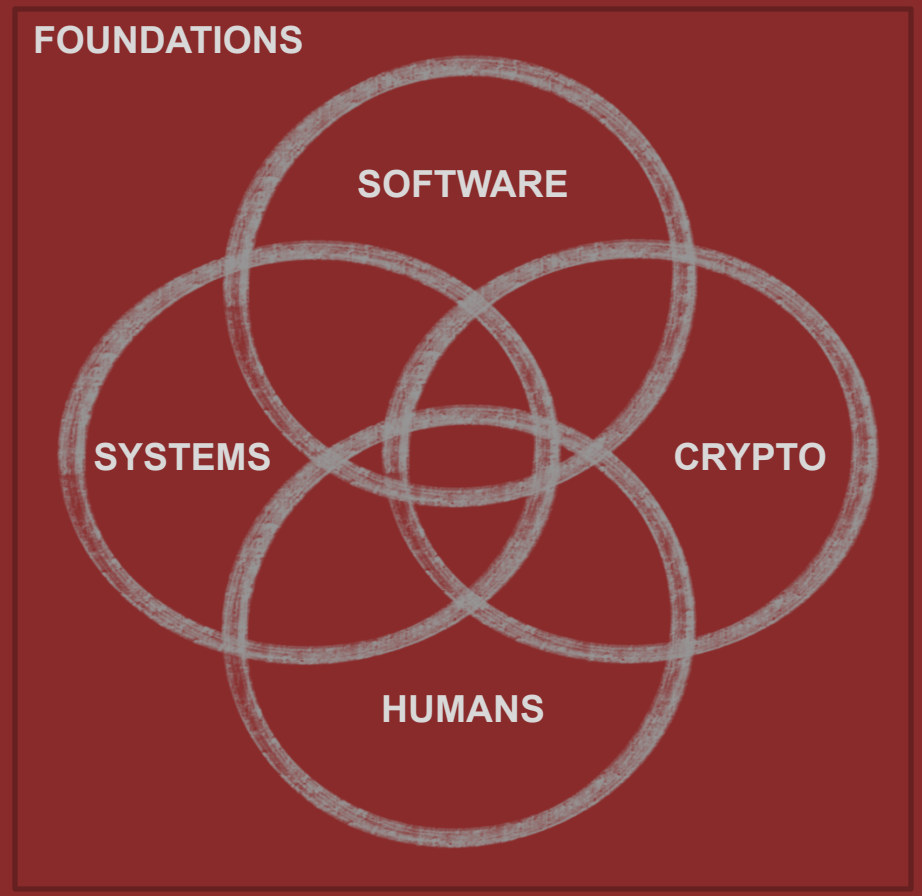
Διάλεξη #15 - Encryption Modes

Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών

Εισαγωγή στην Ασφάλεια

Θανάσης Αυγερινός



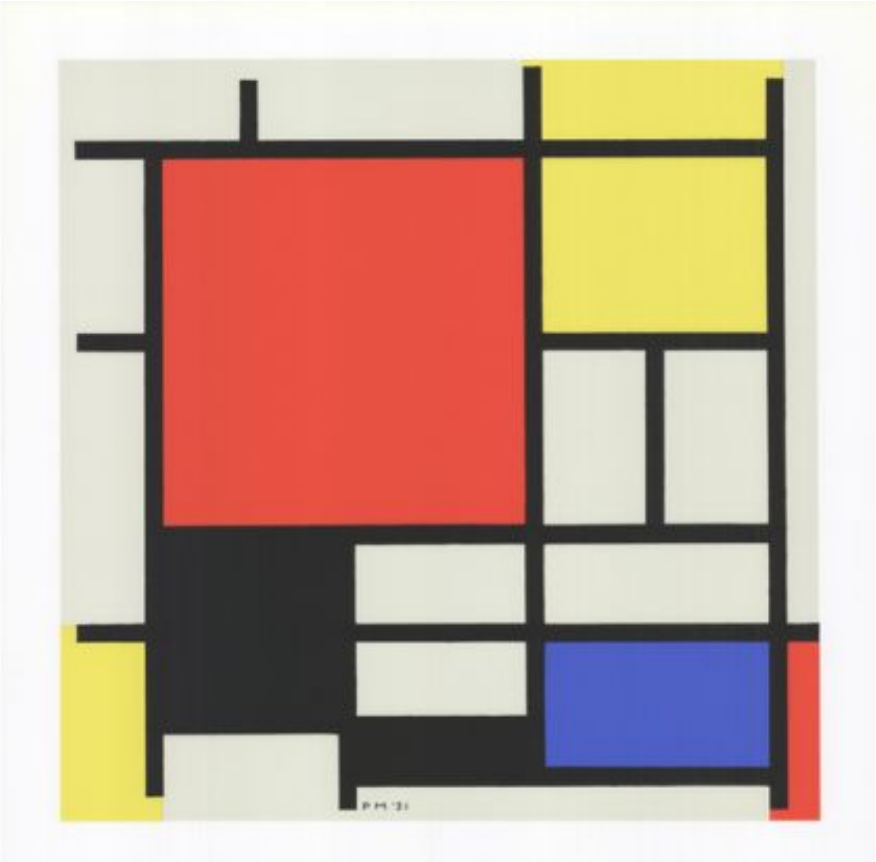
Huge thank you to David Brumley from Carnegie Mellon University for the guidance and content input while developing this class (some slides from Dan Boneh @ Stanford!)

Ανακοινώσεις / Διευκρινίσεις

- Η Εργασία #2 θα ανοίξει σήμερα, στο ίδιο format με την προηγούμενη
- Η Εργασία #3 (ομαδική) προγραμματίζεται για 30 Μαΐου-1 Ιουνίου

Την προηγούμενη φορά

- PseudoRandom Functions (PRFs)
- PseudoRandom Permutations (PRPs)
- Block Ciphers
- Semantic Security



Warm Up

Interview Question

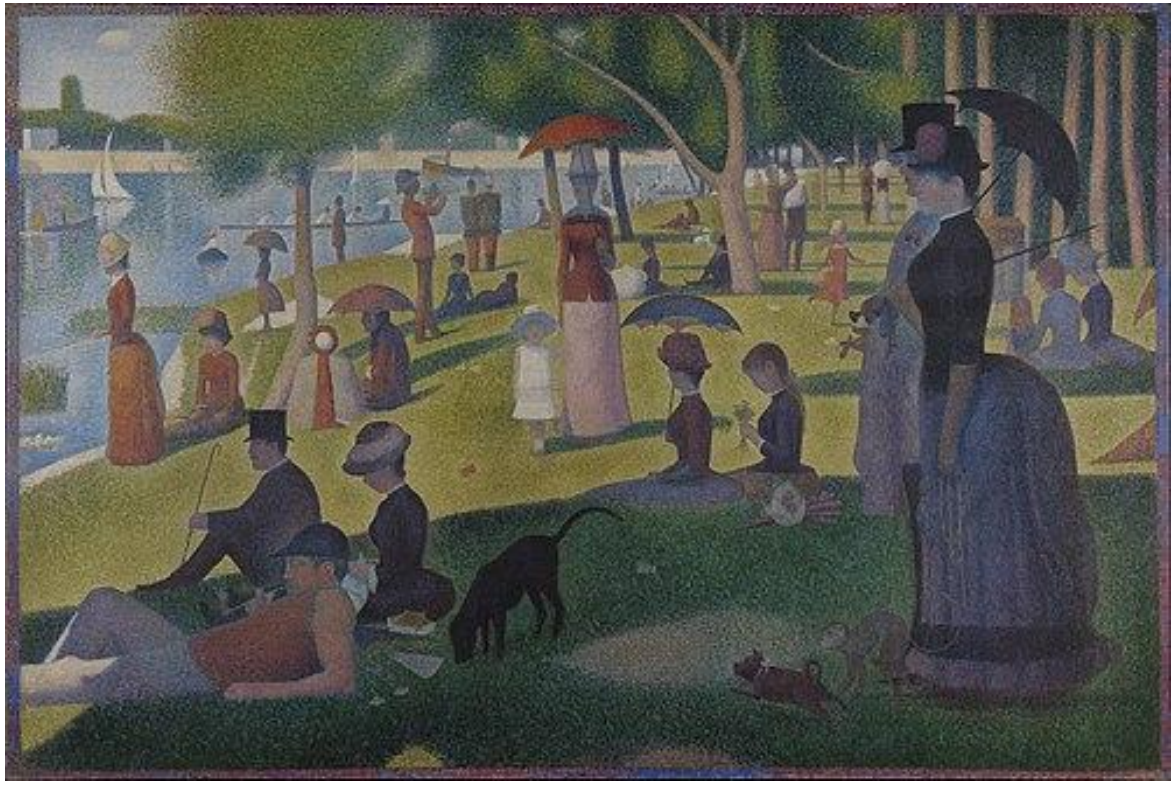
You have a message that you want to transfer from A to B securely and efficiently. Do you:

(A) Encrypt and then compress - Compress(Enc(m))
(B) Compress and then encrypt - Enc(Compress(m))

Why?

