COS433/Math 473: Cryptography

Mark Zhandry

Princeton University

Spring 2017

Announcements

Homework 3 due tomorrow

Homework 4 up

Take-home midterm tentative dates:

- Posted 3pm am Monday 3/13
- Due 1pm Wednesday 3/15

Last Time

CPA Security

Pseudorandom Functions

Pseudorandom Functions

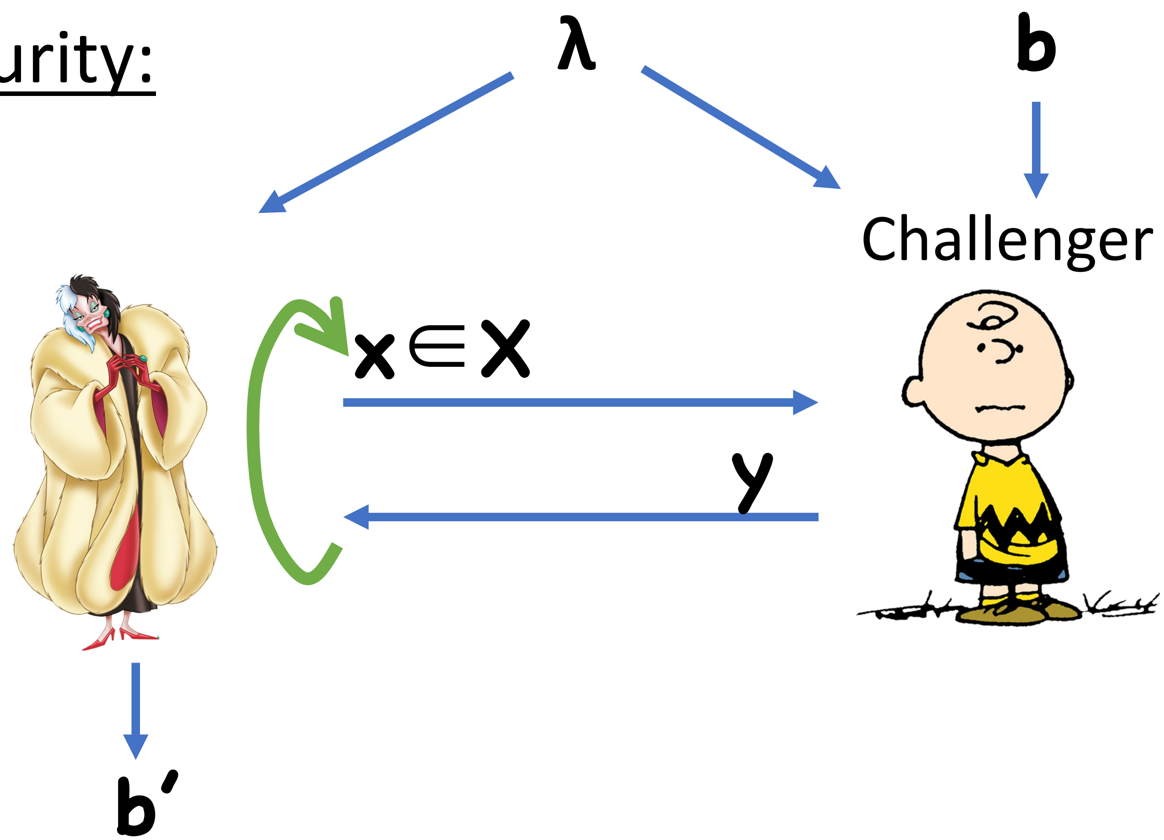
Functions that "look like" random functions

Syntax:

- Key space $\{0,1\}^\lambda$
- Domain X (usually $\{0,1\}^m$, m may depend on λ)
- Co-domain/range Y (usually $\{0,1\}^n$, may depend on λ)
- Function $F:\{0,1\}^\lambda \times X \rightarrow Y$

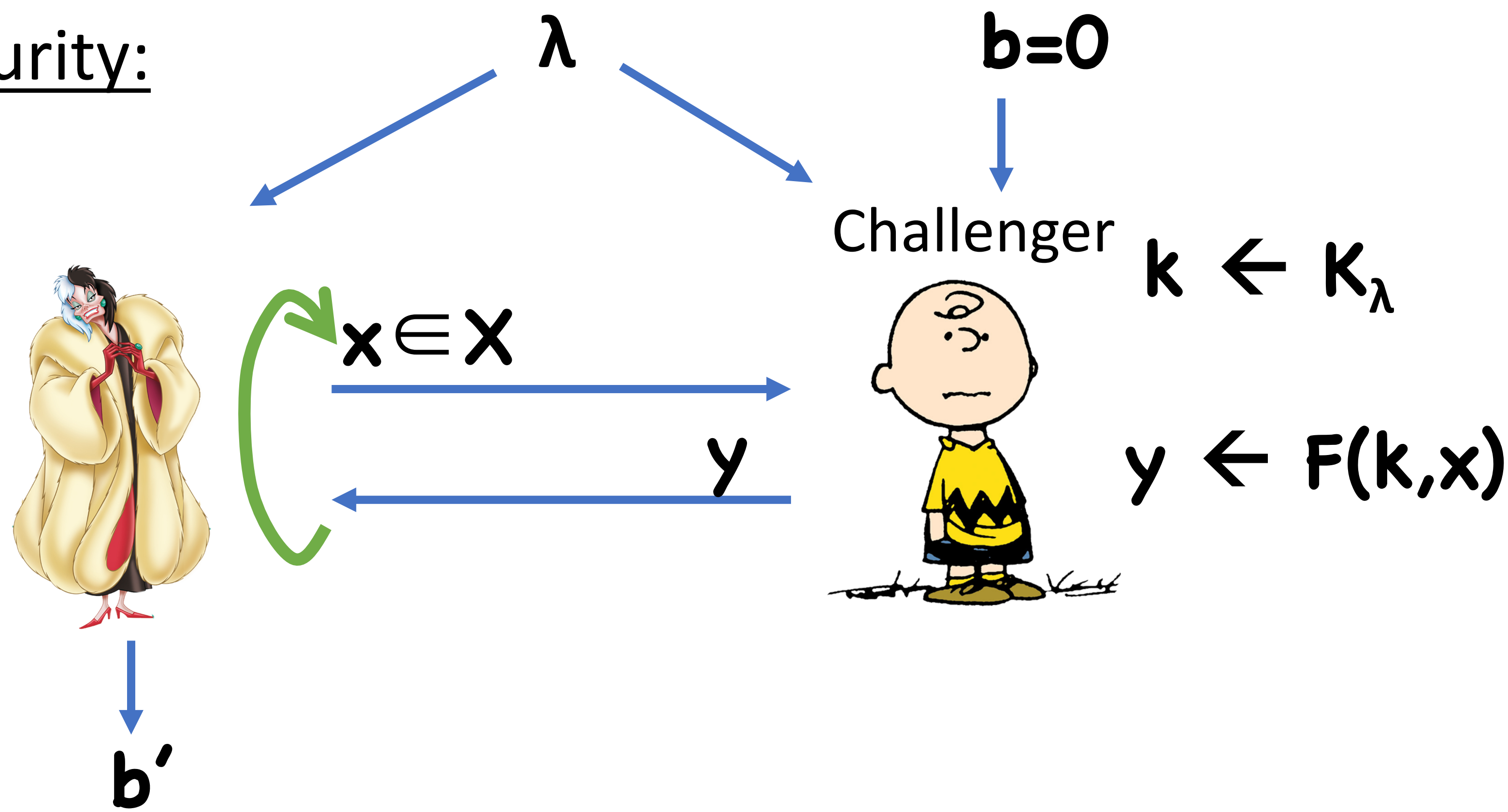
Pseudorandom Functions

<u>Security:</u>



Pseudorandom Functions

<u>Security:</u>



PRF-Exp$_0$( **, λ)**

Pseudorandom Functions

<u>Security:</u>

λ

b=1

Challenger

$H \leftarrow \mathrm{Funcs}(X,Y)$

$x \in X$

y

$y = H(x)$

b'

PRF-Exp$_1$( **, λ)**

PRF Security Definition

Definition: F is a secure PRF if, for all probabilistic polynomial time (PPT)  , there exists a negligible function **ε** such that

$\Big|$ Pr[1←PRF-Exp$_0$( , λ)]

$-$ Pr[1←PRF-Exp$_1$( , λ)] $\Big|$ $\leq$ $\varepsilon(\lambda)$

Using PRFs to Build Encryption

$\mathbf{Enc}(k, m)$:

- Choose random $r \leftarrow X$
- Compute $y \leftarrow F(k,r)$
- Compute $c \leftarrow y \oplus m$
- Output (r,c)

$\mathbf{Dec}(k, (r,c))$:

- Compute $y' \leftarrow F(k,r)$
- Compute and output $m' \leftarrow c \oplus y'$

Correctness:

- $y' = y$ since F is deterministic
- $m' = c \oplus y = y \oplus m \oplus y = m$

Counter Mode

Enc(k, m):

- Choose random $\mathbf{r}\leftarrow\{0,1\}^{\lambda/2}$
- For $\mathbf{i=1,\ldots,|m|}$,
  - Compute $\mathbf{y_i\leftarrow F(k,r||i)}$
  - Compute $\mathbf{c_i\leftarrow y_i\oplus m_i}$
- Output $\mathbf{(r,c)}$ where $\mathbf{c=(c_1,\ldots,c_{|m|})}$

Write **i** as $\boldsymbol{\lambda/2}$-bit string

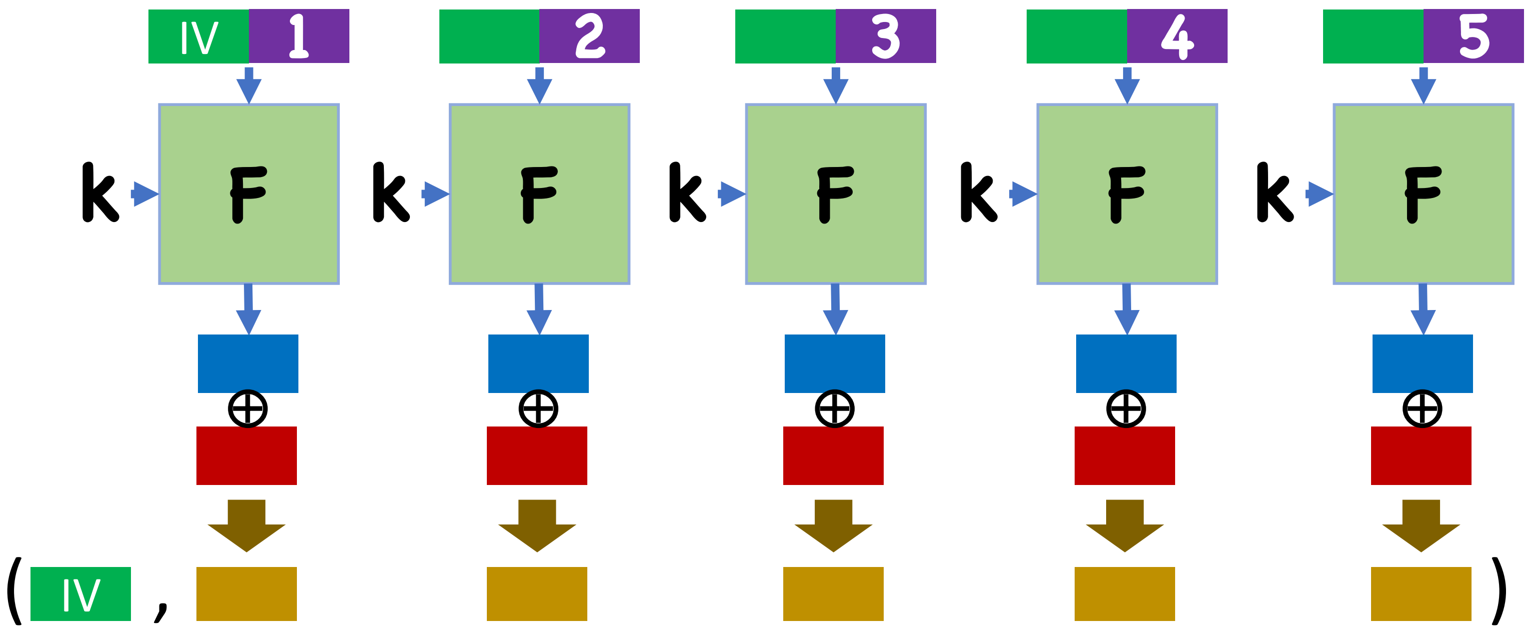
Dec(k, (r,c)):

