

CSCI 1515 Applied Cryptography

This Lecture:

- Block Cipher Modes of Operation
- Public Key Infrastructure (PKI)

Block Cipher Modes of Operation

Given: $F: \{0,1\}^\lambda \times \{0,1\}^\lambda \rightarrow \{0,1\}^\lambda$ ¹²⁸

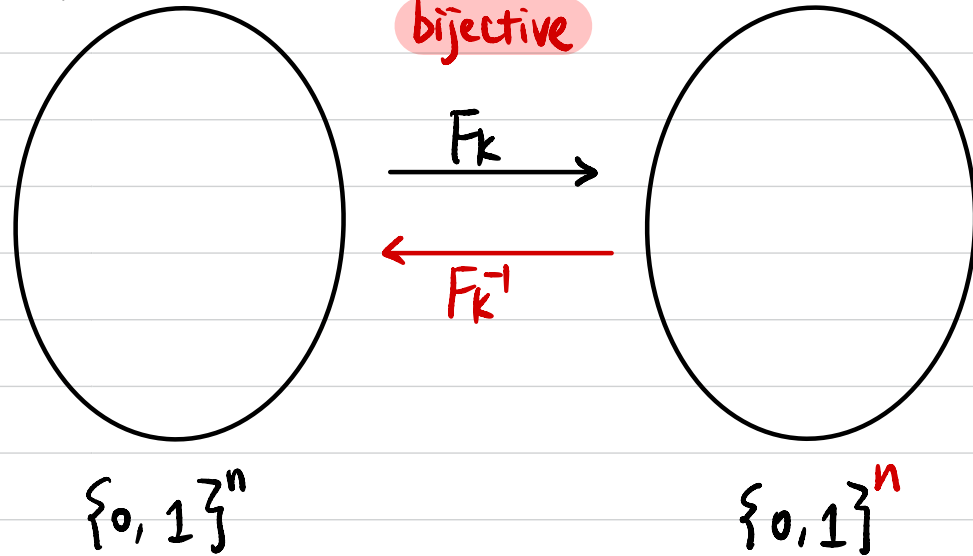
Assumed to be a pseudorandom permutation (PRP).

Goal: Construct a symmetric-key encryption (SKE) scheme for arbitrary-length messages with chosen-plaintext Attack (CPA) security.

- $k \xleftarrow{\$} \{0,1\}^\lambda$
- $\text{Enc}_k(m) \quad |m| = \alpha \cdot \lambda \quad (\text{If not, pad it to a multiple of } \lambda)$
- $\text{Dec}_k(c)$

Pseudorandom Permutation (PRP)

$$k \leftarrow \{0, 1\}^{\lambda} \quad F_k:$$



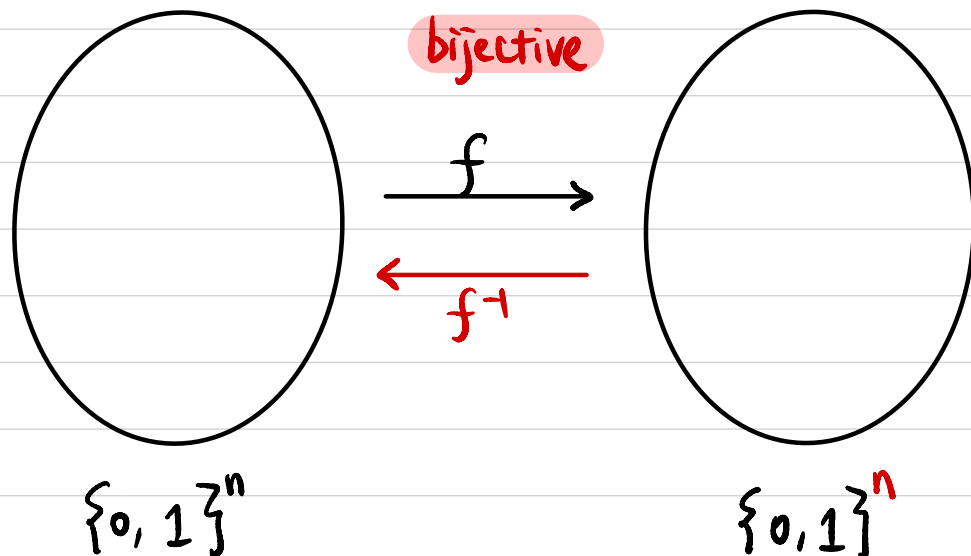
How many possible F_k 's ?
 2^{λ}

$$f \leftarrow \{ F \mid F: \{0, 1\}^n \rightarrow \{0, 1\}^n, \\ F \text{ is bijective} \}$$

$2^n!$

$f:$

$\sum \sum^c$ (not knowing k)



How many possible f 's ?

