CS 578 – Cryptography

Prof. Michael Backes

PRPs, PRFs, and Security Definitions of Ciphers (cont'd)

May 9, 2006

Administrative Announcements

- Handouts today:
  - Lecture notes, next exercise sheet
- Office hours:
  - Moved Thursday's TA office hour to Monday 14:00-16:00
  - Additional office hour by myself on Monday 12:00-13:00
- Result of quizzes sent by weekly email
- Remarks on the mid-term exam:
  - Takes place on Tuesday, May 30, 1 hour, instead of lecture 11:00 - 13:00 (likely to happen in 2 groups)
  - Preceding Friday, May 26, Q&A lecture!

Recall: Stream- and block ciphers

- ## Stream Ciphers (PRG):

  - Encrypts long messages, but one-time key use

- ## Block Ciphers:

  - basic "primitive" for encrypting short blocks

- ## Attacks on block ciphers:

  - Exhaustive Search: For const # of PT/CT pairs

  - Linear Cryptanalysis: Large (2^{42}) # of PT/CT pairs

- ## Defining security via games:

  - PRPs, PRFs

  - Semantic security against CT-only attacks for ciphers

Recall: PRFs and PRPs

- PRF: F: $\mathcal{K} \times \mathcal{X} \to \mathcal{Y}$ is a PRF over $(\mathcal{K}, \mathcal{X}, \mathcal{Y})$ if
  - F is "efficiently" computable
  - F indistinguishable from a random function $\mathcal{X} \to \mathcal{Y}$ for a randomly drawn key

- PRP: E: $\mathcal{K} \times \mathcal{X} \to \mathcal{X}$ is a PRP over $(\mathcal{K}, \mathcal{X})$ if
  - E can be efficiently computed
  - For all K $\in$ $\mathcal{K}$, E(K,·): $\mathcal{X} \to \mathcal{X}$ is bijective.
  - For all K $\in$ $\mathcal{K}$, D(K,·) = E^{-1}(K,·) is efficiently computable.
  - F indistinguishable from a random permutation $\mathcal{X} \to \mathcal{X}$ for a randomly drawn key

- Examples: AES, 3DES
- Any PRP on $(\mathcal{K}, \mathcal{X})$ is also a PRF on $(\mathcal{K}, \mathcal{X}, \mathcal{X})$
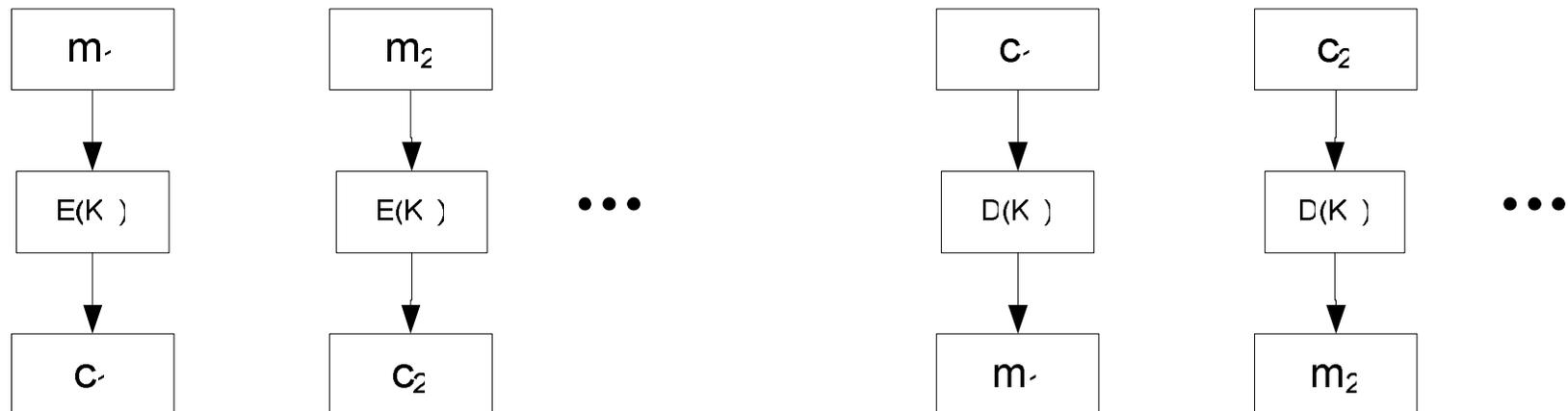
Recall: PRF Attack Game

- For b=0,1, define experiment EXP^{PRF} (b) as:

b

b = 0 K $\leftarrow_R \mathcal{K}$ F := E(K)
b = 1 F $\leftarrow_R$ Func[$\mathcal{X},\mathcal{Y}$]

Chal

x

F(x)

