Provable Security Basics
+
Selected topics in provable security of symmetric schemes

Tom Shrimpton
Portland State University

~~Provable Security Basics~~
~~+~~
~~Selected topics in provable security of symmetric schemes~~

The many faces of symmetric encryption, from a "provable-security" perspective

Tom Shrimpton
Portland State University

What kind of primitive
is encryption?

How do you know
a notion is any good?

Are all reasonable
notions equally good?

How do we find
security notions
for encryption?

How do you prove
a construction meets
a security notion?

The many faces of symmetric encryption, from a "provable-security" perspective

How do you build
an authenticated encryption
scheme?

[...]

Does sharing a key
provide a useful
authentication check?

Nonce-based encryption?
What's a nonce?

Building a “privacy-providing” primitive

“I want my communication with Bob to be private” -- Alice

What kind of “communication”?

SMS? Voice? Video? HTML? Javascript? Powerpoint slides? Financial data?

Building a "privacy-providing" primitive

"I want my communication with Bob to be private" -- Alice

What kind of "communication"?

SMS? Voice? Video? HTML? Javascript? Powerpoint slides? Financial data?

"Private" from whom?

A nosey eavesdropper, sniffing wireless packets in a coffee shop?

A business competitor, who pays an ISP to send your traffic for some analysis?

A nation/state agency, with huge computing resources and lots of "side information"?

Building a "privacy-providing" primitive

"I want my communication with Bob to be private" -- Alice

What kind of "communication"?

SMS? Voice? Video? HTML? Javascript? Powerpoint slides? Financial data?

"Private" from whom?

A nosey eavesdropper, sniffing wireless packets in a coffee shop?

A business competitor, who pays an ISP to send your traffic for some analysis?

A nation/state agency, with huge computing resources and lots of "side information"?

What do you mean by "private"?

No one (other than Bob) can recover the full contents of the communication?

No one can recover more than 1/2 of the contents? (Does it matter which $\frac{1}{2}$?)

No one can determine the "type" of the communication? (e.g. financial data vs. HTML)

…

What kind of "communication"?

SMS? Voice? Video? HTML? Javascript? Powerpoint slides? Financial data?

"All of that, and maybe other things, too."

"Private" from whom?

A nosey eavesdropper, sniffing wireless packets in a coffee shop?

A business competitor, who pays an ISP to send your traffic for some analysis?

A nation/state agency, with huge computing resources and lots of "side information"?

"From the most powerful attacker you can manage."

What do you mean by "private"?

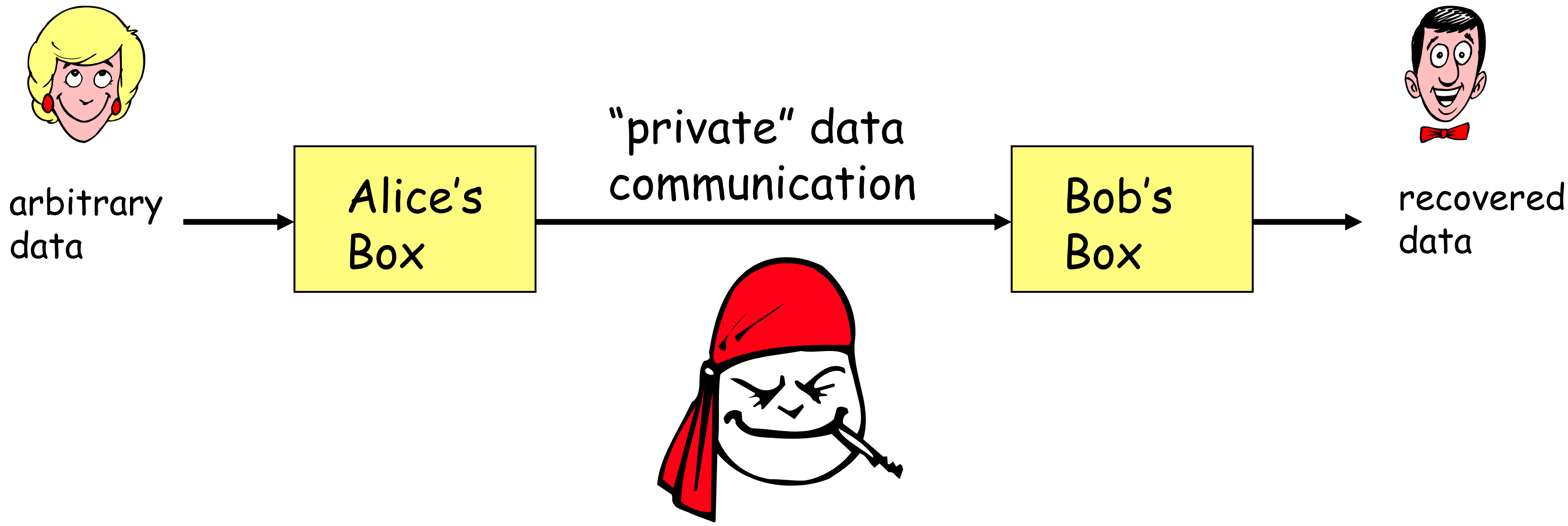
No one (other than Bob) can recover the full contents of the communication?

No one can recover more than 1/2 of the contents? (Does it matter which $\frac{1}{2}$?)

No one can determine the "type" of the communication? (e.g. financial data vs. HTML)

…

"You are annoying! Just make it work, and make sure it is fast, too."



API of Alice's Box

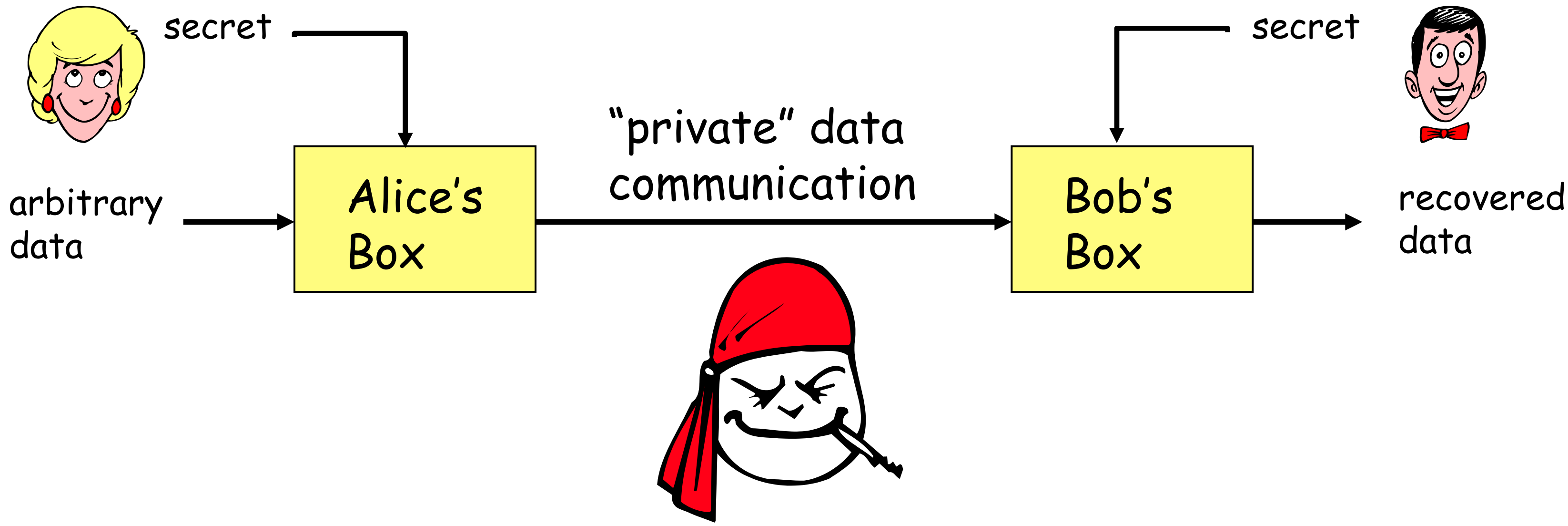
Inputs: 1. bitstrings of any length

Outputs: bitstrings of any length
(but as short as possible
to save communication costs)

