CS 578 – Cryptography

Prof. Michael Backes

PRPs, PRFs, and Security Definitions of Ciphers

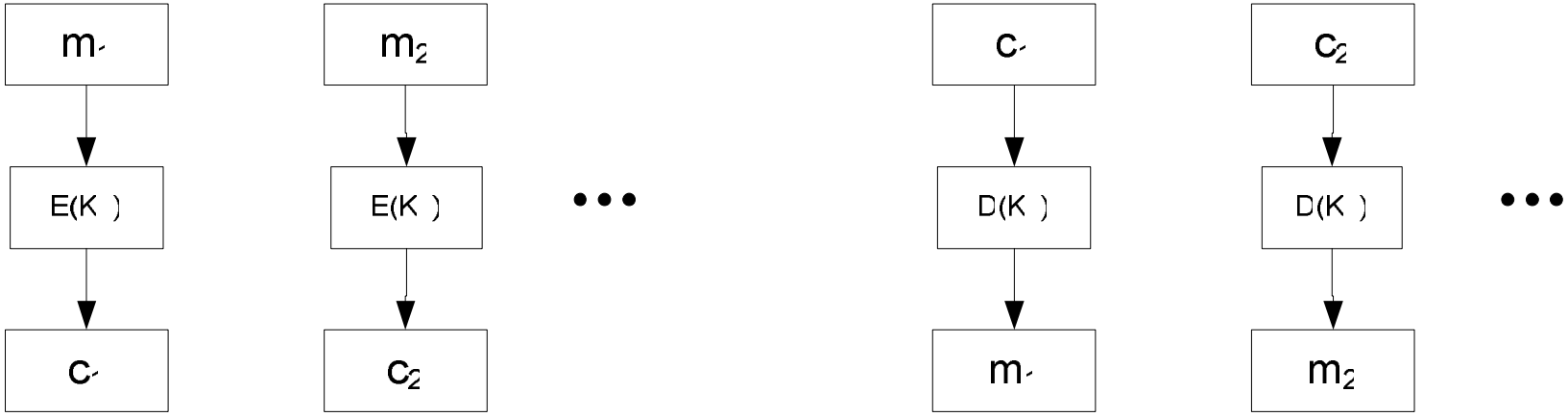
May 5, 2006

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
- What we are doing today:
  - Security definitions and basic building blocks: PRP, PRF
  - Security of modes of operations for block ciphers

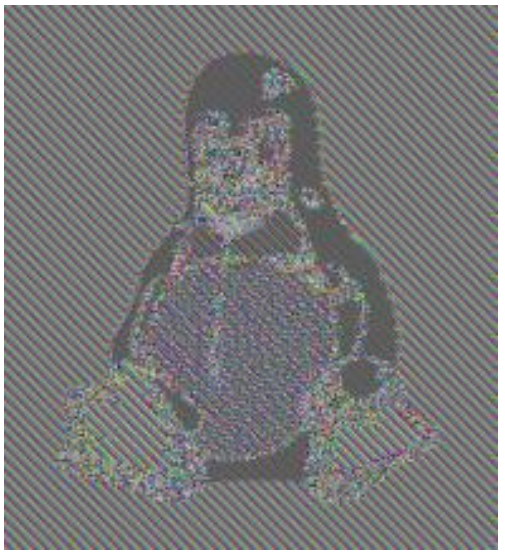
Recall: Electronic Codebook

- Electronic Codebook (ECB)

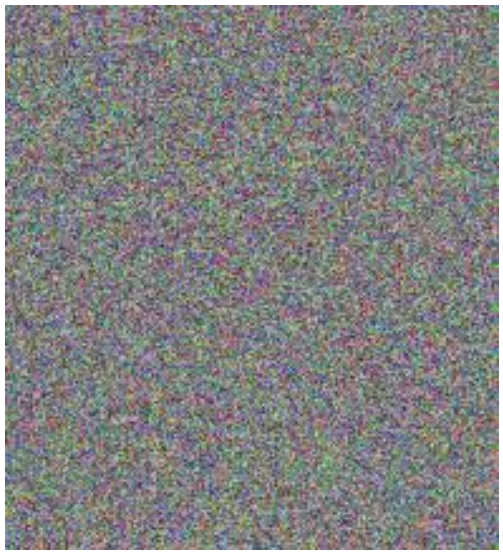


- “Not secure” because the adversary can tell if two blocks encrypt the same message