Adv

b*
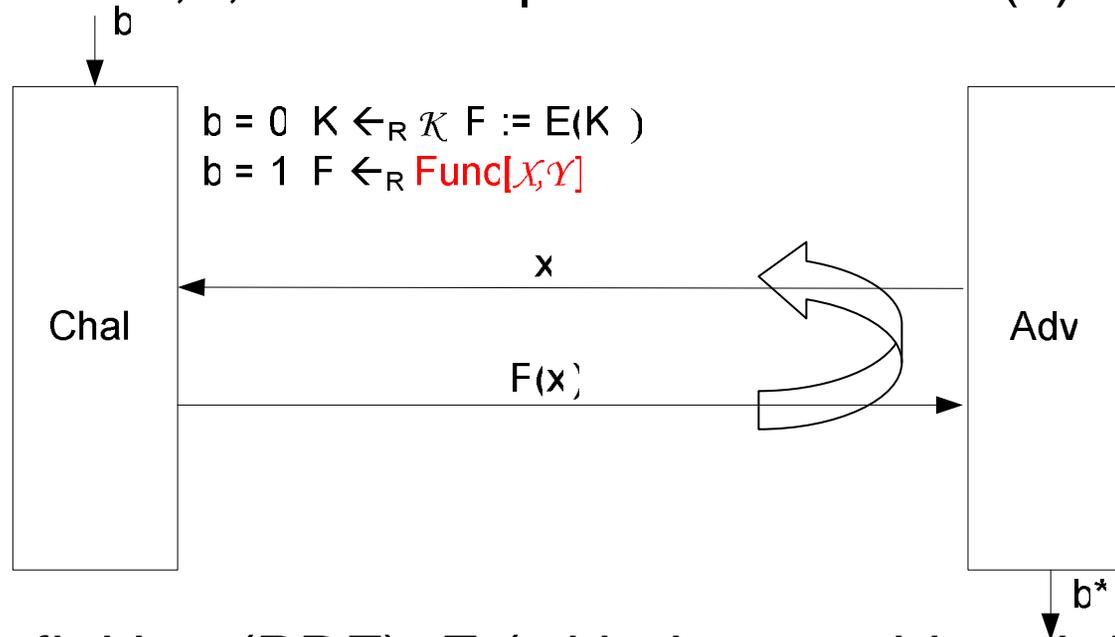
- Definition (PRF). E (with the considered domains, ranges, etc.) is a PRF if for all efficient adversaries A, we have that Adv^{PRF}[A,E] = |Pr[EXP^{PRF} (0)=1] – Pr[EXP^{PRF} (1)=1]| is negligible.

Recall: Electronic Codebook

- Electronic Codebook (ECB)

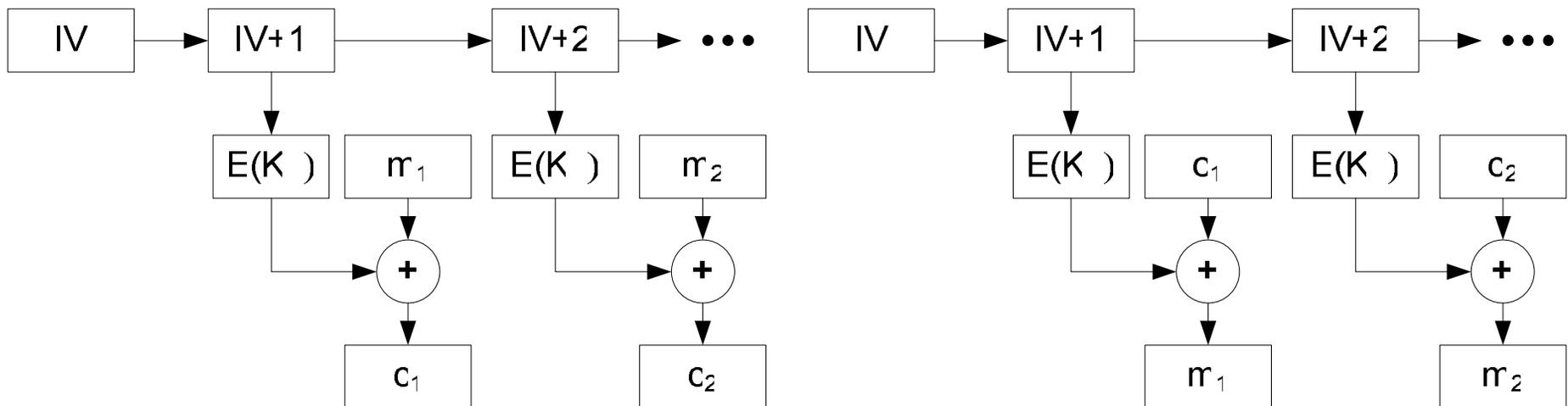| m_1		m_2			c_1		c_2	
↓		↓			↓		↓	
$E(K)$		$E(K)$	•••		$D(K)$		$D(K)$	•••
↓		↓			↓		↓	
c_1		c_2			m_1		m_2	

- "Not secure" because the adversary can tell if two blocks encrypt the same message

Recall: Countermode

- Countermode (CTR)

- Should be "secure" if E is "secure"…

Recall: Definitions of Security

- **Security always defined in two parameters:**
  1. **What "power" does the adversary have?**
     - Adv. sees only one ciphertext (i.e. CT-only attack)
     - Adv. sees many PT/CT pair (CPA)
     - (Adv. gets chosen CTs decrypted (CCA))
  2. **What "goal" is the adversary trying to achieve?**
     - Semantic security: learn info about (new) PT from CT

Power / Goal	One-time key (CT-only attack)	Many-time key (CPA)	CCA
Semantic Security	Stream ciphers (det) ctr mode	(rand) CBC (rand) ctr mode	Later

Recall: Semantic Security (CT-only attack)