API of Bob's Box

Inputs: 1. bitstrings of any length

Outputs: bitstrings of any length



API of Alice's Box

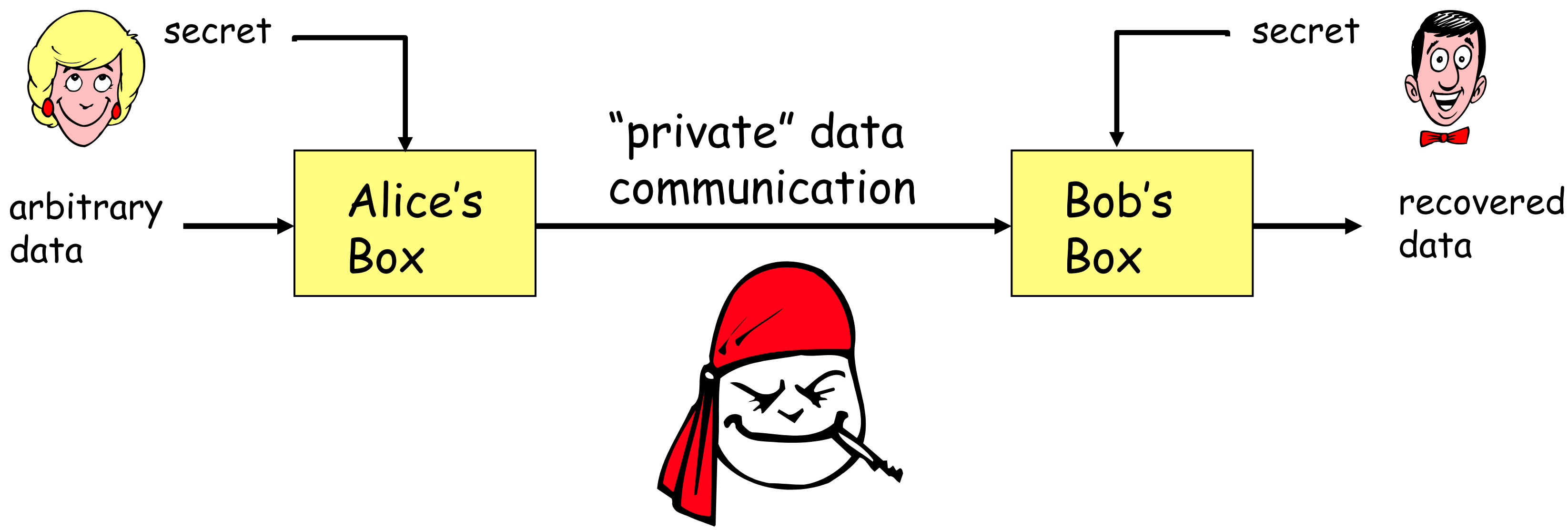
Inputs: 1. bitstrings of any length
2. something that the adversary does not know (the "secret")

Outputs: bitstrings of any length (but as short as possible to save communication costs)

API of Bob's Box

Inputs: 1. bitstrings of any length
2. something that the adversary does not know (the "secret")

Outputs: bitstrings of any length



API of Alice's Box

Inputs: 1. bitstrings of any length
2. something that the adversary does not know (the "secret")

Outputs: bitstrings of any length (but as short as possible to save communication costs)

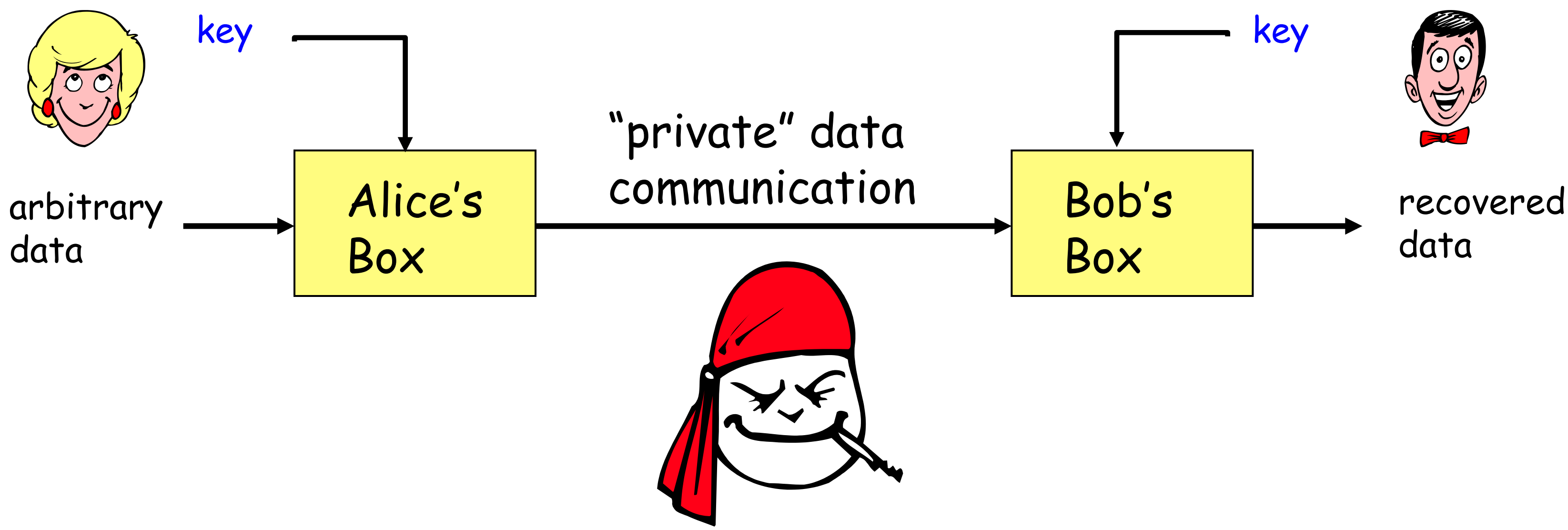
API of Bob's Box

Inputs: 1. bitstrings of any length
2. something that the adversary does not know (the "secret")

Outputs: bitstrings of any length

Should we assume that the adversary does not know the algorithms inside of Alice and Bob's boxes?

NO.



API of Alice's Box

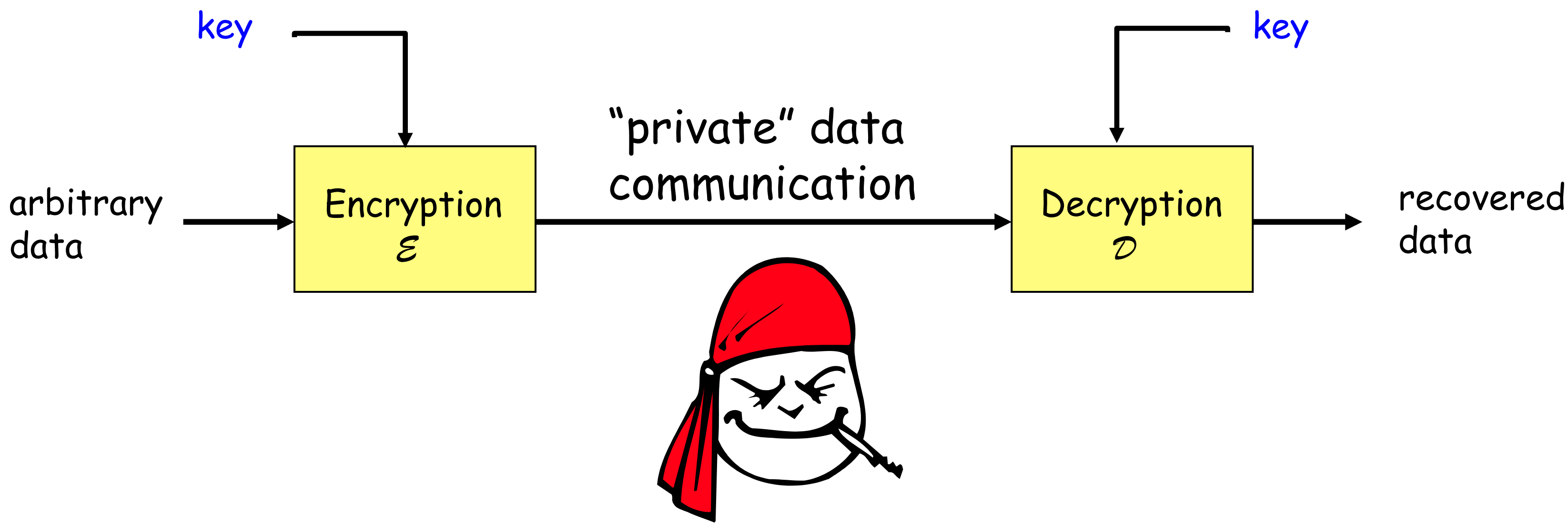
Inputs: 1. bitstrings of any length
2. a (short) secret "key"