ECB Reveals Patterns



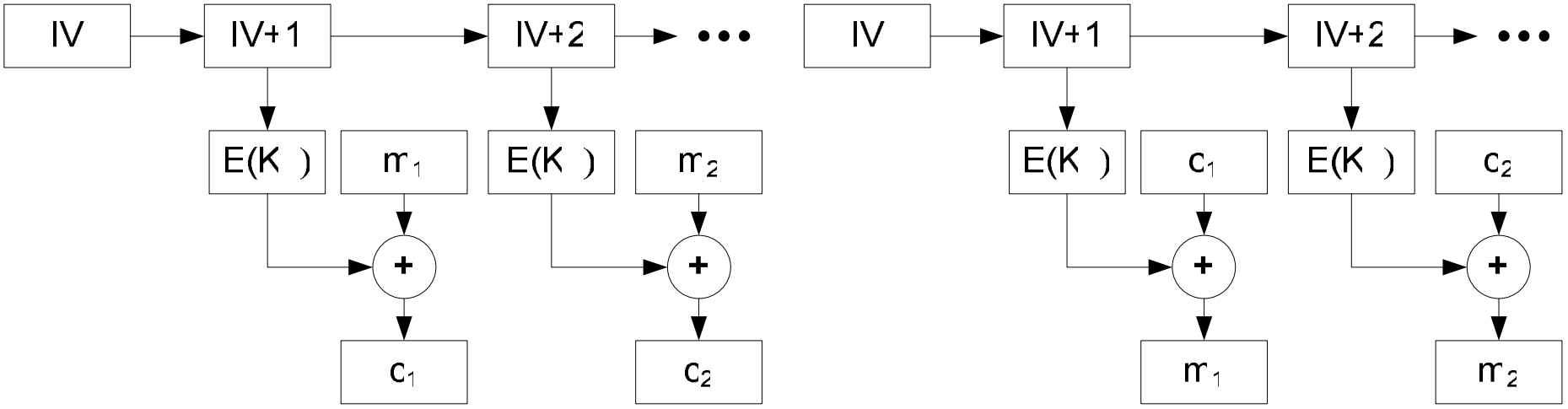
ECB Encryption



Other mode of operation

Recall: Countermode

- Countermode (CTR)



- Should be “secure” if E is “secure”…

Security of these Constructions

- So far no (good) definition of security for these constructions and ciphers in general
- Security of modes clearly depends on properties of E (mode can only be secure if E is a “good” block cipher)
- Security should not only hold for specific E (AES, 3DES, etc.) but for all “secure” E’s

→ Rethink what a good block cipher is, then abstract it, and reason about the abstraction in larger contexts (e.g., in modes)!

Pseudo-random Permutations (PRPs)

- Model block ciphers as pseudo-random permutations (PRP)
- Let E: $\mathcal{K} \times \mathcal{X} \rightarrow \mathcal{X}$ such that
  - E can be efficiently computed
  - For all $K \in \mathcal{K}$, the function $E(K,\cdot): \mathcal{X} \rightarrow \mathcal{X}$ is bijective.
  - For all $K \in \mathcal{K}$, the function $D(K,\cdot) = E^{-1}(K,\cdot)$ is efficiently computable.
- Which property need E satisfy to be a PRP?