- Let (E,D) be a cipher over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$. Define $\text{EXP}^{\text{CT-only}}(b)$ as:
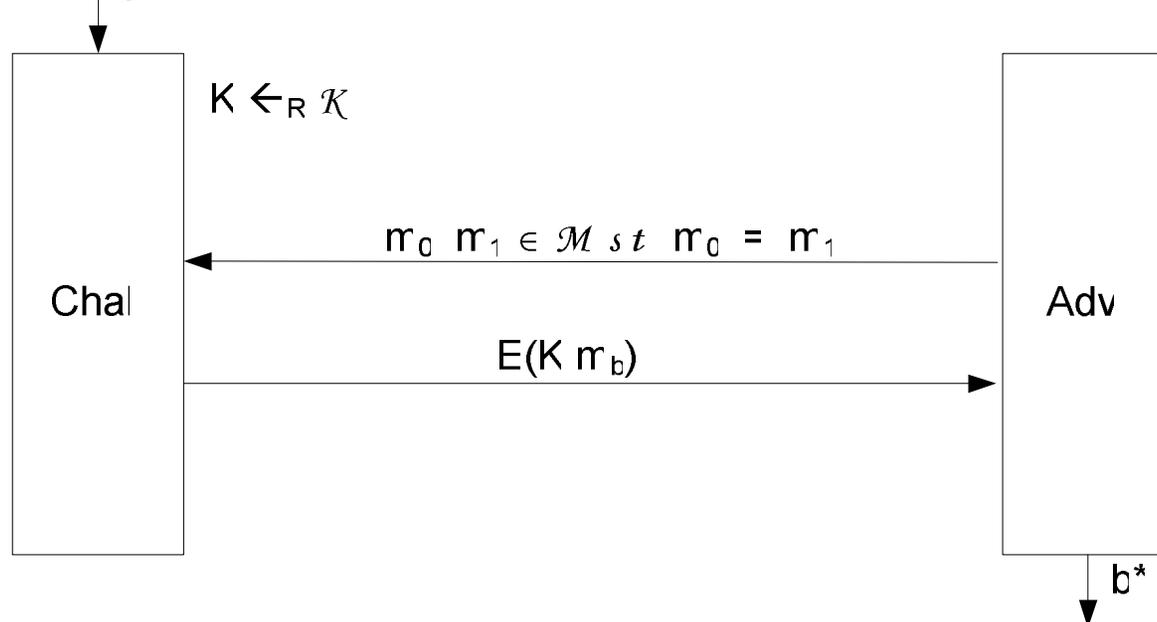
- Definition (Semantic Security). A cipher (E,D) is semantically secure under CT-only attack if for all efficient adversaries A, we have that $\text{Adv}^{\text{CT-only}}[A,E] = |\Pr[\text{EXP}^{\text{CT-only}}(0)=1] - \Pr[\text{EXP}^{\text{CT-only}}(1)=1]|$ is negligible.

First Implications of Semantic Security

- Semantic Security states that a CT leaks nothing about a PT to efficient adversaries

- E.g., assume an adversary A learns "the x-th bit of m" given $E(K,m)$ with probability $½ + p$

- Claim: If A is efficiently computable and p is not negligible, then E cannot be semantically secure!
  [proofsketch on the board again]

- Works not only for "x-th bit" but for any samplable predicate on messages (!!)

Semantic Security of ECB?

- Recall: Electronic Codebook (ECB)
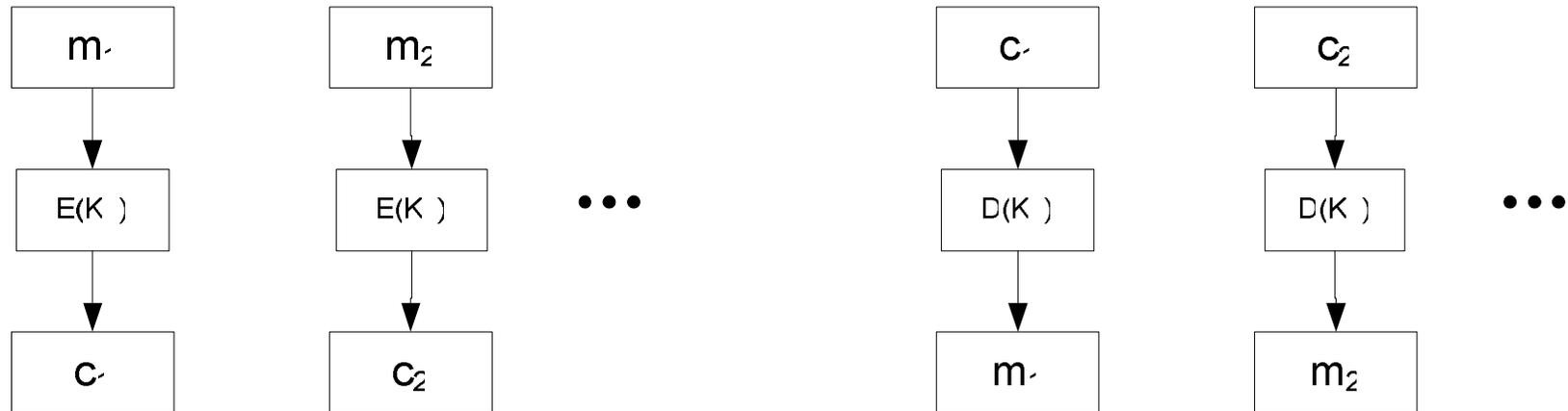
- Semantically Secure under CT-only attack?