Chosen-Plaintext Attack (CPA) Security

$k \leftarrow \text{Gen}(1^\lambda)$

Alice



Bob



$$c_0 \leftarrow \text{Enc}_k(m_0)$$

$$c_1 \leftarrow \text{Enc}_k(m_1)$$

$$c_2 \leftarrow \text{Enc}_k(m_2)$$

$\vdots$

$$m_0, m_1 \in \{0, 1\}^n$$

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

$$c \leftarrow \text{Enc}_k(m_b)$$

③ choose



(PPT)

⑤ Output b'

$c_0, c_1, c_2, \dots$



$$m_0 := \text{Dec}_k(c_0)$$

$$m_1 := \text{Dec}_k(c_1)$$

$$m_2 := \text{Dec}_k(c_2)$$

$\vdots$

c

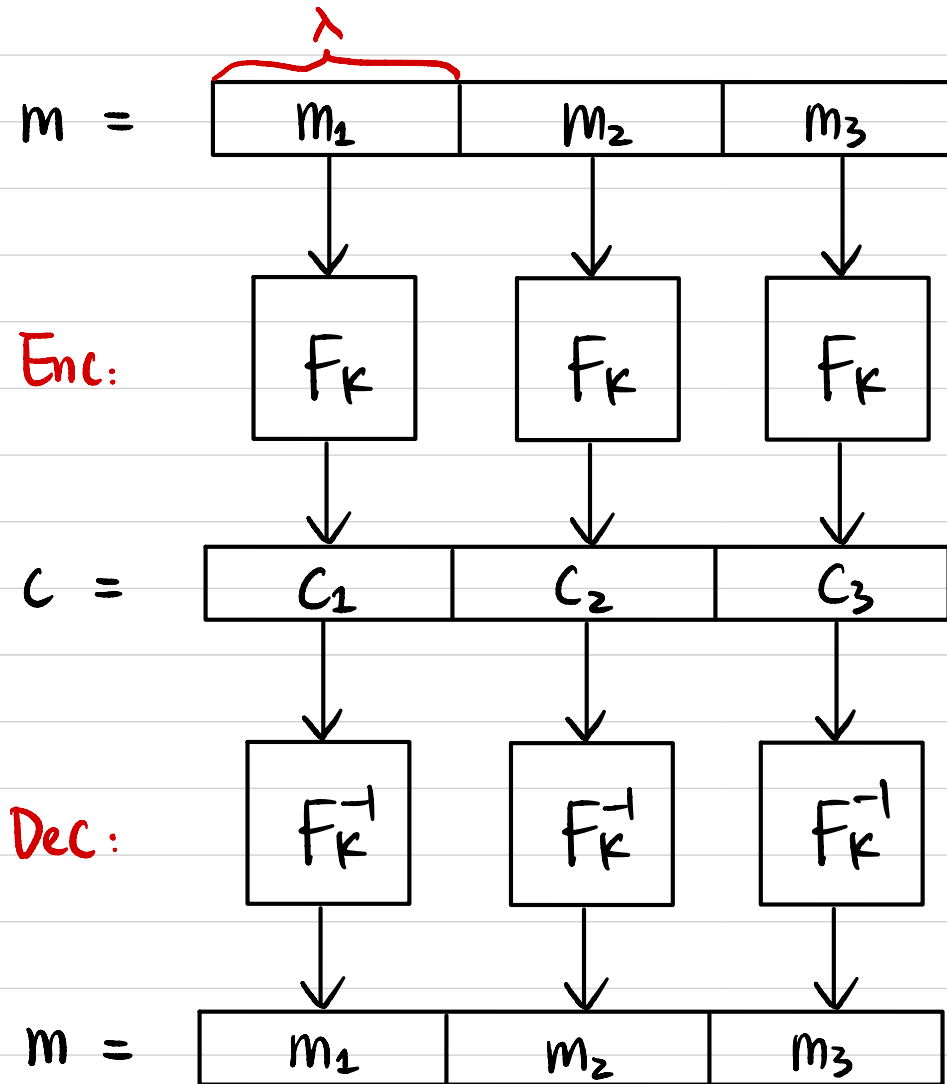


④ see