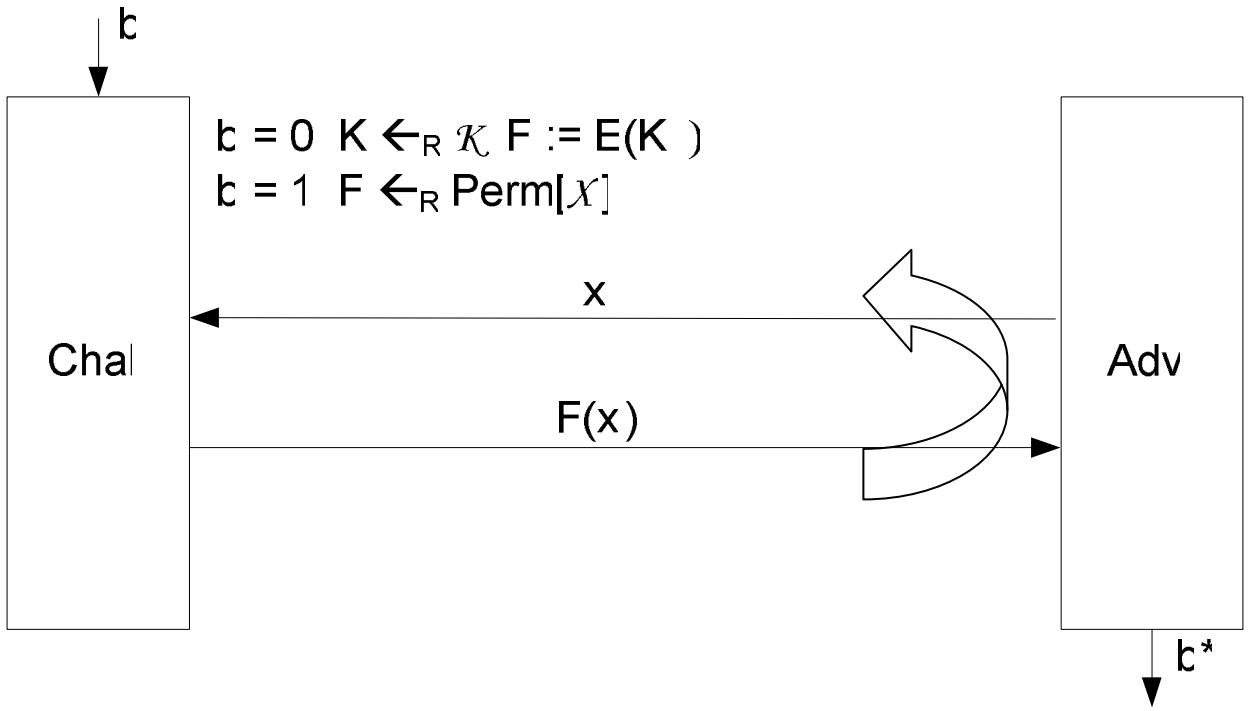
PRP Attack Game

Definition (PRP Attack game for E)

1. Given a random bit b, the challenger plays one of two experiments:
   - Exp(0) : Let K $\leftarrow_R$ $\mathcal{K}$, F := E(K,·)
   - Exp(1) : Let F $\leftarrow_R$ Perm($\mathcal{X}$)
2. Adversary submits queries to F: $\mathcal{X} \rightarrow \mathcal{X}$
   For i-th query x_i, the challenger outputs $F(x_i)$
3. The adversary outputs b* and wins if b* = b.

PRP Attack Game (cont'd)

- For b=0,1, define experiment EXP(b) as:



PRP Attack Game (cont'd)

- Let EXP(b)=1 denote the event that the adversary outputs 1 in Experiment b
- The advantage of adversary A attacking E is $Adv^{PRP}[A,E] := |Pr[EXP(0)=1] - Pr[EXP(1)=1]|$
- Definition (PRP). E (with the considered domains, ranges, etc.) is a PRP if for all efficient adversaries A, we have that $Adv^{PRP}[A,E]$ is negligible (in the key size).
- Side remark:
  - A function f: N → $R^{\geq 0}$ is negligible if $\forall c \in N\ \exists n_c\ \forall n \geq n_c \in : f(n) < 1/n^c$
  - $Adv^{PRP}[A,E]$ being negligible defined in the size of the key → only meaningful for keys+messages of different length ($(\mathcal{K}_k)_{k\in N}$, $(\mathcal{X}_k)_{k\in N}$ instead of fixed $\mathcal{K}$, $\mathcal{X}$), thus formally sequences of PRPs…