Outputs: bitstrings of any length

API of Bob's Box

Inputs: 1. bitstrings of any length
2. a (short) secret "key"

Outputs: bitstrings of any length



API of Encryption

Inputs: 1. bitstrings of any length
2. a (short) secret "key"

Outputs: bitstrings of any length

API of Decryption

Inputs: 1. bitstrings of any length
2. a (short) secret "key"

Outputs: bitstrings of any length

An Encryption Scheme is a triple of algorithms $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$

Key-generation algorithm

$\mathcal{K}$ samples from a set of the same name

Encryption algorithm

$$\mathcal{E} : \mathcal{K} \times \{0,1\}^* \to \{0,1\}^* \cup \{\perp\}$$

key plaintext ciphertext "invalid"

Decryption algorithm

$$\mathcal{D} : \mathcal{K} \times \{0,1\}^* \to \{0,1\}^*$$

An Encryption Scheme is a triple of algorithms $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$

Key-generation algorithm

$\mathcal{K}$ samples from a set of the same name

Encryption algorithm

$\mathcal{E}\colon \mathcal{K} \times \{0,1\}^* \to \{0,1\}^* \cup \{\perp\}$

May be randomized or stateful

$C \xleftarrow{\$} \mathcal{E}_K(M)$

Decryption algorithm

$\mathcal{D}\colon \mathcal{K} \times \{0,1\}^* \to \{0,1\}^*$

Always deterministic

$M \leftarrow \mathcal{D}_K(C)$

An Encryption Scheme is a triple of algorithms $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$

Key-generation algorithm $\mathcal{K}$ samples from a set of the same name

Encryption algorithm $\mathcal{E}: \mathcal{K} \times \{0,1\}^* \to \{0,1\}^* \cup \{\perp\}$

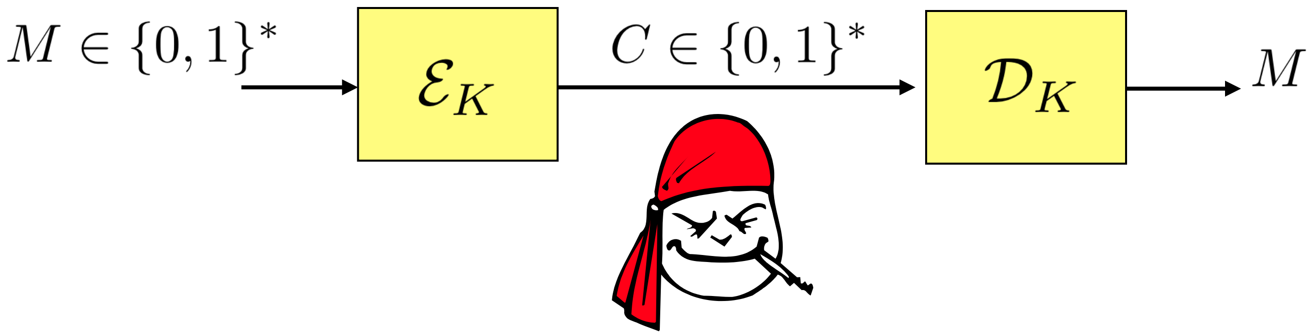
Decryption algorithm $\mathcal{D}: \mathcal{K} \times \{0,1\}^* \to \{0,1\}^*$

Correctness condition:

For all K,M such that $\mathcal{E}(K,M) \neq \perp$, Pr[$\mathcal{D}(K, \mathcal{E}(K,M)) = M$] = 1

over coins of encryption alg.

Developing a notion of “privacy”



1. What kinds of things do we want to prevent the adversary from achieving?

Adversary tries to:

recover the key

recover the plaintext

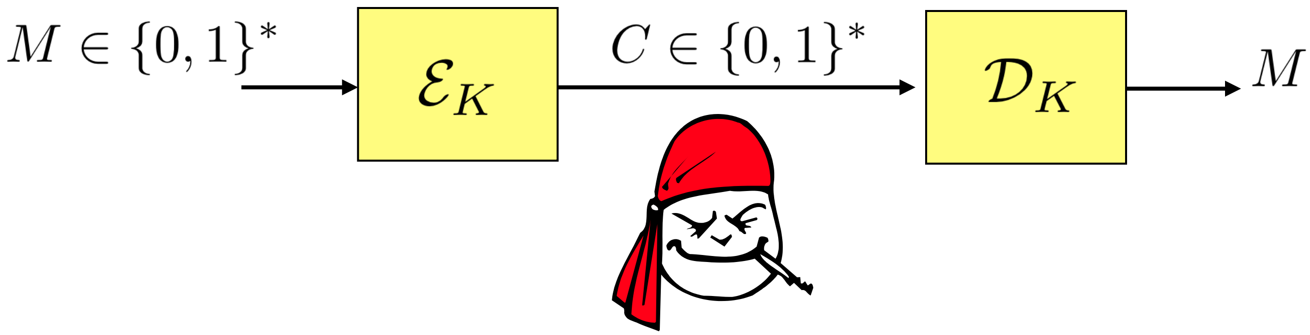
determine if this plaintext was sent before

determine the parity of the plaintext

determine if the first and last half of the
plaintext are the same

…

Developing a notion of "privacy"



1. What kinds of things do we want to prevent the adversary from achieving?

Adversary tries to:

recover the key

recover the plaintext

determine if this plaintext was sent before

determine the parity of the plaintext

determine if the first and last half of the plaintext are the same

…

2. What can the adversary "do" with respect to M and C in it's attack?

Adversary can:

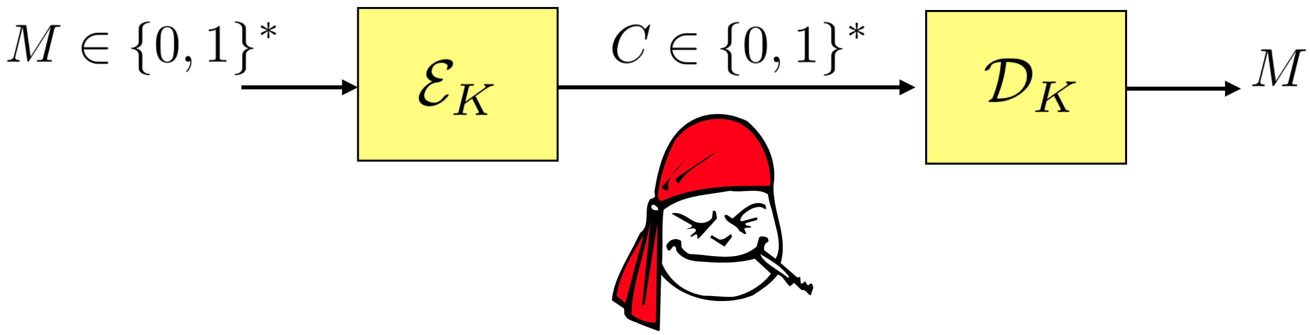
observe ciphertexts

observe plaintexts and ciphertexts

pick the plaintexts, and then see the corresponding ciphertexts

adaptively pick the plaintexts, and see the corresponding ciphertexts

Developing a notion of "privacy"



1. What kinds of things do we want to prevent the adversary from achieving?

Adversary tries to:

recover the key

recover the plaintext

determine if this plaintext was sent before

determine the parity of the plaintext

determine if the first and last half of the plaintext are the same

…

2. What can the adversary "do" with respect to M and C in it's attack?

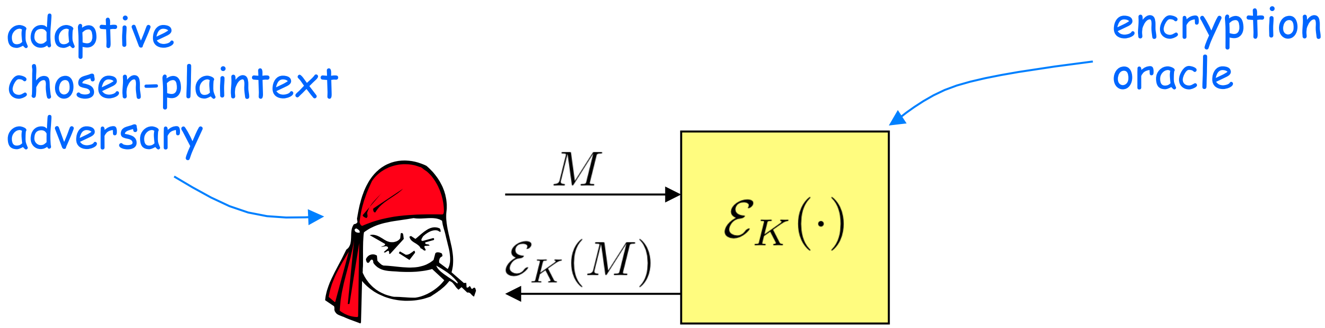
Adversary can:

observe ciphertexts

observe plaintexts and ciphertexts

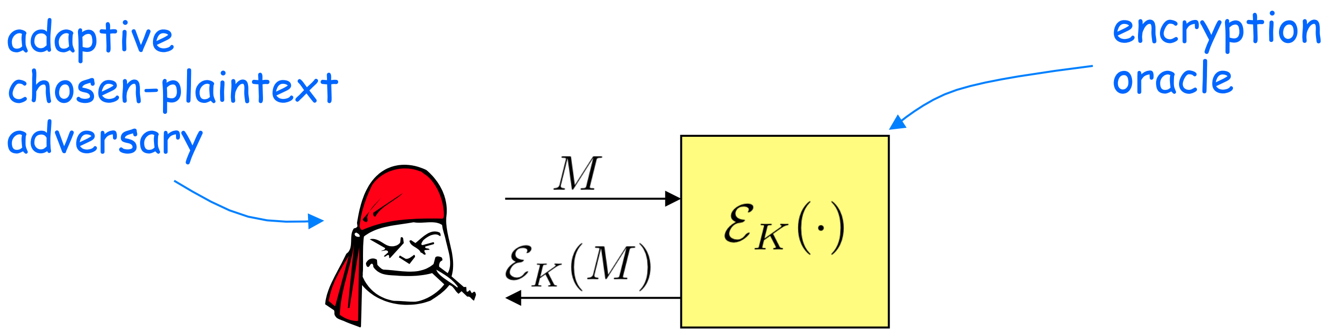
pick the plaintexts, and then see the corresponding ciphertexts

adaptively pick the plaintexts, and see the corresponding ciphertexts



Communication is private if…

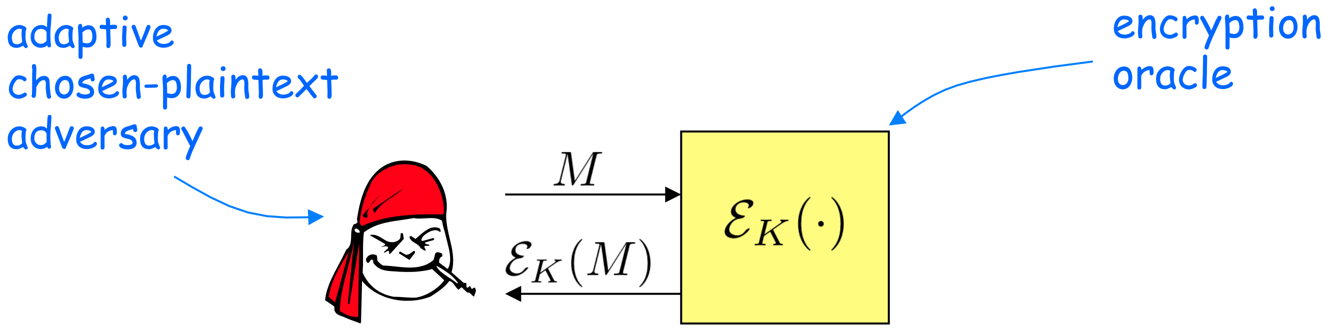
Adversary can't recover the key



Communication is private if…

Adversary can't recover the key

✗ $\mathcal{E}_K(M) = M$

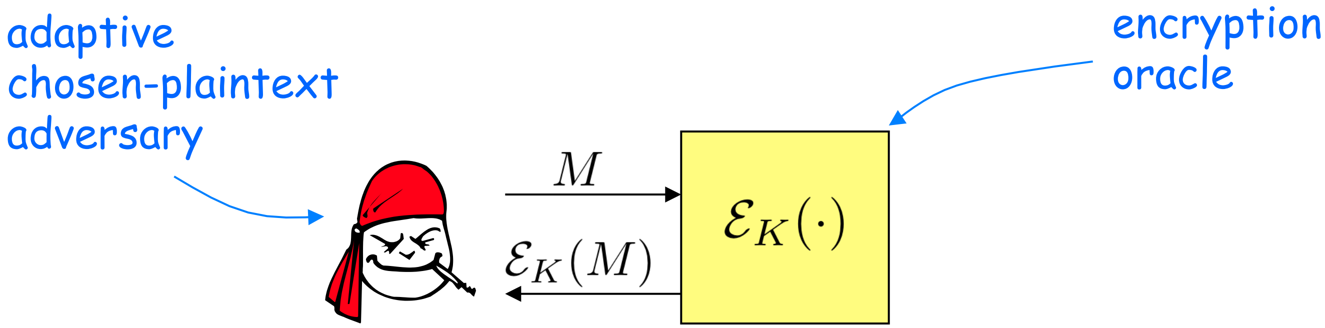


Communication is private if…

Adversary can't recover the key

✗ $\mathcal{E}_K(M) = M$

Adversary can't recover the plaintext



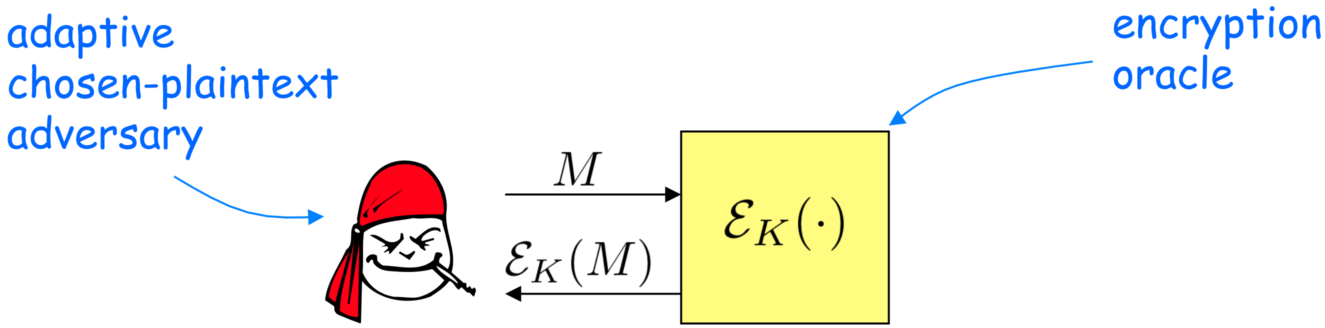
Communication is private if…

Adversary can't recover the key

✗ $\mathcal{E}_K(M) = M$

Adversary can't recover the plaintext

✗ $\mathcal{E}_K(M) = M[1..10] || \text{random looking bits}$



Communication is private if…

Adversary can't recover the key

✗ $\mathcal{E}_K(M) = M$

Adversary can't recover the plaintext

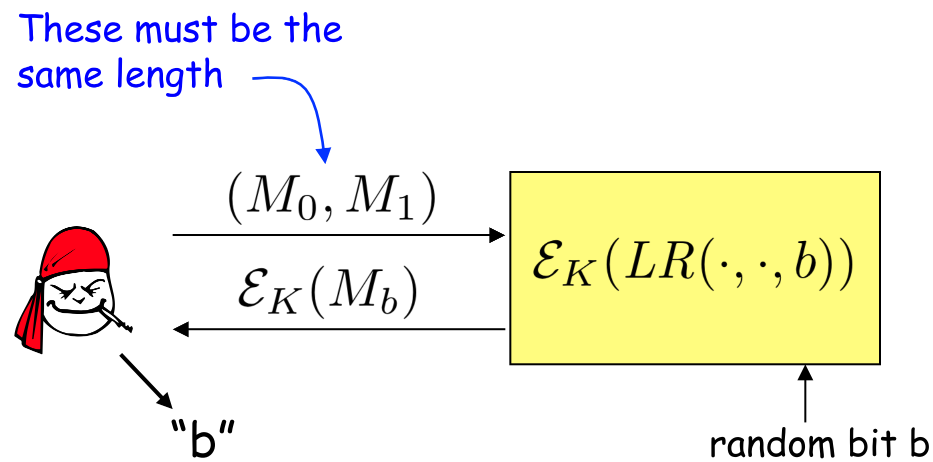
✗ $\mathcal{E}_K(M) = M[1..10] || \text{random looking bits}$

"Anything that is efficiently computable about the plaintexts *given* the ciphertexts is efficiently computable *without* seeing the ciphertexts."