$$\Pr[b = b'] \leq \frac{1}{2} + \text{negligible}$$

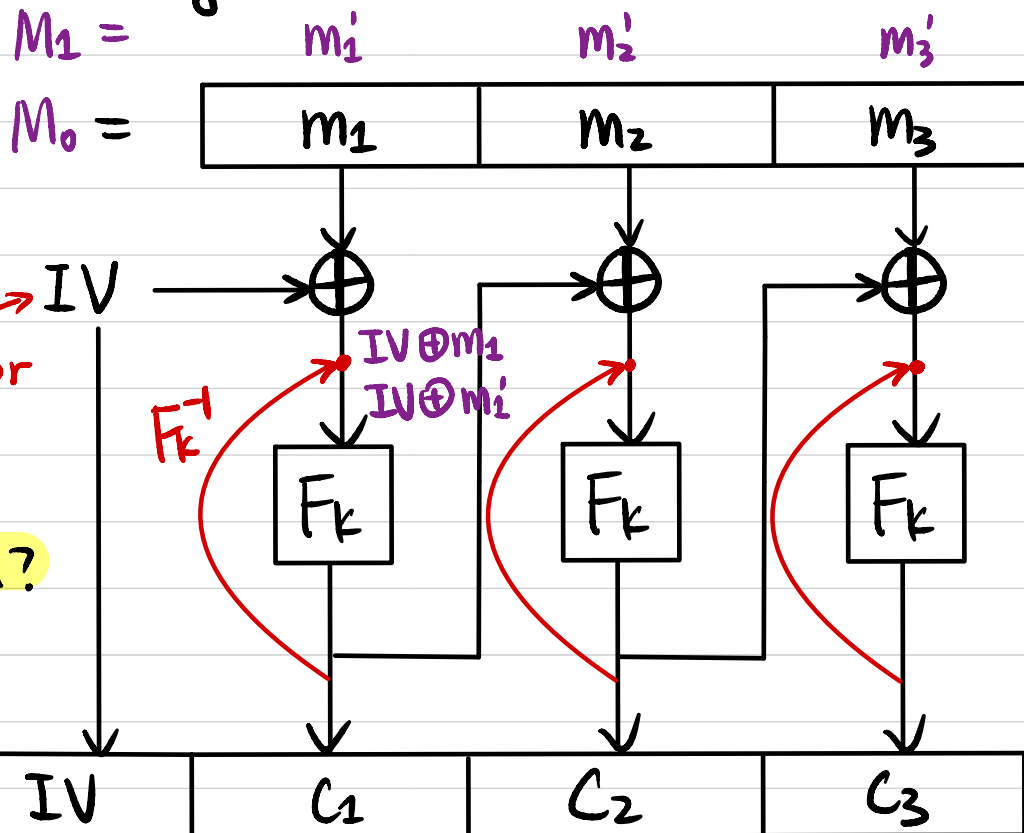
2^{-128}

Electronic Code Book (ECB) Mode



CPA Secure? **NO!**

Cipher Block Chaining (CBC) Mode

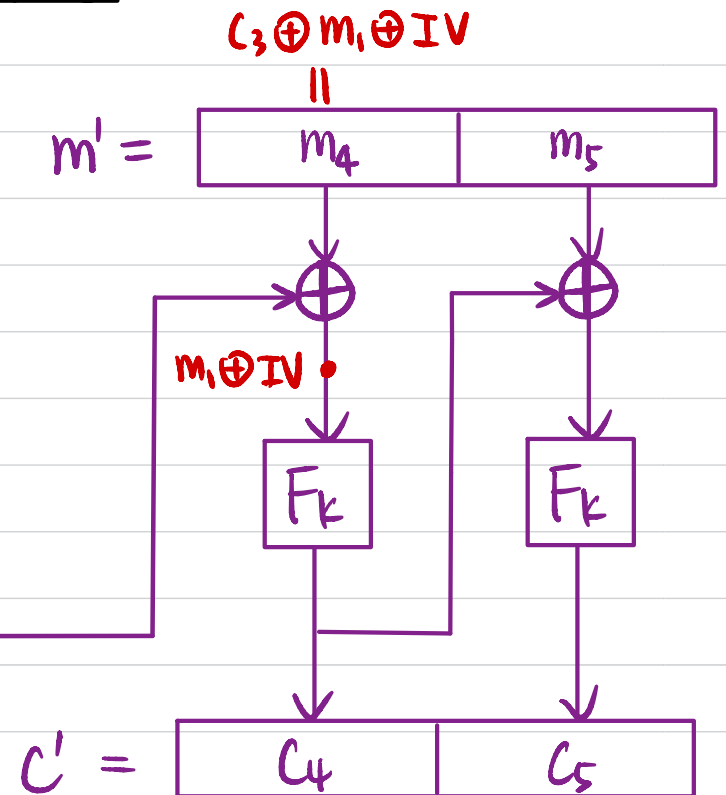
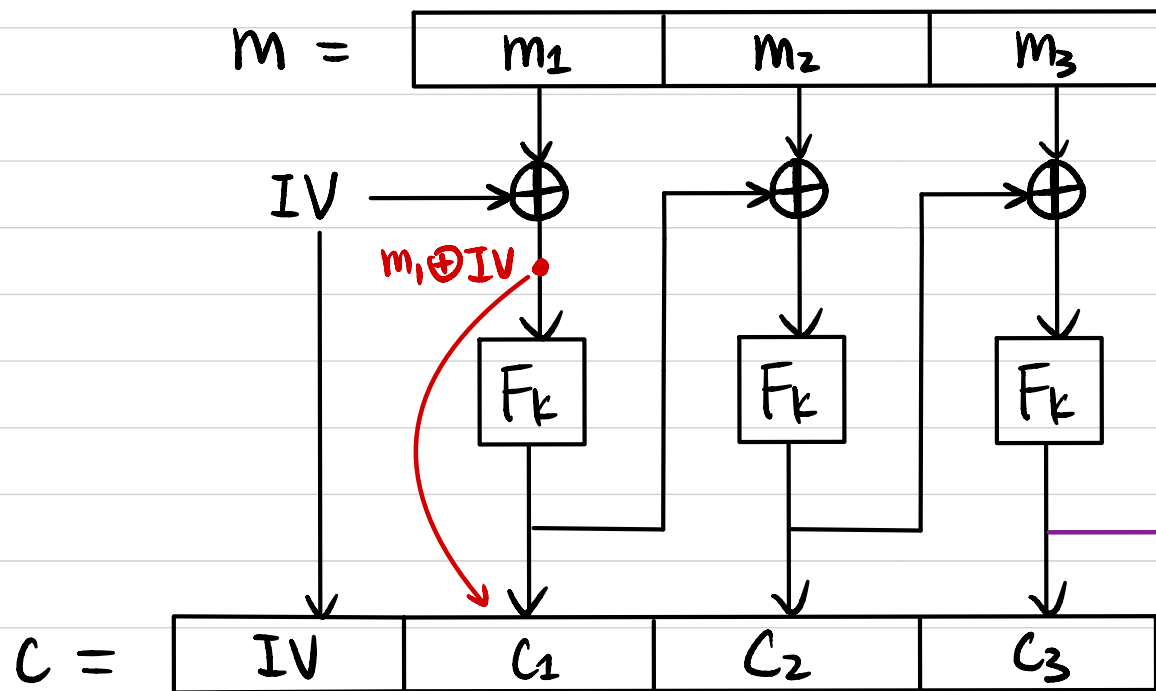


How to decrypt?

CPA Secure? YES!