Examples of PRPs

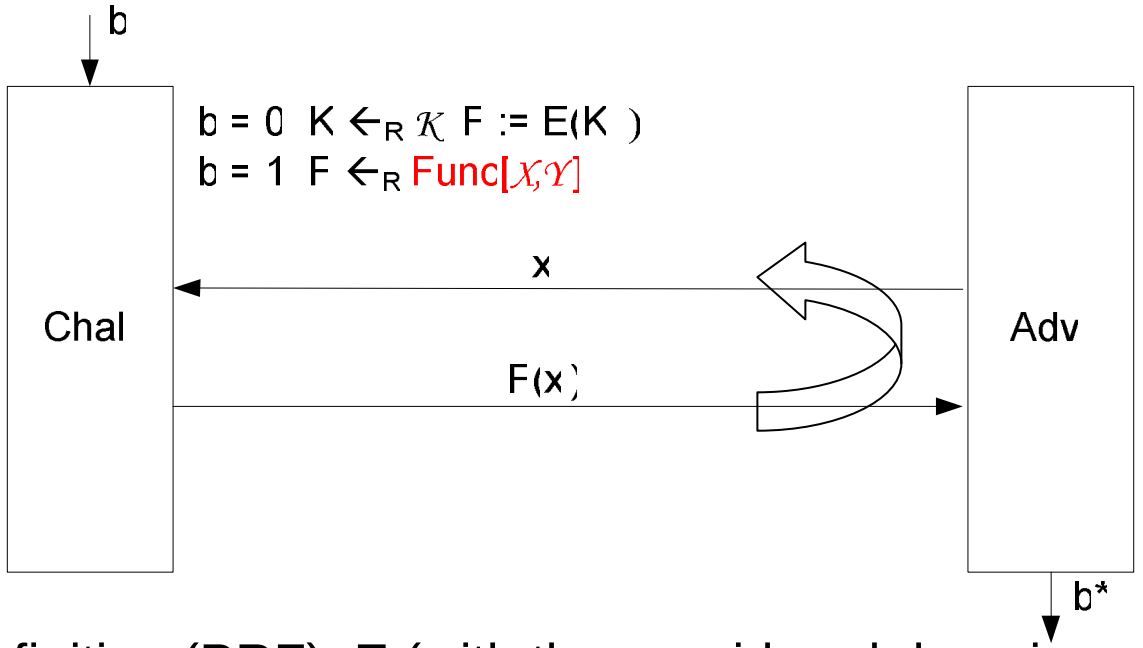
- Example PRPs: 3DES, AES, …
  - For 3DES: $\mathcal{K} = \{0,1\}^{168}$, $\mathcal{X} = \{0,1\}^{64}$
  - 3DES PRP-Assumption:
    All 2^{80}-time algorithms A have
    $\mathrm{Adv}^{\mathrm{PRP}}[A,3DES] \leq 2^{-40}$

Pseudo-random Functions (PRFs)

- Related concept: Pseudo-random function (PRF)
- Definition is essentially the same:
  E is a PRF over $(\mathcal{K},\mathcal{X},\mathcal{Y})$ if
  - E: $\mathcal{K}\times\mathcal{X}\rightarrow\mathcal{Y}$
  - E is efficiently computable
  - E satisfies the same attack game as for PRP except for a modified Experiment 1:
    Exp(0) : Let K $\leftarrow_R$ $\mathcal{K}$, F := E(K,·)
    Exp(1) : Let F $\leftarrow_R$ Func($\mathcal{X},\mathcal{Y}$)
- The advantage of adversary A attacking E is
  $Adv^{PRF}[A,E] := |Pr[EXP(0)=1] - Pr[EXP(1)=1]|$

PRF Attack Game

- For b=0,1, define experiment EXP(b) as:



- Definition (PRF). E (with the considered domains, ranges, etc.) is a PRF if for all efficient adversaries A, we have that $Adv^{PRF}[A,E]$ is negligible.

PRF Switching Lemma

- Lemma: Let E be a PRP over $(\mathcal{K}, \mathcal{X})$. Then E is a PRF over $(\mathcal{K}, \mathcal{X}, \mathcal{X})$.
- More precise bound on adversary advantage: If E is a PRP over $(\mathcal{K}, \mathcal{X})$, then for every q-query adversary A:
  $|Adv^{PRF}[A,E] - Adv^{PRP}[A,E]| \leq q^2/2|\mathcal{X}|$.