- For $\mathbf{i=1,\ldots,l}$,
  - Compute $\mathbf{y_i\leftarrow F(k,r||i)}$
  - Compute $\mathbf{m_i\leftarrow y_i\oplus c_i}$
- Output $\mathbf{m=m_1,\ldots,m_l}$

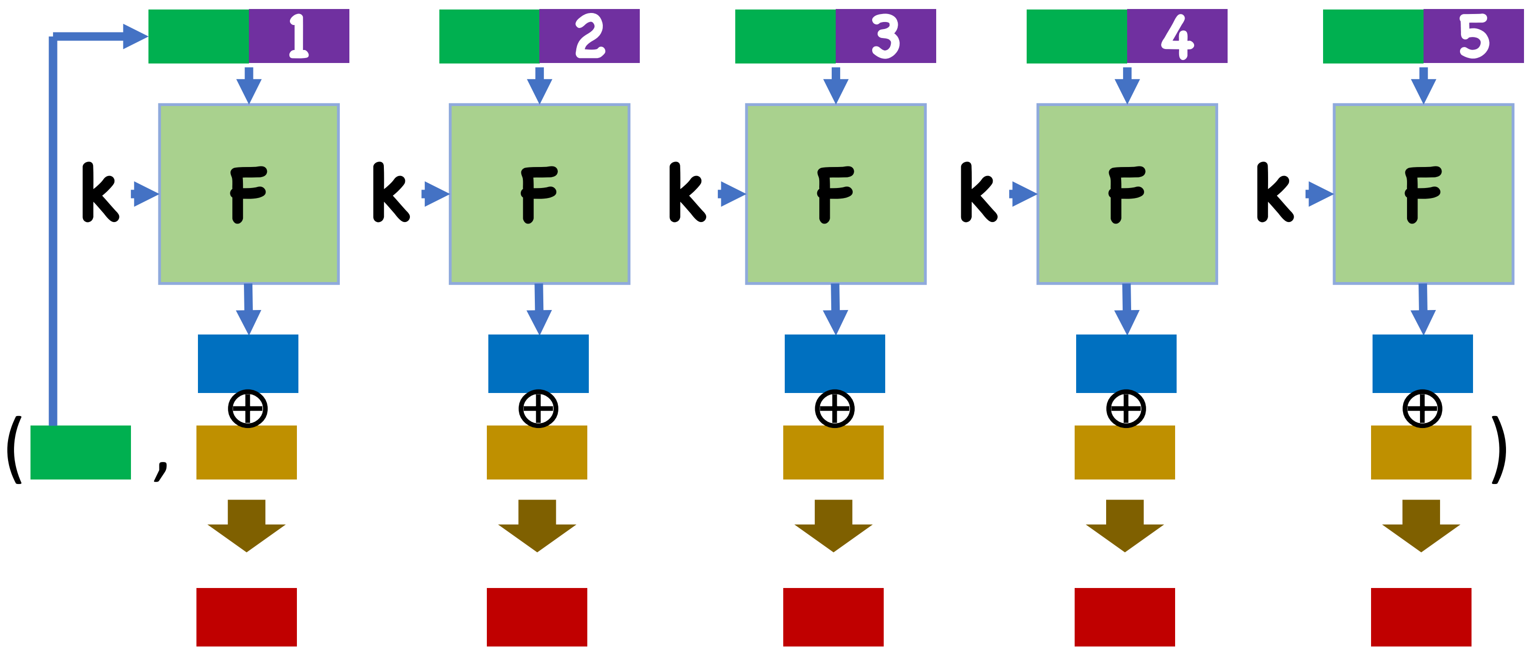
Handles any message of length at most $\mathbf{2^{\lambda/2}}$

- Includes all polynomial-length messages

Counter Mode



Counter Mode Decryption



This Time

Pseudorandom Permutations/Block Ciphers

Modes of Operation

Pseudorandom Permutations

(also known as block ciphers)

Functions that "look like" random **permutations**

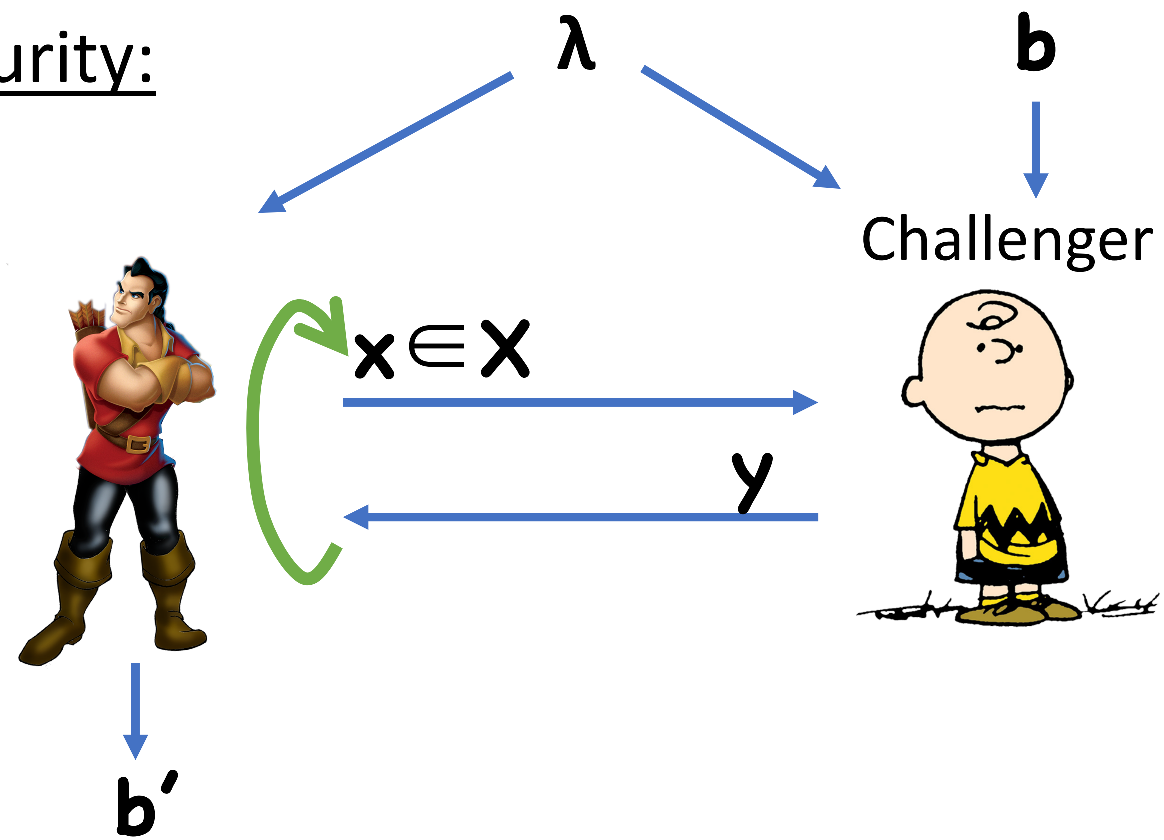
Syntax:

- Key space $\{0,1\}^\lambda$
- Domain X (usually $\{0,1\}^n$, n usually depends on λ)
- Range X
- Function $F:\{0,1\}^\lambda \times X \to X$
- Function $F^{-1}:\{0,1\}^\lambda \times X \to X$

Correctness: $\forall k,x,\ F^{-1}(k, F(k, x)) = x$

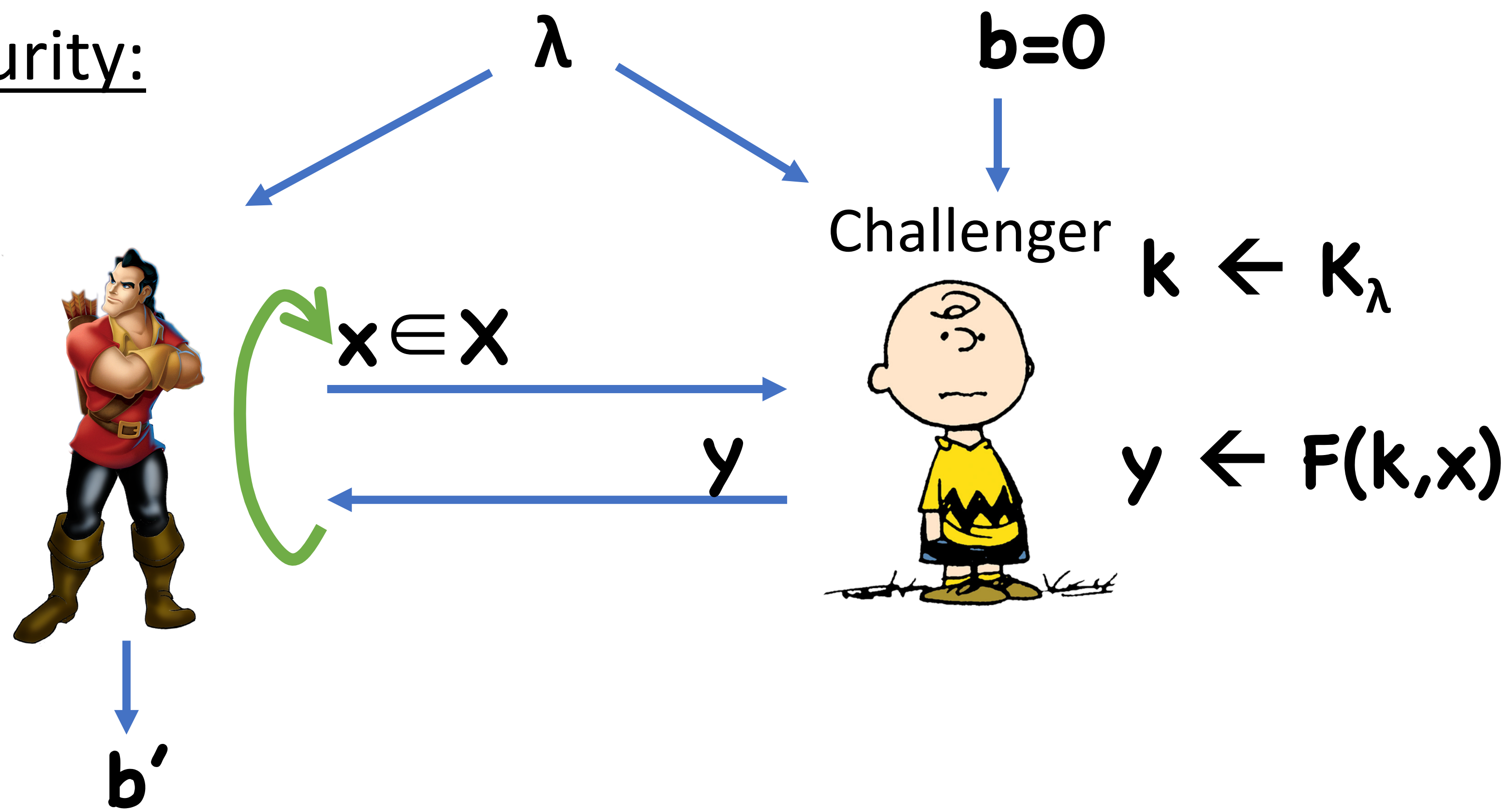
Pseudorandom Permutations

Security:



Pseudorandom Permutations

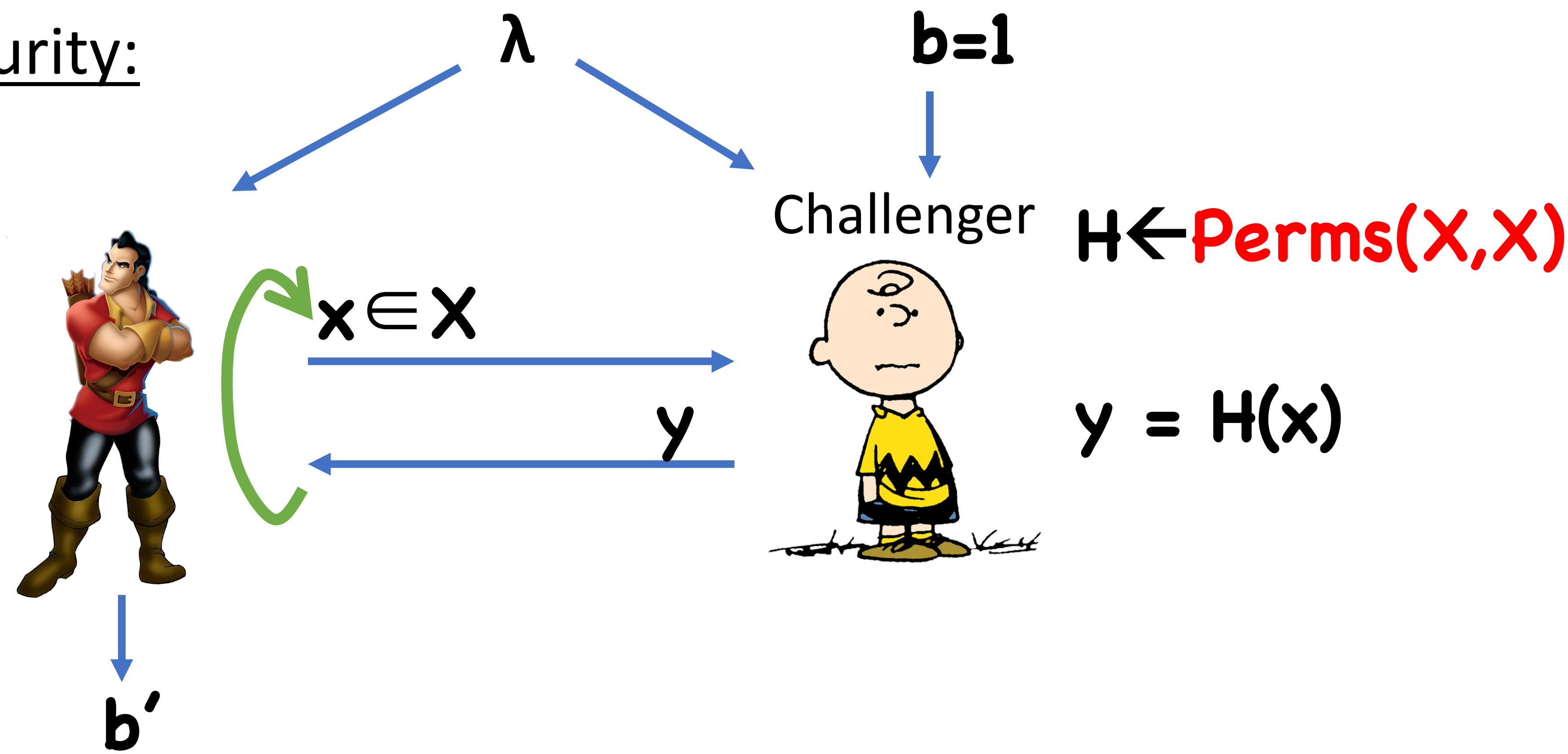
Security:



PRF-Exp$_0$( **, λ)**

Pseudorandom Permutations

Security:



PRF-Exp$_1$( **, λ)**

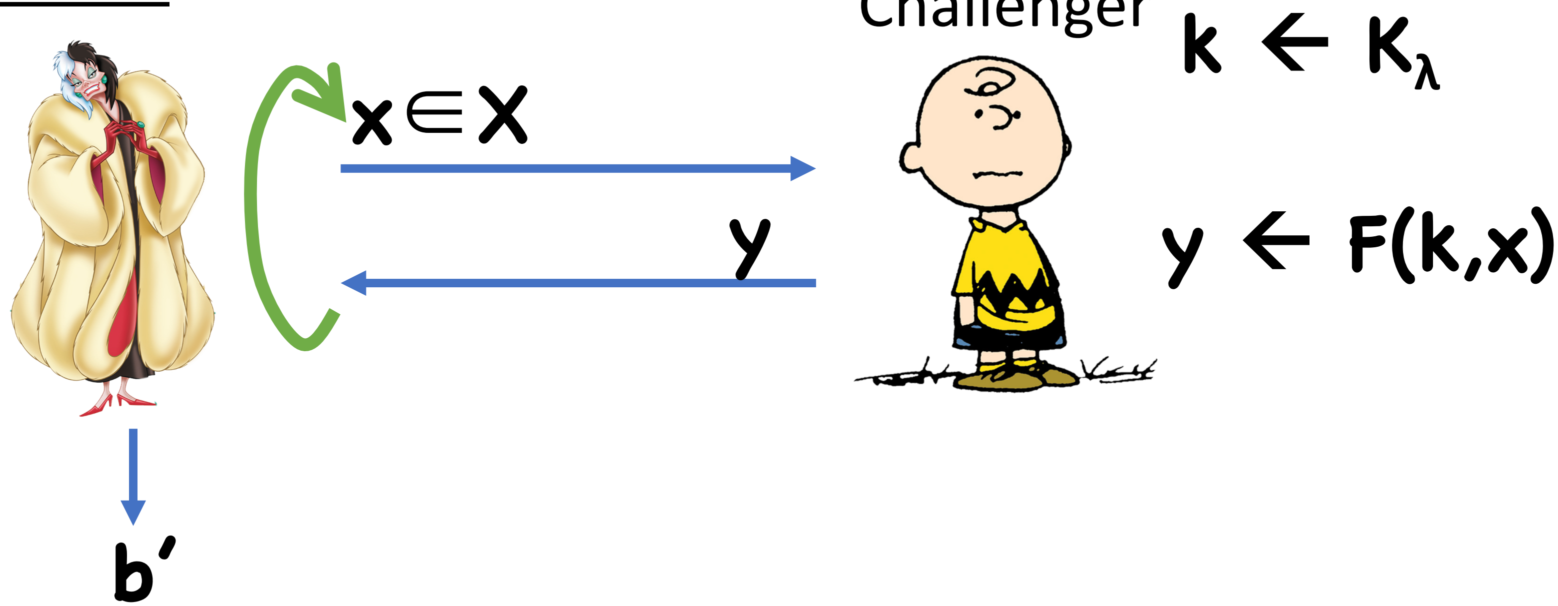
Theorem: A PRP (F, F^{-1}) is secure iff F is a secure as a PRF

Proof

Secure as PRP $\Rightarrow$ Secure as PRF

- Assume , hybrids

<u>Hybrid 0:</u>

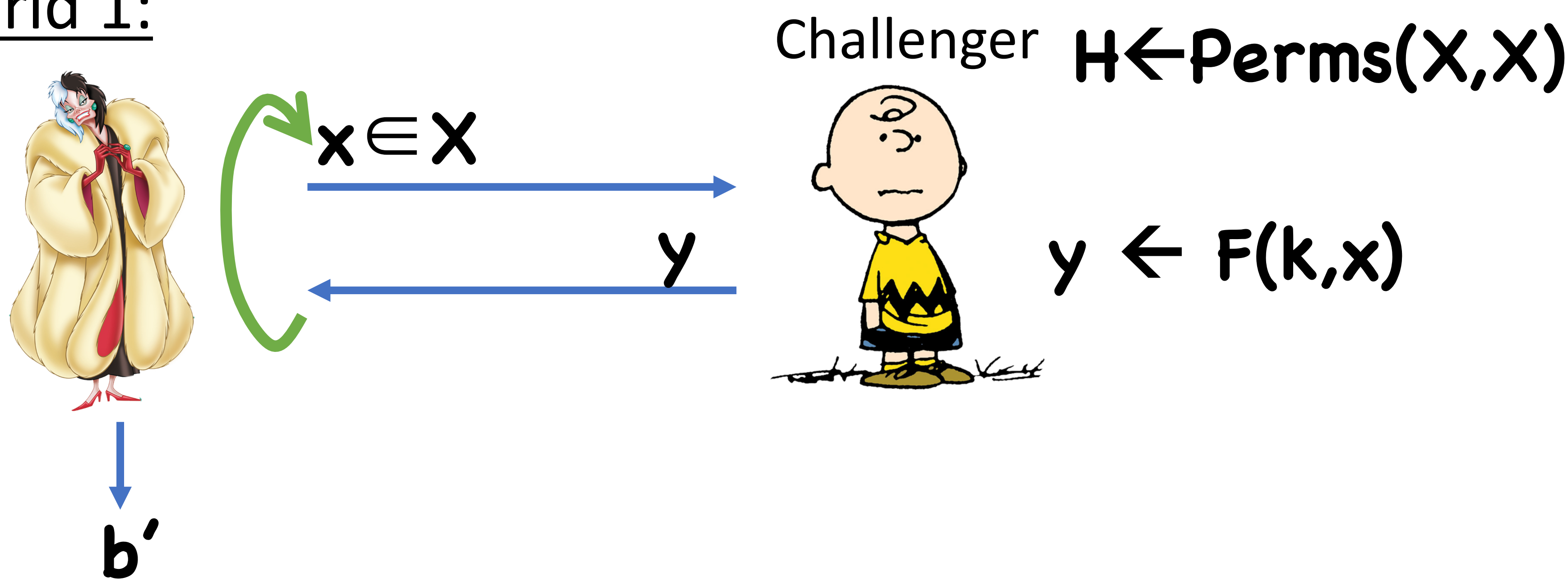


Proof

Secure as PRP $\Rightarrow$ Secure as PRF

- Assume , hybrids

<u>Hybrid 1:</u>

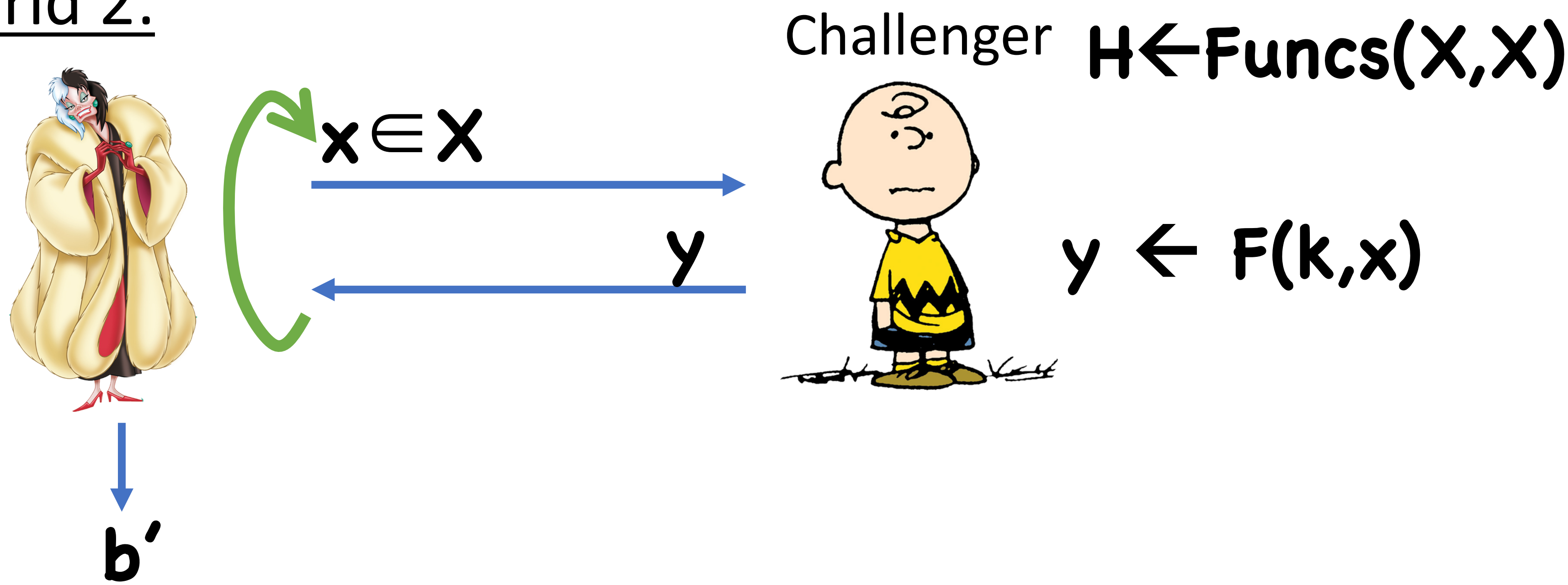


Proof

Secure as PRP $\Rightarrow$ Secure as PRF

- Assume , hybrids

<u>Hybrid 2:</u>



Proof

Secure as PRP $\Rightarrow$ Secure as PRF

- Assume , hybrids

Hybrids 0 and 1 are indistinguishable by PRP security

Hybrids 1 and 2?