Can we parallelize the computation? NO for Enc
YES for Dec

Chained Cipher Block Chaining (CBC) Mode

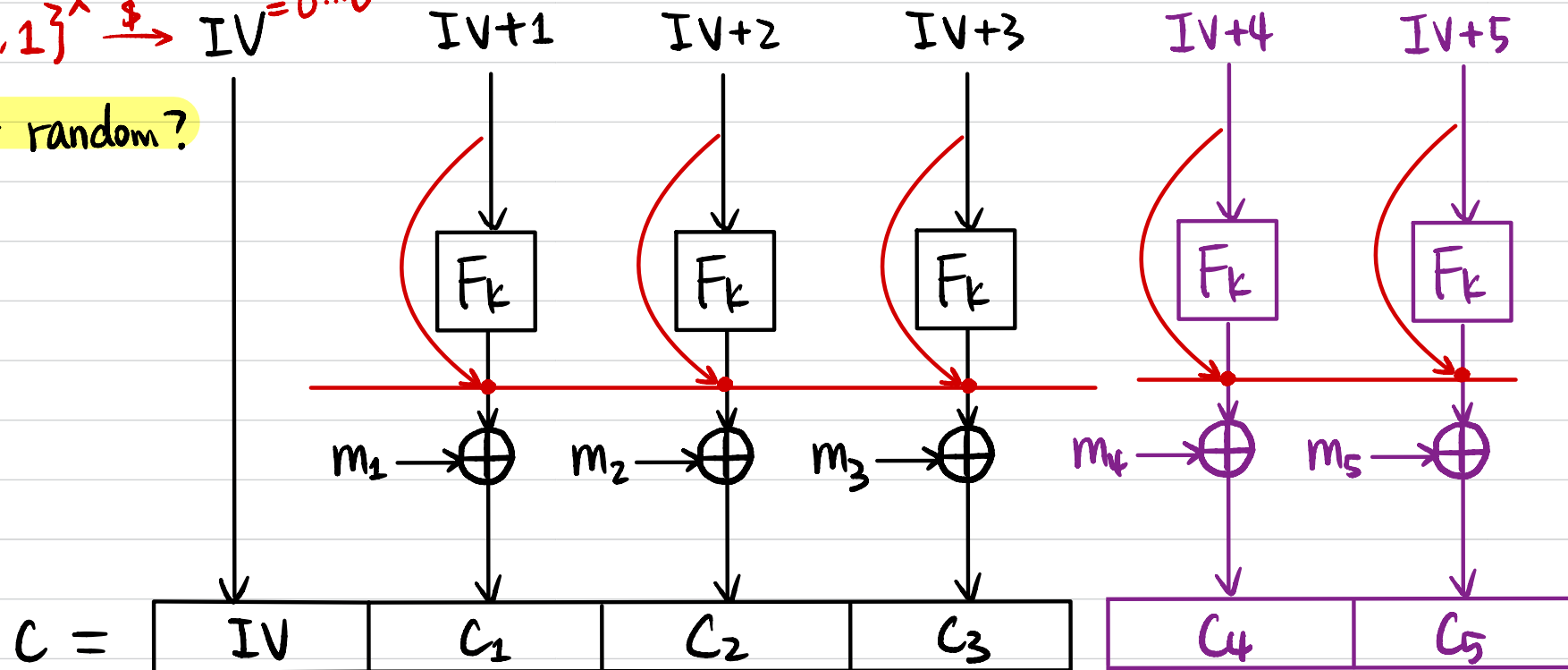


CPA Secure? No!

Counter (CTR) Mode

$\{0,1\}^{\lambda} \xrightarrow{\$} IV = 0 \dots 0$

What if not random?



How to decrypt?

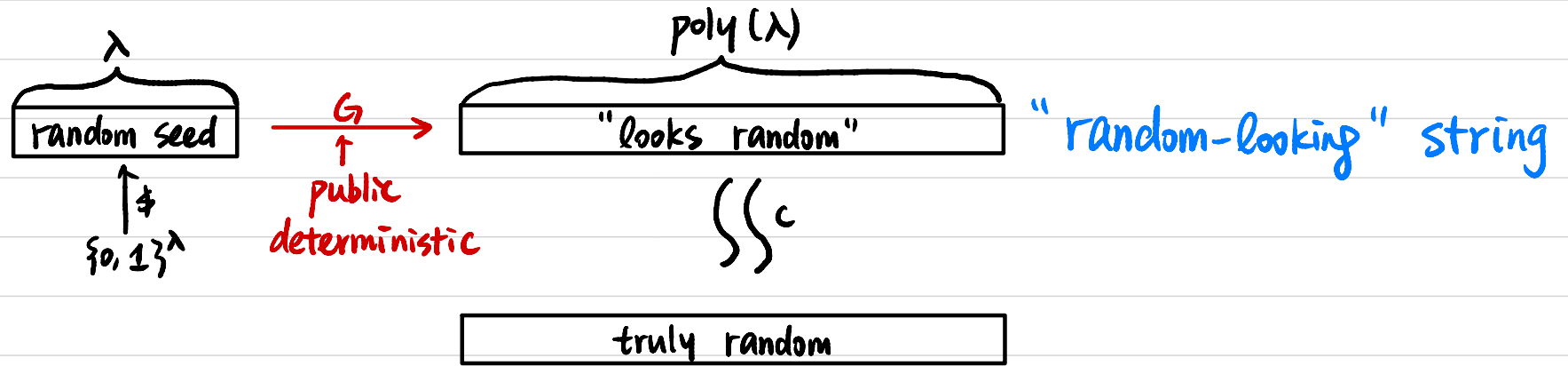
CPA Secure? YES!

