Symmetric Encryption

Viet Tung Hoang

The slides are loosely based on those of Prof. Mihir Bellare, UC San Diego.

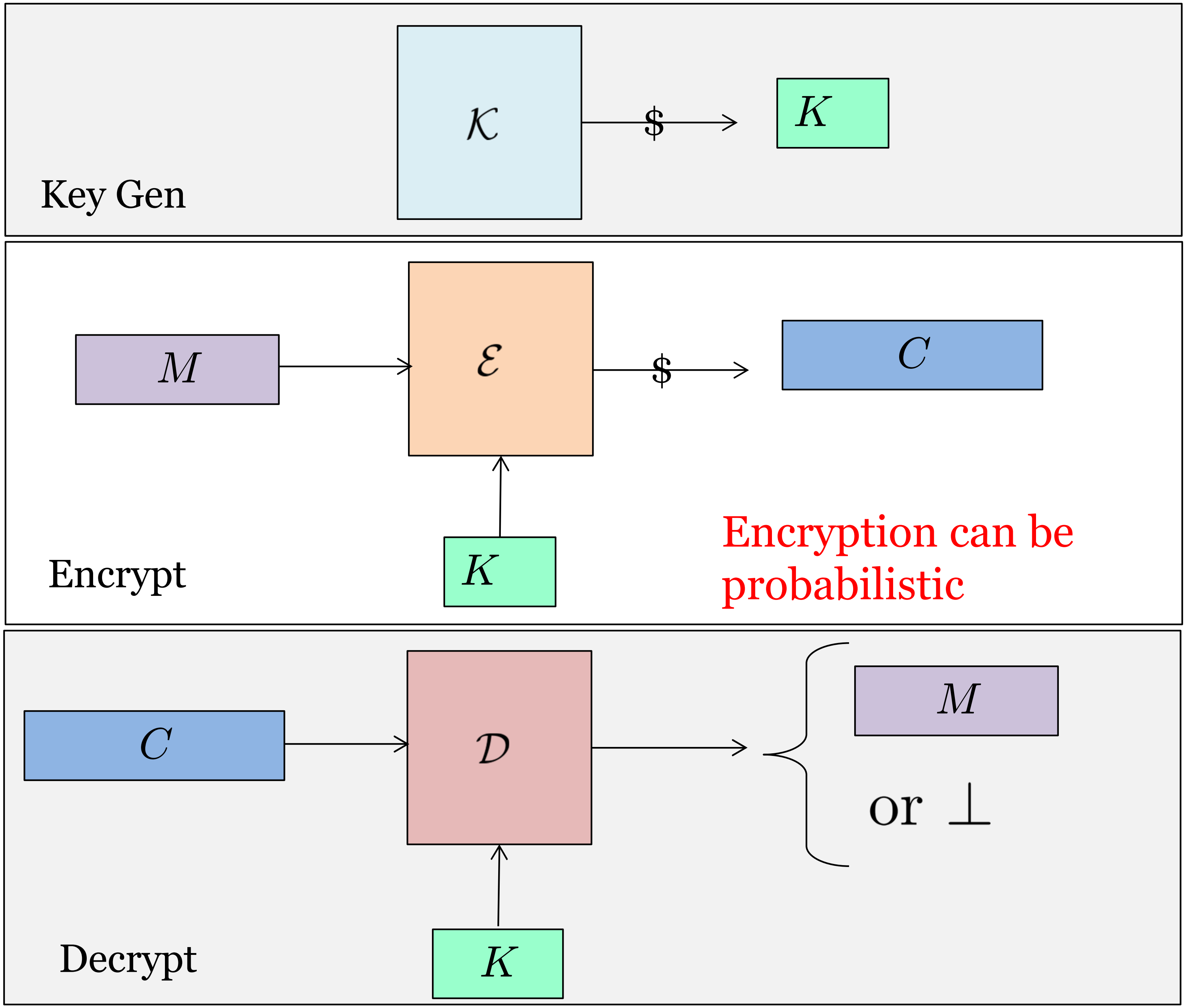
Agenda

1. Modes of Encryption: ECB, CBC, CTR

2. Formalizing Security

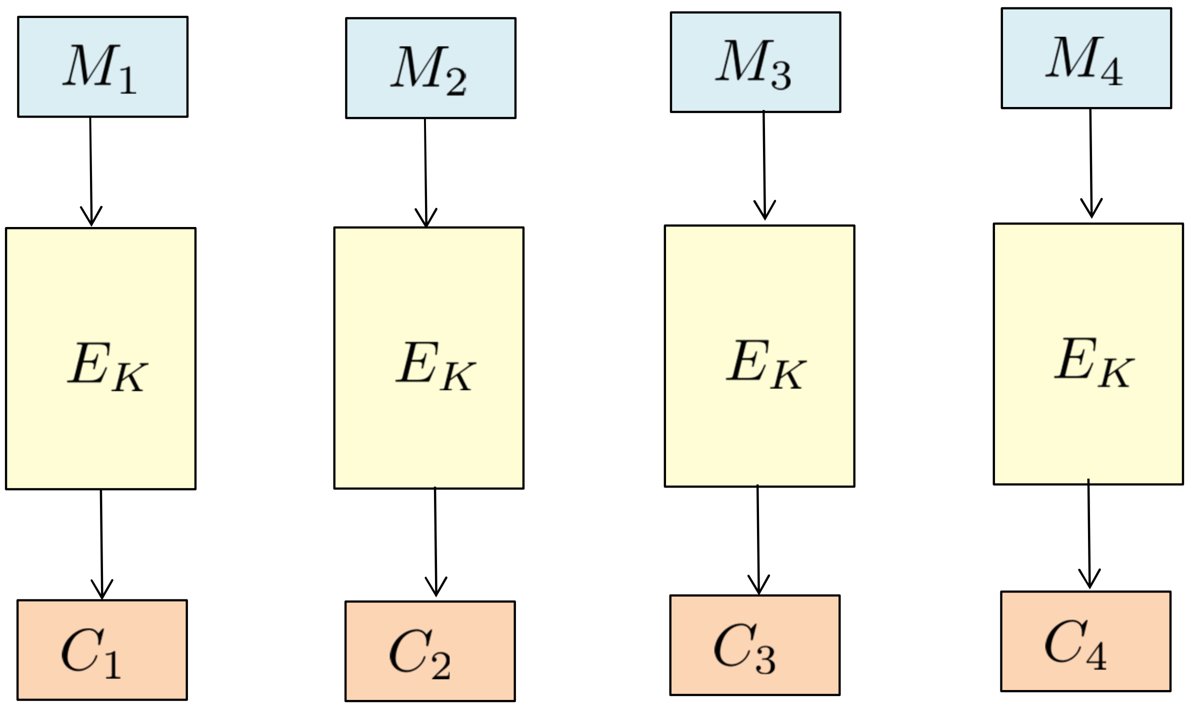
3. Stream Ciphers

Encryption Syntax



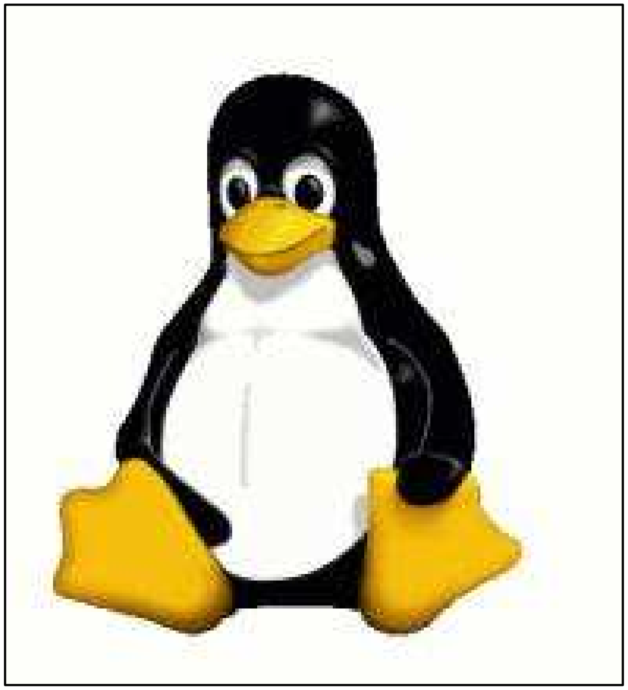
(Bad) Encryption Using Blockcipher: ECB

$$E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$$

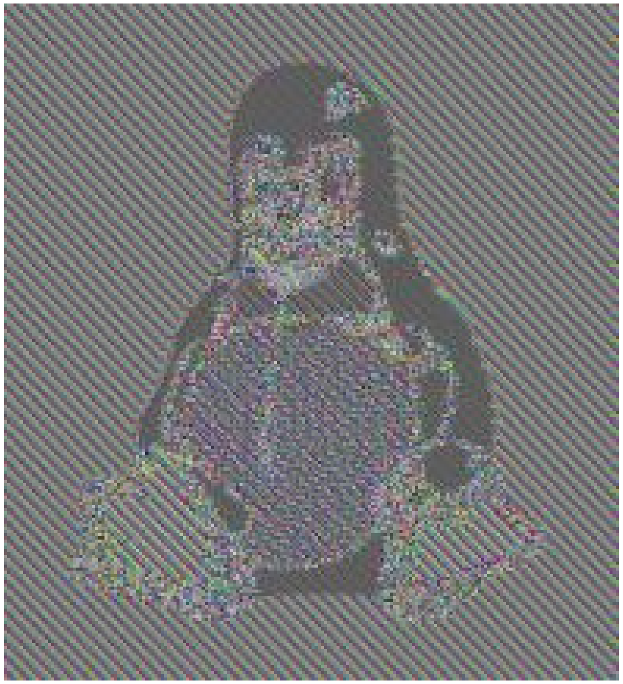


Can encrypt any message whose length is a multiple of n

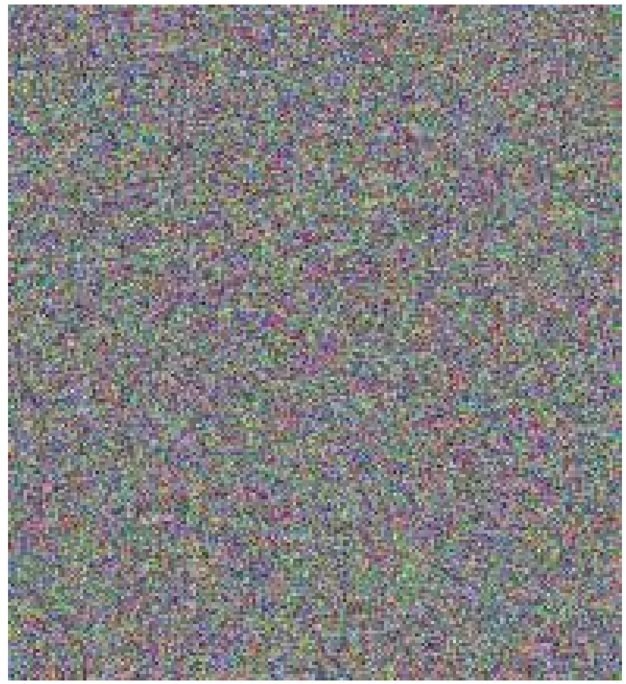