Indistinguishability of ciphertexts under an adaptive chosen-plaintext attack (IND-CPA)

$\underline{\mathrm{Exp}_{\Pi}^{\mathrm{ind\text{-}cpa}}(A):}$

$K \stackrel{\$}{\leftarrow} \mathcal{K}$
$b \stackrel{\$}{\leftarrow} \{0,1\}$
$b' \stackrel{\$}{\leftarrow} A^{\mathcal{E}_K(LR(\cdot,\cdot,b))}$
If $b' = b$ then Return 1
Return 0



Indistinguishability of ciphertexts under an adaptive chosen-plaintext attack (IND-CPA)

$\underline{\mathrm{Exp}_{\Pi}^{\text{ind-cpa}}(A):}$

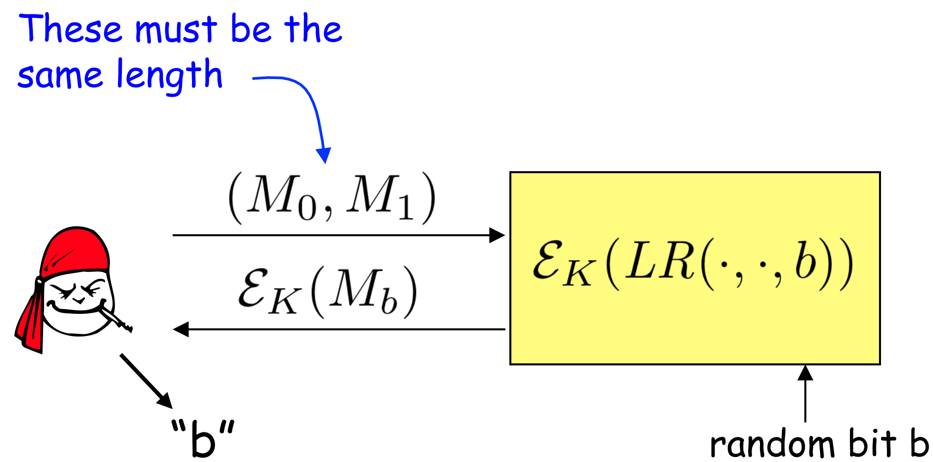
$K \xleftarrow{\$} \mathcal{K}$

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

$b' \xleftarrow{\$} A^{\mathcal{E}_K(LR(\cdot,\cdot,b))}$

If $b' = b$ then Return 1

Return 0



$$\mathrm{Adv}_{\Pi}^{\text{ind-cpa}}(A) = 2\Pr\left(\mathrm{Exp}_{\Pi}^{\text{ind-cpa}}(A) = 1\right) - 1$$

Adversarial "resources":
- the number of oracle queries, q
- the total length in bits of the queries, μ
- the time-complexity of the adversary, t

Exploring IND-CPA

$\underline{\mathrm{Exp}_{\Pi}^{\text{ind-cpa}}(A)\text{:}}$

$K \xleftarrow{\$} \mathcal{K}$
$b \xleftarrow{\$} \{0,1\}$
$b' \xleftarrow{\$} A^{\mathcal{E}_K(LR(\cdot,\cdot,b))}$
If $b' = b$ then Return 1
Return 0

$$\mathrm{Adv}_{\Pi}^{\text{ind-cpa}}(A) = 2\Pr\left(\mathrm{Exp}_{\Pi}^{\text{ind-cpa}}(A) = 1\right) - 1$$

We say $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is IND-CPA secure if the IND-CPA advantage is "small" for all "resource efficient" adversaries

example: adversaries A with

$$t = 2^{20},\ q = 2^{30},\ \mu = 2^{30}$$

achieve advantage at most

$$\mathrm{Adv}_{\Pi}^{\text{ind-cpa}}(A) \leq \frac{1}{2^{40}}$$

But what "small" and "reasonable" mean is up to the user!

Exploring IND-CPA

$\underline{\mathrm{Exp}_{\Pi}^{\text{ind-cpa}}(A):}$

$K \stackrel{\$}{\leftarrow} \mathcal{K}$

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

$b' \stackrel{\$}{\leftarrow} A^{\mathcal{E}_K(LR(\cdot,\cdot,b))}$

If $b' = b$ then Return 1

Return 0

$$\mathrm{Adv}_{\Pi}^{\text{ind-cpa}}(A) = 2\Pr\left(\mathrm{Exp}_{\Pi}^{\text{ind-cpa}}(A) = 1\right) - 1$$

Can this scheme be IND-CPA secure? $\mathcal{E}_K(M) = M$

Exploring IND-CPA

$\underline{\mathrm{Exp}_{\Pi}^{\text{ind-cpa}}(A)\text{:}}$

$K \stackrel{\$}{\leftarrow} \mathcal{K}$

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

$b' \stackrel{\$}{\leftarrow} A^{\mathcal{E}_K(LR(\cdot,\cdot,b))}$

If $b' = b$ then Return 1

Return 0

$$\mathrm{Adv}_{\Pi}^{\text{ind-cpa}}(A) = 2\Pr\left(\mathrm{Exp}_{\Pi}^{\text{ind-cpa}}(A) = 1\right) - 1$$

Can this scheme be IND-CPA secure? $\mathcal{E}_K(M) = M$

Adversary A:

fix distinct strings M_0, M_1 of the same length

ask query (M_0, M_1)

if oracle response $C = M_0$ then return 0

else return 1

Exploring IND-CPA

$\underline{\mathrm{Exp}_{\Pi}^{\text{ind-cpa}}(A):}$

$K \xleftarrow{\$} \mathcal{K}$
$b \xleftarrow{\$} \{0,1\}$
$b' \xleftarrow{\$} A^{\mathcal{E}_K(LR(\cdot,\cdot,b))}$
If $b' = b$ then Return 1
Return 0

$$\mathrm{Adv}_{\Pi}^{\text{ind-cpa}}(A) = 2\Pr\left(\mathrm{Exp}_{\Pi}^{\text{ind-cpa}}(A) = 1\right) - 1$$

Can any deterministic scheme be IND-CPA secure?

Exploring IND-CPA

$\underline{\text{Exp}_{\Pi}^{\text{ind-cpa}}(A):}$

$K \xleftarrow{\$} \mathcal{K}$

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

$b' \xleftarrow{\$} A^{\mathcal{E}_K(LR(\cdot,\cdot,b))}$

If $b' = b$ then Return 1

Return 0

$$\text{Adv}_{\Pi}^{\text{ind-cpa}}(A) = 2\Pr\left(\text{Exp}_{\Pi}^{\text{ind-cpa}}(A) = 1\right) - 1$$

Can any deterministic scheme be IND-CPA secure?

Adversary A:

fix distinct strings M_0, M_1 of the same length

ask query (M_0, M_1), receiving C_1 in return

ask query (M_0, M_0), receiving C_2 in return

if $C_1 = C_2$ then return 0

else return 1

An alternative definition of privacy: “Real or Random” (RoR-CPA)

$\underline{\mathrm{Exp}_{\Pi}^{\mathrm{ror\text{-}cpa}}(A)}$:

$K \xleftarrow{\$} \mathcal{K}$
$b \xleftarrow{\$} \{0,1\}$
$b' \xleftarrow{\$} A^{\mathcal{O}(\cdot)}$
If $b' = b$ then Return 1
Return 0

$\underline{\text{Oracle } \mathcal{O}(M)}$:

$M' \xleftarrow{\$} \{0,1\}^{|M|}$
If $b = 0$ then Return $\mathcal{E}_K(M')$
Return $\mathcal{E}_K(M)$

$$\mathrm{Adv}_{\Pi}^{\mathrm{ror\text{-}cpa}}(A) = 2\Pr\left(\mathrm{Exp}_{\Pi}^{\mathrm{ror\text{-}cpa}}(A) = 1\right) - 1$$

Adversarial “resources”:

- the number of oracle queries, q
- the total length in bits of the queries, μ
- the time-complexity of the adversary, t

Which notion is "better": RoR-CPA or IND-CPA?