Σήμερα

- Encryption Modes
  - Electronic Code Book (ECB)
  - Cipher Block Chaining (CBC)
  - Counter Mode (CTR)
- Mistakes and Attacks



Encryption Modes

Block Ciphers help us encrypt a single block of data securely

To encrypt multiple blocks with a single key we need to find secure *modes of operation* , i.e., ways to combine block ciphers on messages longer than a single block

Using PRPs and PRFs

Goal: build "secure" encryption from a secure PRP (e.g. AES).

First: **one-time keys**

1. Adversary's power:

   Adv sees only one ciphertext (one-time key)

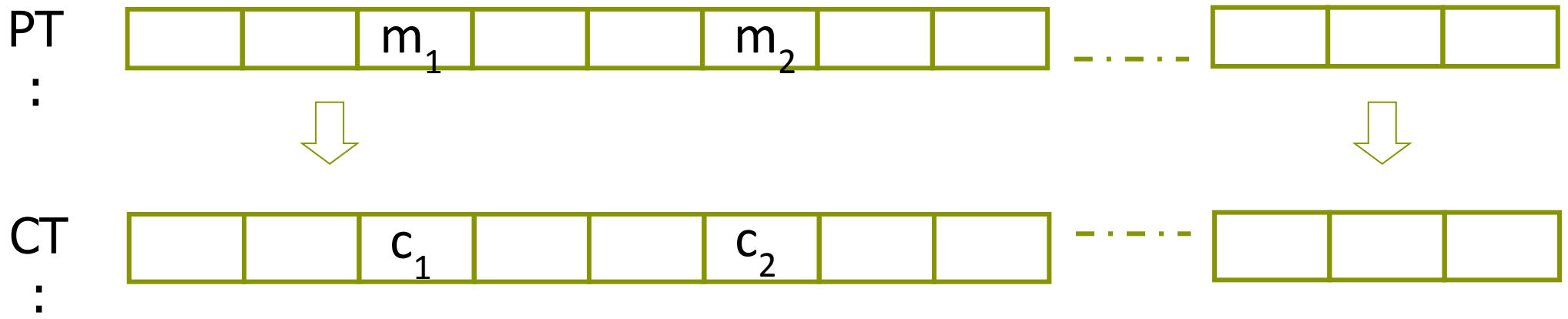
2. Adversary's goal:

   Learn info about PT from CT (semantic security)

Next up: many-time keys (a.k.a chosen-plaintext security)

ECB Mode: Insecure use of a PRP

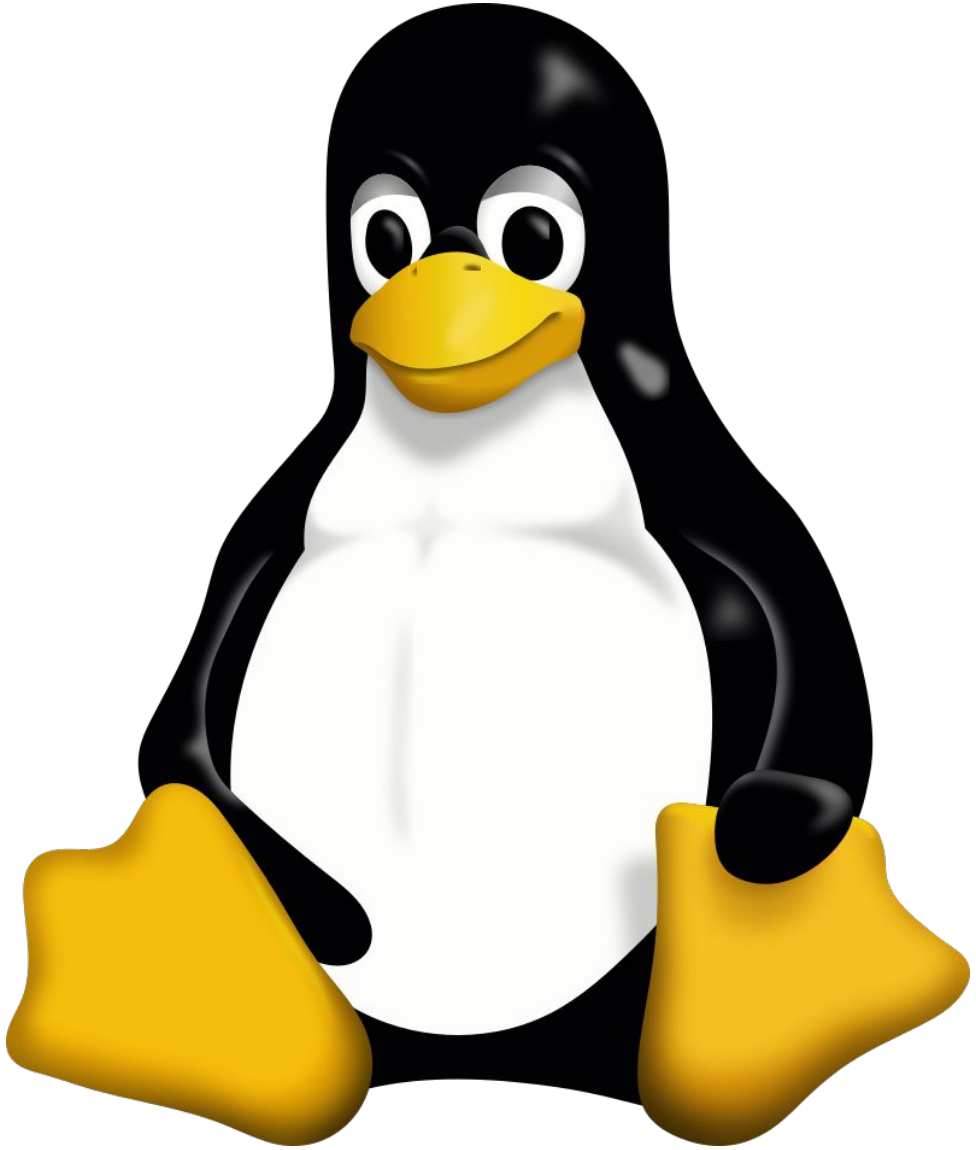
Electronic Code Book (ECB):



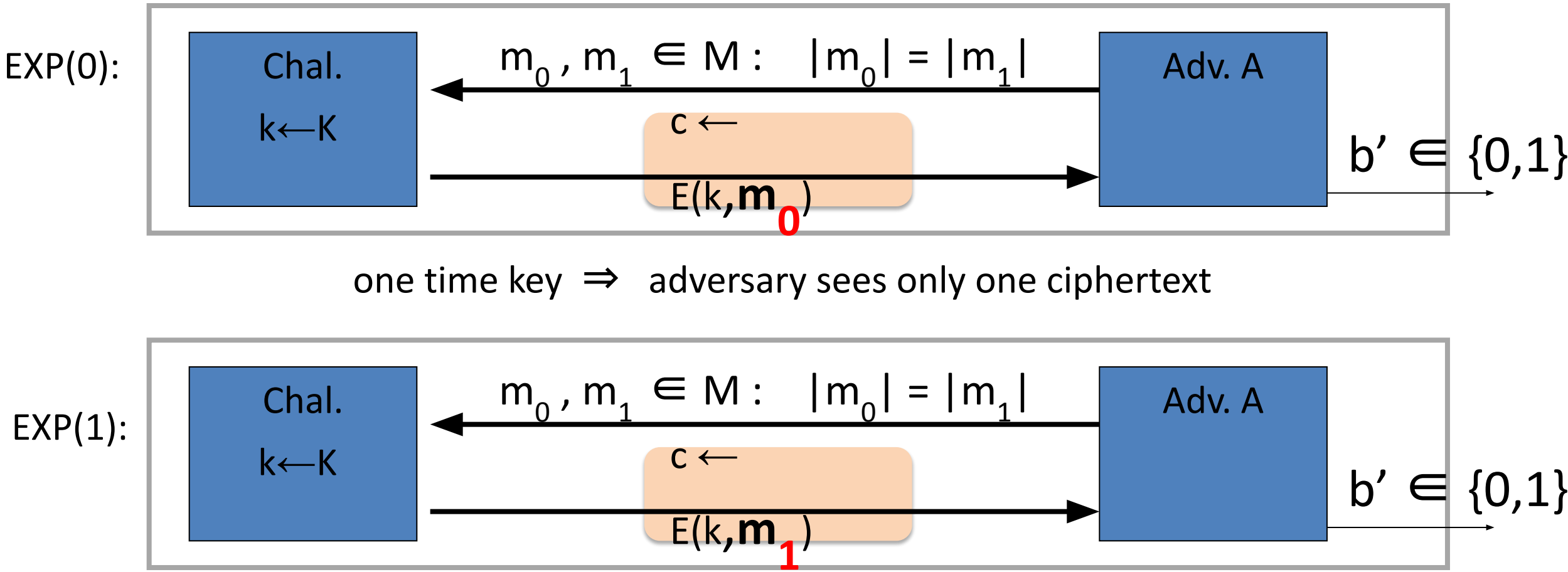
Problem:

– if $m_1 = m_2$ then $c_1 = c_2$

In pictures



Semantic Security (one-time key)



one time key ⇒ adversary sees only one ciphertext

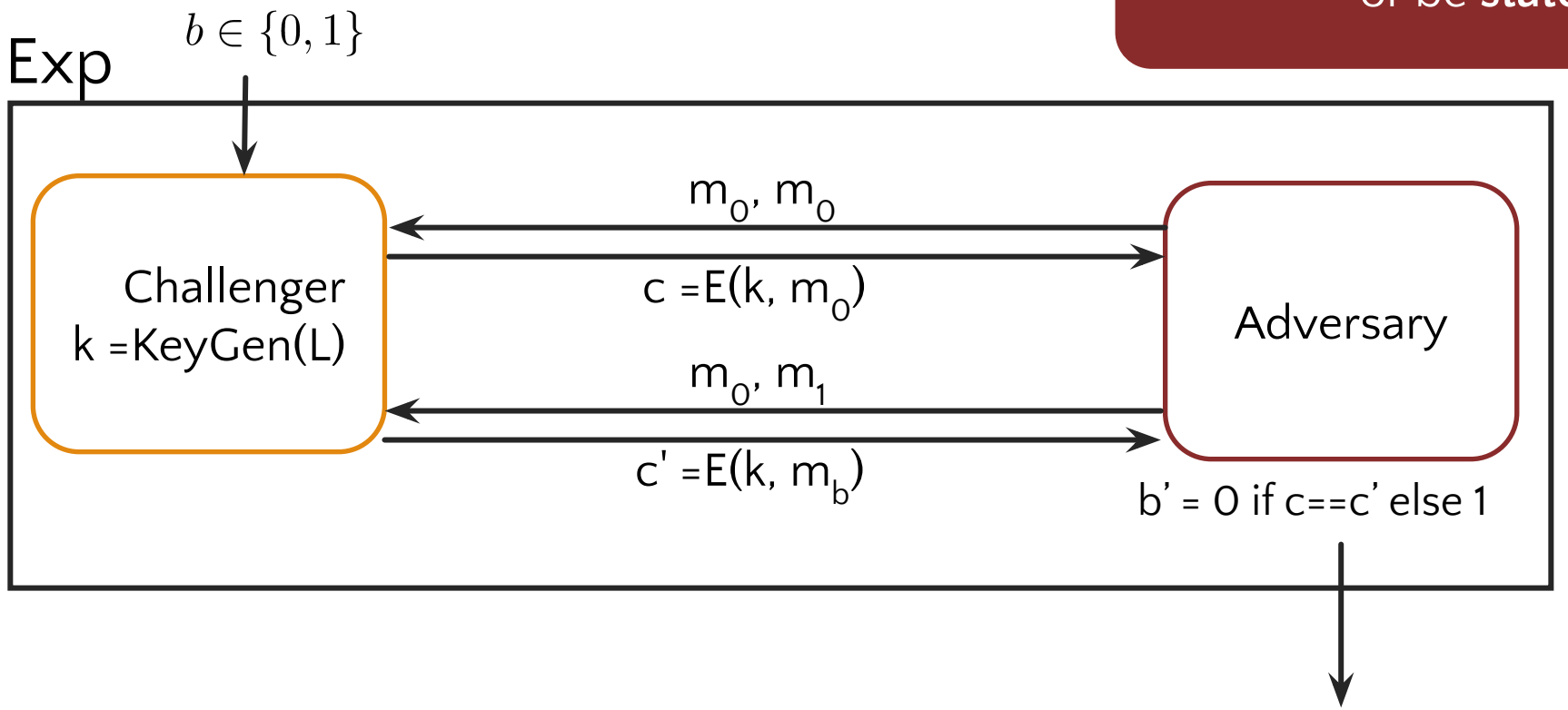
$Adv_{SS}[A,OTP] = \left| \Pr[\ \mathbf{EXP(0)}=1\ ] - \Pr[\ \mathbf{EXP(1)}=1\ ] \right|$ should be "neg."

ECB is not Semantically Secure

ECB is not semantically secure for messages that contain more than one block (many-time key).

Encryption must be **randomized** or be **stateful**!

For *b = 0,1* define experiment *Exp(b)* as:



Semantic Security for many-time key

Key used more than once $\Rightarrow$ adv. sees many CTs with same key

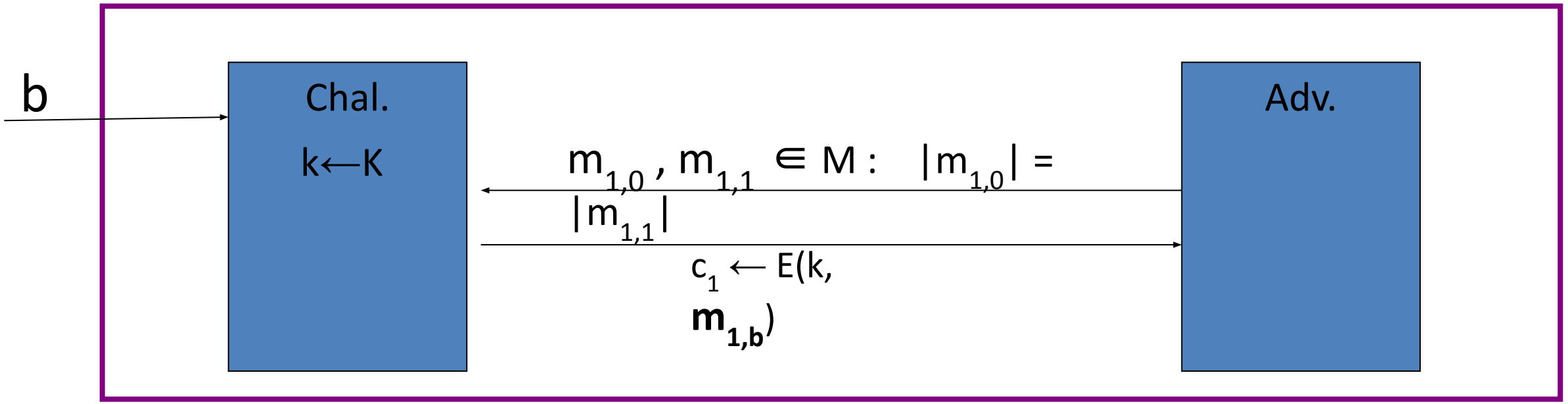
Adversary's power: chosen-plaintext attack (CPA)

- Can obtain the encryption of arbitrary messages of his choice
  (conservative modeling of real life)

Adversary's goal: Break sematic security

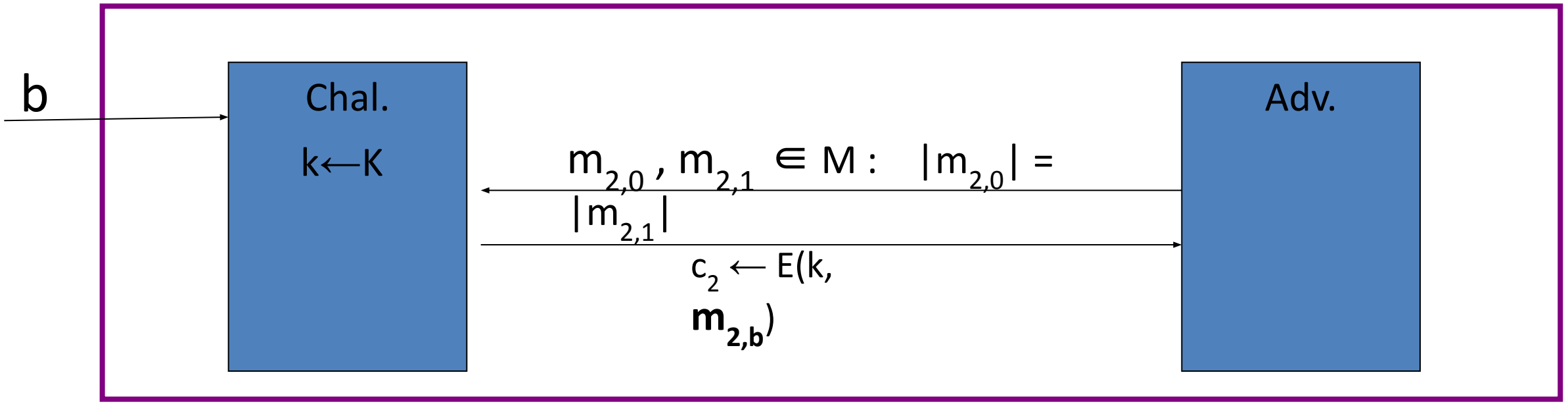
Semantic Security for many-time key

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



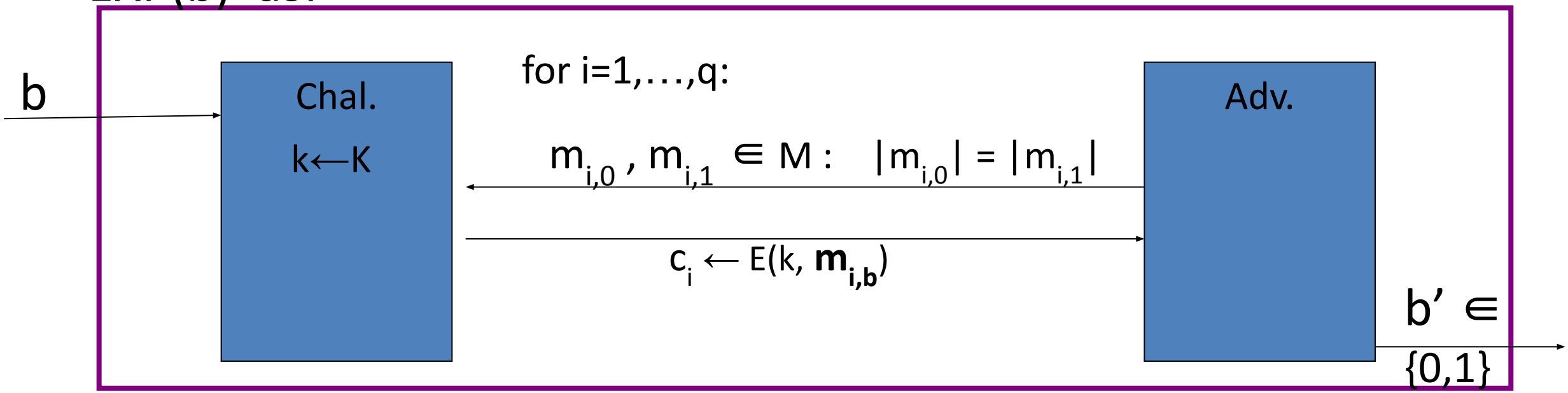
Semantic Security for many-time key

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



Semantic Security for many-time key (CPA security)