ECB Is Insecure



Message

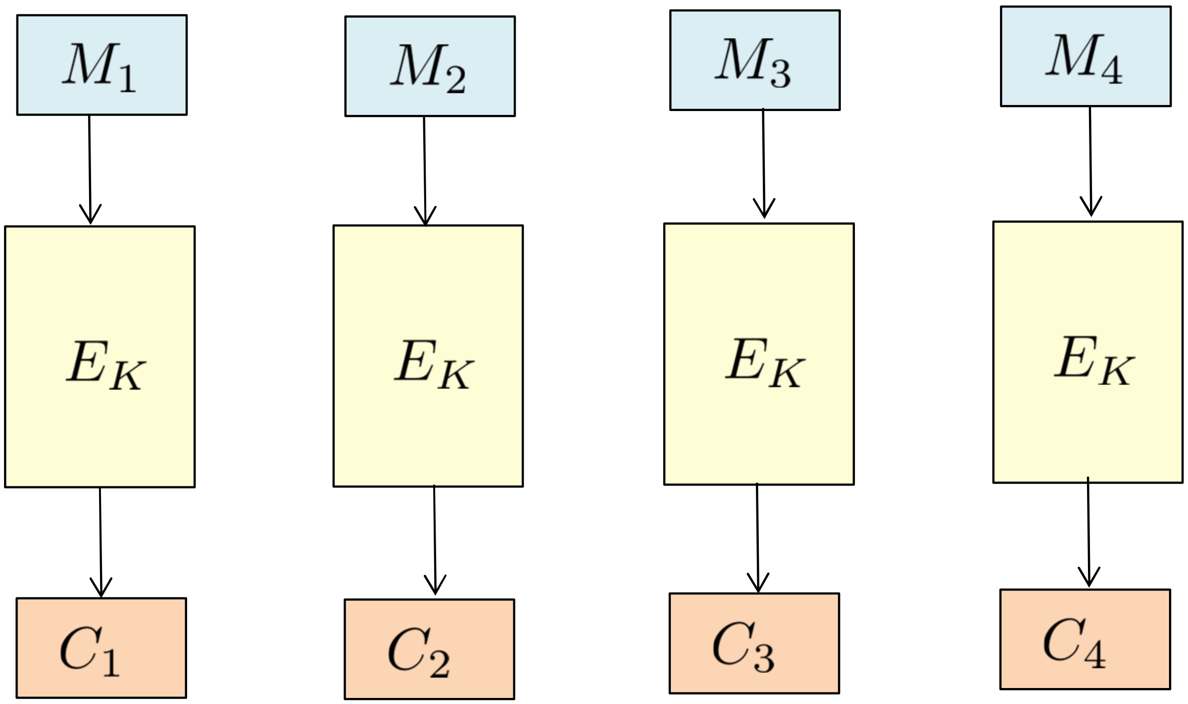


ECB ciphertext



Properly encrypted ciphertext

Why Is ECB So Bad?



If $M_i = M_j$ then $C_i = C_j$

ECB Horror Stories

Half the apps in Android used ECB to encrypt data

An Empirical Study of Cryptographic Misuse in Android Applications

ars TECHNICA

BIZ & IT —

How an epic blunder by Adobe could strengthen hand of password crackers

Adobe used ECB to encrypt passwords

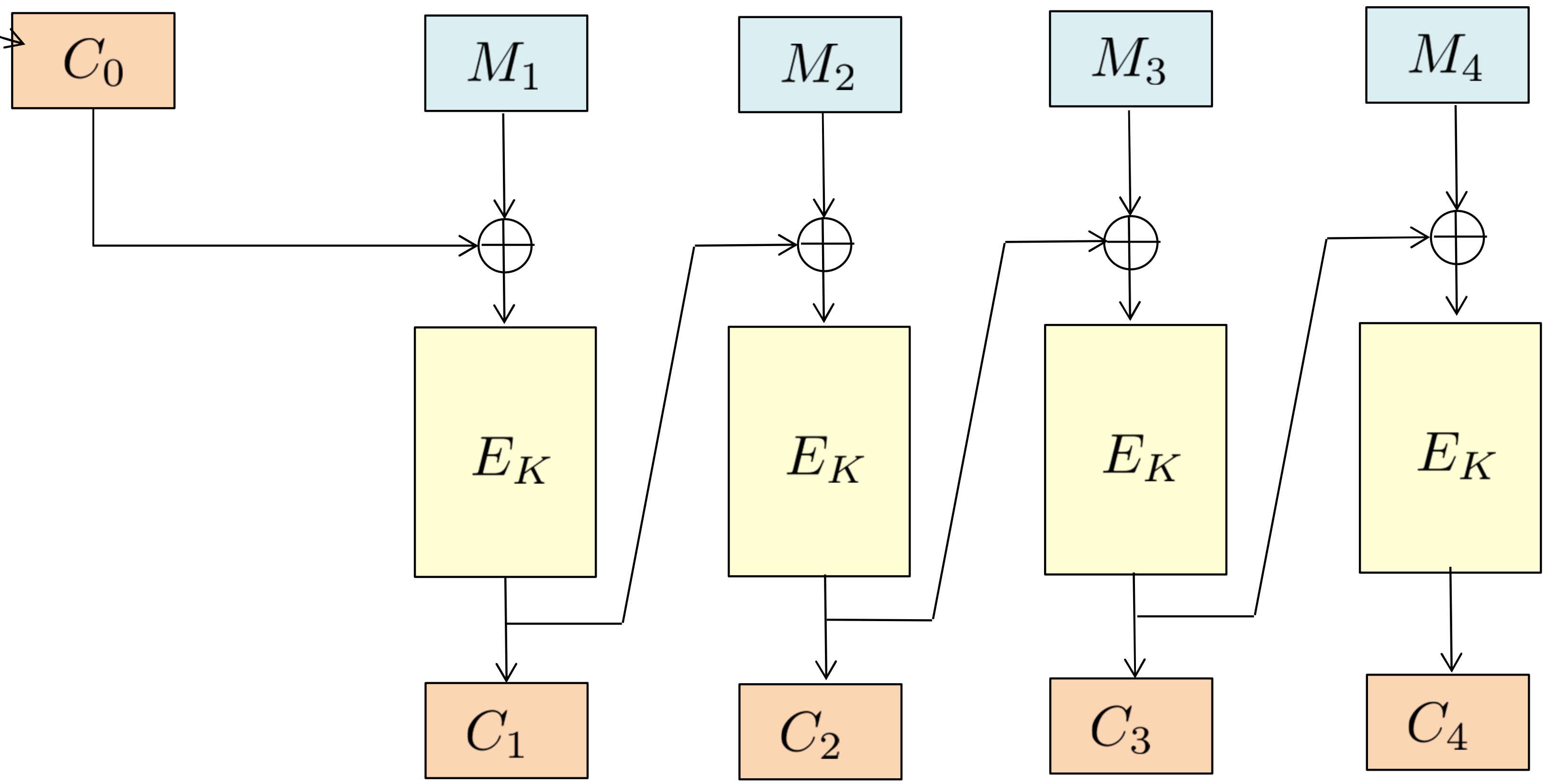
Zoom concedes custom encryption is substandard as Citizen Lab pokes holes in it