Semantic Security and ECB

- ECB is not semantically secure under CT-only attack
  - Consider the following messages
  - m_0 = "hello""hello", m_1 = "hello""world"
  - Leads to outputs of the form
    c_0 = "c" "c", c_1 = "c" "c*"
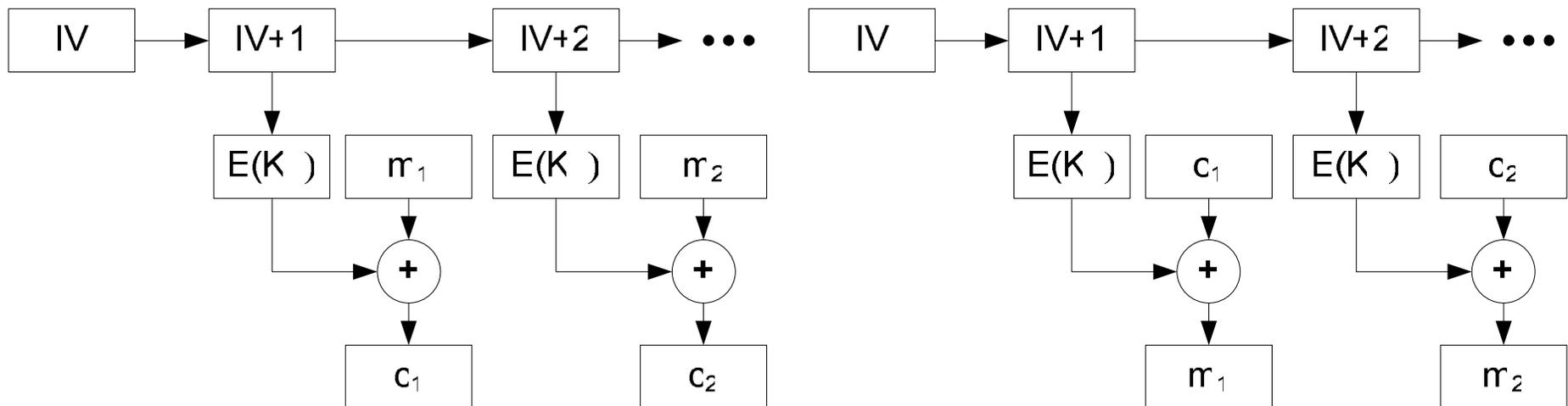 - Easily distinguishable!

Constructions for Semantic Security

- Examples:
    - One-time Pad: $\text{Adv}^{\text{CT-only}}[A, \text{OTP}] = 0$ for all A.
    - Deterministic counter mode from a PRF E: (essentially stream ciphers built from PRF, e.g., AES, 3DES)

$E^{\text{DETCTR}}(K,m) =$

m[1]	m[2]	…	m[L]
E[K,1]	E[K,2]	…	E[K,L]
c[1]	c[2]	…	c[L]

$\oplus$

Deterministic Counter mode

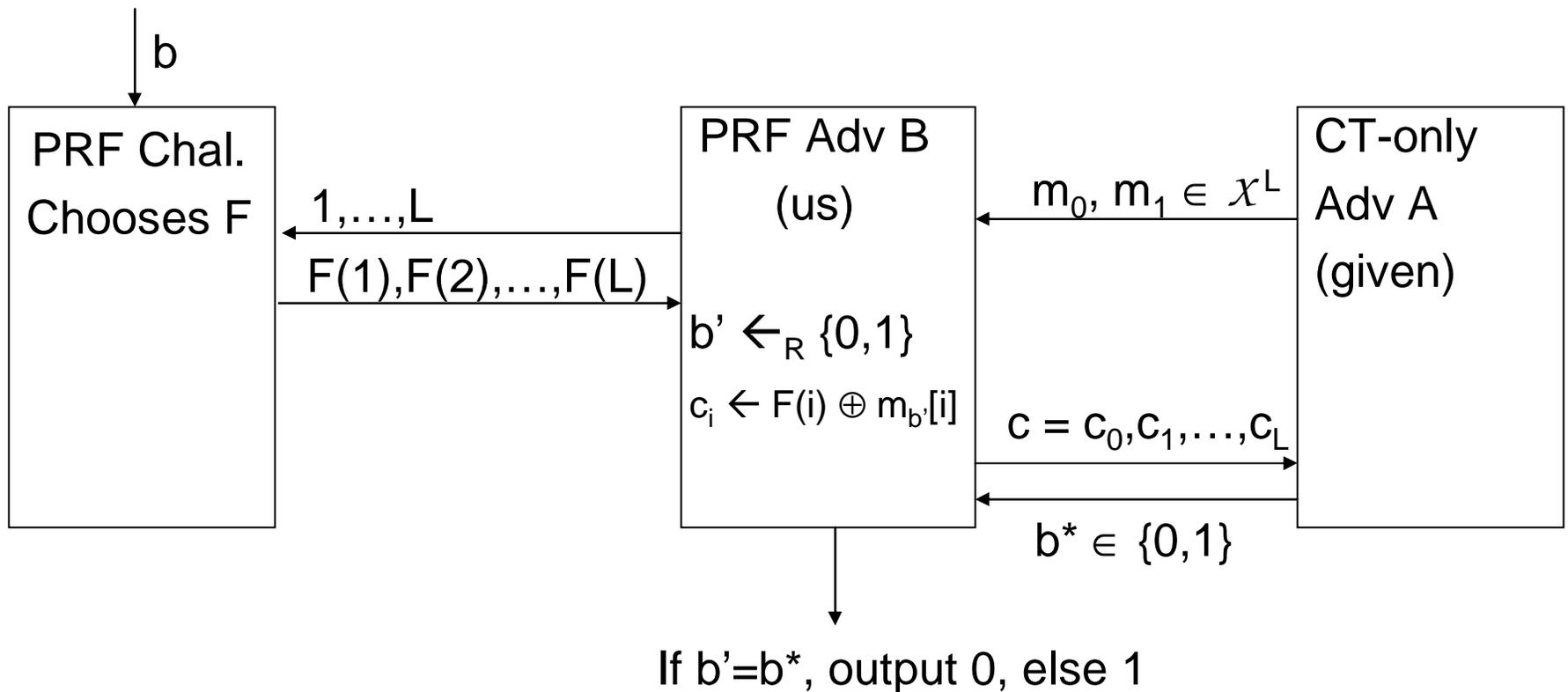- Deterministic Countermode (DETCTR): IV = 0