  [proof on the board]

PRPs and PRFs, Luby-Rackoff

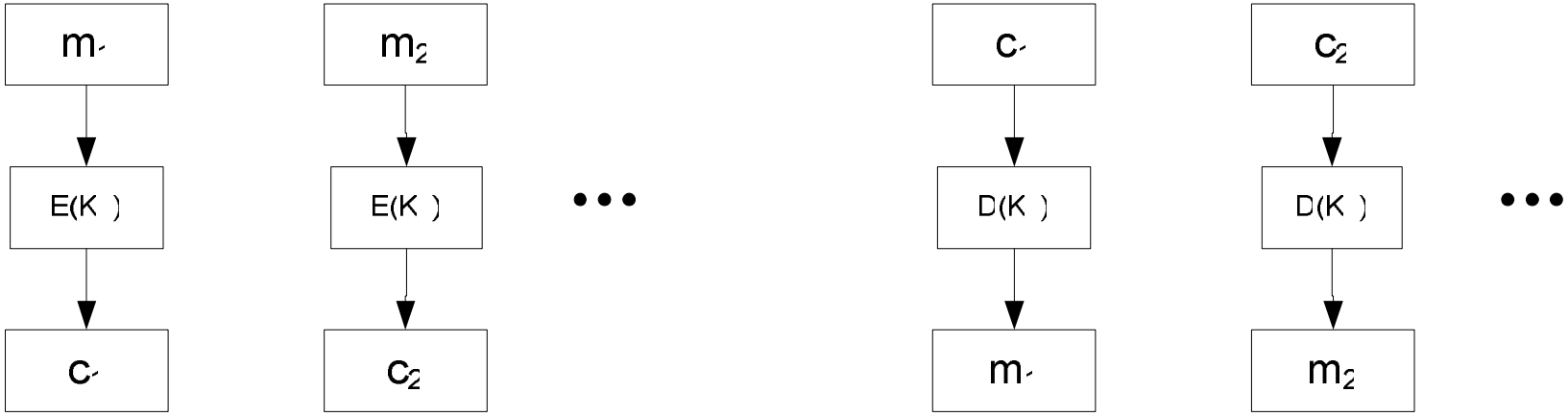
- Examples for PRPs: 3DES, AES, …
  - For 3DES: $\mathcal{K} = \{0,1\}^{168}$, $\mathcal{X} = \{0,1\}^{64}$
  - 3DES PRP Assumption:
    All 280-time algorithms A, we have
    $Adv^{PRP}[A,3DES] \leq 2^{-40}$

→ Also examples for PRFs

- Luby-Rackoff theorem (Justification for DES):
  A 3-round Feistel network whose three round functions are PRFs is itself a PRP.

Using BC (PRPs): Electronic Codebook

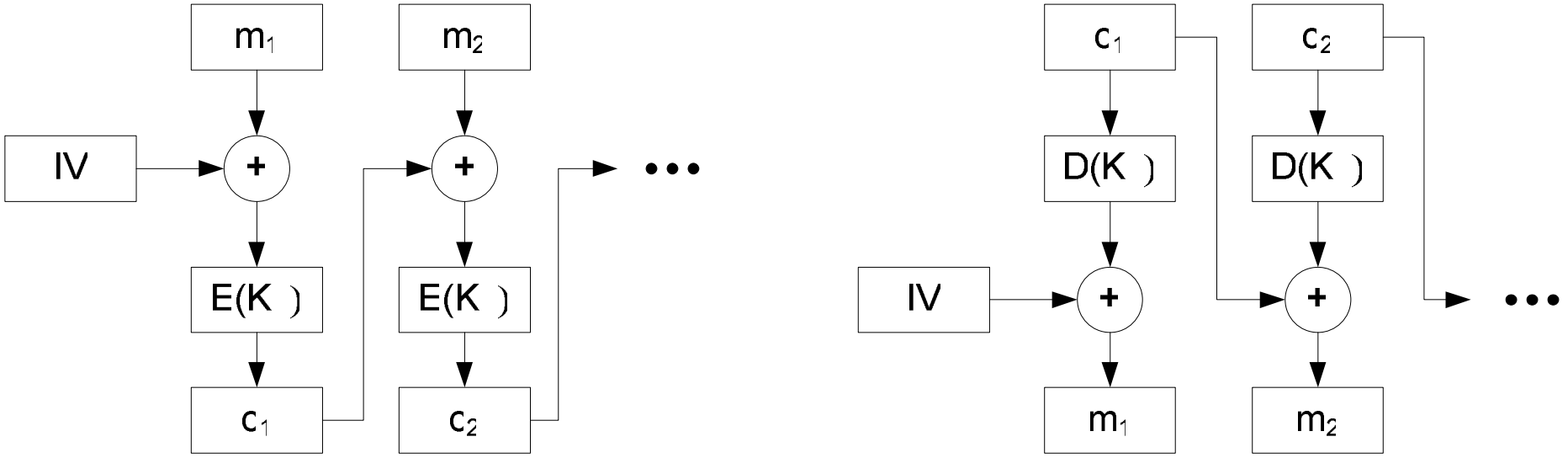
1. Electronic Codebook (ECB)