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



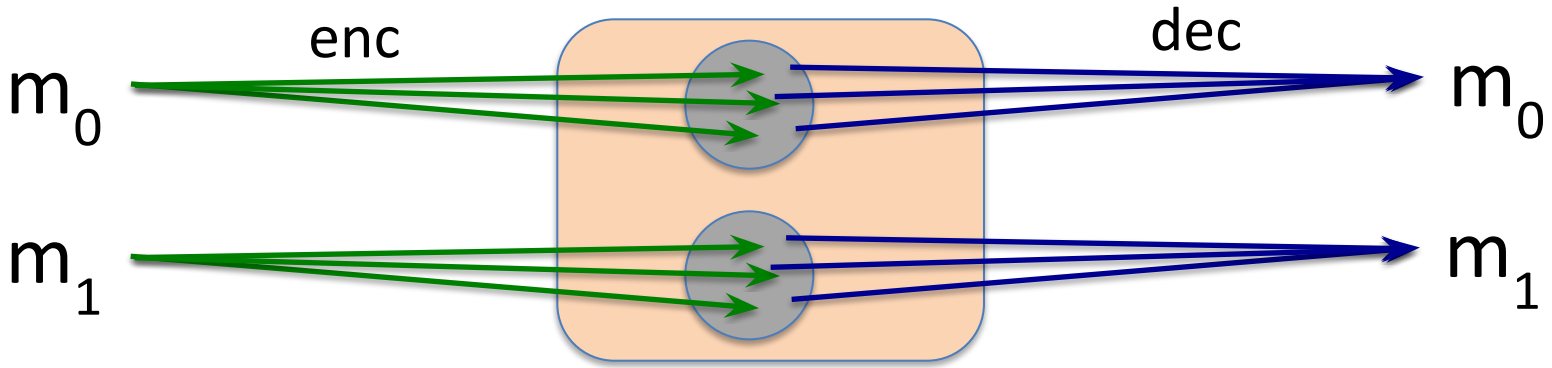
if adv. wants c = E(k, m) it queries with $m_{j,0} = m_{j,1} = m$

Def: $\mathbb{E}$ is sem. sec. under CPA if for all "efficient" A:

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

Solution 1: randomized encryption

- E(k,m) is a randomized algorithm:



⇒ encrypting same msg twice gives different ciphertexts (w.h.p)

⇒ ciphertext must be longer than plaintext

Roughly speaking: CT-size = PT-size + "# random bits"

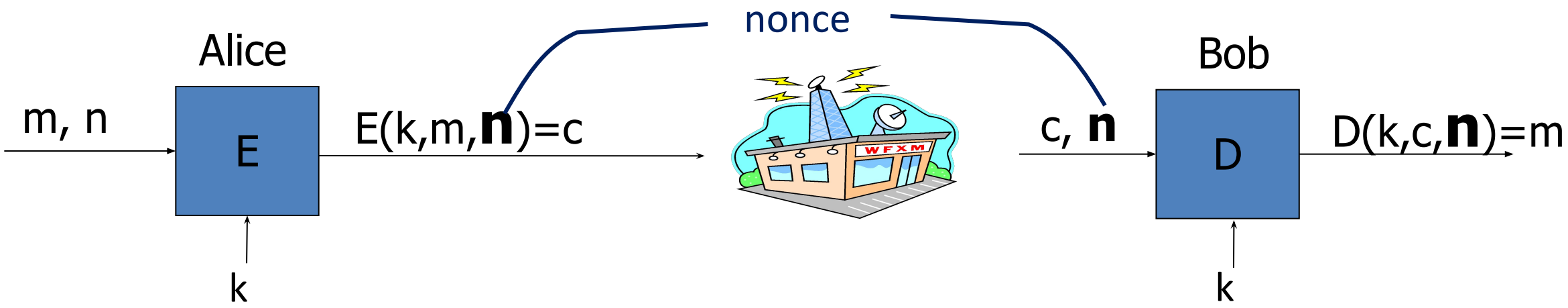
Let $F: K \times R \longrightarrow M$ be a secure PRF.

For $m \in M$ define $E(k,m) = [\, r \xleftarrow{\$} R,\ \text{output } (r, F(k,r) \oplus m) \,]$

Is E semantically secure under CPA?

- Yes, whenever F is a secure PRF
- No, there is always a CPA attack on this system
- Yes, but only if R is large enough so r never repeats (w.h.p)
- It depends on what F is used

Solution 2: nonce-based Encryption



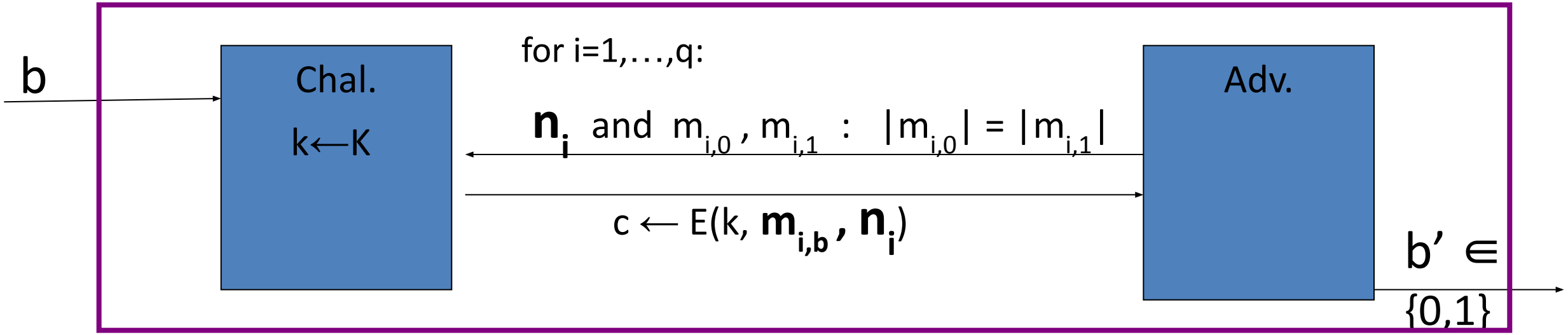
- nonce n: a value that changes from msg to msg.
  (k,n) pair never used more than once (freshness)

- method 1: nonce is a **counter** (e.g. packet counter)
  - used when encryptor keeps state from msg to msg
  - if decryptor has same state, need not send nonce with CT

- method 2: encryptor chooses a **random nonce**, $n \leftarrow \mathcal{N}$

CPA security for nonce-based encryption

System should be secure when nonces are chosen adversarially.



All nonces $\{n_1, \ldots, n_q\}$ must be distinct.

Def: nonce-based $\mathbb{E}$ is sem. sec. under CPA if for all "efficient" A:

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

Let $F: K \times R \longrightarrow M$ be a secure PRF. Let $r = 0$ initially.