Deterministic ctr-mode Security

- Theorem: For any L>0:
  If E is a PRF over $(\mathcal{K}, \mathcal{X})$ then E^{DETCTR} (using E) is a semantically secure cipher over $(\mathcal{K}, \mathcal{X}^L, \mathcal{X}^L)$ under CT-only attack.
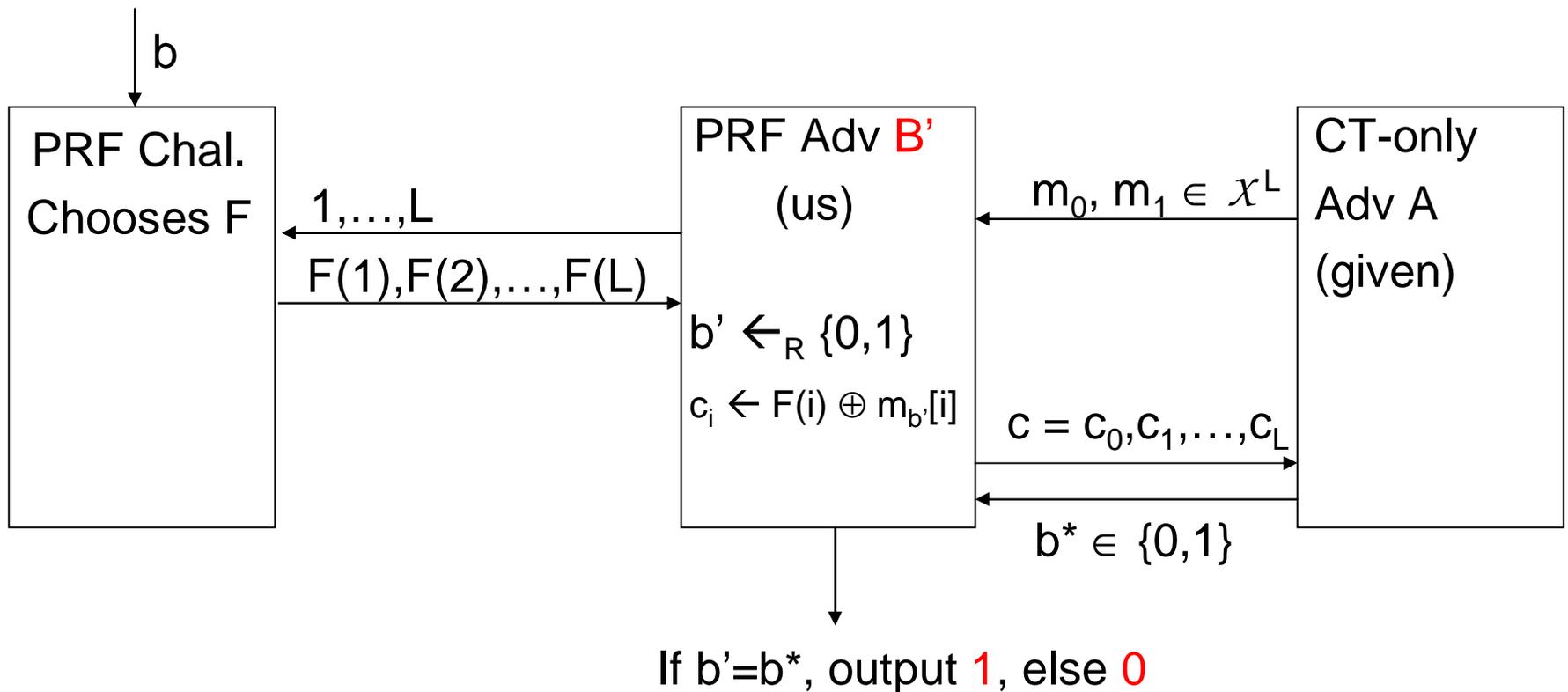
  More precisely, for any adversary A attacking E^{DETCTR} there exists a PRF adversary B such that
  $Adv^{\text{CT-only}}[A, E^{\text{DETCTR}}] = 2 \cdot Adv^{\text{PRF}}[B,E]$

Proof Overview

b

PRF Chal.
Chooses F

1,…,L

F(1),F(2),…,F(L)

PRF Adv B
(us)

$m_0, m_1 \in \mathcal{X}^L$

CT-only
Adv A
(given)

$b' \leftarrow_R \{0,1\}$

$c_i \leftarrow F(i) \oplus m_{b'}[i]$

$c = c_0,c_1,…,c_L$

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

If b'=b*, output 0, else 1

Proof Overview

b

PRF Chal.
Chooses F

1,…,L

F(1),F(2),…,F(L)

PRF Adv B'
(us)