$\underline{\mathrm{Exp}_{\Pi}^{\text{ror-cpa}}(A)\text{:}}$

$K \xleftarrow{\$} \mathcal{K}$
$b \xleftarrow{\$} \{0,1\}$
$b' \xleftarrow{\$} A^{\mathcal{O}(\cdot)}$
If $b' = b$ then Return 1
Return 0

$\underline{\text{Oracle } \mathcal{O}(M)\text{:}}$

$M' \xleftarrow{\$} \{0,1\}^{|M|}$
If $b = 0$ then Return $\mathcal{E}_K(M')$
Return $\mathcal{E}_K(M)$

$\underline{\mathrm{Exp}_{\Pi}^{\text{ind-cpa}}(A)\text{:}}$

$K \xleftarrow{\$} \mathcal{K}$
$b \xleftarrow{\$} \{0,1\}$
$b' \xleftarrow{\$} A^{\mathcal{O}(\cdot)}$
If $b' = b$ then Return 1
Return 0

$\underline{\text{Oracle } \mathcal{O}(M_0, M_1)\text{:}}$

If $b = 0$ then Return $\mathcal{E}_K(M_0)$
Return $\mathcal{E}_K(M_1)$

Claim: Any encryption scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ that is IND-CPA secure, is also RoR-CPA secure

Claim: Any encryption scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ that is IND-CPA secure, is also RoR-CPA secure

---

Proof idea: show the contrapositive, if a scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is not RoR-CPA secure, then it is not IND-CPA secure.

Claim: Any encryption scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ that is IND-CPA secure, is also RoR-CPA secure

---

Proof idea: show the contrapositive, if a scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is not RoR-CPA secure, then it is not IND-CPA secure.

Let A be an efficient RoR-CPA adversary, gaining advantage $\mathrm{Adv}_{\Pi}^{\mathrm{ror\text{-}cpa}}(A)$

We build an efficient IND-CPA adversary B, that runs A as a "black-box" subroutine, that gains advantage

$$\mathrm{Adv}_{\Pi}^{\mathrm{ind\text{-}cpa}}(B) \geq \mathrm{Adv}_{\Pi}^{\mathrm{ror\text{-}cpa}}(A)$$

Claim: Any encryption scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ that is IND-CPA secure, is also RoR-CPA secure

---

Proof idea: show the contrapositive, if a scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is not RoR-CPA secure, then it is not IND-CPA secure.

Let A be an efficient RoR-CPA adversary, gaining advantage $\mathrm{Adv}_{\Pi}^{\mathrm{ror\text{-}cpa}}(A)$

We build an efficient IND-CPA adversary B, that runs A as a "black-box" subroutine, that gains advantage

$$\mathrm{Adv}_{\Pi}^{\mathrm{ind\text{-}cpa}}(B) \geq \mathrm{Adv}_{\Pi}^{\mathrm{ror\text{-}cpa}}(A)$$

Conclusion: if $\mathrm{Adv}_{\Pi}^{\mathrm{ind\text{-}cpa}}(B)$ is small for all efficient B, then $\mathrm{Adv}_{\Pi}^{\mathrm{ror\text{-}cpa}}(A)$ must be small, too

$$\frac{1}{2}\mathbf{Adv}_{\Pi}^{\mathrm{ror\text{-}cpa}}(A) + \frac{1}{2} \quad \leq \quad \Pr(\mathbf{Exp}_{\Pi}^{\mathrm{ror\text{-}cpa}}(A) = 1)$$

So, we start with
an RoR-adversary A
that gains some
RoR advantage

$$\frac{1}{2}\mathbf{Adv}_{\Pi}^{\text{ror-cpa}}(A) + \frac{1}{2} \quad \leq \quad \Pr(\mathbf{Exp}_{\Pi}^{\text{ror-cpa}}(A) = 1)$$

<u>$\mathbf{Exp}_{\Pi}^{\text{ror-cpa}}(A)$:</u>

$K \stackrel{\$}{\leftarrow} \mathcal{K}$

$d \stackrel{\$}{\leftarrow} \{0,1\}$

$d' \stackrel{\$}{\leftarrow} A^{\mathcal{O}(\cdot)}$

If $d' = d$ then Return 1

Return 0

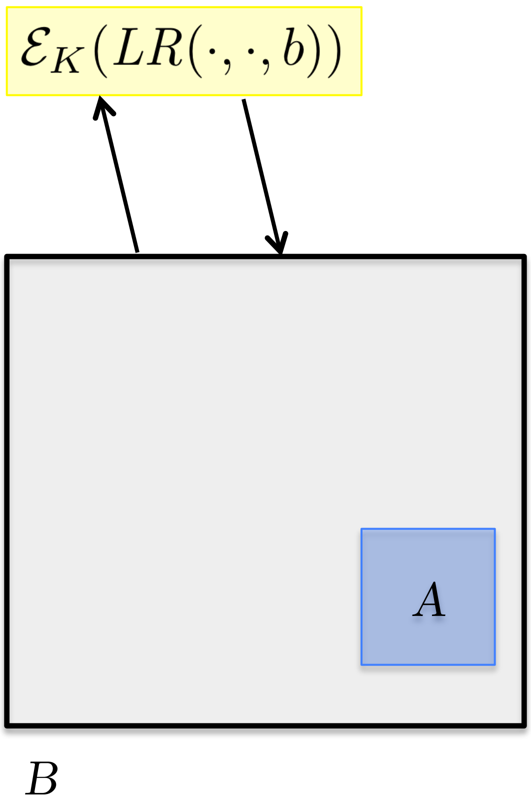
<u>Oracle $\mathcal{O}(M)$:</u>

$M' \stackrel{\$}{\leftarrow} \{0,1\}^{|M|}$

If $d = 0$ then Return $\mathcal{E}_K(M')$

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

$$\frac{1}{2}\mathbf{Adv}_{\Pi}^{\text{ror-cpa}}(A) + \frac{1}{2} \quad \leq \quad \Pr(\mathbf{Exp}_{\Pi}^{\text{ror-cpa}}(A) = 1)$$



$\mathbf{Exp}_{\Pi}^{\text{ror-cpa}}(A)$:

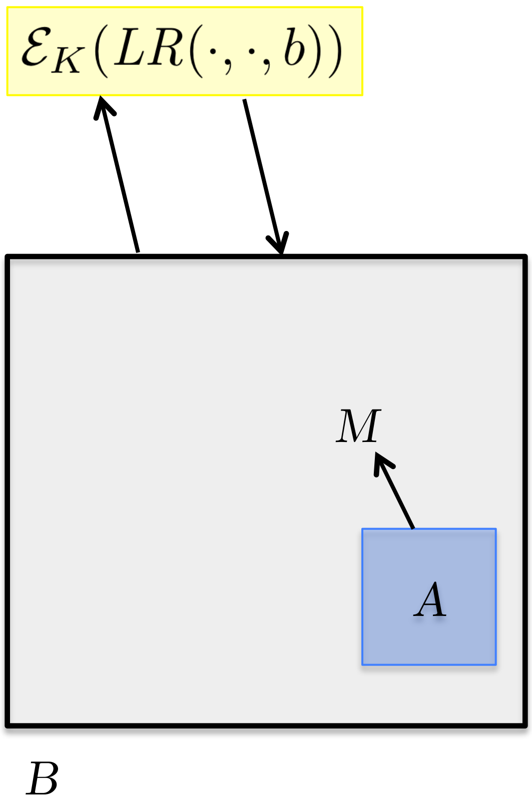
$K \xleftarrow{\$} \mathcal{K}$
$d \xleftarrow{\$} \{0,1\}$
$d' \xleftarrow{\$} A^{\mathcal{O}(\cdot)}$
If $d' = d$ then Return 1
Return 0

Oracle $\mathcal{O}(M)$:

$M' \xleftarrow{\$} \{0,1\}^{|M|}$
If $d = 0$ then Return $\mathcal{E}_K(M')$
Return $\mathcal{E}_K(M)$

Want to build a good IND-CPA adversary B
by running A and simulating its expected experiment

$$\frac{1}{2}\mathbf{Adv}^{\text{ror-cpa}}_{\Pi}(A) + \frac{1}{2} \quad \le \quad \Pr(\mathbf{Exp}^{\text{ror-cpa}}_{\Pi}(A) = 1)$$



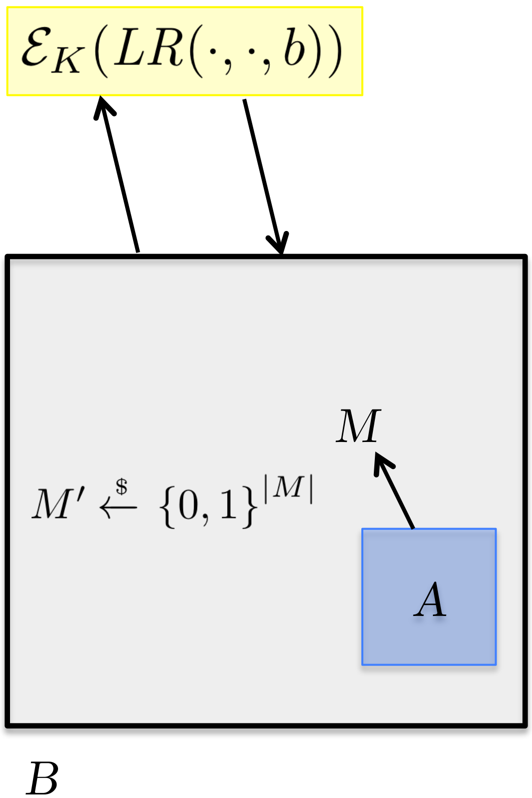
<u>$\mathbf{Exp}^{\text{ror-cpa}}_{\Pi}(A)$:</u>