- In Hybrid 1,  sees random **distinct** answers
- In Hybrid 2,  sees random answers
- Except with probability $\approx \mathbf{q^2/2^{n+1}}$, random answers will be distinct anyway

Proof

Secure as PRF $\Rightarrow$ Secure as PRP

- Assume , hybrids

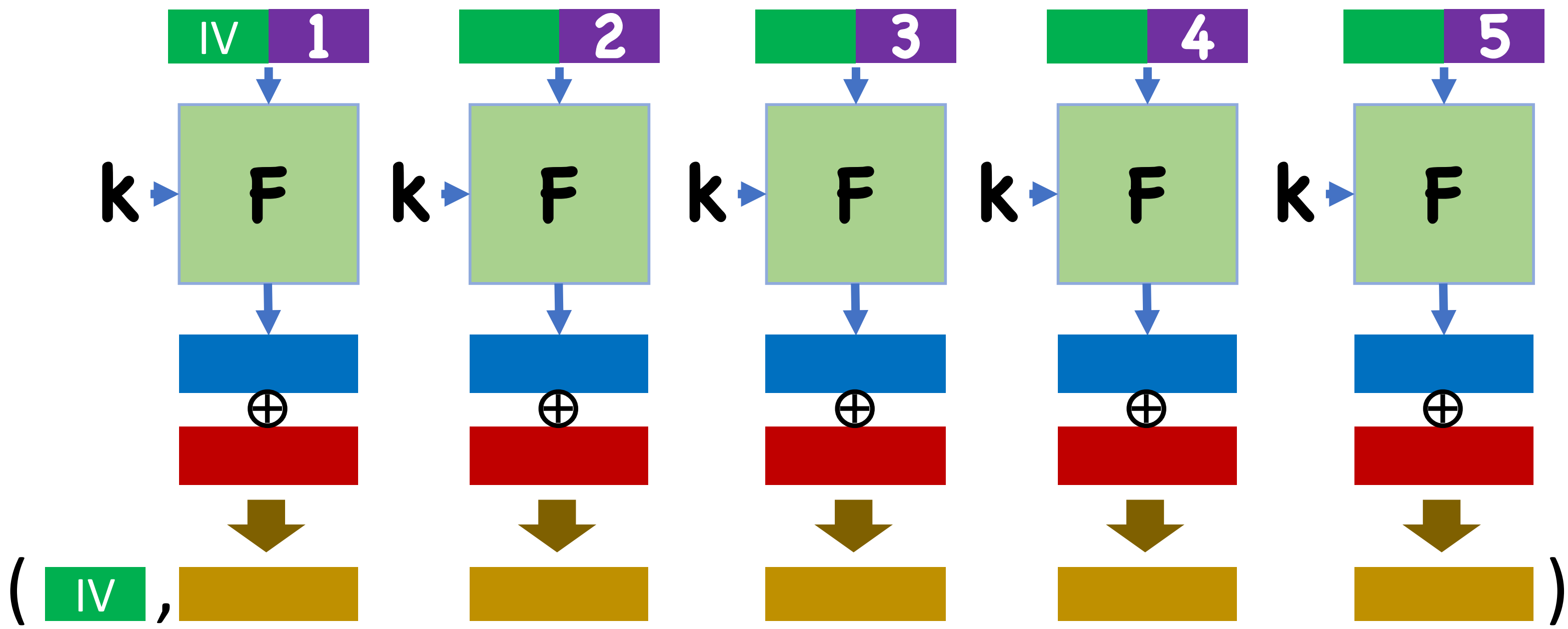
Proof essentially identical to other direction

Suppose (F, F^{-1}) is a secure PRP

Is (F^{-1}, F) also a secure PRP?

How to use block ciphers for encryption

Counter Mode (CTR)



Electronic Code Book (ECB)

Enc(k, m):

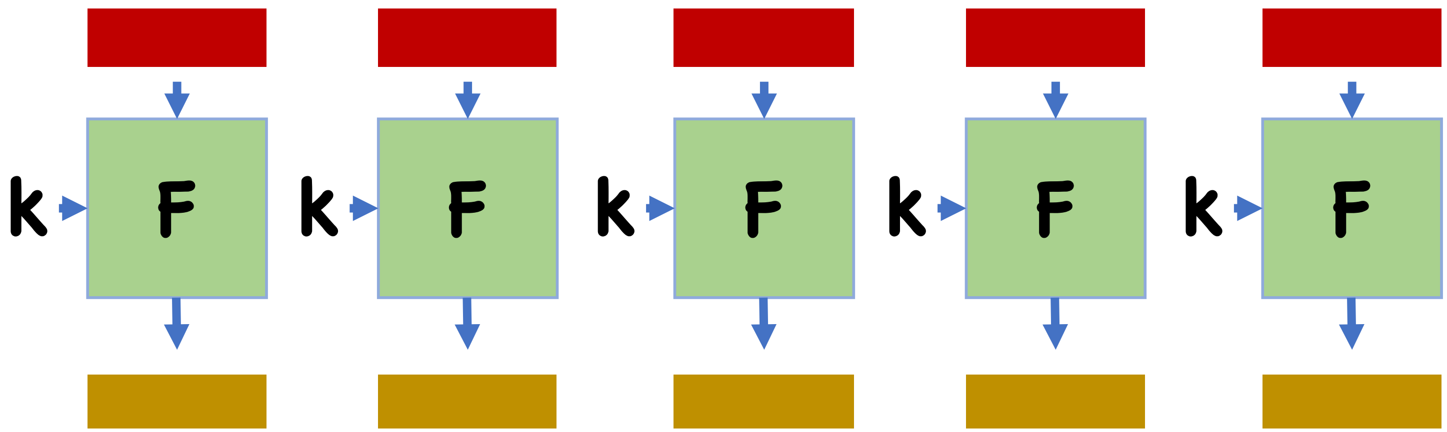
- Break $\mathbf{m}$ into $\mathbf{t}$ blocks $\mathbf{m_i}$ of $\mathbf{n}$ bits
- For each block $\mathbf{m_i}$, let $\mathbf{c_i = F(k, m_i)}$
- Output $\mathbf{c = (c_1, \ldots, c_t)}$

Dec(k, c):

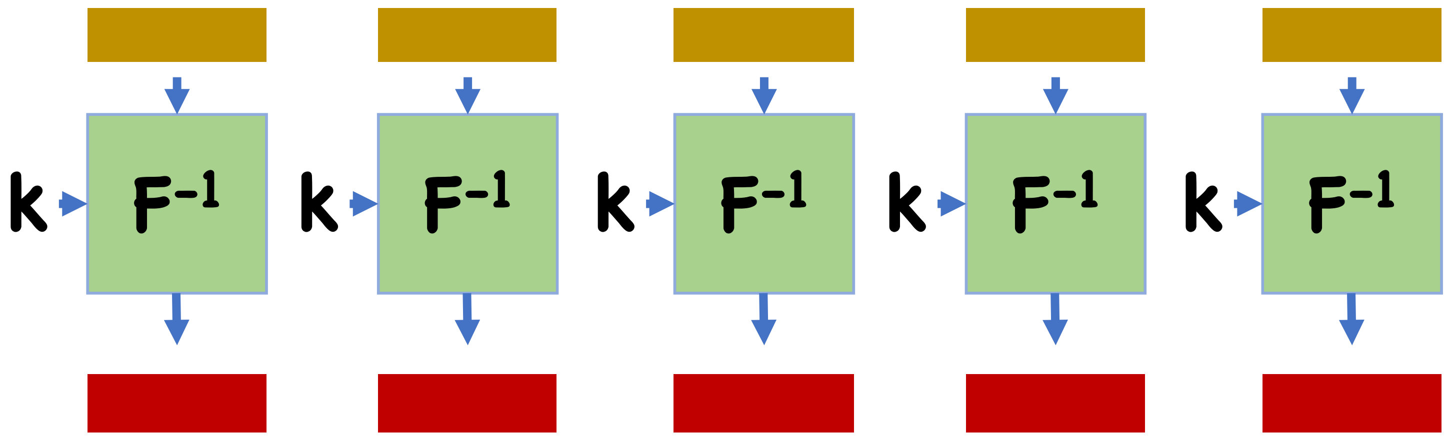
- Break $\mathbf{c}$ into $\mathbf{t}$ blocks $\mathbf{c_i}$ of $\mathbf{n}$ bits
- For each block $\mathbf{c_i}$, let $\mathbf{m_i = F^{-1}(k, c_i)}$
- Output $\mathbf{m = (m_1, \ldots, m_t)}$

substitution cipher for $\mathbf{n}$-bit alphabet

Electronic Code Book (ECB)



ECB Decryption



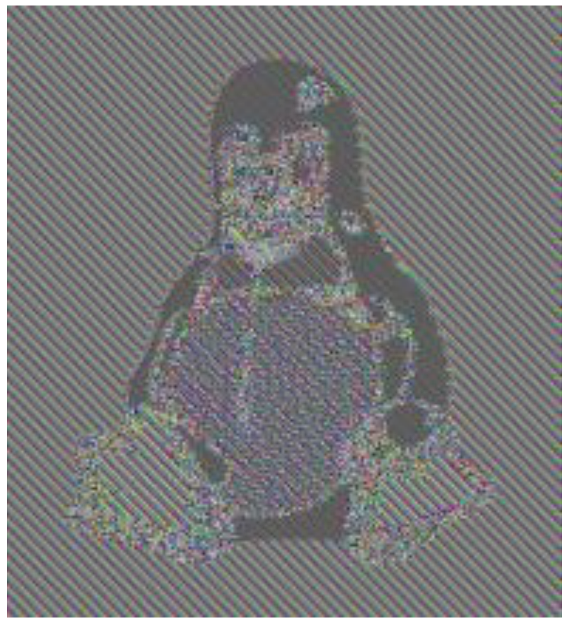
Security of ECB?

Is ECB mode CPA secure?

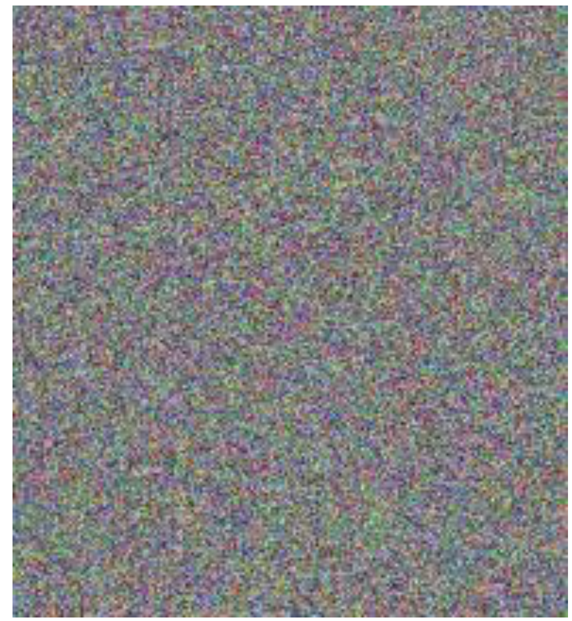
Is ECB mode *one-time* secure?

