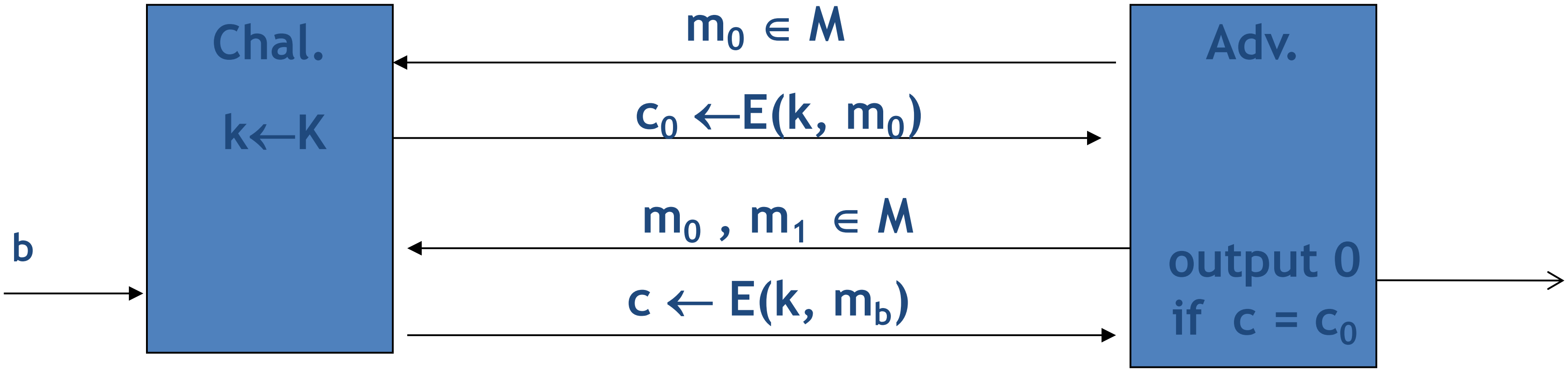
$$\text{Adv}_{\text{CPA}}[A,\mathbb{E}] = \left|\Pr[\text{EXP}(0)=1] - \Pr[\text{EXP}(1)=1]\right|$$

is "negligible."

Security for many-time key

Fact: stream ciphers are insecure under CPA.

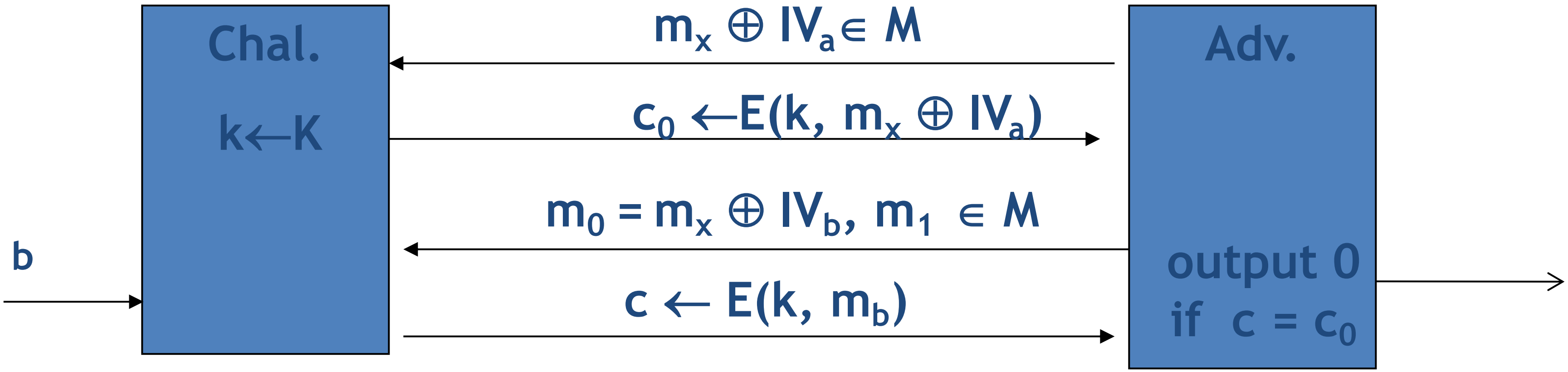
- More generally: if E(k,m) always produces same ciphertext, then cipher is insecure under CPA.



If secret key is to be used multiple times $\Rightarrow$

given the same plaintext message twice,
the encryption alg. must produce different outputs.

CBC is not Semantically Secure (when IV is predictable)



Chal.

$k \leftarrow K$

b

$m_x \oplus IV_a \in M$

$c_0 \leftarrow E(k, m_x \oplus IV_a)$

$m_0 = m_x \oplus IV_b,\ m_1 \in M$

$c \leftarrow E(k, m_b)$

Adv.

output 0 if $c = c_0$

Then $Adv_{SS}[A, CBC] = 1$

If an attacker can predict the IV, CBC is not CPA-secure.

Common rules for CPA security

1. Do not use ECB (Electronic Codebook) mode for encryption.
2. Do not use a non-random IV (Initialization vector) for CBC (Cipher Block Chaining) encryption.
3. Do not use constant encryption keys.
4. Do not use constant salts for PBE (Password-based encryption).
5. Do not use fewer than 1,000 iterations for PBE.
6. Do not use static seeds for SecureRandom

"An Empirical Study of Cryptographic Misuse in Android Applications", ACM CCS 2013

What is the best recommendation?

It depends on the situation.

Overall, CTR is the best and most modern way to achieve privacy-only encryption.

It is insecure if a nonce gets reused on encryption or decryption.

“Evaluation of Some Blockcipher Modes of Operation”, Phillip Rogaway, 2011

However …

CBC and CTR modes *are* not secure against chosen-ciphertext attacks.

CPA security cannot guarantee security under **active attacks**.

Questions?

Sungkyunkwan
Campus
established
university
Sciences
campus
Graduate
School
Suwon
Seoul
Natural
Korean
University
edit
constructed
English
Professors
Social
Global
Building
Institute
Confucian
Humanities
schools
Administration
Academic
ASLE-Korea