Zoom used ECB to encrypt video conferencing

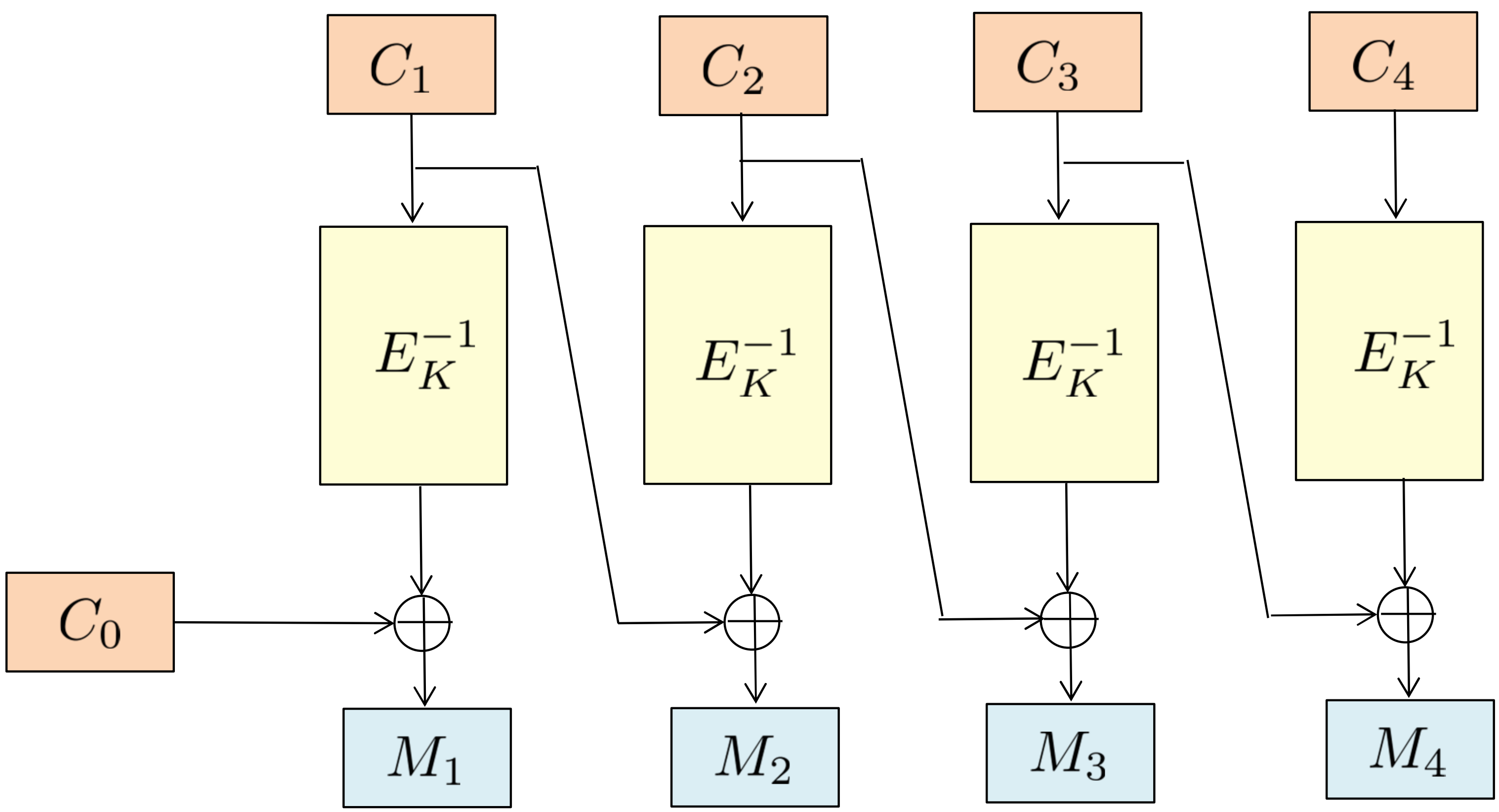
Randomized Encryption: CBC

sequential

randomly chosen



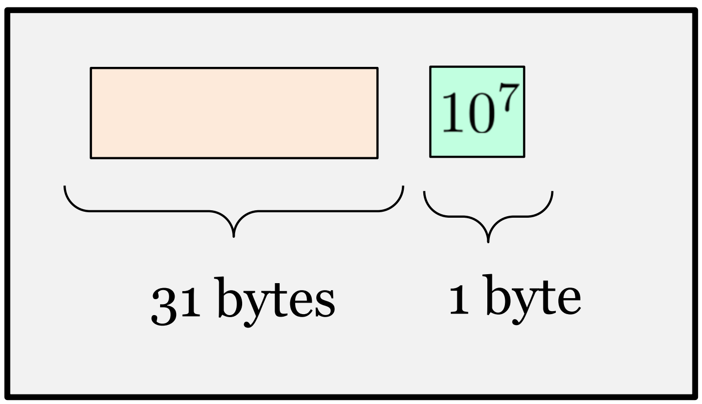
Decryption of CBC

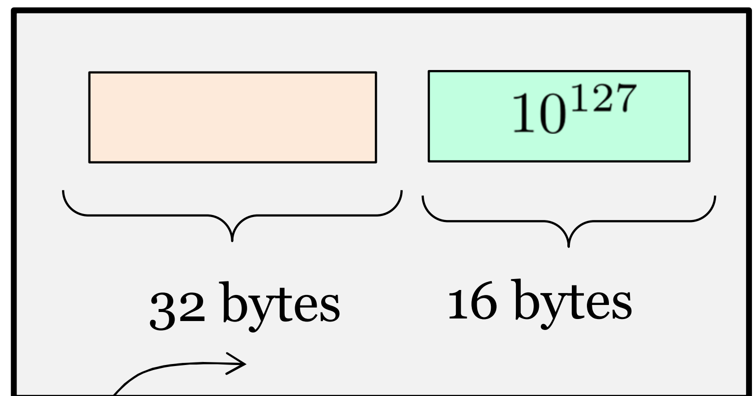


Dealing with Fragmentary Data

Naive solution: Pad with 10^*

Example: Suppose that the block length is 16 bytes.