Security of ECB

Plaintex

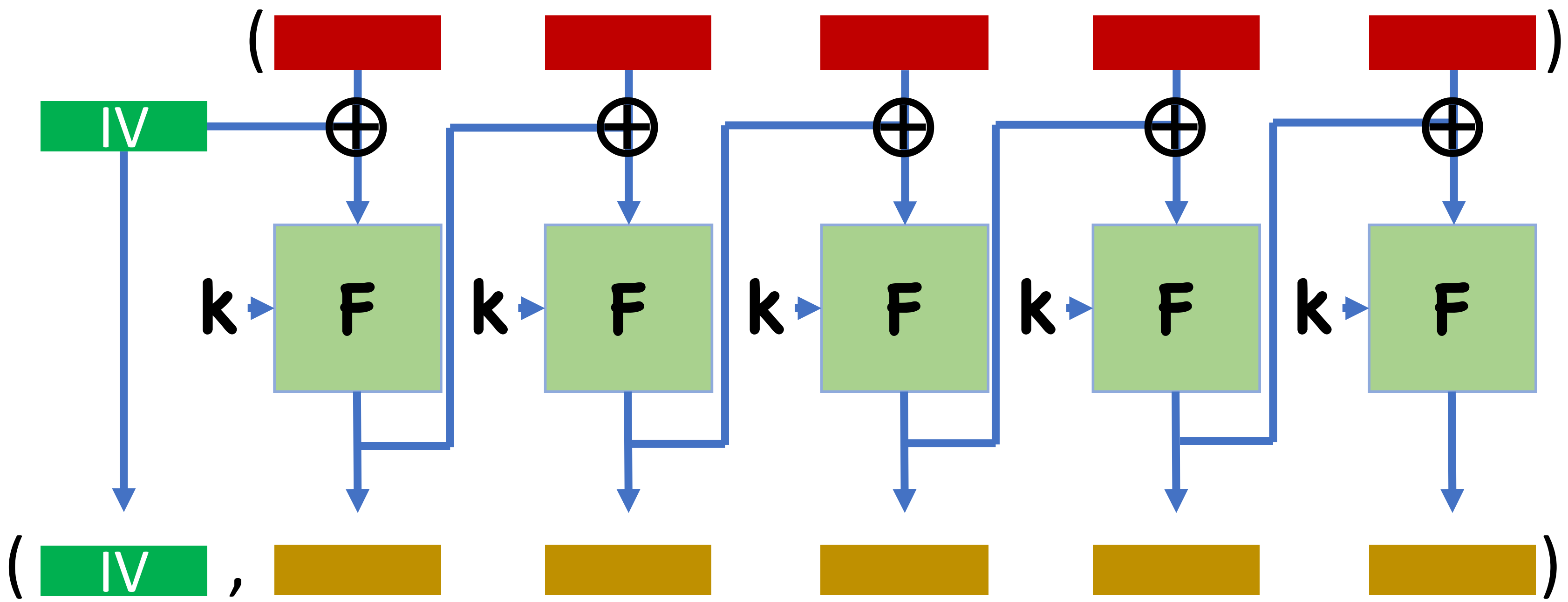


Ciphertext



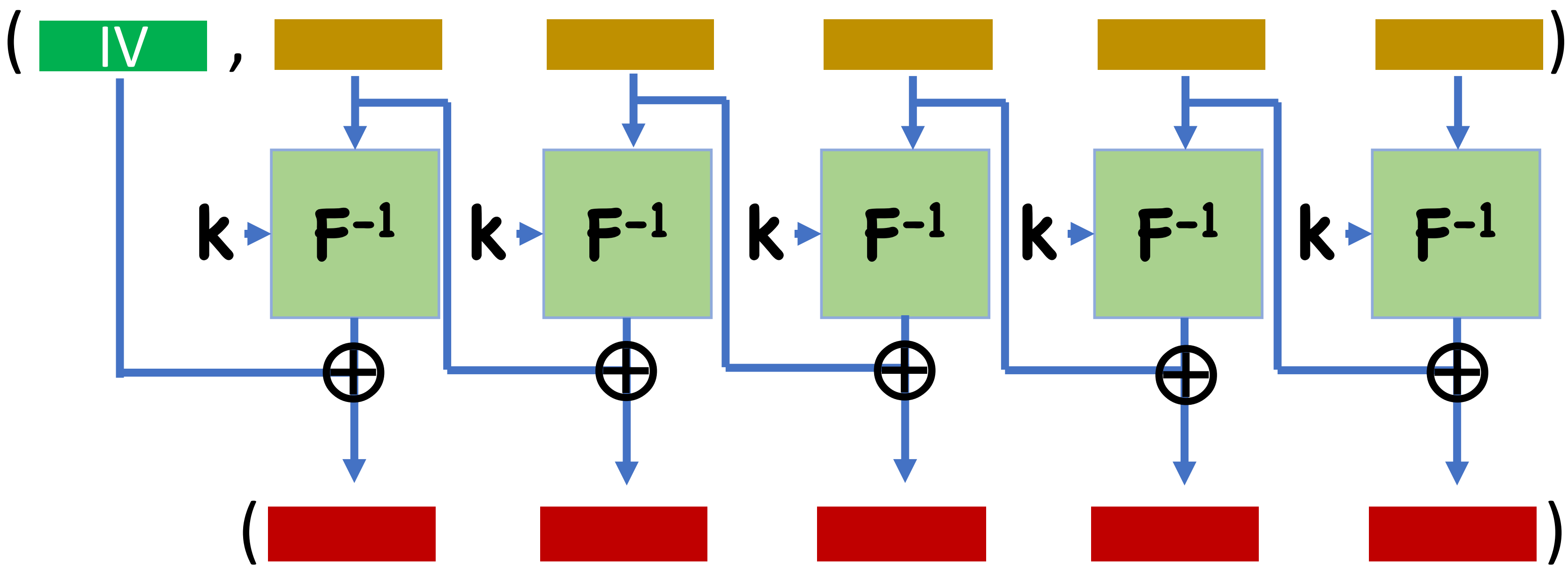
Ideal

Cipher Block Chaining (CBC) Mode



(For now, assume all messages are multiples of the block length)

CBC Mode Decryption



Theorem: If (F, F^{-1}) is a secure pseudorandom permutation, then CBC mode encryption is CPA secure