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

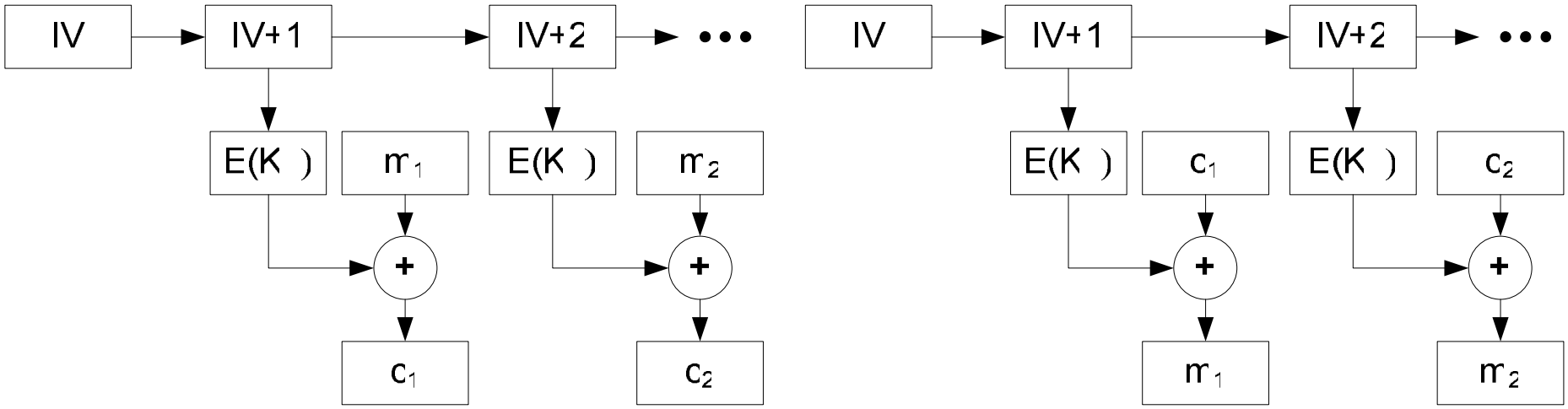
Using BC (PRPs): Cipherblock Chaining

2. Cipherblock Chaining (CBC)
   - Initial value randomly chosen and output as well (IV=c_0)
   - Very often used, but main problem: Sequential



Using BC (PRPs): Countermode

3. Countermode (CTR)
   - Randomized (deterministic) countermode: use random IV (IV=0) for every new message
   - Countermode similar to stream ciphers
   - No need for decryption here
   - Faster and even better security than CBC (later)



Security of these Constructions

- Arguing about security of these modes depends on properties of E
- Argue by assuming E to be PRP (or PRF), i.e., show CBC or countermode “secure” provided that E is a PRP (or PRF).
- Now we have to define security for encryption schemes…