$K \xleftarrow{\$} \mathcal{K}$
$d \xleftarrow{\$} \{0,1\}$
$d' \xleftarrow{\$} A^{\mathcal{O}(\cdot)}$
If $d' = d$ then Return 1
Return 0

<u>Oracle $\mathcal{O}(M)$:</u>

$M' \xleftarrow{\$} \{0,1\}^{|M|}$
If $d = 0$ then Return $\mathcal{E}_K(M')$
Return $\mathcal{E}_K(M)$

$$\frac{1}{2}\mathbf{Adv}_{\Pi}^{\text{ror-cpa}}(A) + \frac{1}{2} \quad \leq \quad \Pr(\mathbf{Exp}_{\Pi}^{\text{ror-cpa}}(A) = 1)$$



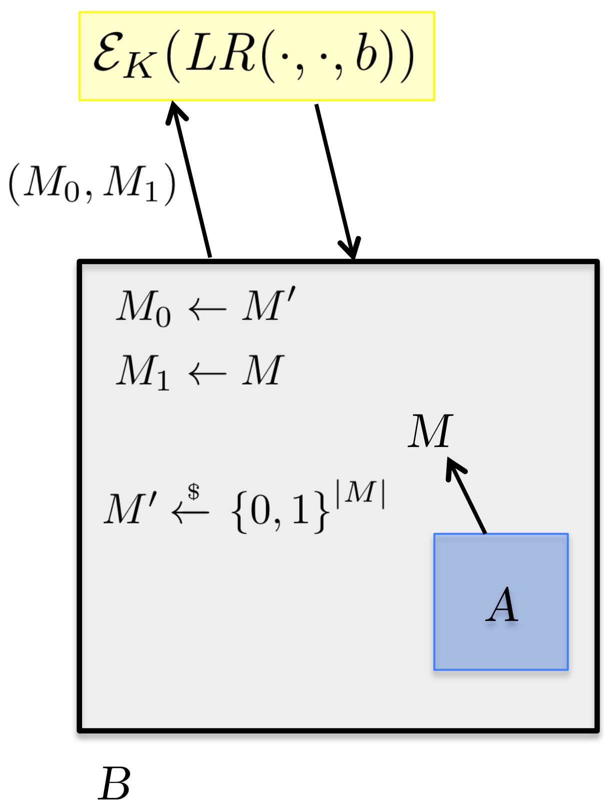
$\mathbf{Exp}_{\Pi}^{\text{ror-cpa}}(A)$:

$K \stackrel{\$}{\leftarrow} \mathcal{K}$
$d \stackrel{\$}{\leftarrow} \{0,1\}$
$d' \stackrel{\$}{\leftarrow} A^{\mathcal{O}(\cdot)}$
If $d' = d$ then Return 1
Return 0

Oracle $\mathcal{O}(M)$:

$M' \stackrel{\$}{\leftarrow} \{0,1\}^{|M|}$
If $d = 0$ then Return $\mathcal{E}_K(M')$
Return $\mathcal{E}_K(M)$

$$\frac{1}{2}\mathbf{Adv}_{\Pi}^{\text{ror-cpa}}(A) + \frac{1}{2} \quad \leq \quad \Pr(\mathbf{Exp}_{\Pi}^{\text{ror-cpa}}(A) = 1)$$



$\mathbf{Exp}_{\Pi}^{\text{ror-cpa}}(A)$:

$K \xleftarrow{\$} \mathcal{K}$

$d \xleftarrow{\$} \{0,1\}$

$d' \xleftarrow{\$} A^{\mathcal{O}(\cdot)}$

If $d' = d$ then Return 1

Return 0

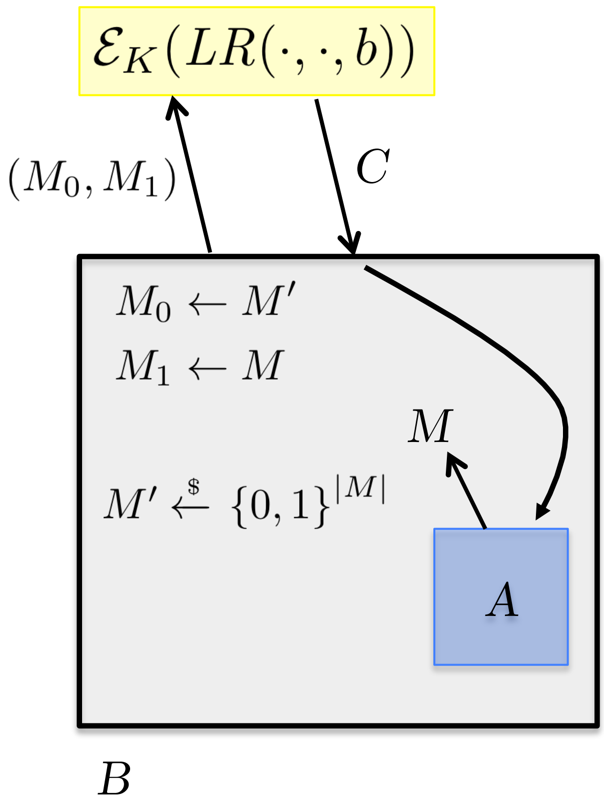
Oracle $\mathcal{O}(M)$:

$M' \xleftarrow{\$} \{0,1\}^{|M|}$

If $d = 0$ then Return $\mathcal{E}_K(M')$

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

$$\frac{1}{2}\mathbf{Adv}^{\text{ror-cpa}}_{\Pi}(A) + \frac{1}{2} \quad \leq \quad \Pr(\mathbf{Exp}^{\text{ror-cpa}}_{\Pi}(A) = 1)$$



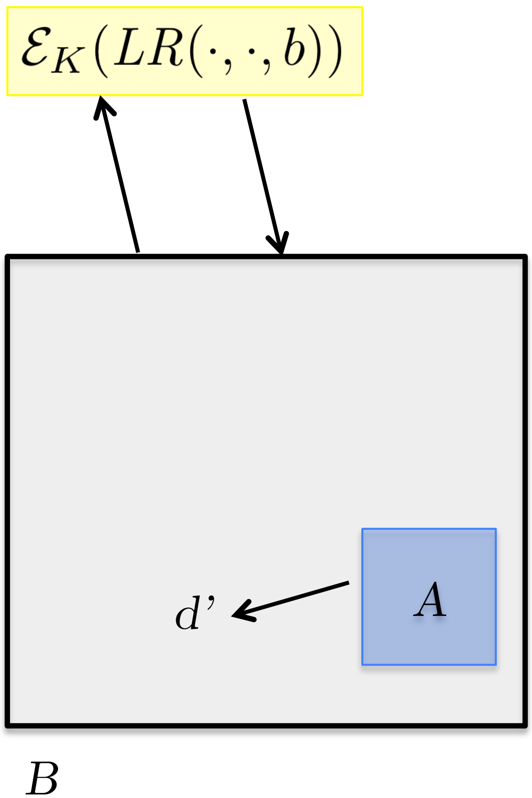
$\underline{\mathbf{Exp}^{\text{ror-cpa}}_{\Pi}(A)\text{:}}$

$K \stackrel{\$}{\leftarrow} \mathcal{K}$
$d \stackrel{\$}{\leftarrow} \{0,1\}$
$d' \stackrel{\$}{\leftarrow} A^{\mathcal{O}(\cdot)}$
If $d' = d$ then Return 1
Return 0

$\underline{\text{Oracle } \mathcal{O}(M)\text{:}}$

$M' \stackrel{\$}{\leftarrow} \{0,1\}^{|M|}$
If $d = 0$ then Return $\mathcal{E}_K(M')$
Return $\mathcal{E}_K(M)$

$$\frac{1}{2}\mathbf{Adv}_{\Pi}^{\text{ror-cpa}}(A) + \frac{1}{2} \quad \leq \quad \Pr(\mathbf{Exp}_{\Pi}^{\text{ror-cpa}}(A) = 1)$$