$b' \leftarrow_R \{0,1\}$

$c_i \leftarrow F(i) \oplus m_{b'}[i]$

$m_0, m_1 \in \mathcal{X}^L$

CT-only
Adv A
(given)
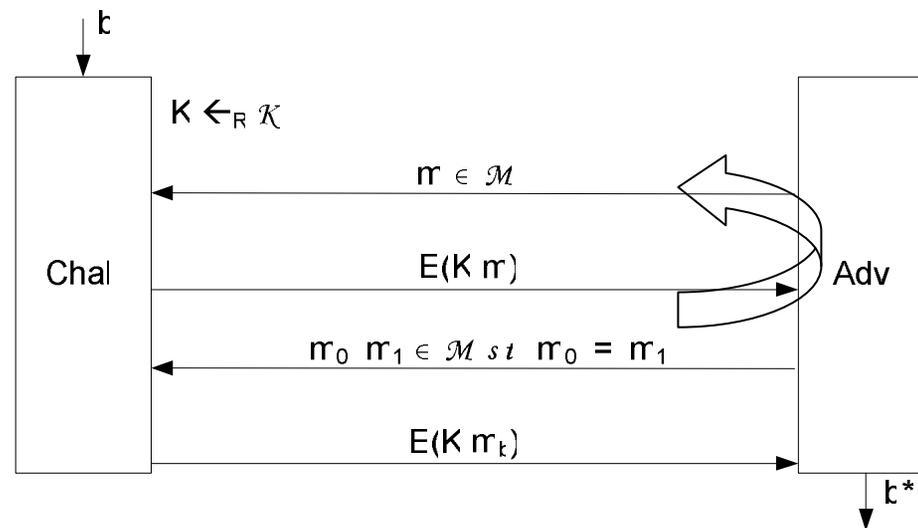
$c = c_0, c_1, …, c_L$

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

If b'=b*, output 1, else 0

Semantic Security under CPA attack

- Let (E,D) be a cipher defined over $(\mathcal{K},\mathcal{M},\mathcal{C})$. For b = 0,1 define $\text{EXP}^{CPA}(b)$ as:


- Definition. A cipher (E,D) is semantically secure under CPA if for all efficient adversaries A, we have that
$\text{Adv}^{CPA}[A,E] = |\text{Pr}[\text{EXP}^{CPA}(0)=1] - \text{Pr}[\text{EXP}^{CPA}(1)=1]|$ is negligible

Randomized Encryption

- Fact: Stream ciphers are insecure under CPA.

- Fact: No deterministic function can be secure under CPA!!

- Consequence: Good encryption algorithms must be randomized

Security of CBC

- Cipherblock Chaining (CBC)
  - Very often used, but main problem: Sequential
  - Initial value random chosen and output as well
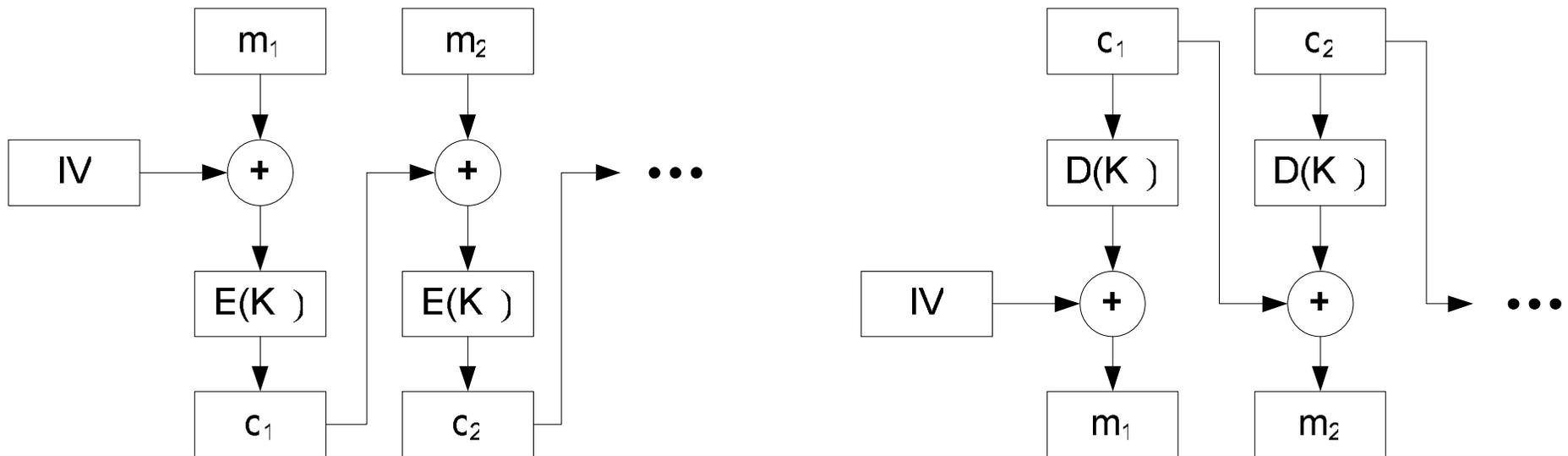
Security of CBC (cont'd)