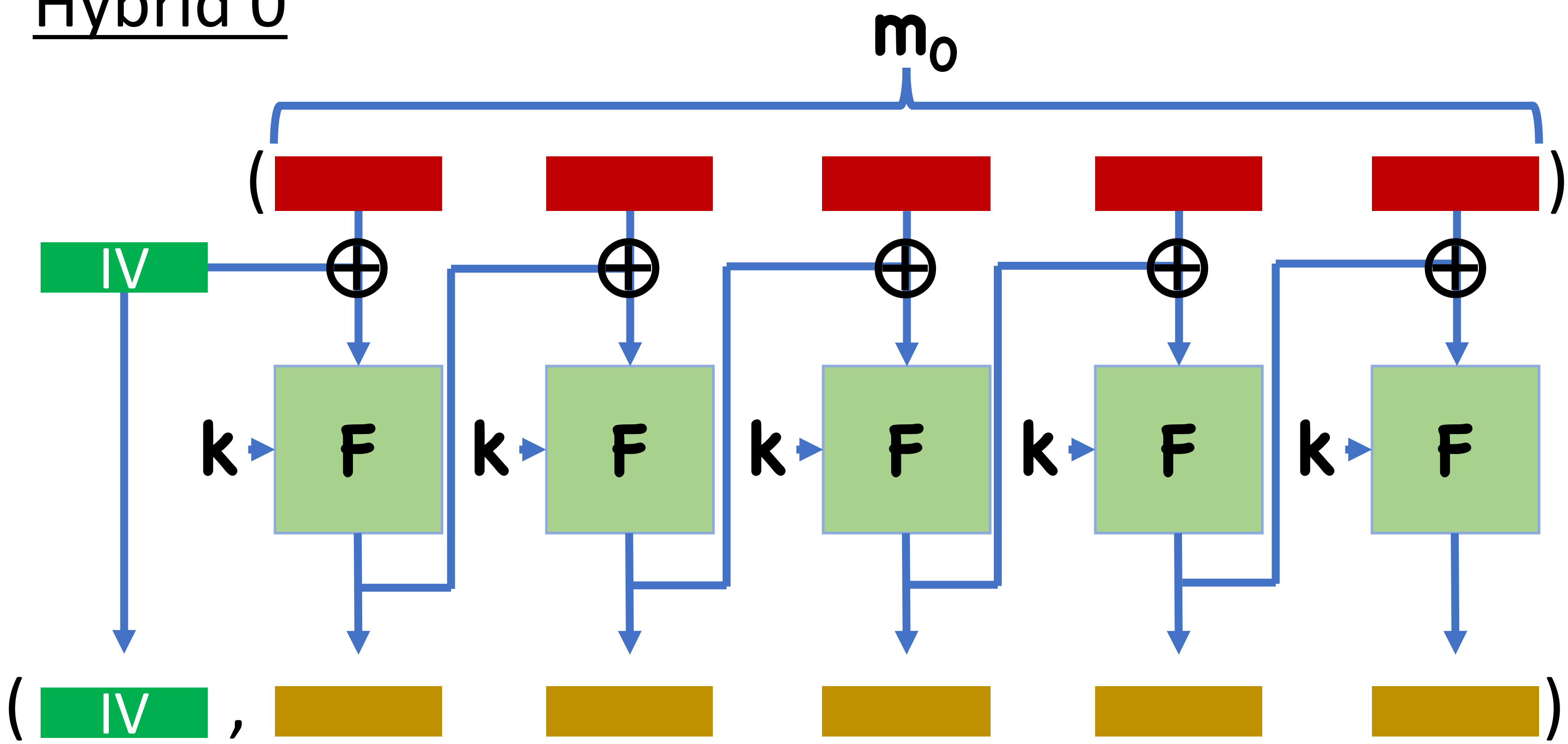
Proof Sketch

Assume toward contradiction an adversary  for CBC mode

Hybrids…

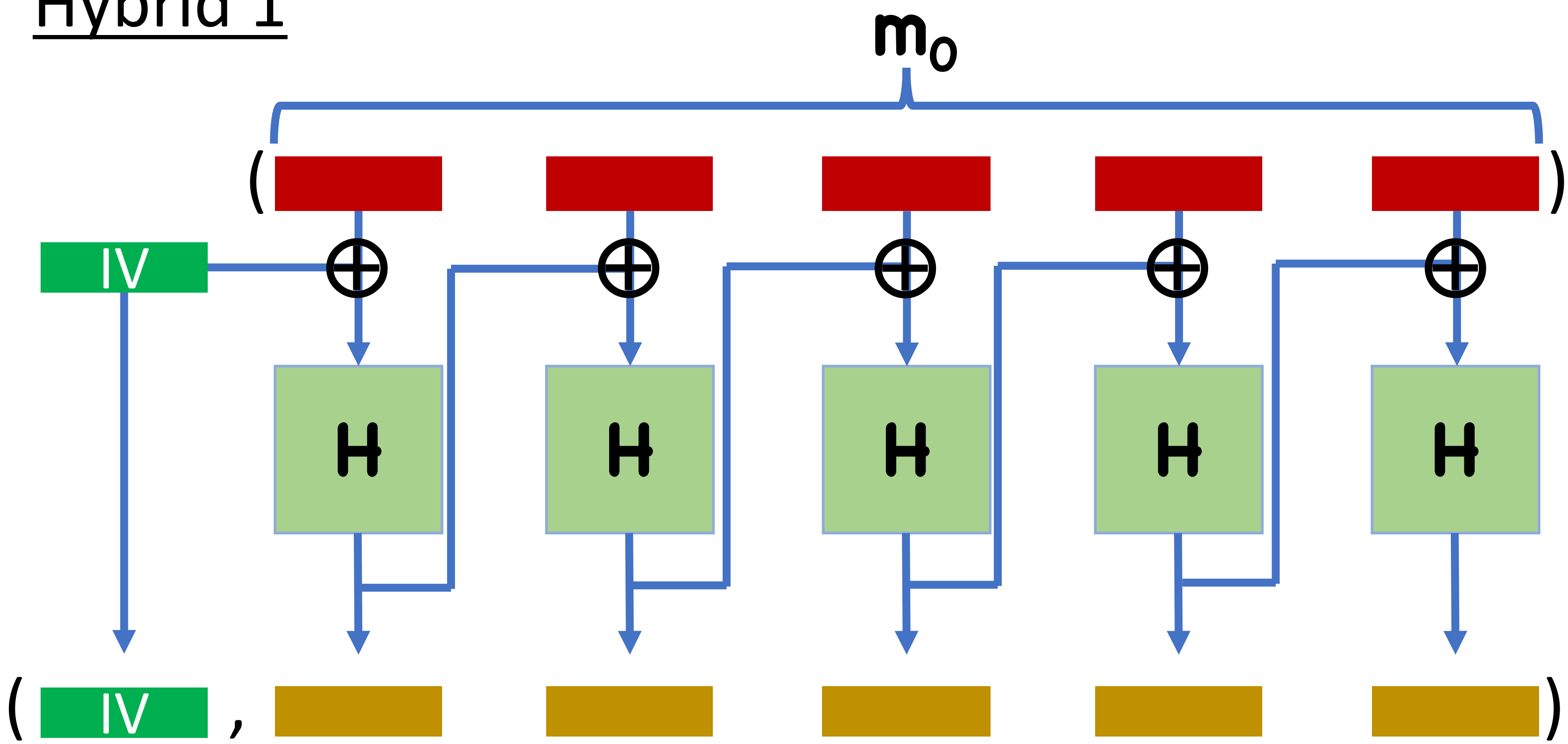
Proof Sketch

Hybrid 0



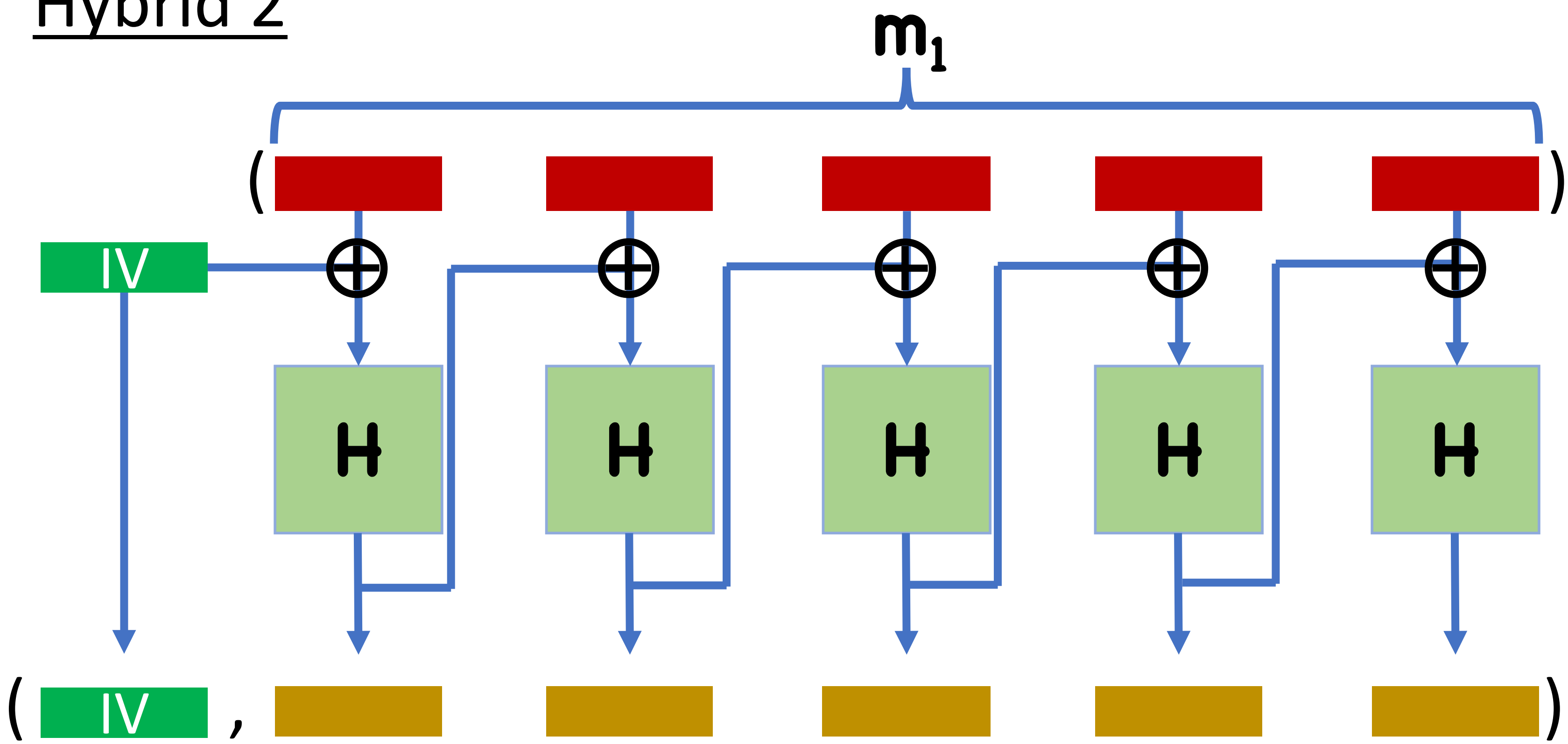
Proof Sketch

Hybrid 1



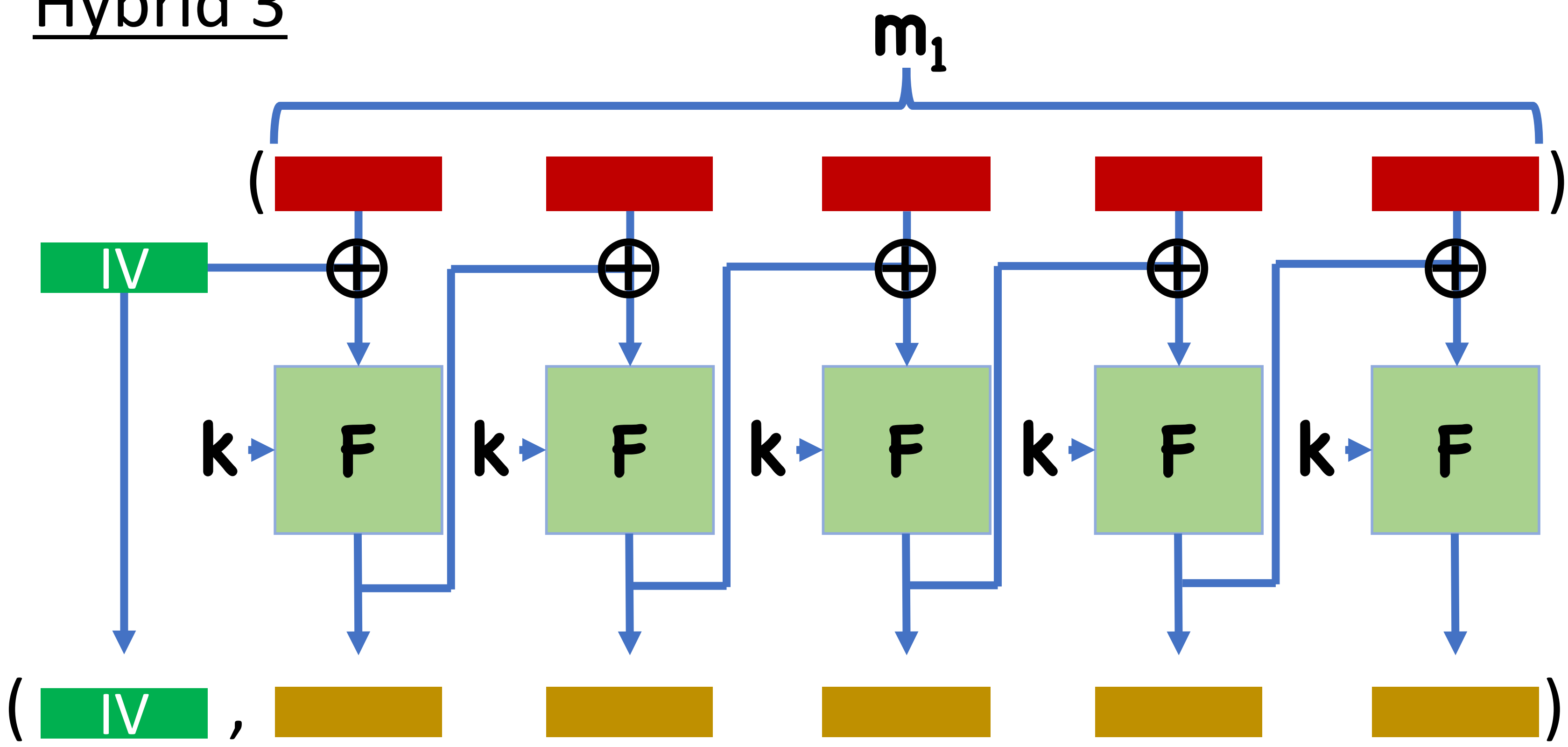
Proof Sketch

Hybrid 2



Proof Sketch

Hybrid 3



Proof Sketch

Hybrid 0,1 differ by replacing calls to **F** with calls to random permutation **H**