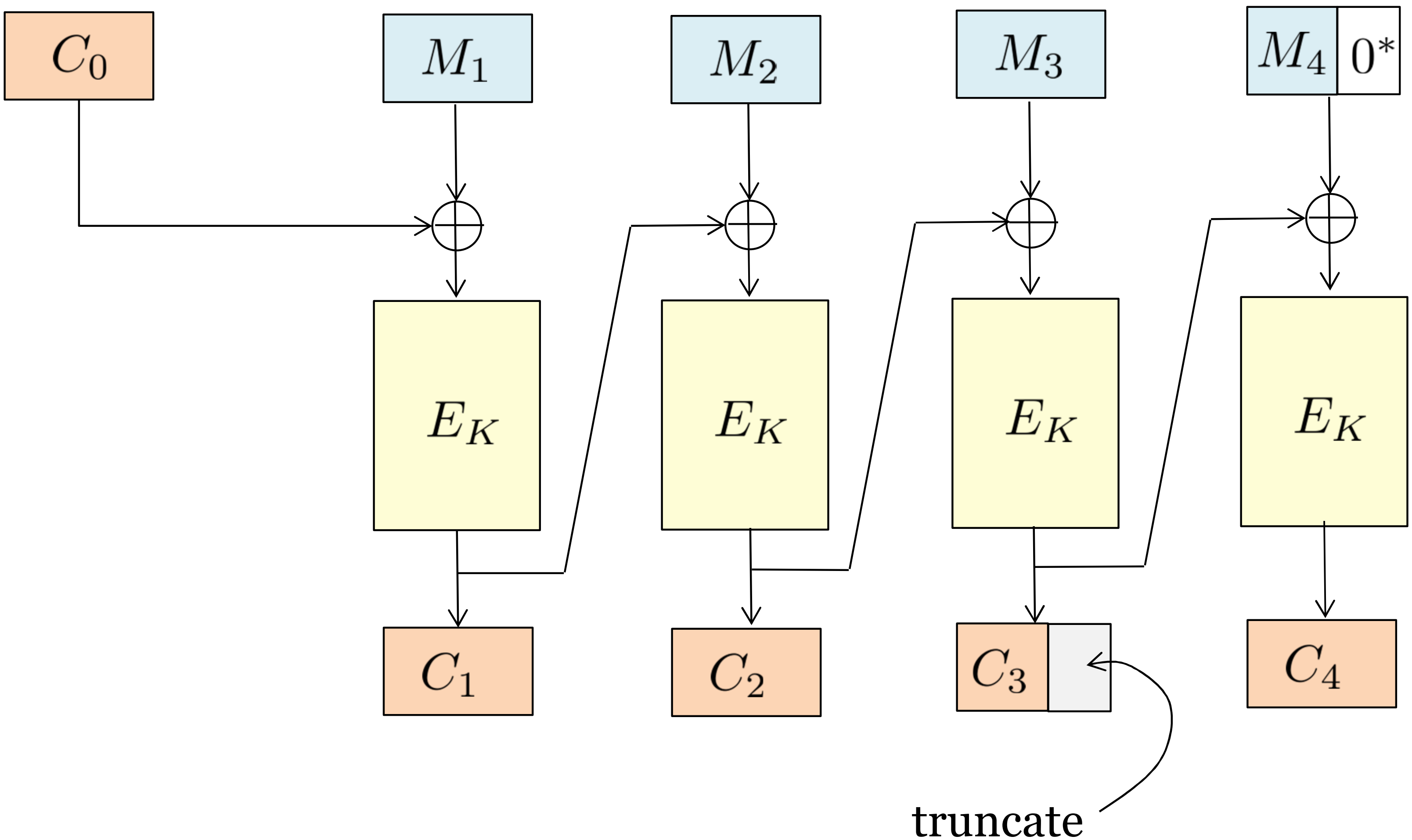




Padding is required, otherwise can't decrypt

Problem: Waste bandwidth, and for full-length msg, waste a blockcipher call

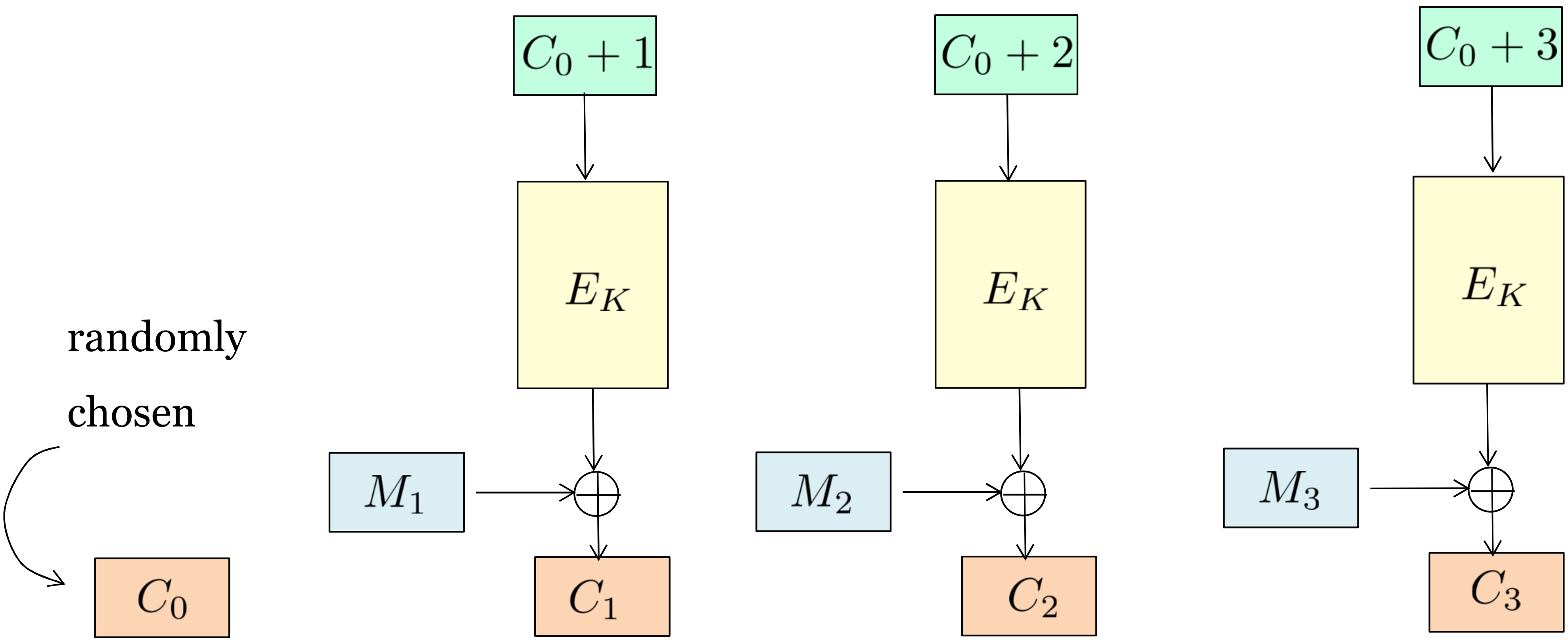
Ciphertext Stealing in CBC



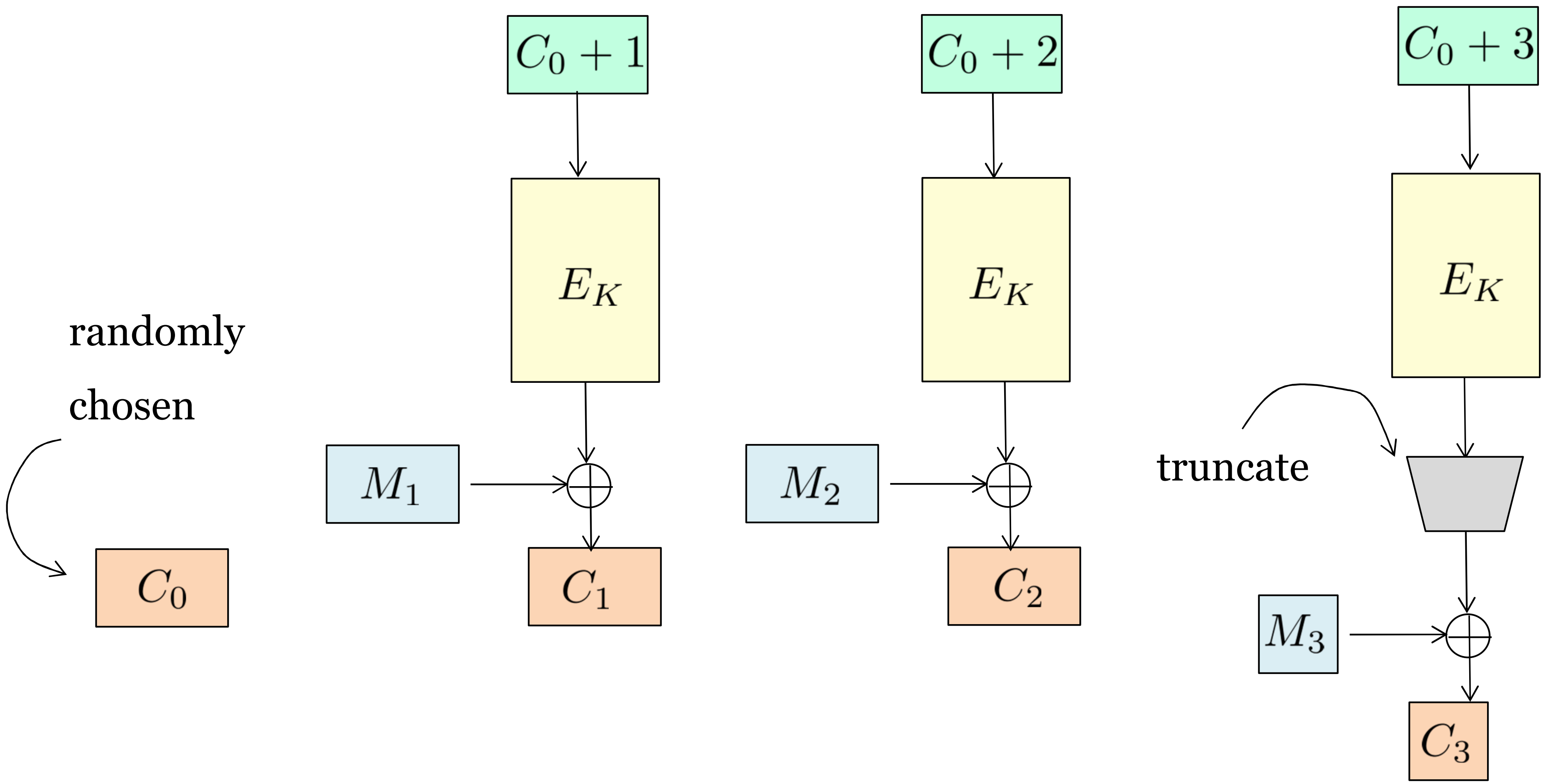
Exercise: How to use ciphertext stealing if msg is shorter than 1 block?

Randomized Encryption: CTR

fully parallelizable



Dealing with Fragmentary Data



Agenda

1. Modes of Encryption: ECB, CBC, CTR

2. **Formalizing Security**

3. Stream Ciphers


1982

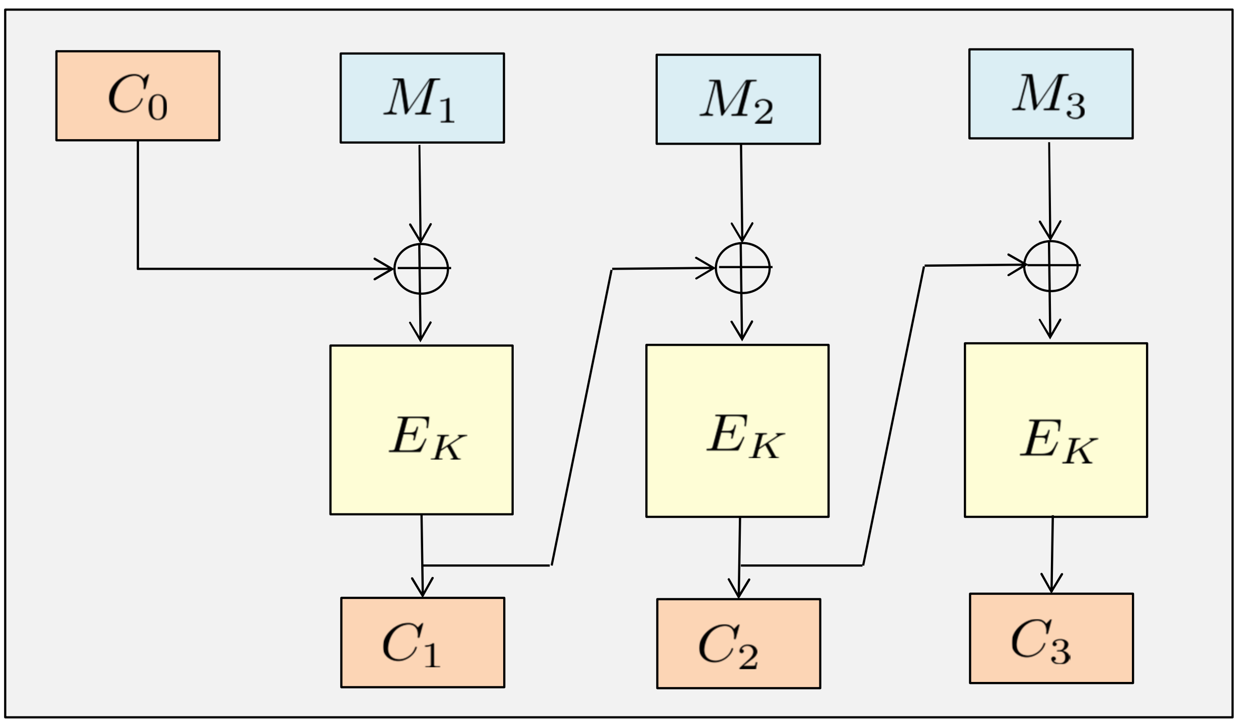
Formalizing Security: Intuition

Should hide

all partial information

about the plaintexts

Except message length



CBC trivially leaks message length

Formalizing Security: Informal Definition

Adversary can't even distinguish the encryption of its **own chosen messages**

"A good disguise should not allow a mother to distinguish her own children"