For $m \in M$ define $E(k,m) = [\ r{+}{+},$ output $(r, F(k,r) \oplus m)\ ]$

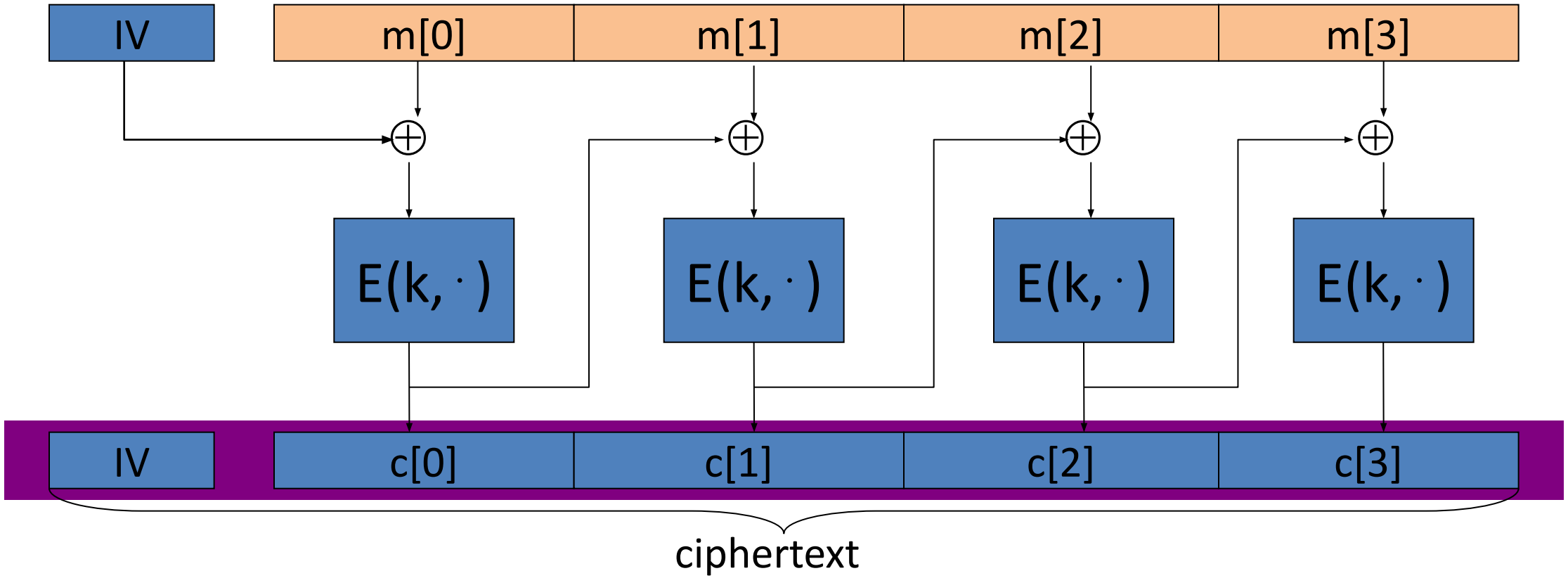
Is E CPA secure nonce-based encryption?

- Yes, whenever F is a secure PRF
- No, there is always a nonce-based CPA attack on this system
- Yes, but only if R is large enough so r never repeats
- It depends on what F is used

Cipher Block Chaining

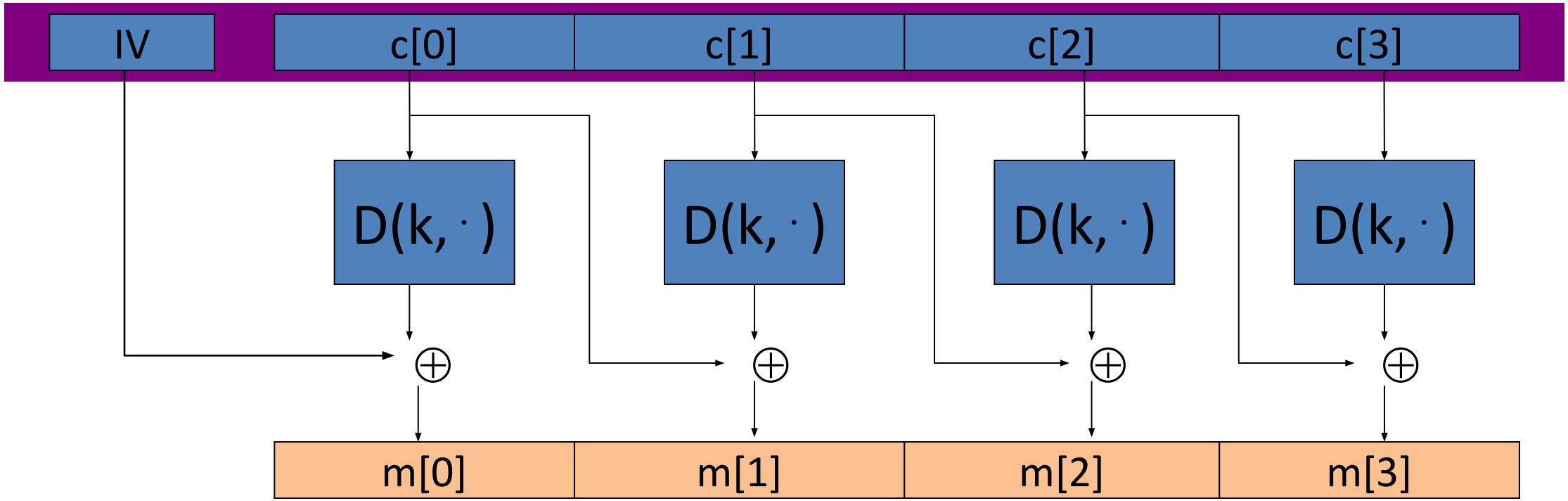
Construction 1: CBC with random IV

Let (E,D) be a PRP. $E_{CBC}(k,m)$: choose **random** $IV \in X$ and do:



Decryption circuit

In symbols: $c[0] = E\big(k, IV \oplus m[0]\big) \Rightarrow m[0] =$ [redacted]



CBC: CPA Analysis

<u>CBC Theorem</u>: For any L>0,

If E is a secure PRP over (K,X) then

E_{CBC} is a sem. sec. under CPA over (K, X^L, X^{L+1}).

In particular, for a q-query adversary A attacking E_{CBC} there exists a PRP adversary B s.t.:

$$Adv_{CPA}[A, E_{CBC}] \leq 2 \cdot Adv_{PRP}[B, E] + 2\, q^2 L^2 / |X|$$

Note: CBC is only secure as long as $q^2L^2 << |X|$

An example

$$\mathrm{Adv}_{\mathrm{CPA}}[A, E_{\mathrm{CBC}}] \le 2 \cdot \mathrm{PRP\ Adv}[B, E] + \mathbf{2\, q^2\, L^2 / |X|}$$

q = # messages encrypted with k , L = length of max message

Suppose we want $\mathrm{Adv}_{\mathrm{CPA}}[A, E_{\mathrm{CBC}}] \le 1/2^{32}$ $\Leftarrow$ $q^2 L^2 / |X| < 1/ 2^{32}$

- AES: $|X| = 2^{128} \Rightarrow q L < 2^{48}$

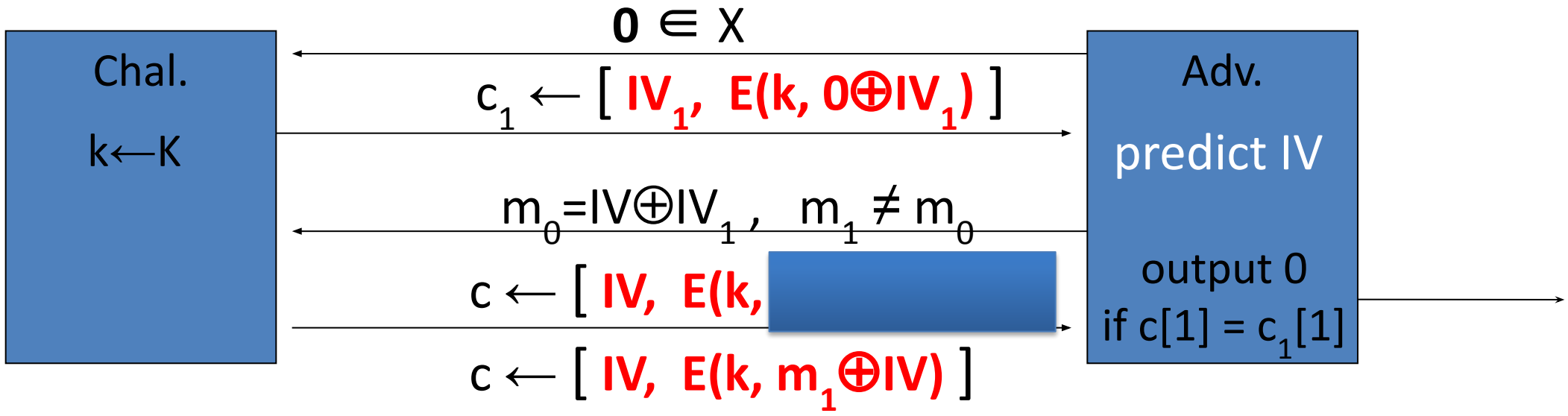
  So, after 2^{48} AES blocks, must change key

- 3DES: $|X| = 2^{64} \Rightarrow q L < 2^{16}$

Warning: an attack on CBC with rand. IV

CBC where attacker can predict the IV is not CPA-secure !!