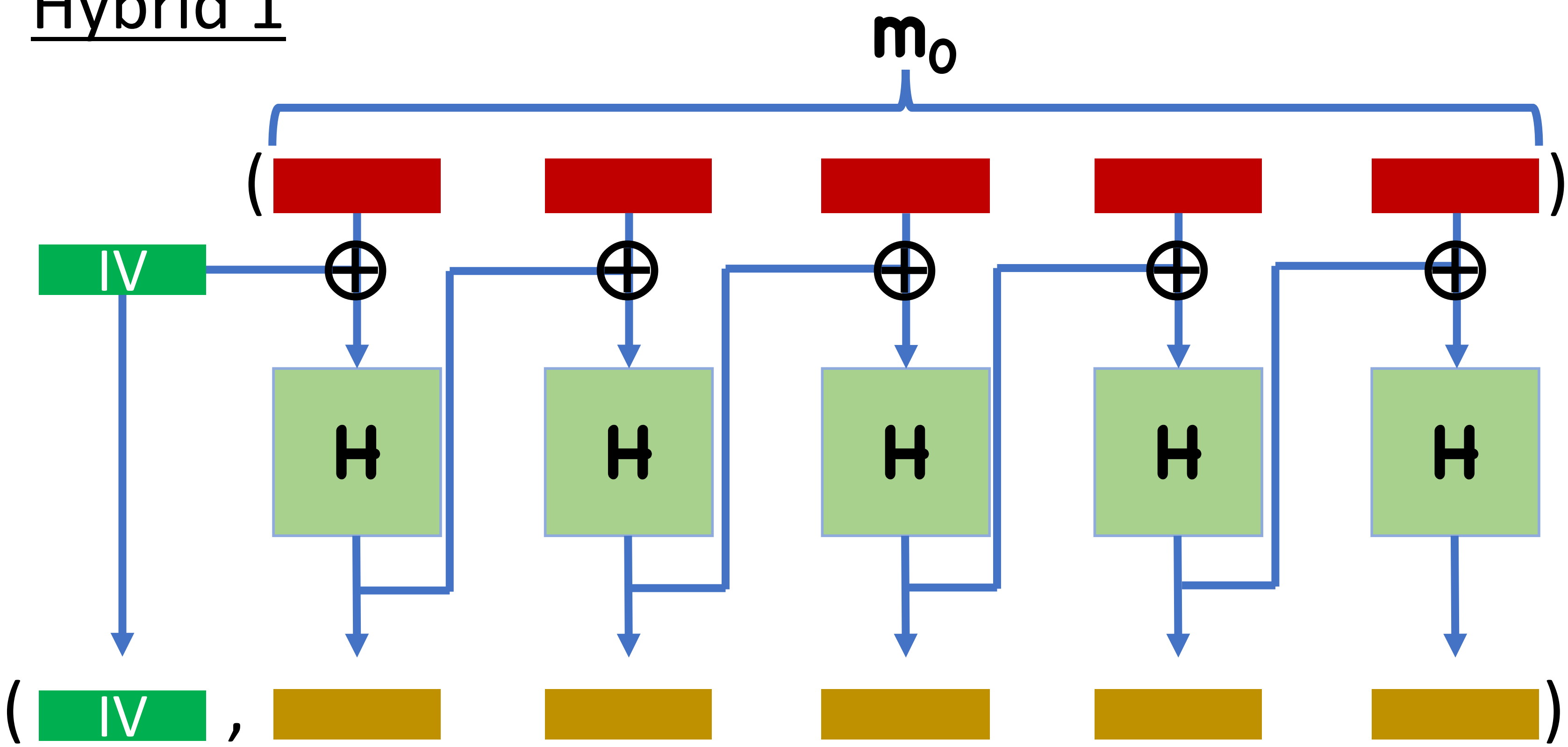
- Indistinguishable by PRP security

Same for Hybrids 2,3

All that is left is to show indistinguishability of 1,2

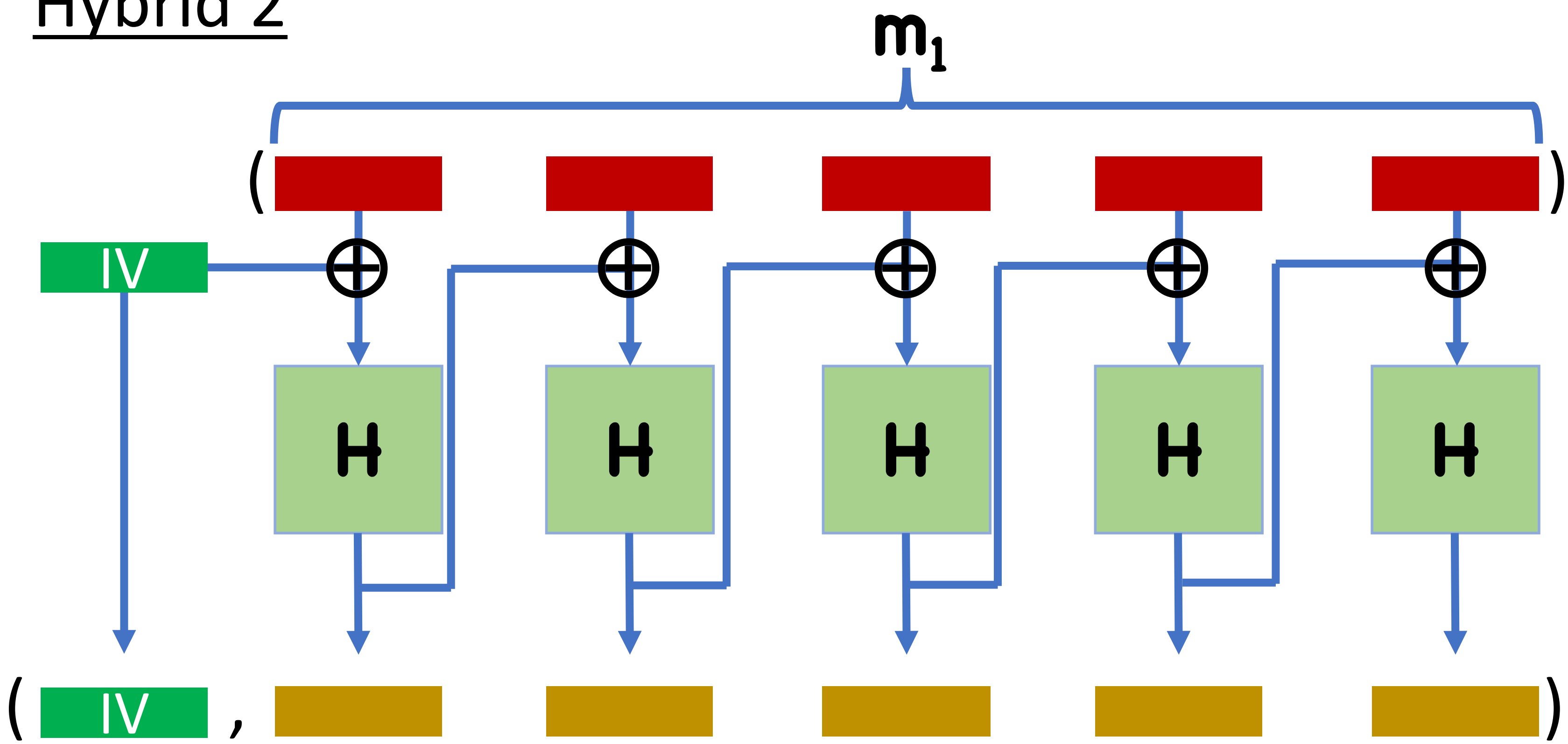
Proof Sketch

<u>Hybrid 1</u>



Proof Sketch

Hybrid 2



Proof Sketch

Idea:

- As long as, say, the sequence of left messages queried by  does not result in two calls to **F** on the same input, all outputs will be random (distinct) outputs
- For each message, first query to **F** will be uniformly random
- Second query gets XORed with output of first query to F $\Rightarrow$ $\approx$ uniformly random

Proof Sketch

Idea:

- Since queries to $\mathbf{F}$ are (essentially) uniformly random, probability of querying same input twice is exponentially small
- Ciphertexts will be essentially random
- True regardless of encrypting $\mathbf{m_0}$ or $\mathbf{m_1}$

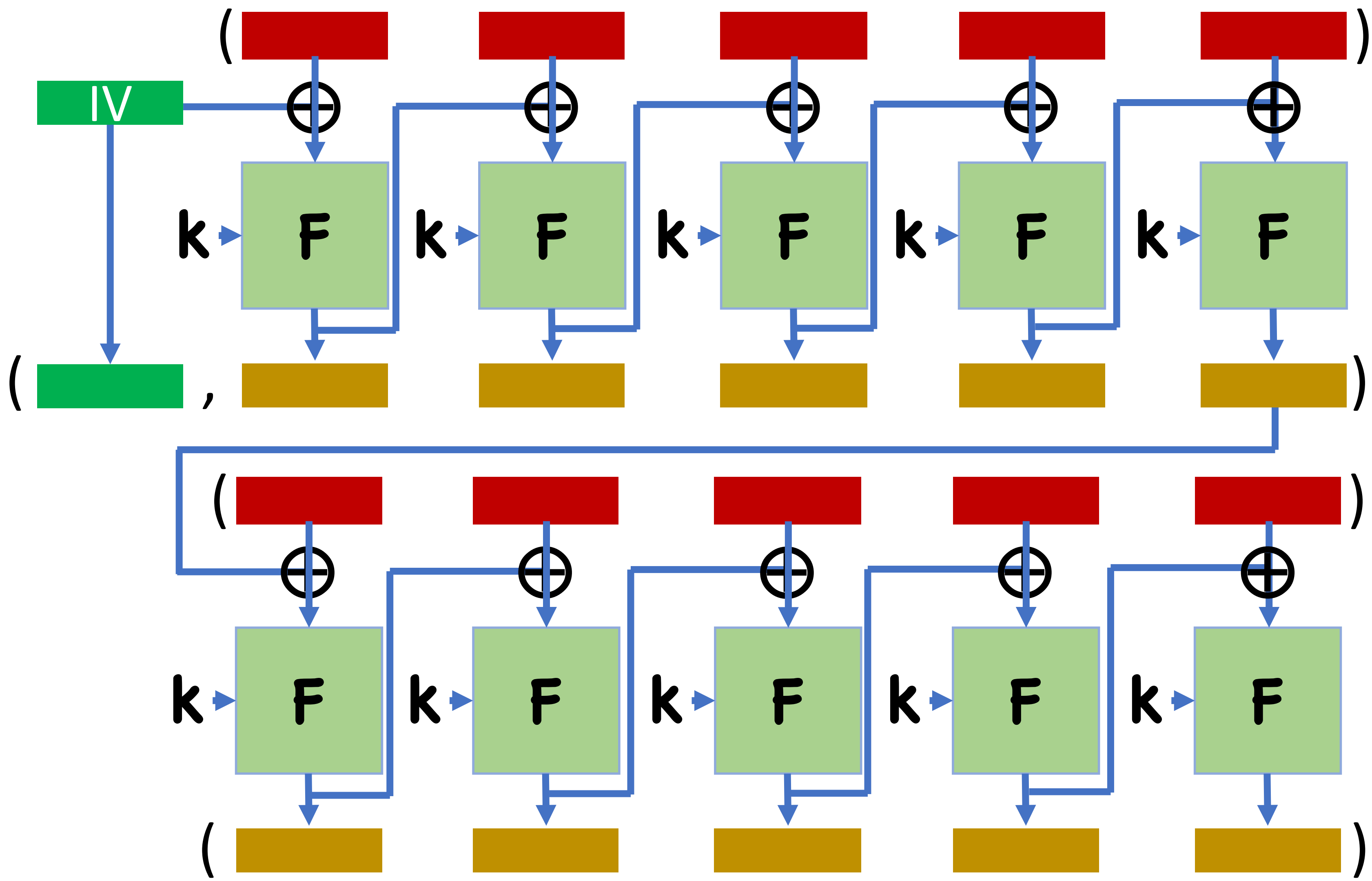
Stateful Variants of CBC

Chained CBC
- IV is set to last block of previous ciphertext

Deterministic IV
- Sender keeps a counter
- To encrypt, IV is set to counter, and counter is incremented