Goldwasser and Micali

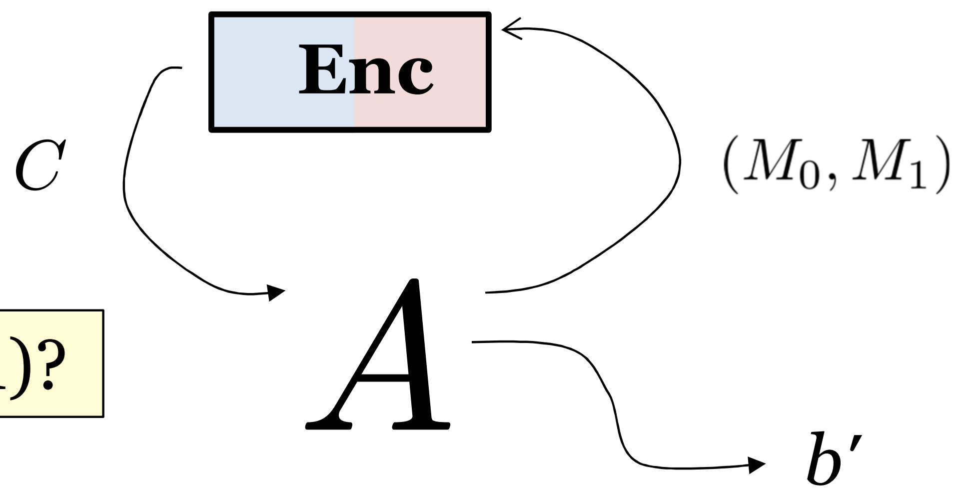
Formalizing Security: Left-or-Right

Left$_{\mathcal{E}}$

procedure Enc(M_0, M_1)
Return $\mathcal{E}_K(M_0)$

Right$_{\mathcal{E}}$

procedure Enc(M_0, M_1)
Return $\mathcal{E}_K(M_1)$



Left (0) or Right (1)?

$$\mathbf{Adv}^{\mathrm{lr}}_{\mathcal{E}}(A) = \Pr[\mathrm{Right}^{A}_{\mathcal{E}} \Rightarrow 1] - \Pr[\mathrm{Left}^{A}_{\mathcal{E}} \Rightarrow 1]$$

In each query, the two messages must have the same length

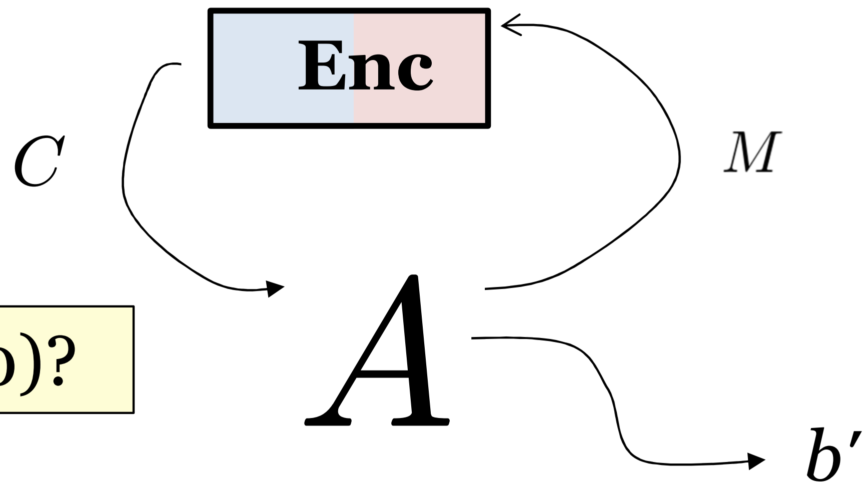
Formalizing Security: Real-or-Random

Real$_{\mathcal{E}}$

procedure Enc(M)
Return $\mathcal{E}_K(M)$

Rand$_{\mathcal{E}}$

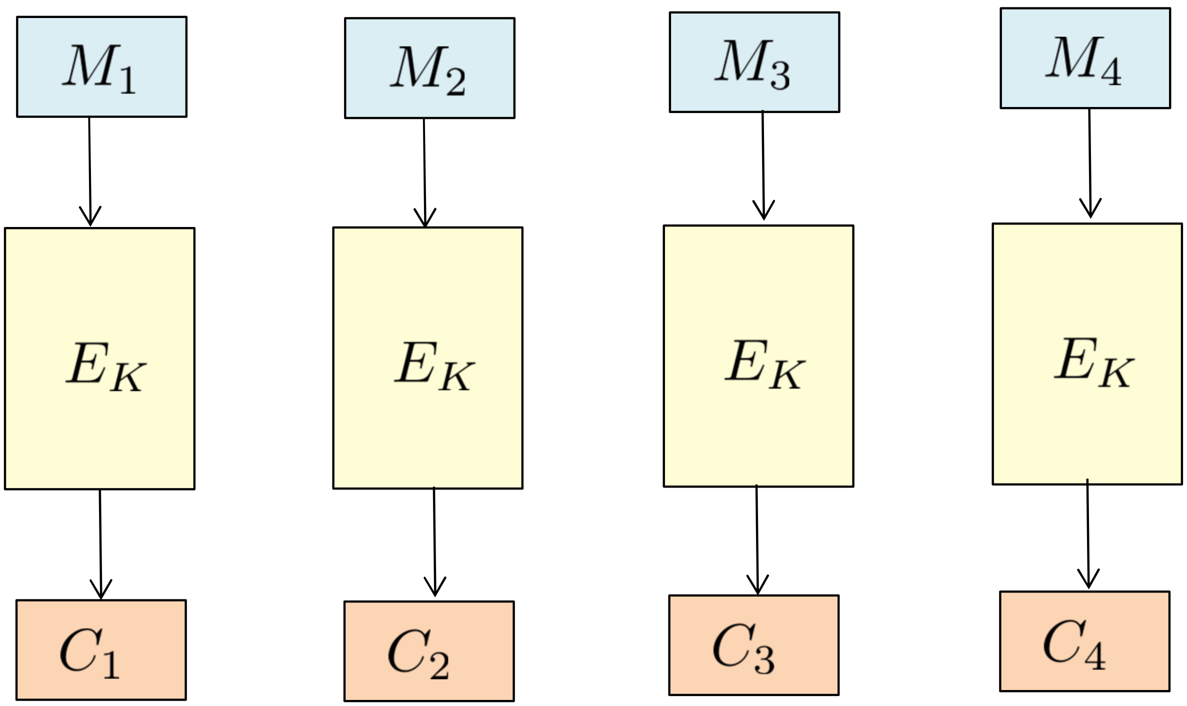
procedure Enc(M)
$C \xleftarrow{\$} \mathcal{E}_K(M')$; $C' \xleftarrow{\$} \{0,1\}^{|C|}$; Return C'



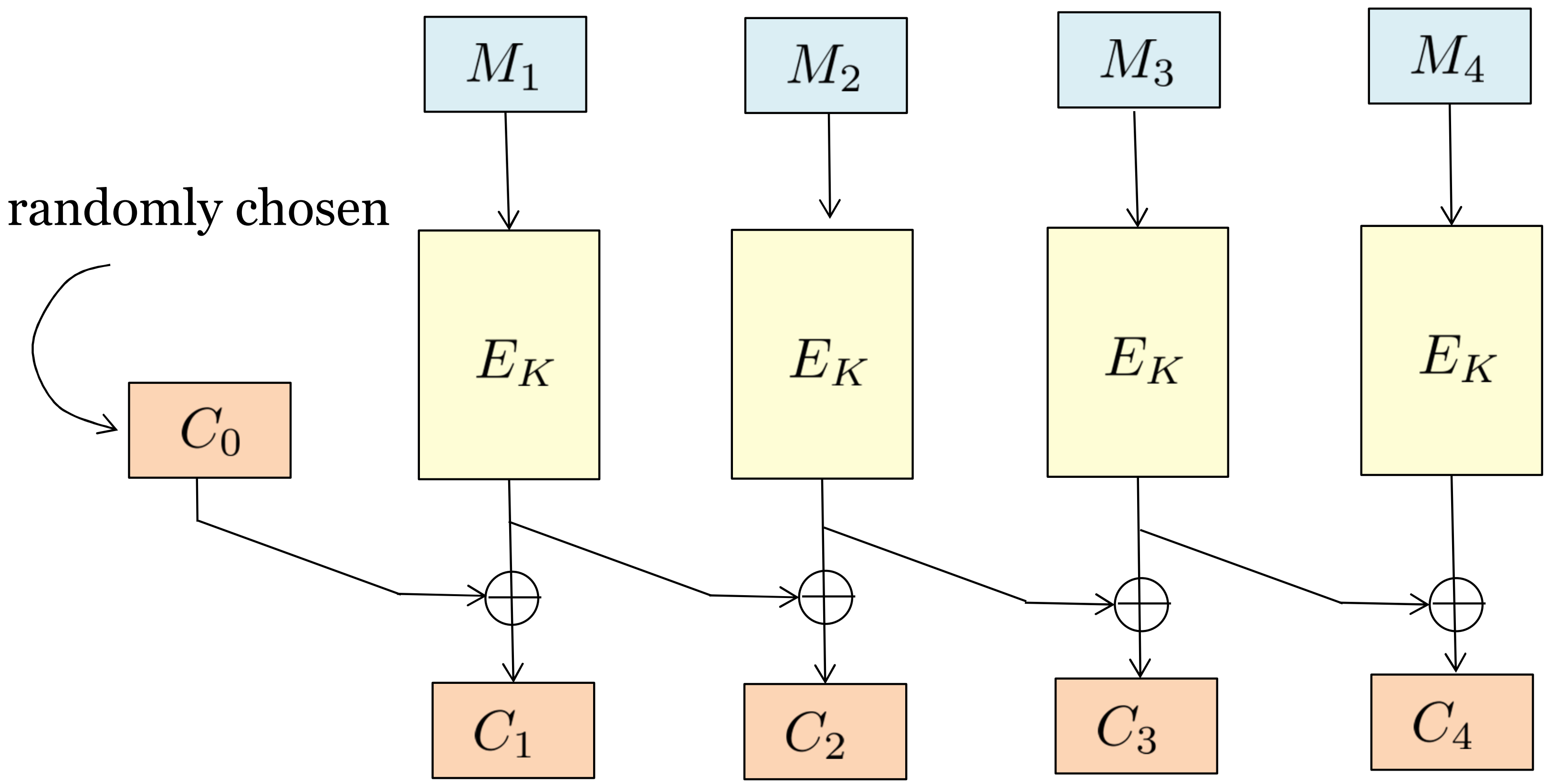
Real (1) or Rand (0)?

$$\mathbf{Adv}^{\mathrm{rr}}_{\mathcal{E}}(A) = \Pr[\mathrm{Real}^{A}_{\mathcal{E}} \Rightarrow 1] - \Pr[\mathrm{Rand}^{A}_{\mathcal{E}} \Rightarrow 1]$$

Exercise: Break LR Security of ECB



Exercise: Breaking RR Security



Question: Break the real-or-random security of this scheme using a single query of a 2-block message.