Suppose given $c \leftarrow E_{CBC}(k,m)$ can predict IV for next message

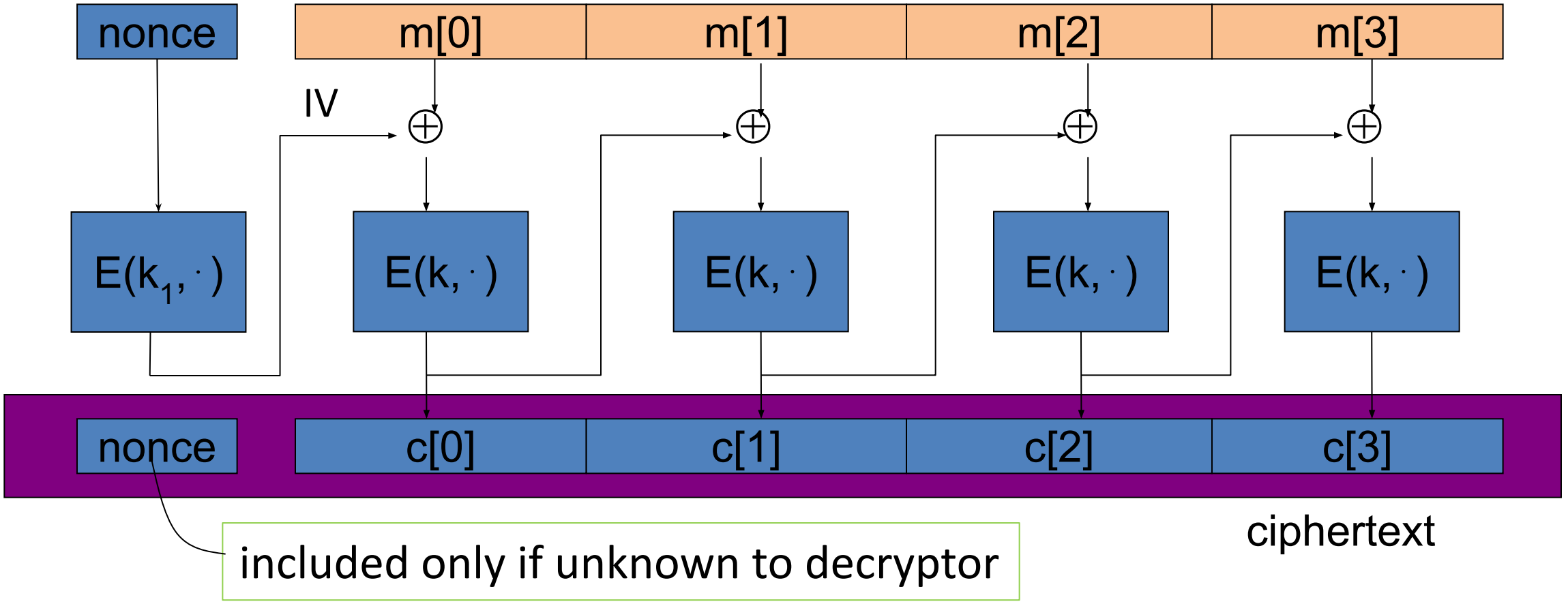


Bug in SSL/TLS 1.1: IV for record #i is last CT block of record #(i-1)
(CVE-2011-3389 Beast Attack)

Construction 1’: nonce-based CBC

- Cipher block chaining with <u>unique</u> nonce: key = (k,k_1)

  unique nonce means: (key, n) pair is used for only one message

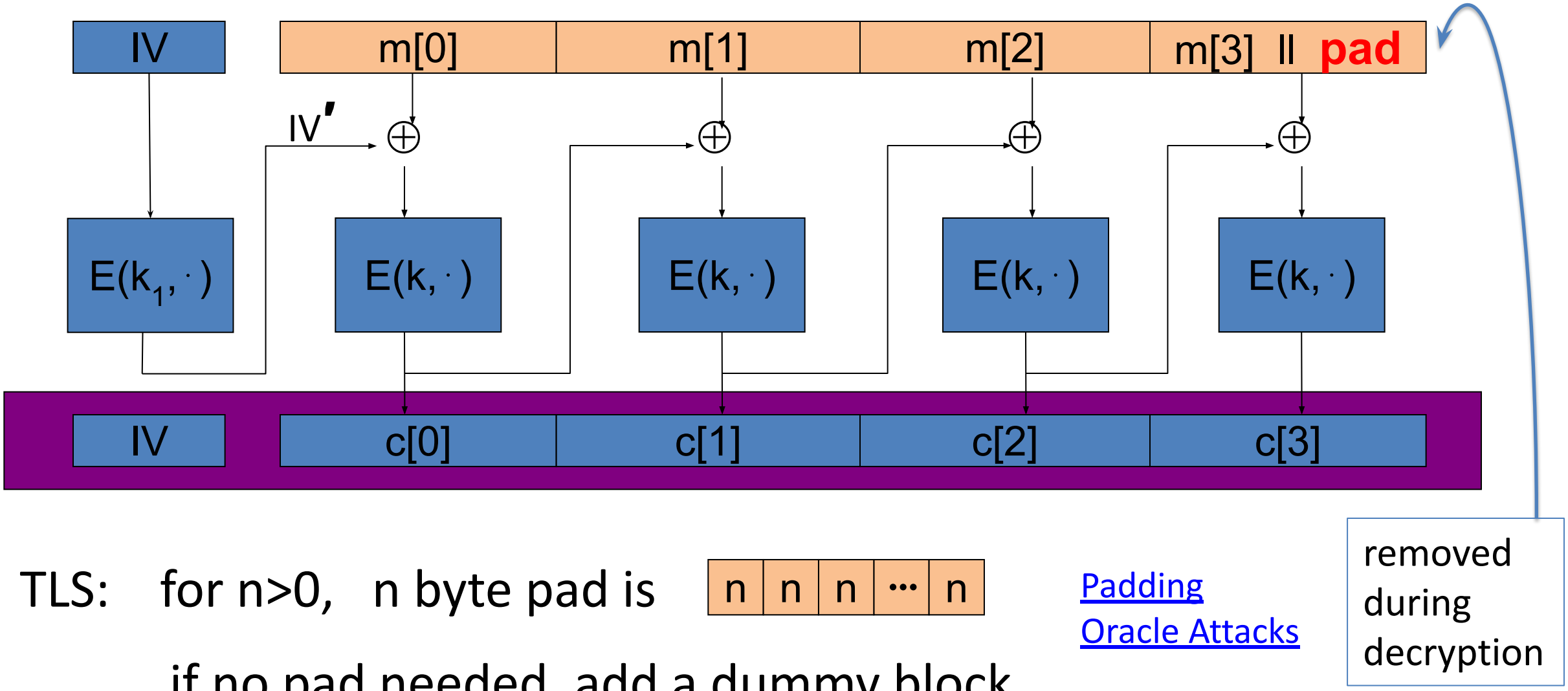


An example Crypto API (OpenSSL)

```
void AES_cbc_encrypt(
    const unsigned char *in,
    unsigned char *out,
    size_t length,
    const AES_KEY *key,
    unsigned char *ivec,      ← user supplies IV
    AES_ENCRYPT or AES_DECRYPT);
```

When nonce is non random need to encrypt it before use

A CBC technicality: padding



TLS: for n>0, n byte pad is

if no pad needed, add a dummy block

Padding Oracle Attacks

Using CBC

Samsung Shattered Encryption on 100M Phones

One cryptography expert said that 'serious flaws' in the way Samsung phones encrypt sensitive material, as revealed by academics, are 'embarrassingly bad.'

Samsung shipped an estimated 100 million smartphones with botched encryption, including models ranging from the 2017 Galaxy S8 on up to last year's Galaxy S21.

Researchers at Tel Aviv University found what they called "severe" cryptographic design flaws that could have let attackers siphon the devices' hardware-based cryptographic keys: keys that unlock the treasure trove of security-critical data that's found in smartphones.

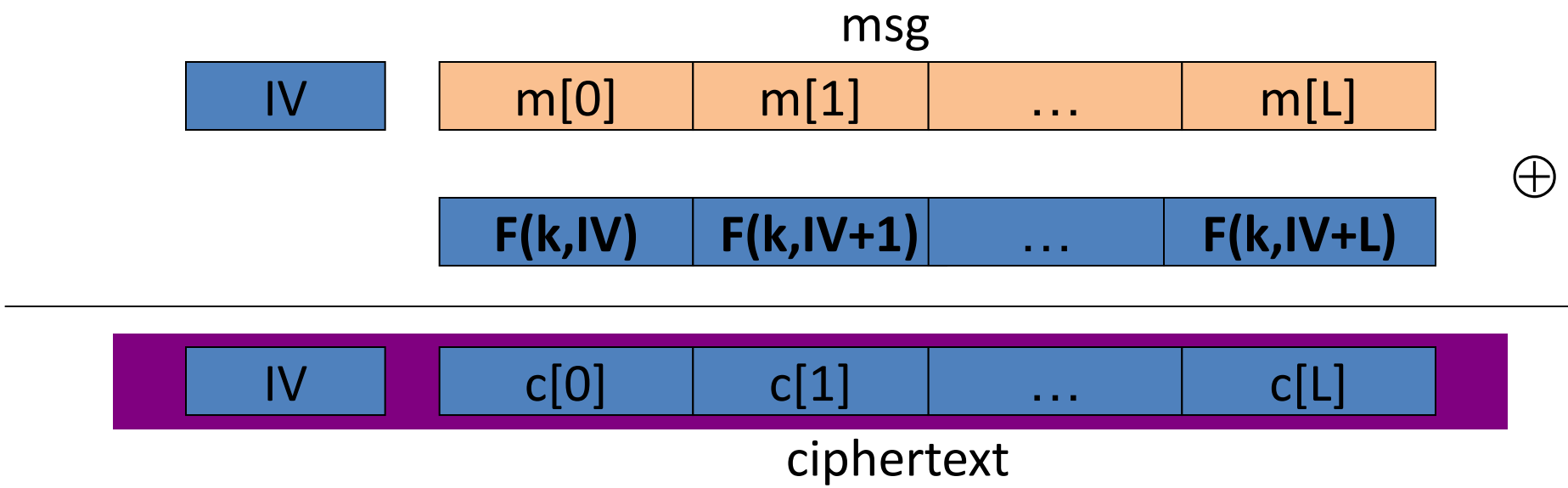
What's more, cyber attackers could even exploit Samsung's cryptographic missteps – since addressed in multiple CVEs – to downgrade a device's security protocols. That would set up a phone to be vulnerable to future attacks: a practice known as IV (initialization vector) reuse attacks. IV reuse attacks screw with the encryption randomization that ensures that even if multiple messages with identical plaintext are encrypted, the generated corresponding ciphertexts will each be distinct.