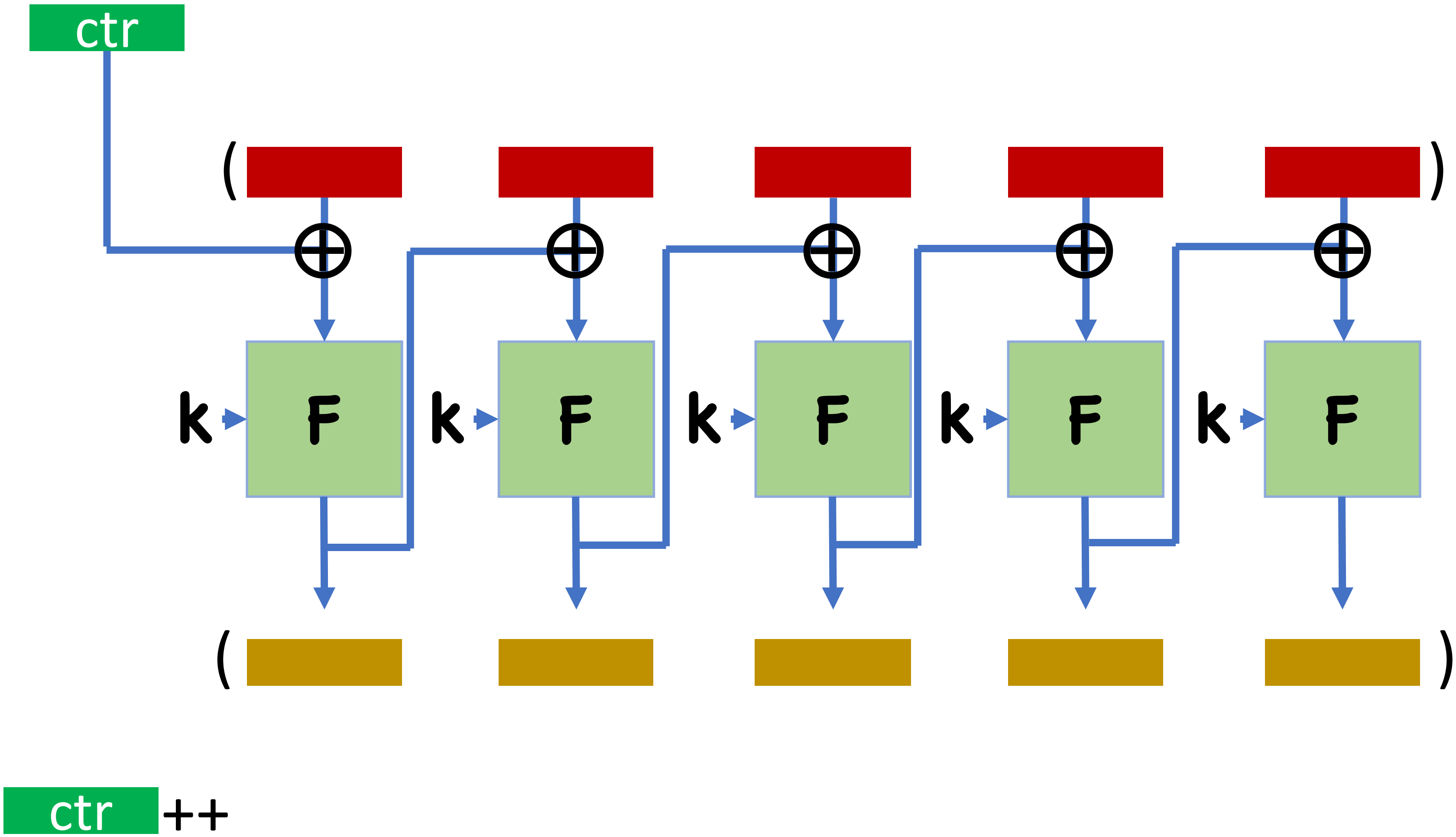
Both variants mean no need to send IV

Chained CBC



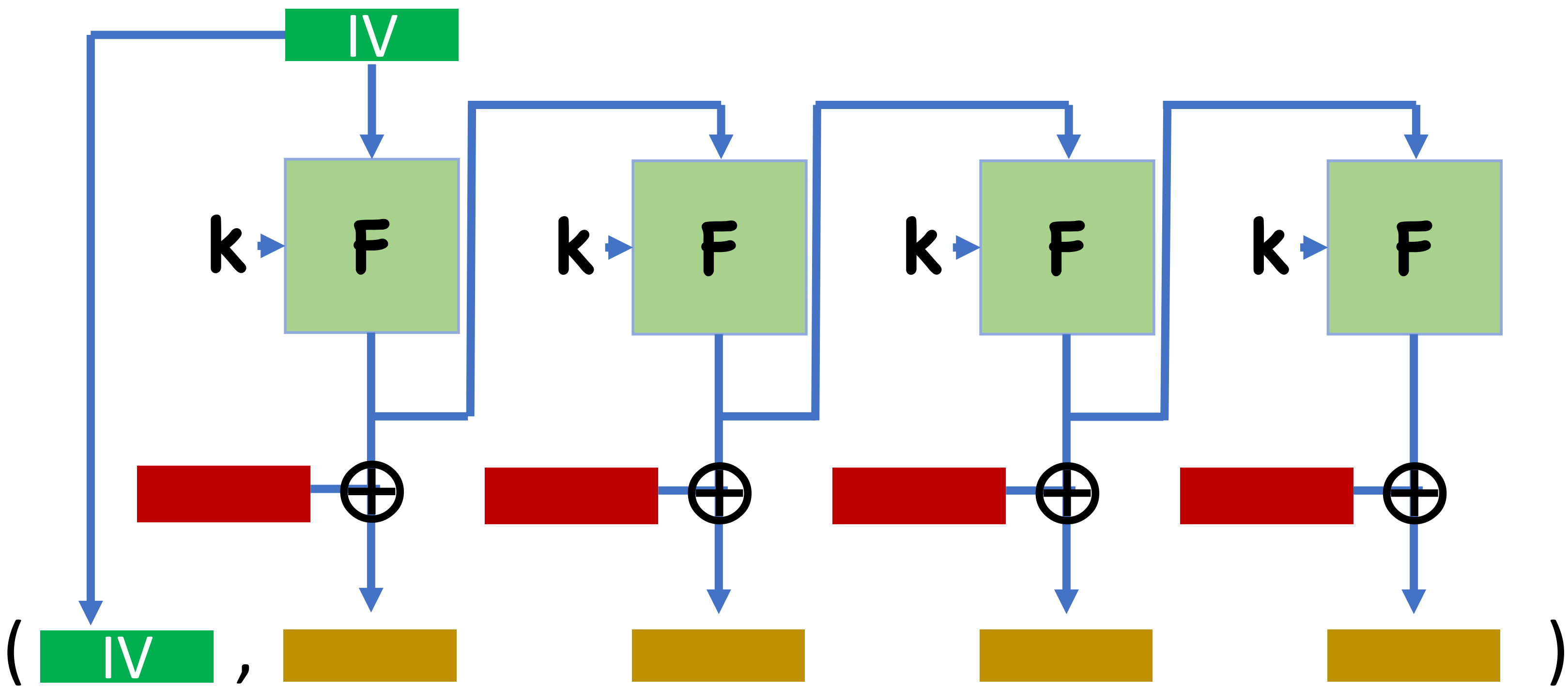
Is Chained CBC Secure?

Deterministic IV



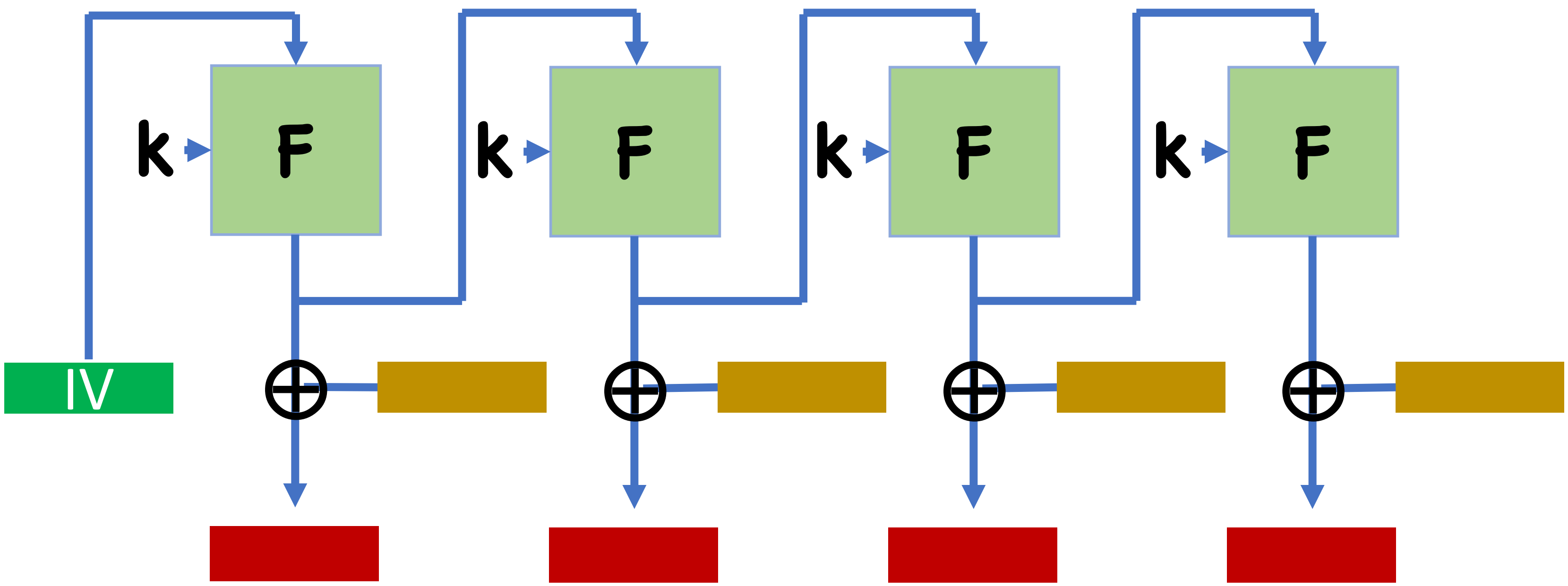
Is Deterministic IV Secure?

Output Feedback Mode (OFB)



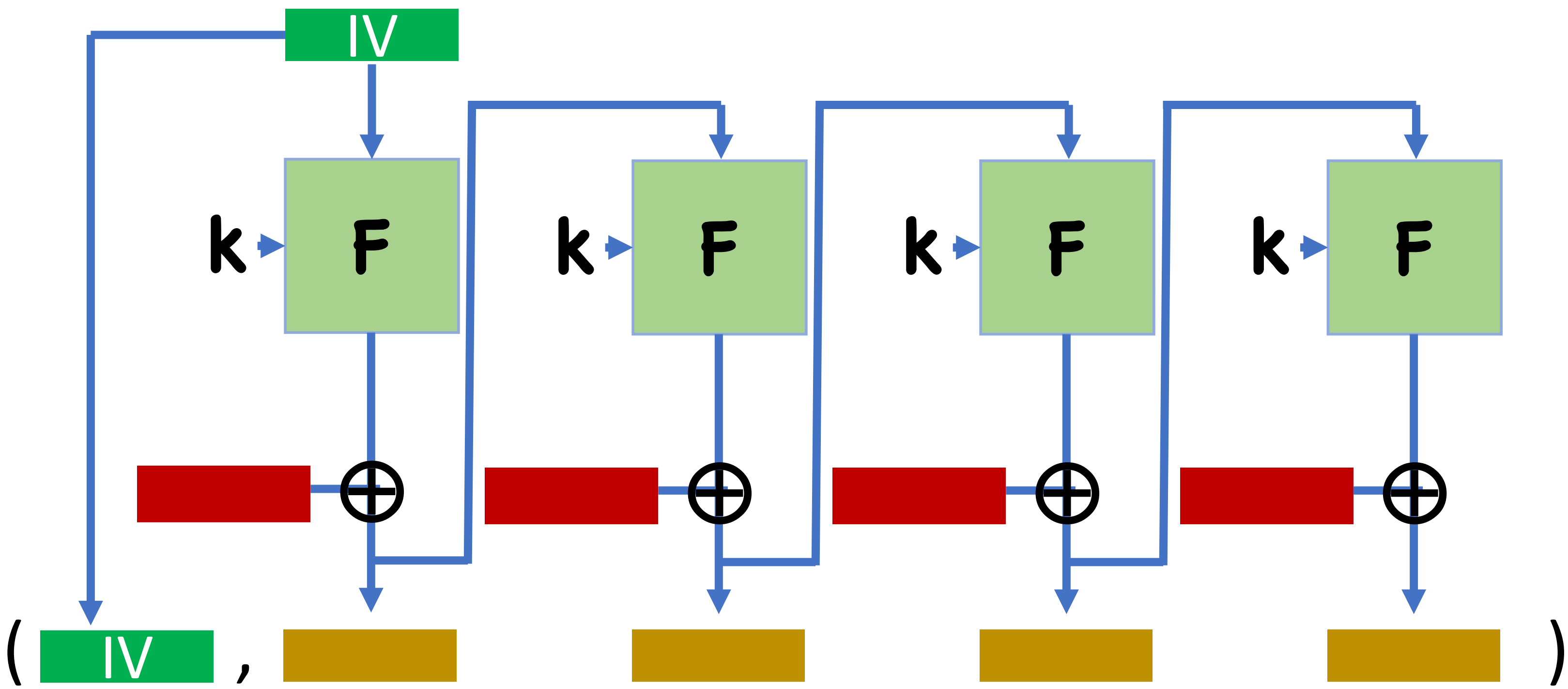
Turn block cipher into self stream cipher

OFB Decryption



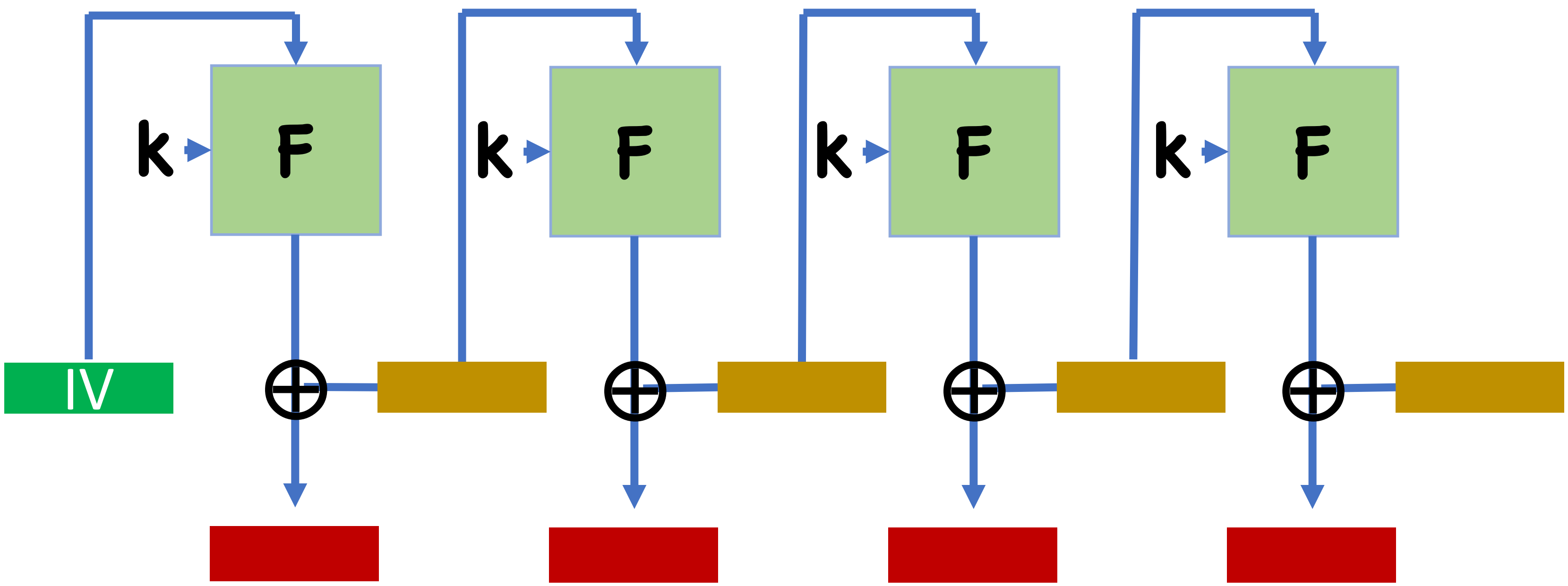
What happens if a block is lost in transmission?

Cipher Feedback (CFB)



Turn block cipher into **self-synchronizing** stream cipher

CFB Decryption



What happens if a block is lost in transmission?

Security of OFB, CFB modes

Security very similar to CBC

Define 4 hybrids

- 0: encrypt left messages
- 1: replace PRP with random permutation
- 2: encrypt right messages
- 3: replace random permutation with PRP

0,1 and 2,3 are indistinguishable by PRP security

1,2 are indistinguishable since ciphertexts are essentially random

Summary

PRPs/Block Ciphers

Modes of operations: ECB, Counter, CBC, OFB, CFB

Next Time

Constructing PRPs/block ciphers