"Stateful" CTR Mode? YES!

Can we parallelize the computation? YES!

PRG from PRF $\boxed{k} \xrightarrow{G} \boxed{F_k(1) \parallel F_k(2) \parallel \dots}$

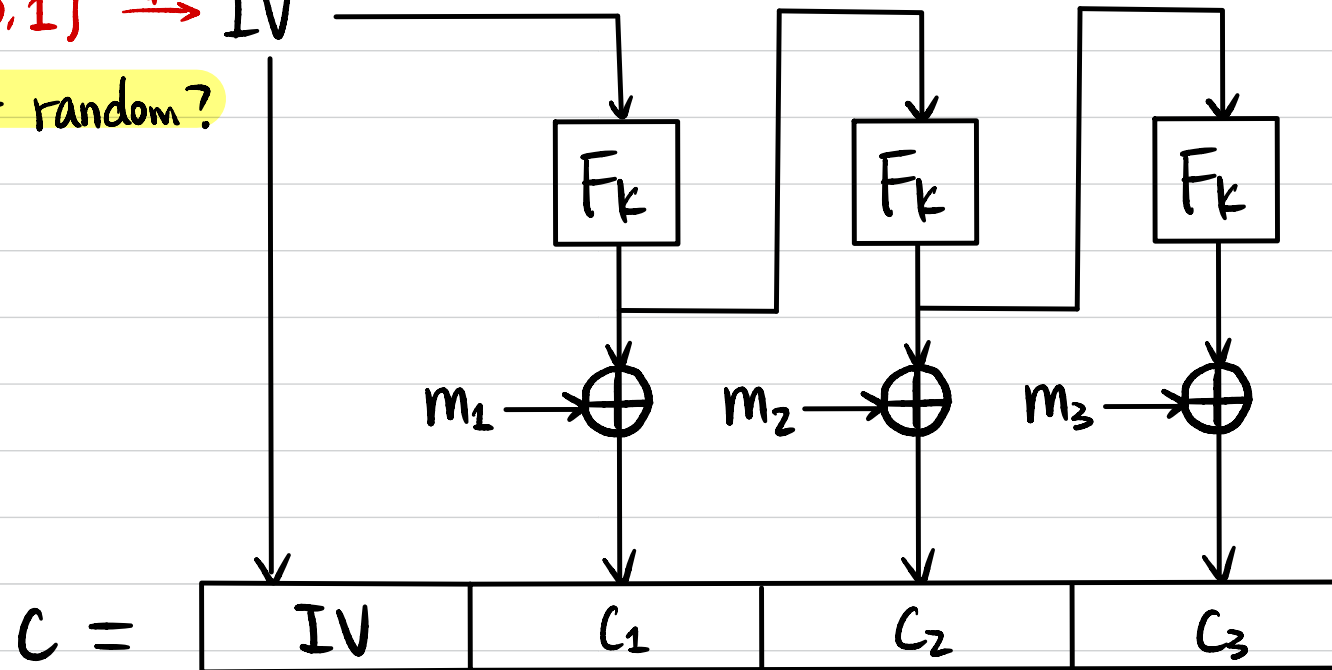
Pseudorandom Generator (PRG)



Output Feedback (OFB) Mode

$\{0,1\}^n \xrightarrow{\$} \text{IV}$

What if not random?



How to decrypt?