https://threatpost.com/samsung-shattered-encryption-on-100m-phones/178606/

Construction 2: rand ctr-mode

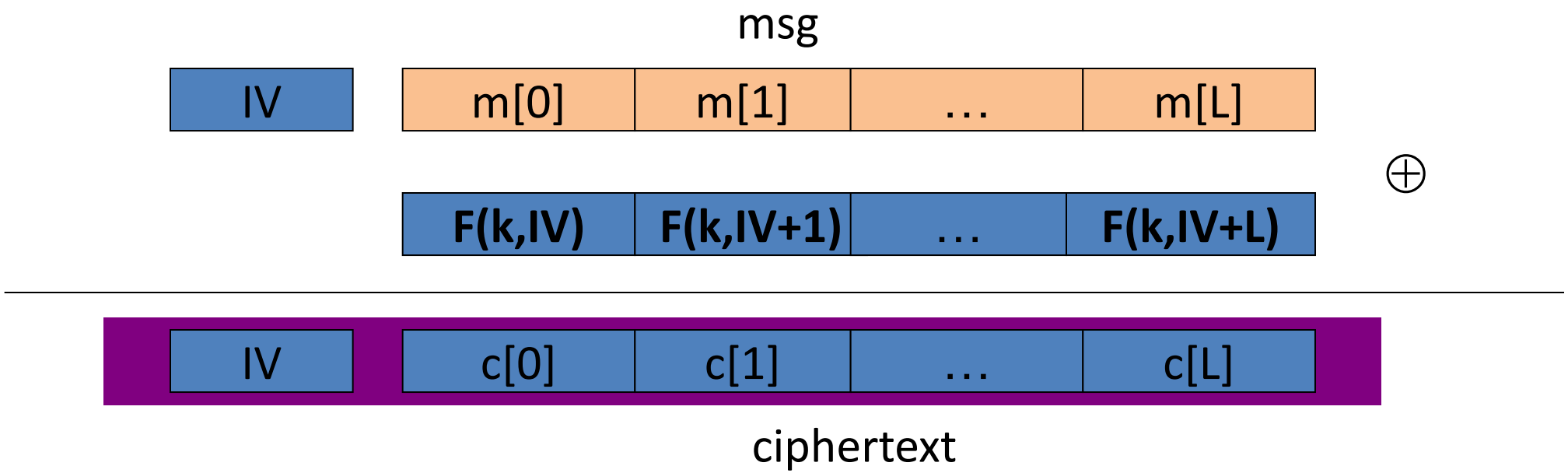
Let $F: K \times \{0,1\}^n \longrightarrow \{0,1\}^n$ be a secure PRF.

E(k,m): choose a random $IV \in \{0,1\}^n$ and do:

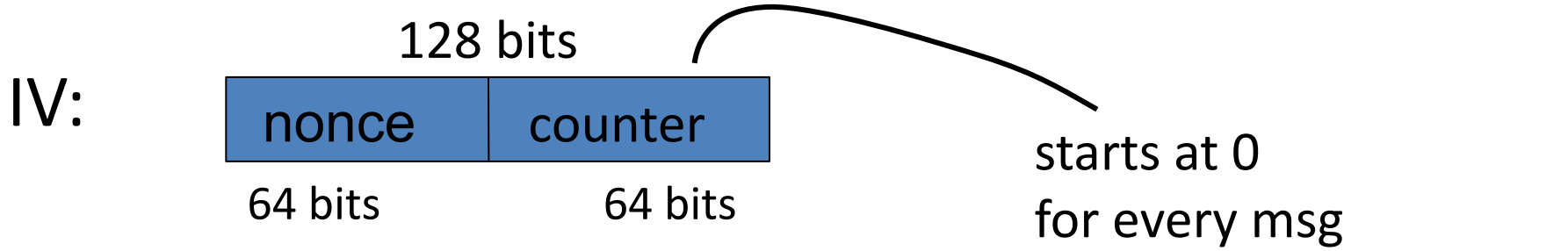


note: parallelizable (unlike CBC)

Construction 2’: nonce ctr-mode



To ensure F(k,x) is never used more than once, choose IV as:



rand ctr-mode (rand. IV): CPA analysis

- Counter-mode Theorem: For any L>0,

  If F is a secure PRF over (K,X,X) then

  E_{CTR} is a sem. sec. under CPA over (K, X^L, X^{L+1}).

  In particular, for a q-query adversary A attacking E_{CTR}

  there exists a PRF adversary B s.t.:

$$Adv_{CPA}[A, E_{CTR}] \le 2 \cdot Adv_{PRF}[B, F] + \mathbf{2\, q^2\, L \,/\, |X|}$$

Note: ctr-mode only secure as long as $q^2 L << |X|$. Better than CBC !

An example

$$Adv_{CPA}[A, E_{CTR}] \le 2 \cdot Adv_{PRF}[B, E] + \mathbf{2\, q^2\, L\, /\, |X|}$$

q = # messages encrypted with k , L = length of max message

Suppose we want $Adv_{CPA}[A, E_{CTR}] \le 1/2^{32}$ $\Leftarrow$ $q^2\, L\, /|X| < 1/\, 2^{32}$

- AES: $|X| = 2^{128}$ $\Rightarrow$ $q\, L^{1/2} < 2^{48}$

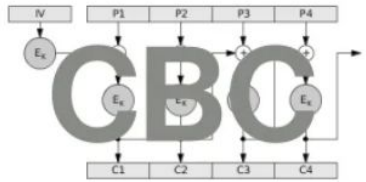
  So, after 2^{32} CTs each of len 2^{32}, must change key

  (total of 2^{64} AES blocks)

Comparison: ctr vs. CBC

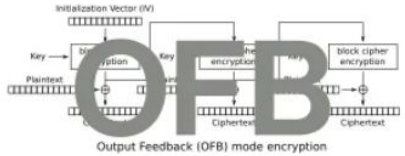
	CBC	ctr mode
uses	PRP	PRF
parallel processing	No	Yes
Security of rand. enc.	$q^2 L^2 << \|X\|$	$q^2 L << \|X\|$
dummy padding block	Yes	No
1 byte msgs (nonce-based)	16x expansion	no expansion

(for CBC, dummy padding block can be solved using ciphertext stealing)



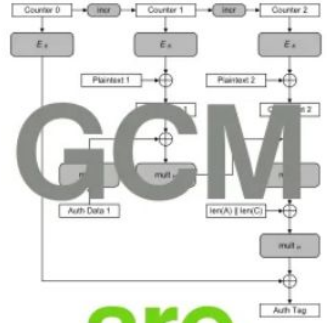
CBC

All



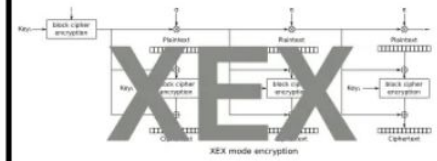
OFB

modes



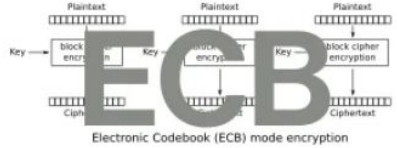
GCM

are



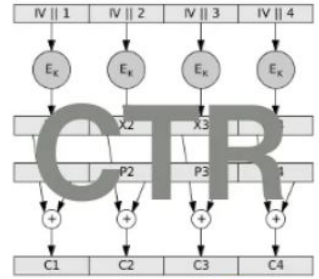
XEX

beautiful



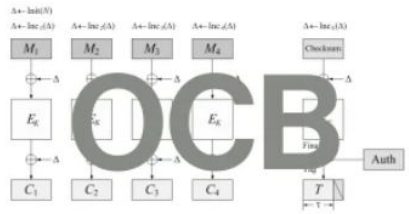
ECB

not you



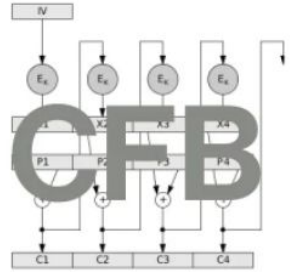
CTR

and



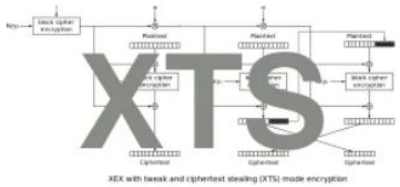
OCB

deserve



CFB

to be



XTS

used

Summary

- PRPs and PRFs: a useful abstraction of block ciphers.
- We examined two security notions: (security against eavesdropping)
  1. Semantic security against one-time CPA.
  2. Semantic security against many-time CPA.