Agenda

1. Modes of Encryption: ECB, CBC, CTR

2. Formalizing Security

3. **Stream Ciphers**

Real-world Broken Stream Ciphers

RC4

Encryption scheme for Web traffic and Wifi traffic

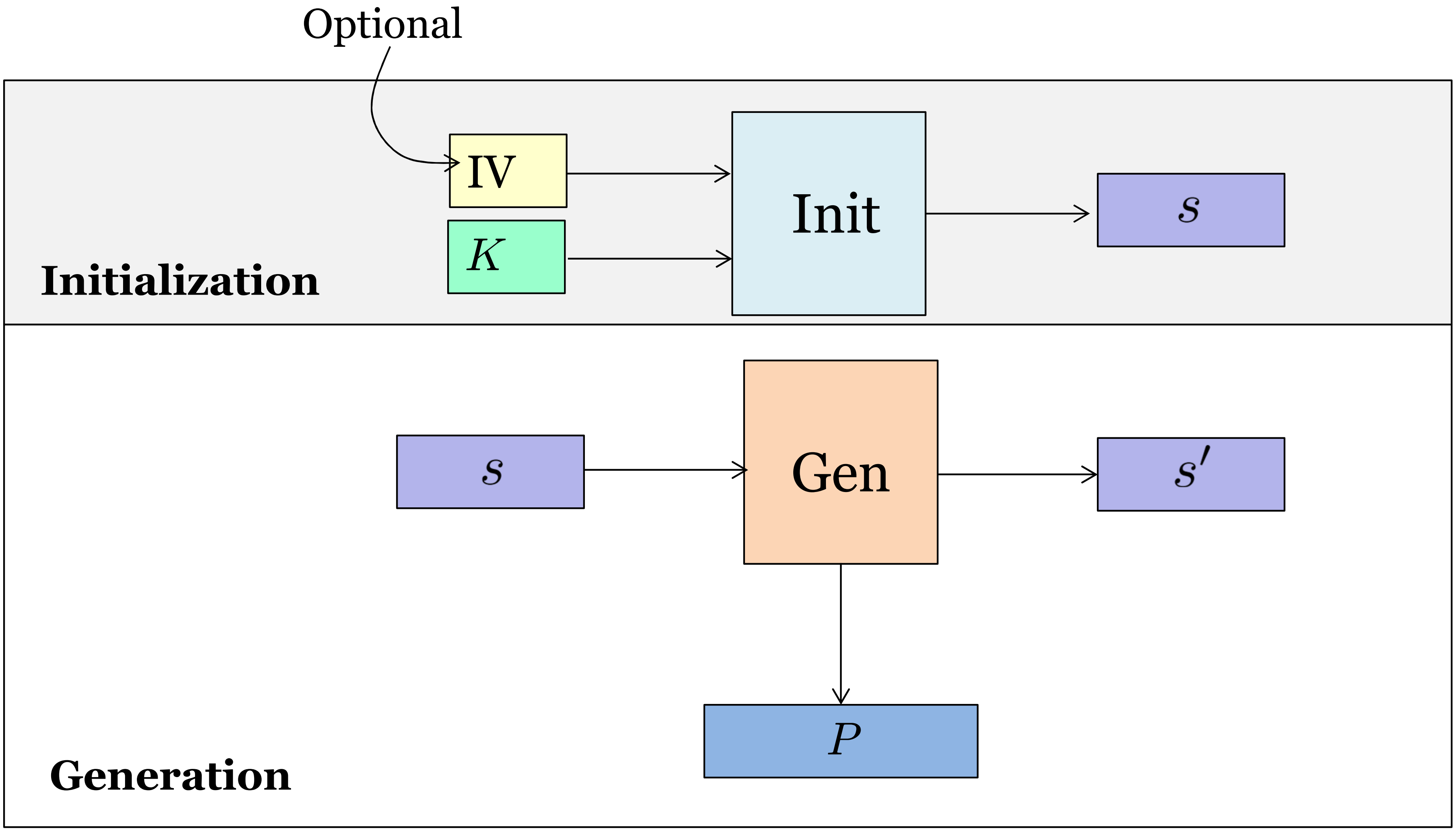
A5/1 Stream cipher

Cellular encryption
in GSM networks

E0 Stream cipher