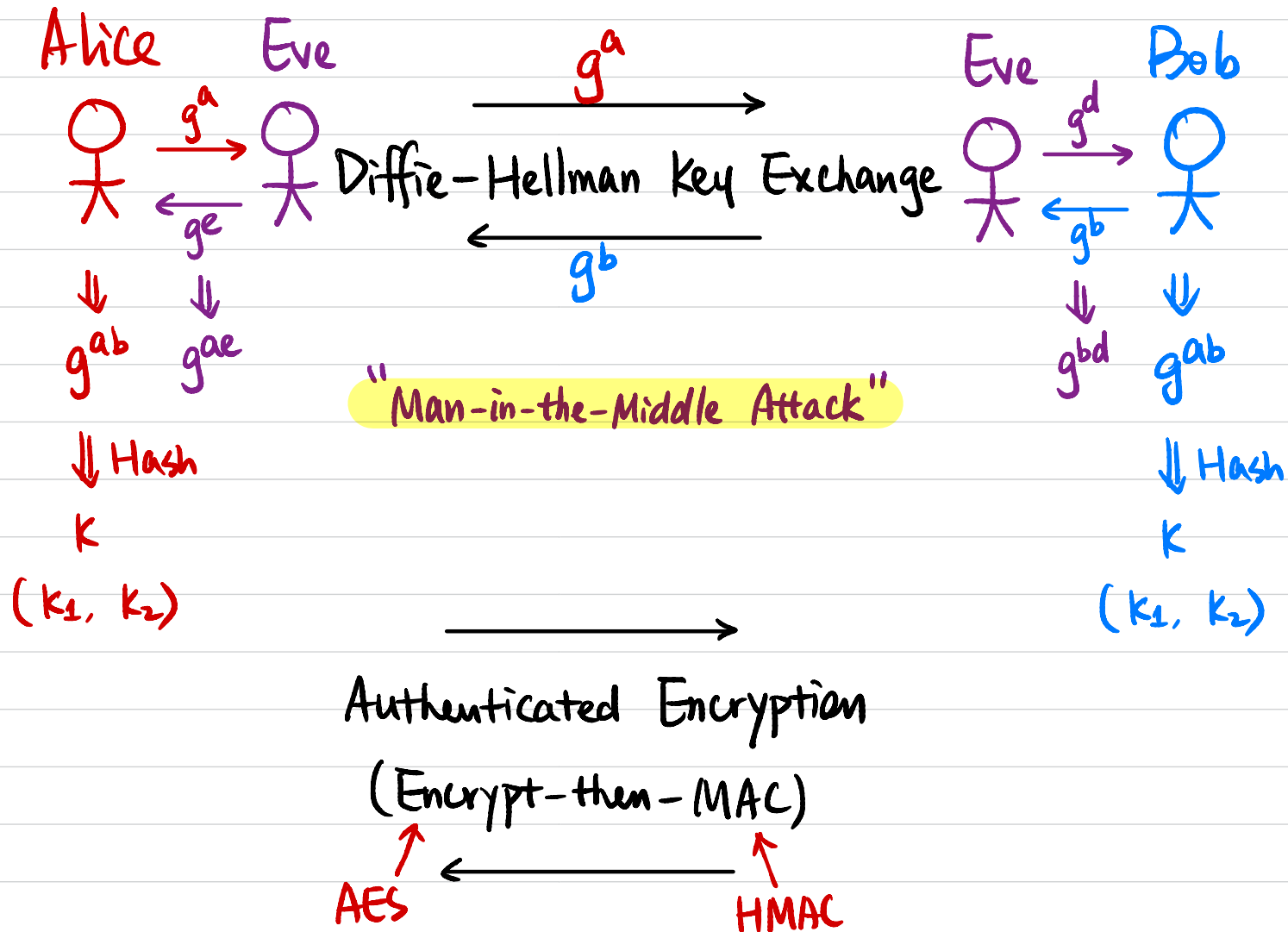
CPA Secure?

"Stateful" OFB Mode?