  Note: neither mode ensures data integrity.
- Stated security results summarized in the following table:

Goal \ Power	**one-time key**	**Many-time key (CPA)**	**CPA and integrity**
Sem. Sec.	steam-ciphers det. ctr-mode	rand CBC rand ctr-mode	later

Block Cipher Attacks

Exhaustive Search for block cipher key

Goal: given a few input output pairs $(m_i, c_i = E(k, m_i))$ i=1,..,3
find key k.

Lemma: Suppose DES is an ***ideal cipher***
(2^{56} random invertible functions)
Then $\forall$ m, c there is at most **<u>one</u>** key k s.t. c = DES(k, m)

Proof: $P[\exists k' \neq k : c = DES(k,m) = DES(k',m)] \leq$

$$\sum_{k' \in \{0,1\}^{56}} P[DES(k,m) = DES(k',m)] \leq 2^{56} \cdot \frac{1}{2^{64}} = \frac{1}{2^8}$$

with prob. ≥ 1 – 1/256 ≈ 99.5%

Exhaustive Search for block cipher key

For two DES pairs $(m_1, c_1=\text{DES}(k, m_1))$, $(m_2, c_2=\text{DES}(k, m_2))$

unicity prob. $\approx 1 - 1/2^{71}$

For AES-128: given two inp/out pairs, unicity prob. $\approx 1 - 1/2^{128}$

$\Rightarrow$ two input/output pairs are enough for exhaustive key search.

Strengthening DES against ex. search

Method 1: **Triple-DES**

- Let $E : K \times M \longrightarrow M$ be a block cipher
- Define **3E**: $K^3 \times M \longrightarrow M$ as

$$\mathbf{3E}\big((k_1,k_2,k_3), m\big) = E(k_1, D(k_2, E(k_3, m)))$$

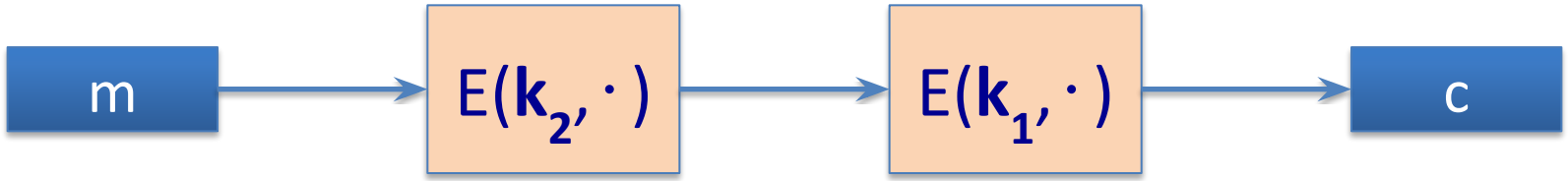
For 3DES: key-size = 3×56 = 168 bits. 3×slower than DES.

(simple attack in time $\approx 2^{118}$)

Why not double DES?

- Define $2E\big((k_1,k_2), m\big) = E\big(k_1 , E(k_2 , m)\big)$

key-len = 112 bits for DES



Attack: $M = (m_1,\ldots, m_{10})$, $C = (c_1,\ldots,c_{10})$.

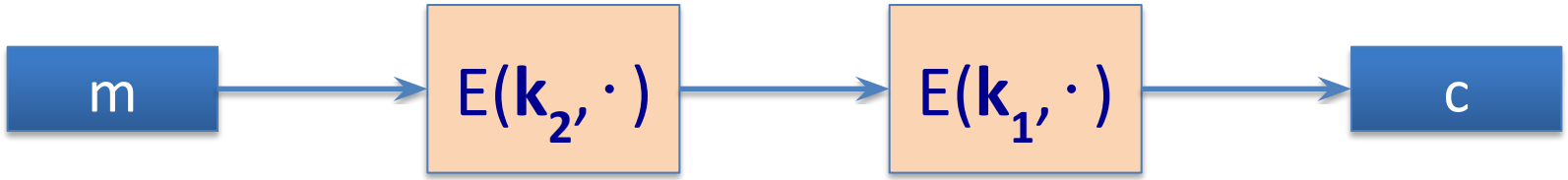
- step 1: build table.

  sort on 2^{nd} column

$k^0 = 00\ldots00$	$E(k^0, M)$
$k^1 = 00\ldots01$	$E(k^1, M)$
$k^2 = 00\ldots10$	$E(k^2, M)$
⋮	⋮
$k^N = 11\ldots11$	$E(k^N, M)$

2^{56} entries

Meet in the middle attack



Attack: $M = (m_1, \ldots, m_{10})$, $C = (c_1, \ldots, c_{10})$

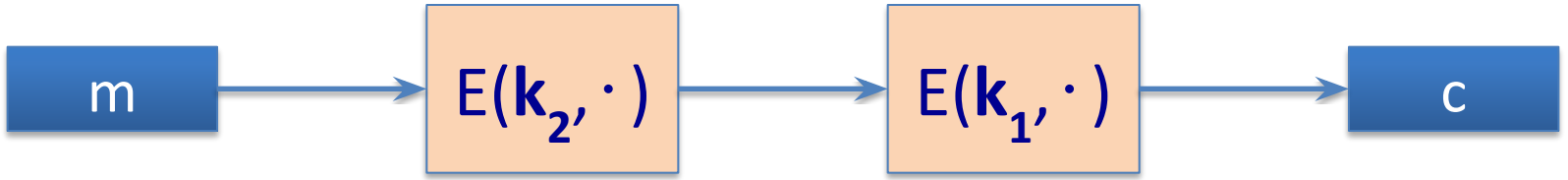
$k^0 = 00\ldots00$	$E(k^0, M)$
$k^1 = 00\ldots01$	$E(k^1, M)$
$k^2 = 00\ldots10$	$E(k^2, M)$
⋮	⋮
$k^N = 11\ldots11$	$E(k^N, M)$

- step 1: build table.
- Step 2: for all $k \in \{0,1\}^{56}$ do:

  test if $D(k, C)$ is in 2^{nd} column.

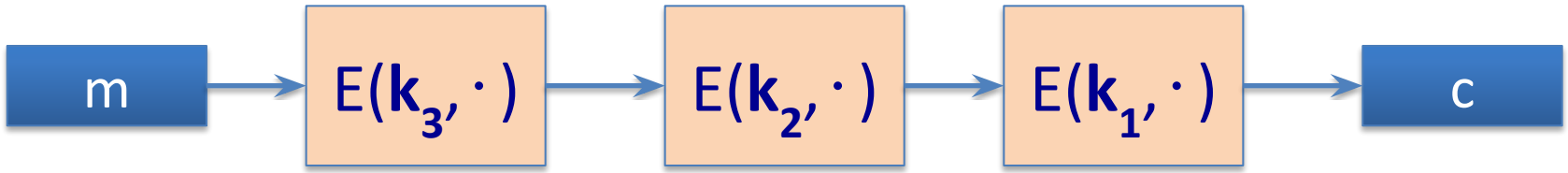
if so then $E(k^i, M) = D(k, C) \Rightarrow (k^i, k) = (k_2, k_1)$

Meet in the middle attack



Time = $2^{56}\log(2^{56}) + 2^{56}\log(2^{56}) < 2^{63}$ << 2^{112} , space ≈ 2^{56}

Same attack on 3DES: Time = 2^{118} , space ≈ 2^{56}



Method 2: DESX

$E : K \times \{0,1\}^n \longrightarrow \{0,1\}^n$ a block cipher

Define EX as $EX((k_1,k_2,k_3), m) = k_1 \oplus E(k_2, m \oplus k_3)$

For DESX: key-len = 64+56+64 = 184 bits

… but easy attack in time $2^{64+56} = 2^{120}$

Note: $k_1 \oplus E(k_2, m)$ and $E(k_2, m \oplus k_1)$ does nothing !!

Quantum attacks

Generic search problem:

Let $f: X \longrightarrow \{0,1\}$ be a function.

Goal: find $x \in X$ s.t. $f(x)=1$.

Classical computer: best generic algorithm time = $O(|X|)$

Quantum computer [Grover '96] : time = $O(|X|^{1/2})$

Can quantum computers be built: unknown

Quantum exhaustive search

Given m, c=E(k,m) define

$$f(k) = \begin{cases} 1 & \text{if } E(k,m) = c \\ 0 & \text{otherwise} \end{cases}$$

Grover $\Rightarrow$ quantum computer can find k in time $O(|K|^{1/2})$

DES: time $\approx 2^{28}$, AES-128: time $\approx 2^{64}$

quantum computer $\Rightarrow$ 256-bits key ciphers (e.g. AES-256)

PRF Switching Lemma

Any secure PRP is also a secure PRF, if $|X|$ is sufficiently large.

<u>Lemma</u>: Let E be a PRP over (K,X)

Then for any q-query adversary A:

$$\left| \mathrm{Adv}_{\mathrm{PRF}}[A,E] - \mathrm{Adv}_{\mathrm{PRP}}[A,E] \right| < q^2 / 2|X|$$

$\Rightarrow$ Suppose $|X|$ is large so that $q^2 / 2|X|$ is "negligible"

Then $\mathrm{Adv}_{\mathrm{PRP}}[A,E]$ "negligible" $\Rightarrow$ $\mathrm{Adv}_{\mathrm{PRF}}[A,E]$ "negligible"

Ευχαριστώ και καλή μέρα εύχομαι!

Keep hacking!