- Cipher Block Chaining (CBC) with a random IV
- CBC theorem: For any L > 0: If E is a PRP over $(\mathcal{K}, \mathcal{X})$ then E^{CBC} is semantically secure under CPA over $(\mathcal{K}, \mathcal{X}^L, \mathcal{X}^{L+1})$.
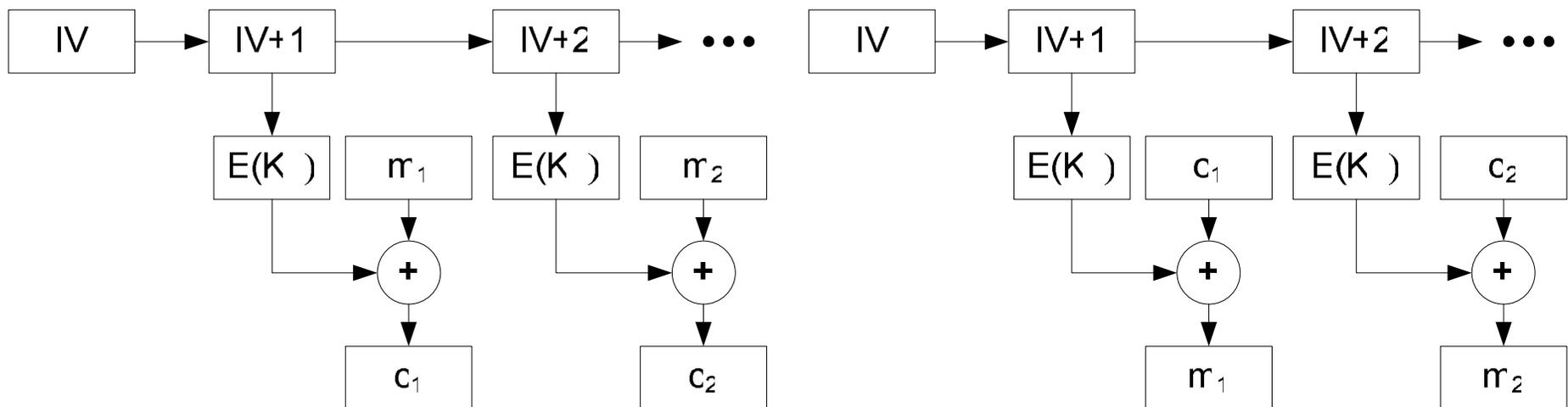
  In particular: For any q-query adversary A attacking E^{CBC} there exists a PRF adversary B such that $Adv^{CPA}[A, E^{CBC}] \leq 2 \cdot Adv^{PRF}[B,E] + 2q^2L^2 / |\mathcal{X}|$

- Note: CBC is only secure as long as $qL << |\mathcal{X}|^{1/2}$

Security of Random ctr-mode

- Random Countermode (RNDCTR)
  - New IV for every encryption (will be send as $IV=c_0$)
  - Note: No need for decryption here → PRF instead of PRP suffices
  - We will see: Better security than CBC

Security of Random ctr-mode (cont'd)

- Randomized counter mode: random IV for every new message to be encrypted

- Counter-mode Theorem: For any L > 0: If E is a PRF over $(\mathcal{K}, \mathcal{X}, \mathcal{X})$ then E^{RNDCTR} is semantically secure under CPA over $(\mathcal{K}, \mathcal{X}^L, \mathcal{X}^{L+1})$.
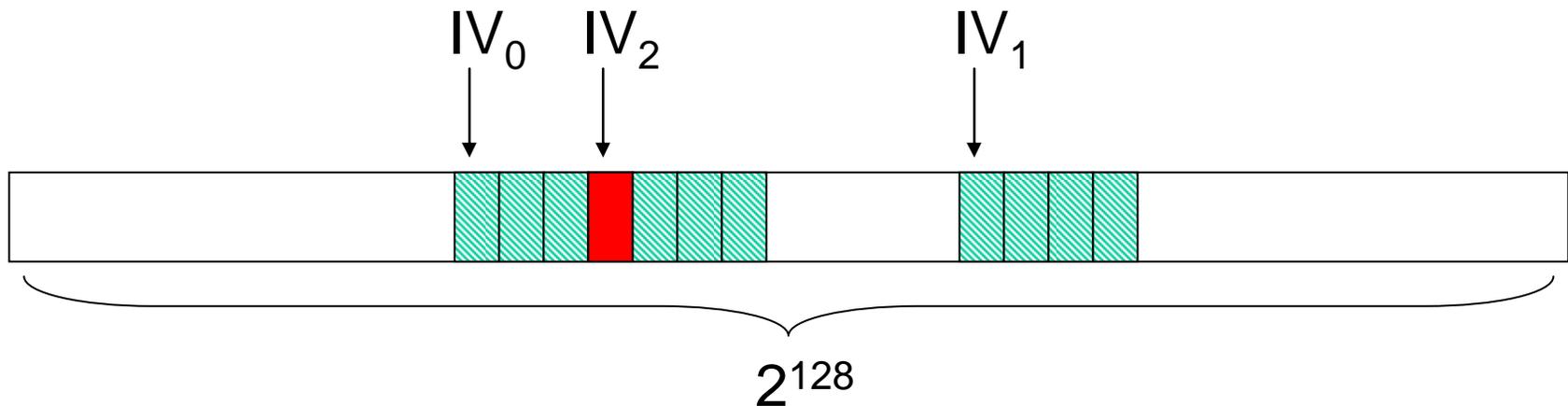
  In particular: For any q-query adversary A attacking E^{RNDCTR} there exists a PRF adversary B such that $Adv^{CPA}[A, E^{RNDCTR}] \leq 2 \cdot Adv^{PRF}[B,E] + 2q^2L /|\mathcal{X}|$

- Note: ctr-mode only secure as long as $q^2L << |\mathcal{X}|$

  Better than CBC!