On 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

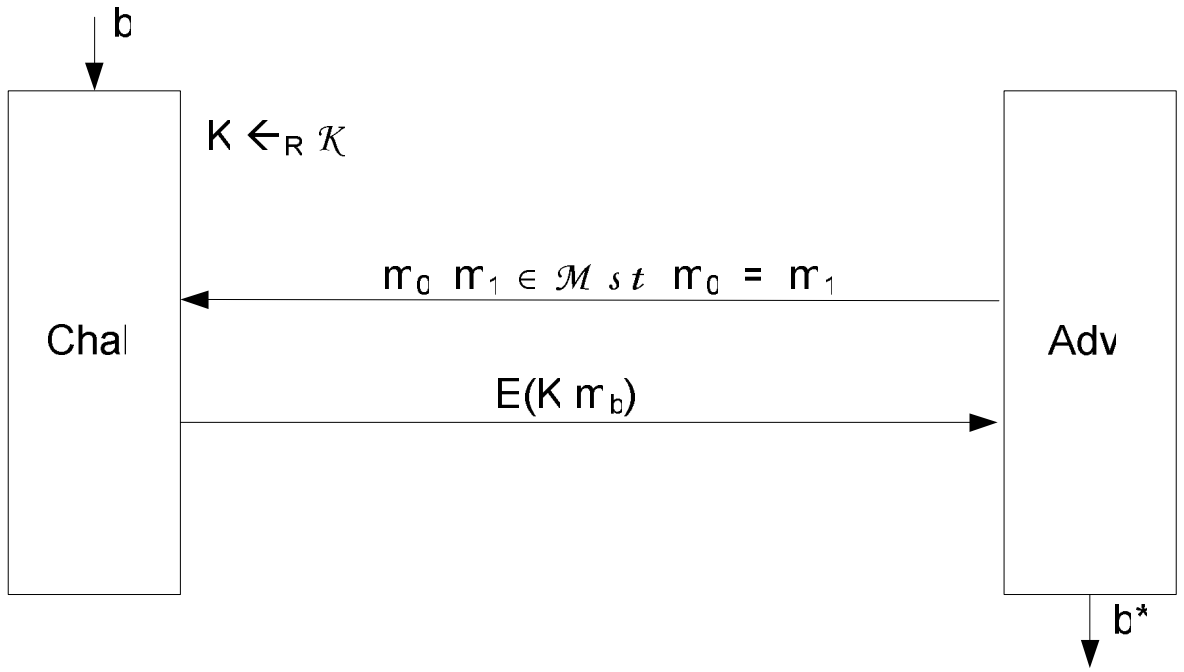
Power / Goal	One-time key (CT-only attack)	Many-time key (CPA)	CCA
Semantic Security	Stream ciphers (det) ctr mode	(rand) CBC (rand) ctr mode	Later

Semantic Security (CT-only Attack)

- Definition (Game for Semantic Security under CT-only attack)
  - Challenger generates $K \leftarrow_R \mathcal{K}$
  - Adversary submits two message m_0, m_1 of the same length to the challenger
  - Challenger picks bit b at random and encrypts $c = E(K, m_b)$ and gives c to the adversary.
  - The adversary outputs b* and wins if b* = b.

Semantic Security (CT-only attack)

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



Semantic Security (CT-only Attack)

- Let EXP(b)=1 denote the event that the adversary outputs 1 if challenger picked b
- The advantage of adversary A attacking E is

$$Adv^{CT\text{-}only}[A,E] = |Pr[EXP(0)=1] - Pr[EXP(1)=1]|.$$

- Definition (Semantic Security). A cipher (E,D) is semantically secure under CT-only attack if for all efficient adversaries A, we have that $Adv^{CT\text{-}only}[A,E]$ is negligible.

Bit Secrecy for 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!

  [proof on the board]

Bit Secrecy for Semantic Security

- Construct adv. B that uses A and breaks Semantic Security
  1. Challenger generates $K \leftarrow_R \mathcal{K}$
  2. B submits two message m_0, m_1 that differ in the x-th bit!
  3. Challenger picks bit b at random and encrypts $c = E(K,m_b)$ and gives c to the adversary.
  4. B runs A on c and outputs the bit that A outputs as her guess to b.
- $Adv^{CT\text{-}only}[B,E]$
  $= |Pr[Exp(0)=1] – Pr[Exp(1)=1]|$
  $= | (½ - p) - (½ + p) | = 2p$