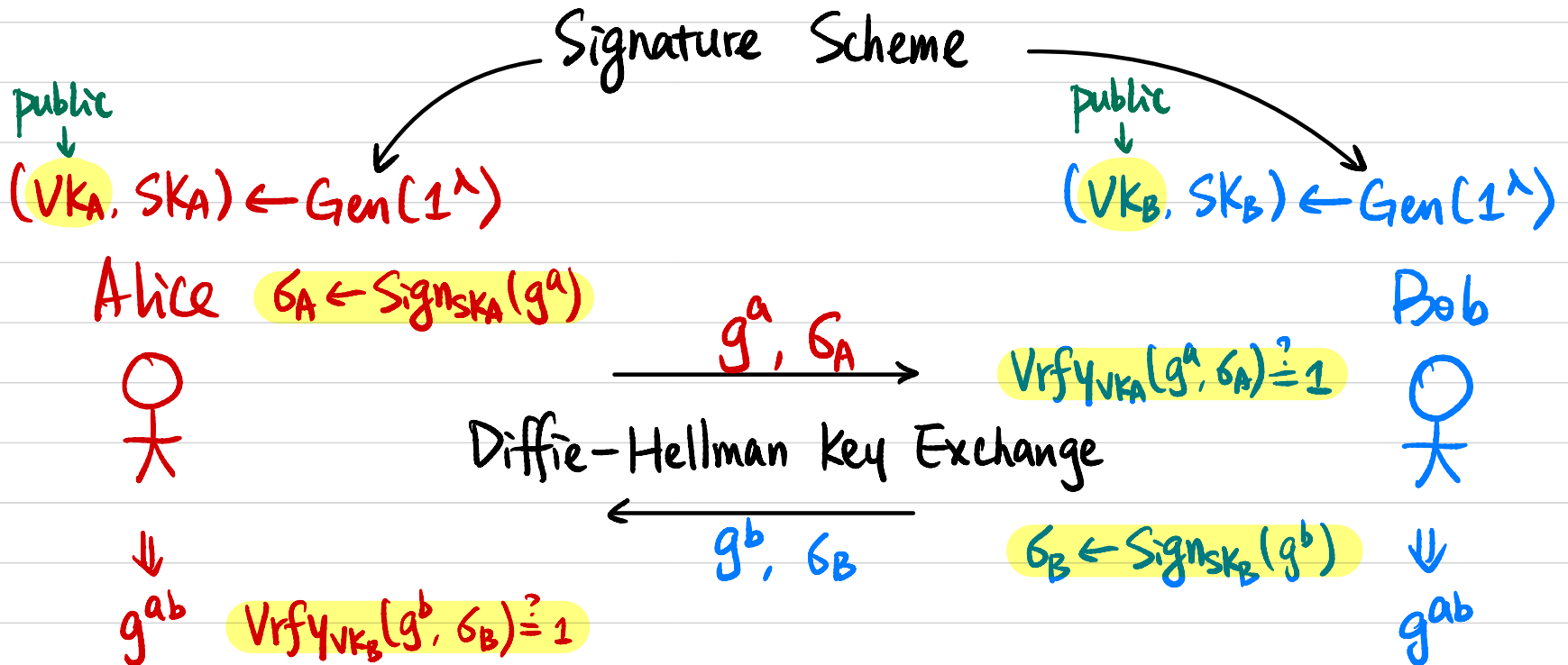
Can we parallelize the computation?

PRG from PRF

Putting it All Together: Secure Communication



Authenticated Key Exchange



Can we prevent Man-in-the-Middle Attack?

One-Sided Secure Authentication

public Where does it come from?
 $(VK_s, SK_s) \leftarrow \text{Gen}(1^\lambda)$

Client



$\Downarrow$
 g^a

$\text{Vrfy}_{VK_s}(g^b, \sigma_s) \stackrel{?}{=} 1$

$\xrightarrow{g^a}$
Diffie-Hellman Key Exchange
 $\xleftarrow{g^b, \sigma_s \leftarrow \text{Sign}_{SK_s}(g^b)}$

Server



$\Downarrow$
 g^b

Can we prevent Man-in-the-Middle Attack?

Public Key Infrastructure (PKI)

Alice



"alice.com"

$(VK_A, SK_A) \leftarrow \text{Gen}(1^\lambda)$

Certificate signing request (CSR)

"alice.com"; VK_A

public
 $(VK, SK) \leftarrow \text{Gen}(1^\lambda)$

Certificate Authority
(CA)



"Certificate"

$\text{cert}_A \leftarrow \text{Sign}_{SK}(\text{"alice.com"} \parallel VK_A)$

cert_A

Standard: X.509 certificate

Public Key Infrastructure (PKI)

Certificate Authority
(CA)

public
 $(VK, SK) \leftarrow \text{Gen}(1^\lambda)$

$\text{Cert}_A \leftarrow \text{Sign}_{SK}(\text{Amazon.com} \parallel VK_A)$

$\text{Cert}_G \leftarrow \text{Sign}_{SK}(\text{Google.com} \parallel VK_G)$



Amazon.com; VK_A

Cert_A

Amazon



$(VK_A, SK_A) \leftarrow \text{Gen}(1^\lambda)$

Google.com; VK_G

Cert_G

Google



$(VK_G, SK_G) \leftarrow \text{Gen}(1^\lambda)$