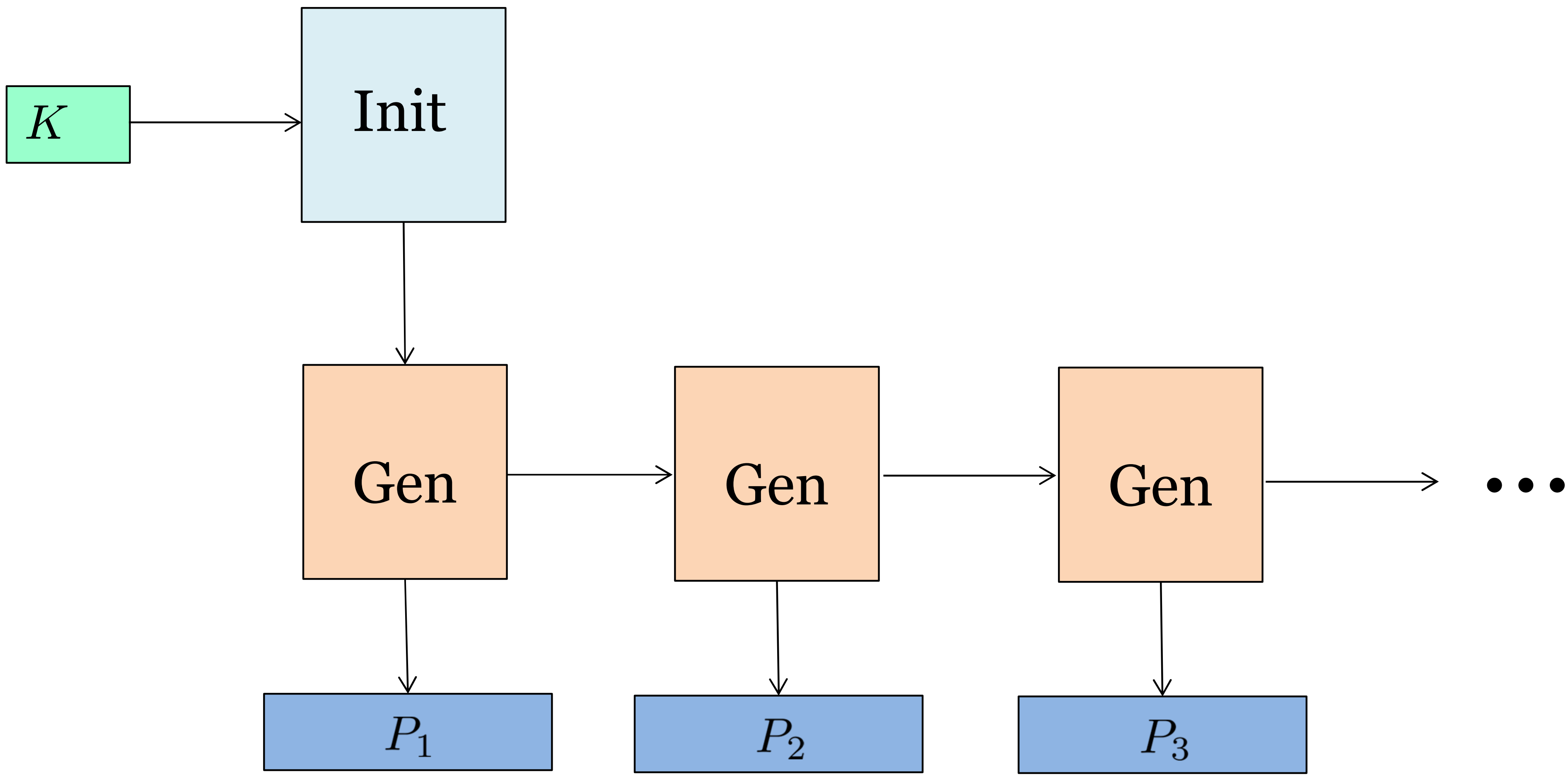
Bluetooth
encryption

Syntax



Use of Stream Cipher

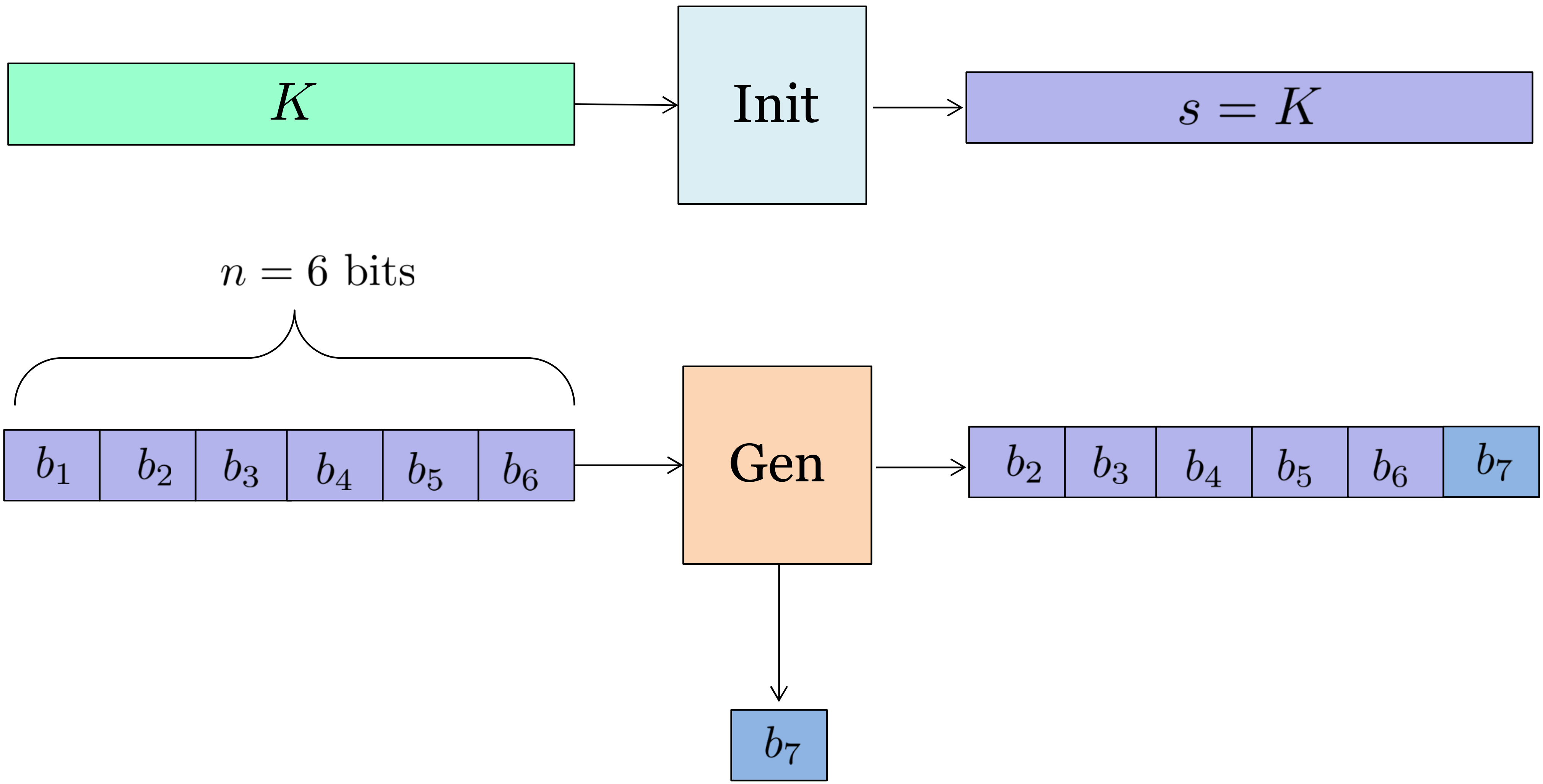
Producing A Stream of One-Time Pad



Question: Formalize a security notion for stream cipher

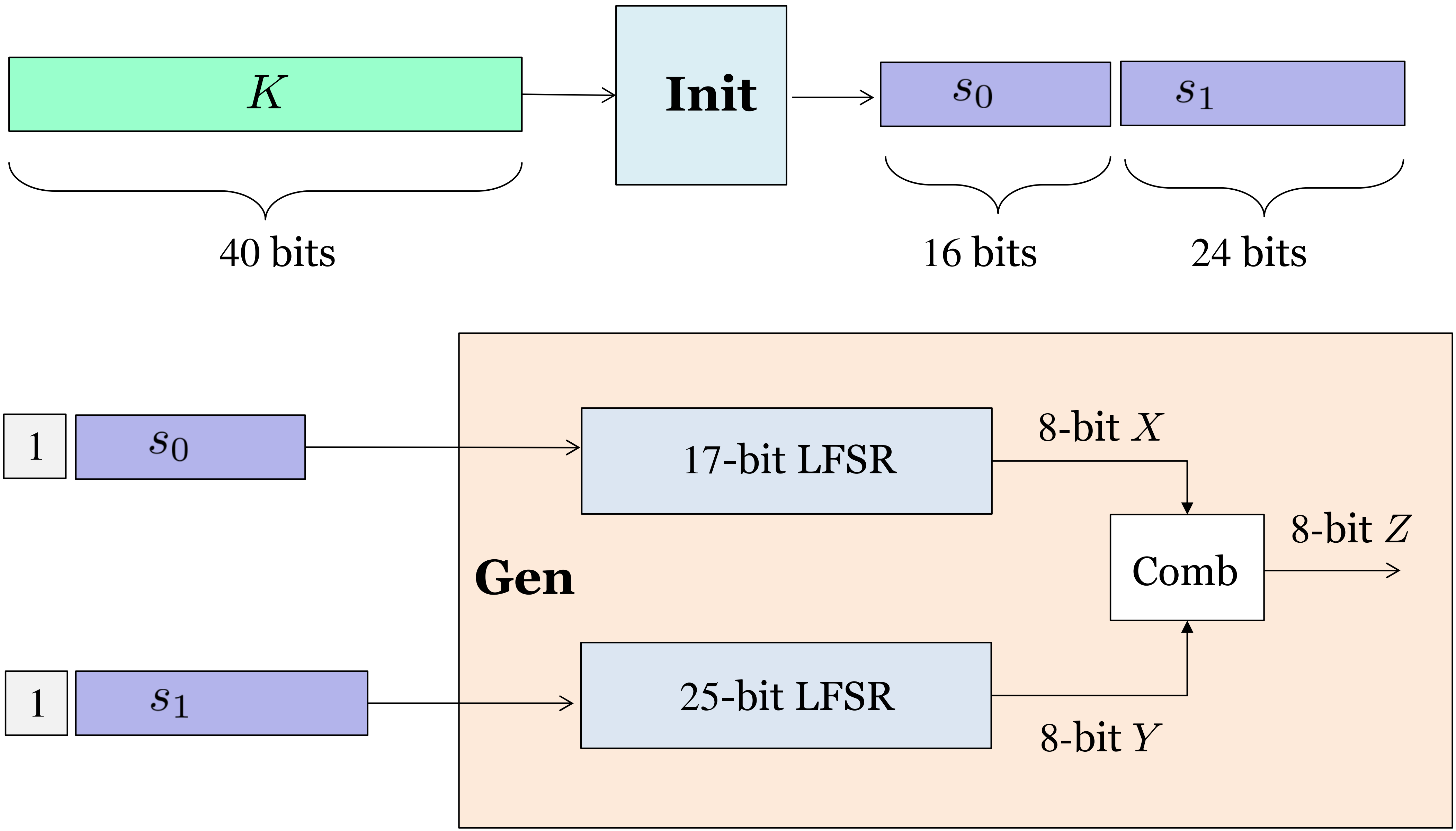
A Wrong Construction

Linear Feedback Shift Register (LFSR)