Security of Random ctr-mode (cont'd)

- Sketch of PRF attack

- Attacker queries $x_0, x_1, \ldots$

- Attacker gets $E(K, x_0)$, $E(K, x_1)$, $\ldots$

Summary of Symmetric Encryption

- **Perfect secrecy and the OTP**: Security against infinitely smart adversaries, but unpractical

- **Stream ciphers**: Fast, but keys only used once. Security treated via security of PRGs

- **Block ciphers**: Basic building blocks for larger encryption systems (modes of operation). Idealized into PRPs/PRFs in security proofs

- **Modes of Operation**: Semantic security: *The* definition of secure encryption. Captures security against all efficient adversaries. So far CT-only and CPA variants.

- Asymmetric encryption still to come

- But now forget about encryption for a while…

Message Integrity

- Goal of message integrity:

| m | tag |

A ⟶ B
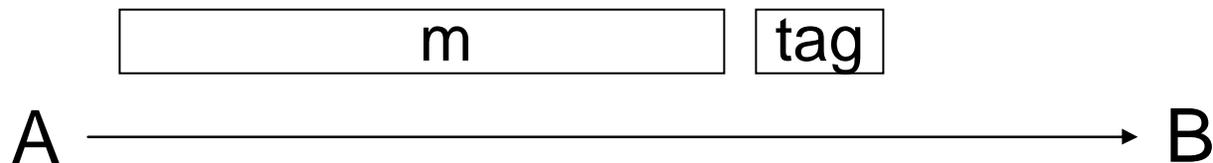
- Alice generates tag, Bob verifies tag
- Goal: Attacker cannot change message, i.e., attacker cannot generate any valid pair (m,tag)

Definition of MAC

- Definition (MAC): A message authentication code (MAC) defined over $(\mathcal{K},\mathcal{M},\mathcal{T})$ is a pair (S,V) of efficient algorithms (S,V) where

  $$S: \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{T} \text{ and } V: \mathcal{K} \times \mathcal{M} \times \mathcal{T} \rightarrow \mathcal{Bool}$$

  s.t. for all $m \in \mathcal{M}$, $K \in \mathcal{K}$: $(t \leftarrow S(K,m)) \rightarrow (V(K,m,t) = true)$

- Definition (Secure MACs, intuitively):

  - Attacker's power: chosen-message attack
    Attacker outputs $m_1 \ldots m_q$, and gets $t_i \leftarrow S(K,m_i)$

  - Attacker's goal: existential forgery
    Produce valid pair (m^*,t^*), i.e., $V(K,m^*,t^*) = true$, where $(m^*,t^*) \notin \{(m_1,t_1), \ldots, (m_q,t_q)\}$

- Attacker cannot even forge MACs on non-sensitive messages

MACS

- For MAC I=(S,V), define the following MAC game:
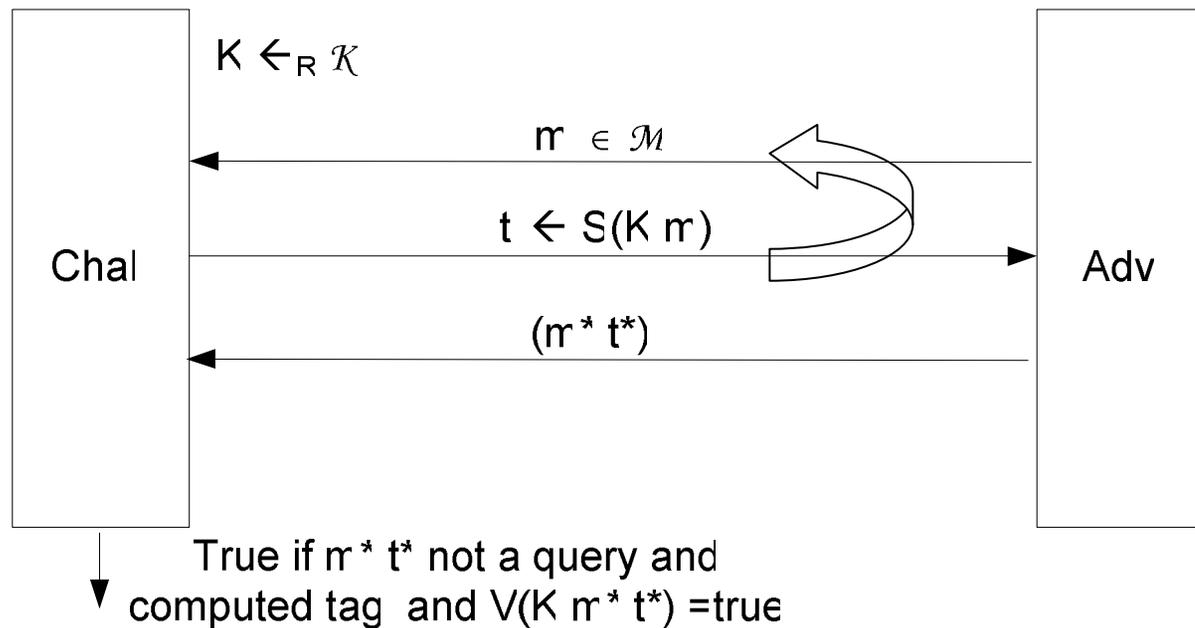
Definition of Secure MACs

- The advantage of adversary A attacking I is $\text{Adv}^{\text{MAC}}[A,I] = \Pr[\text{Challenger outputs true}]$

- Definition (Secure MACs): A MAC I=(S,V) is a secure against existential forgery under chosen-message attacks (CMA) if for all efficient algorithms A: $\text{Adv}^{\text{MAC}}[A,I]$ is negligible.