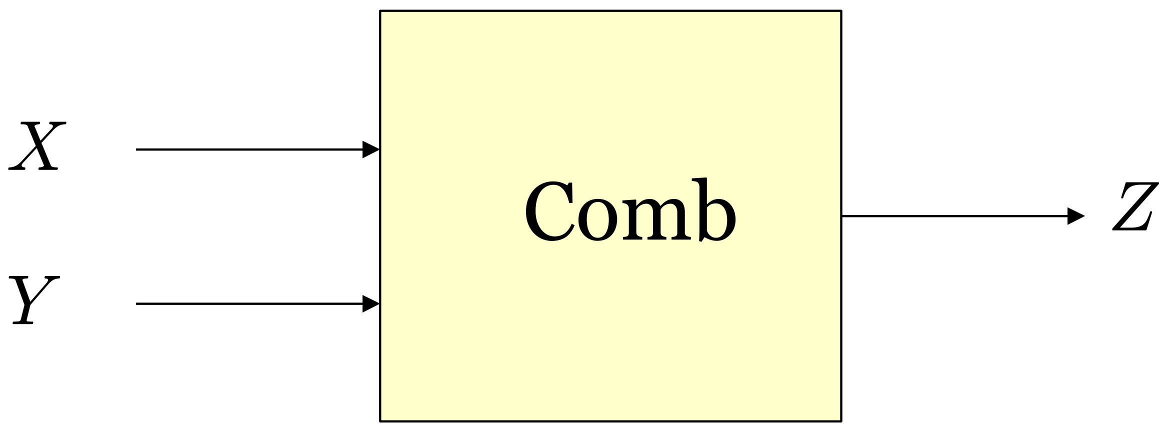


Question: Given n bits of output, recover subsequent bits

Case Study: DVD Encryption System

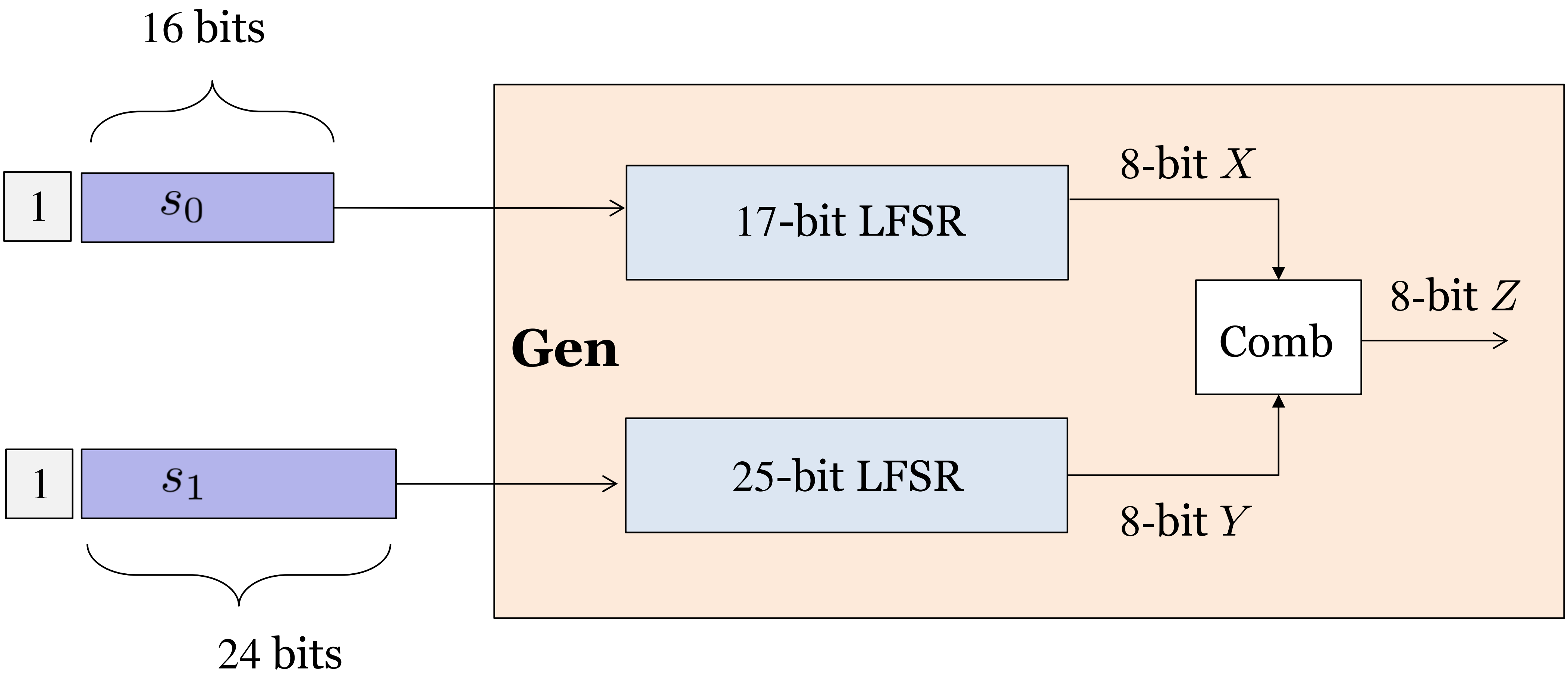


Property of Combiner To Exploit



Invertibility: Given Z and X, it's trivial to compute Y

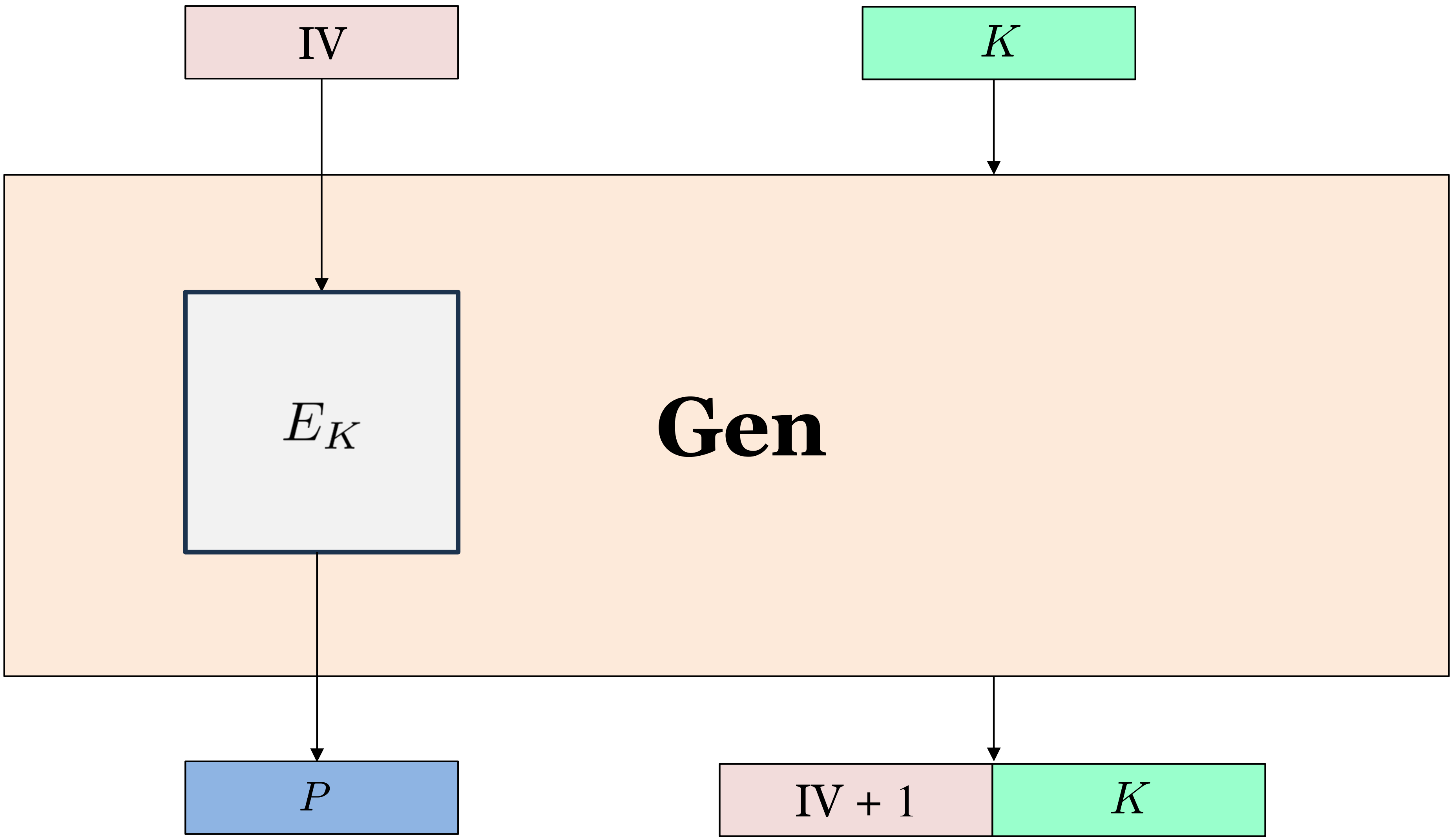
Breaking DVD Encryption System



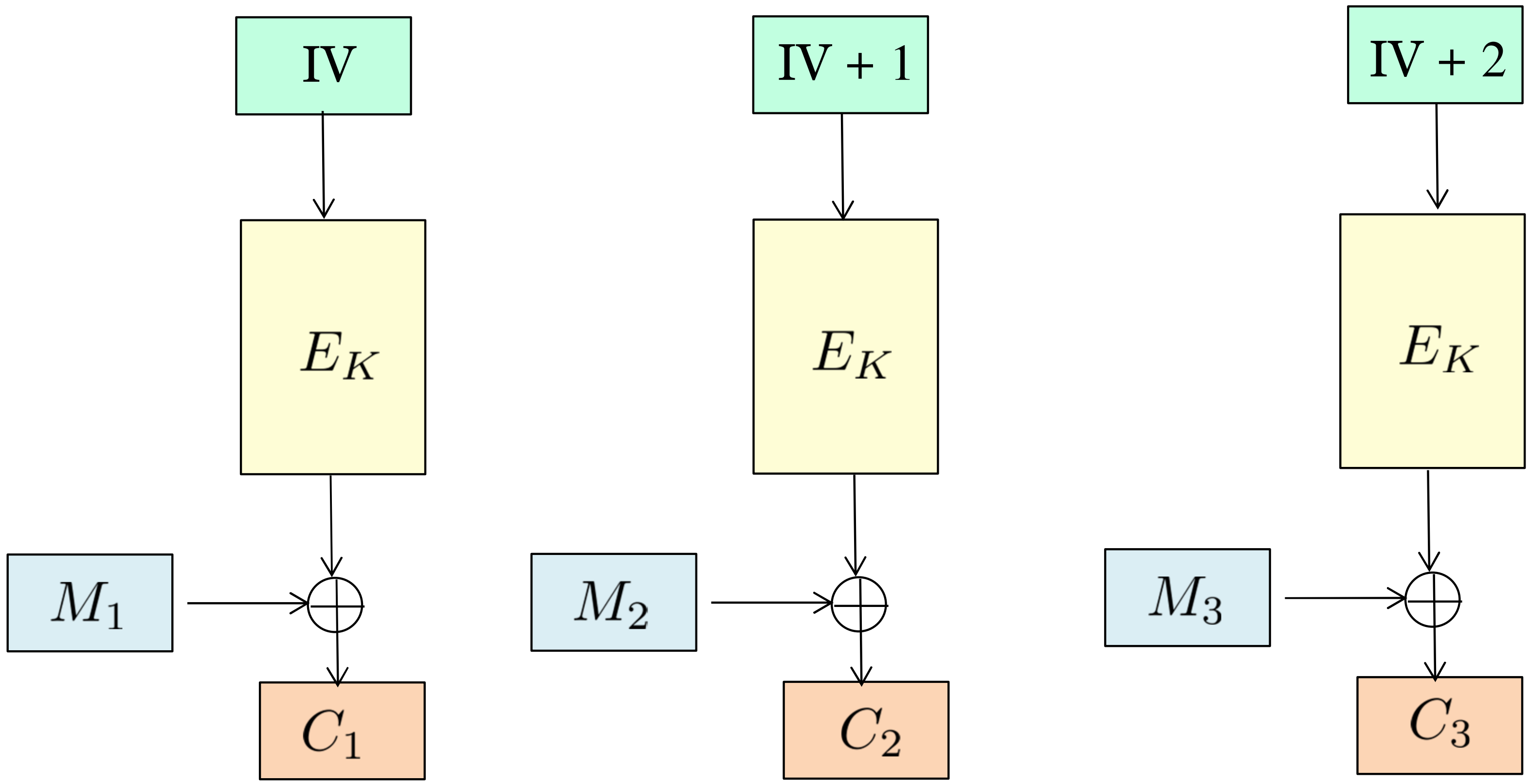
Question: Given the first 128 bits of output, recover subsequent bits using $O(2^{16})$ time by guessing the initial s_0

Building Stream Cipher From Blockcipher

Init sets IV = 0 and outputs (IV, K) as the initial state



How Encryption Looks Like: Stateful CTR



Ciphertext doesn't include IV

Sender and receiver update $\mathrm{IV} \leftarrow \mathrm{IV} + 3$ for the next encryption