$\mathbf{Exp}_{\Pi}^{\text{ror-cpa}}(A)$:

$K \xleftarrow{\$} \mathcal{K}$

$d \xleftarrow{\$} \{0,1\}$

$d' \xleftarrow{\$} A^{\mathcal{O}(\cdot)}$

If $d' = d$ then Return 1

Return 0

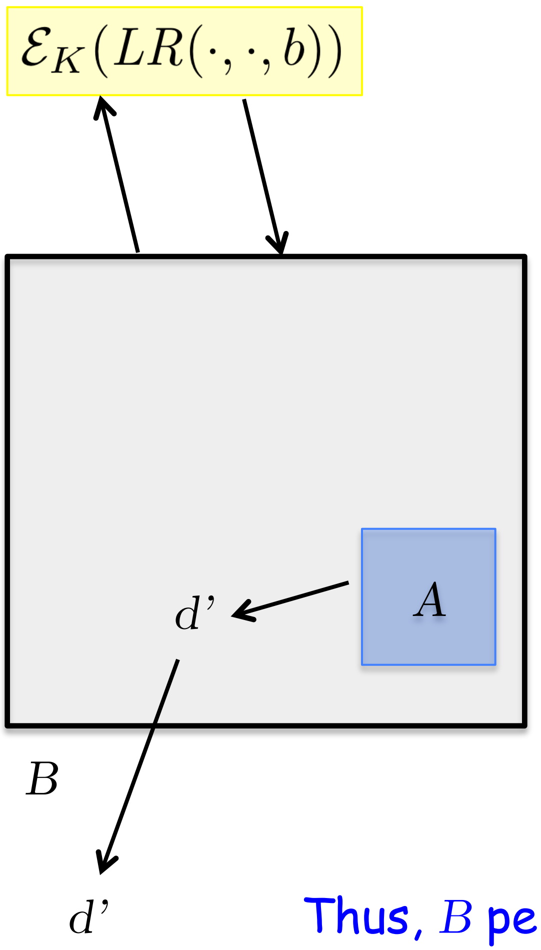
Oracle $\mathcal{O}(M)$:

$M' \xleftarrow{\$} \{0,1\}^{|M|}$

If $d = 0$ then Return $\mathcal{E}_K(M')$

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

$$\frac{1}{2}\mathbf{Adv}_{\Pi}^{\text{ror-cpa}}(A) + \frac{1}{2} \quad \leq \quad \Pr(\mathbf{Exp}_{\Pi}^{\text{ror-cpa}}(A) = 1)$$



$\underline{\mathbf{Exp}_{\Pi}^{\text{ror-cpa}}(A)}$:

$K \xleftarrow{\$} \mathcal{K}$

$d \xleftarrow{\$} \{0,1\}$

$d' \xleftarrow{\$} A^{\mathcal{O}(\cdot)}$

If $d' = d$ then Return 1

Return 0

$\underline{\text{Oracle } \mathcal{O}(M)}$:

$M' \xleftarrow{\$} \{0,1\}^{|M|}$

If $d = 0$ then Return $\mathcal{E}_K(M')$

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

Thus, B perfectly simulates A's expected experiment and will "win" whenever A wins

$$
\begin{aligned}
\frac{1}{2}\mathbf{Adv}_{\Pi}^{\text{ror-cpa}}(A) + \frac{1}{2} &\leq \Pr(\mathbf{Exp}_{\Pi}^{\text{ror-cpa}}(A) = 1) \\
&\leq \Pr(\mathbf{Exp}_{\Pi}^{\text{ind-cpa}}(B) = 1) \\
\mathbf{Adv}_{\Pi}^{\text{ror-cpa}}(A) &\leq 2\Pr(\mathbf{Exp}_{\Pi}^{\text{ind-cpa}}(B) = 1) - 1
\end{aligned}
$$

And hence,

$$
\mathbf{Adv}_{\Pi}^{\text{ror-cpa}}(A) \quad \leq \quad \mathbf{Adv}_{\Pi}^{\text{ind-cpa}}(B)
$$

as we claimed.

So we say “IND-CPA security implies RoR-CPA security”

$$\text{IND-CPA} \Rightarrow \text{RoR-CPA}$$

What about the other way around?

Claim: Any encryption scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ that is RoR-CPA secure, is also IND-CPA secure

---

Proof idea: show the contrapositive, if a scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is not IND-CPA secure, then it is not RoR-CPA secure.

Claim: Any encryption scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ that is RoR-CPA secure, is also IND-CPA secure

---

Proof idea: show the contrapositive, if a scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is not IND-CPA secure, then it is not RoR-CPA secure.

Let A be an efficient IND-CPA adversary, gaining advantage $\mathrm{Adv}_{\Pi}^{\text{ind-cpa}}(A)$

We build an efficient RoR-CPA adversary B, that runs A as a "black-box" subroutine, that gains advantage

$$2\mathrm{Adv}_{\Pi}^{\text{ror-cpa}}(B) \geq \mathrm{Adv}_{\Pi}^{\text{ind-cpa}}(A)$$

Conclusion: if $\mathrm{Adv}_{\Pi}^{\text{ror-cpa}}(B)$ is small for all efficient B, then $\mathrm{Adv}_{\Pi}^{\text{ind-cpa}}(A)$ must be small, too

So we say “IND-CPA security implies RoR-CPA security”

$$\text{IND-CPA} \Rightarrow \text{RoR-CPA}$$

And “RoR-CPA security implies IND-CPA security”, too

$$\text{RoR-CPA} \Rightarrow \text{IND-CPA}$$

(Although the two directions are not equally “tight”)

There are a variety of definitions of IND-CPA that are all *qualitatively* equivalent:

Left-or-Right IND-CPA

Real-or-Random IND-CPA

Real-or-0s IND-CPA

Find-then-Guess IND-CPA

Semantic security

Although not all of the reductions have the same *quantitative* “tightness”

Check out [Bellare, Desai, Pointcheval, Rogaway]

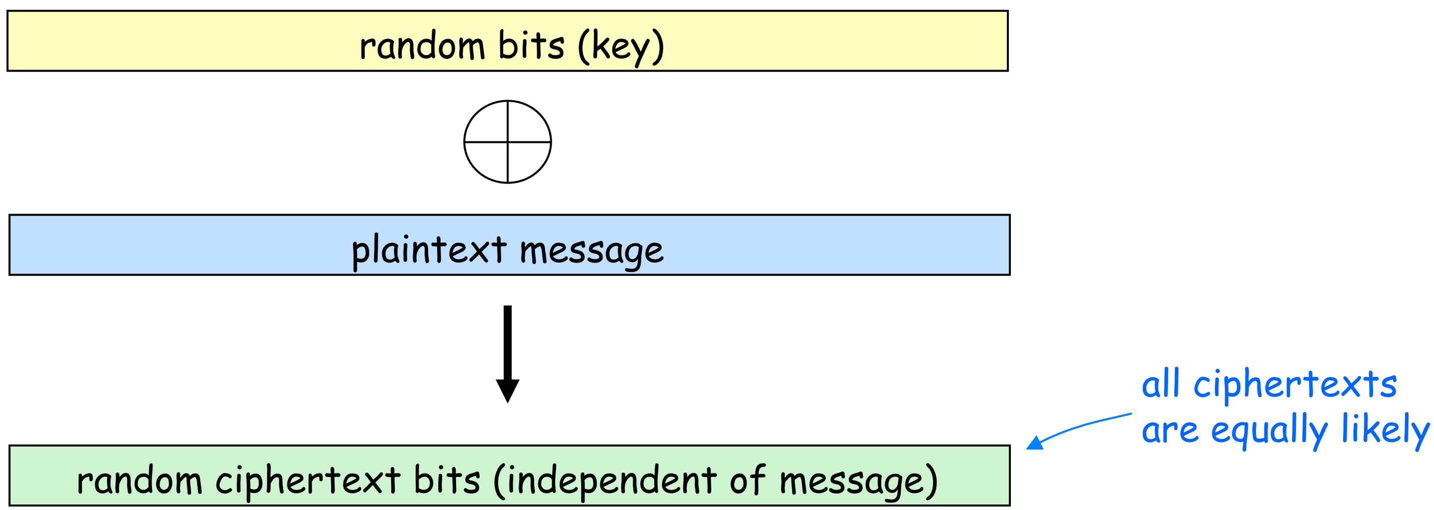
So, now we have

- -- a precise syntax for the object we want to build
- -- a precise target security notion, left-or-right IND-CPA

How should we build this thing?

“Perfect” encryption

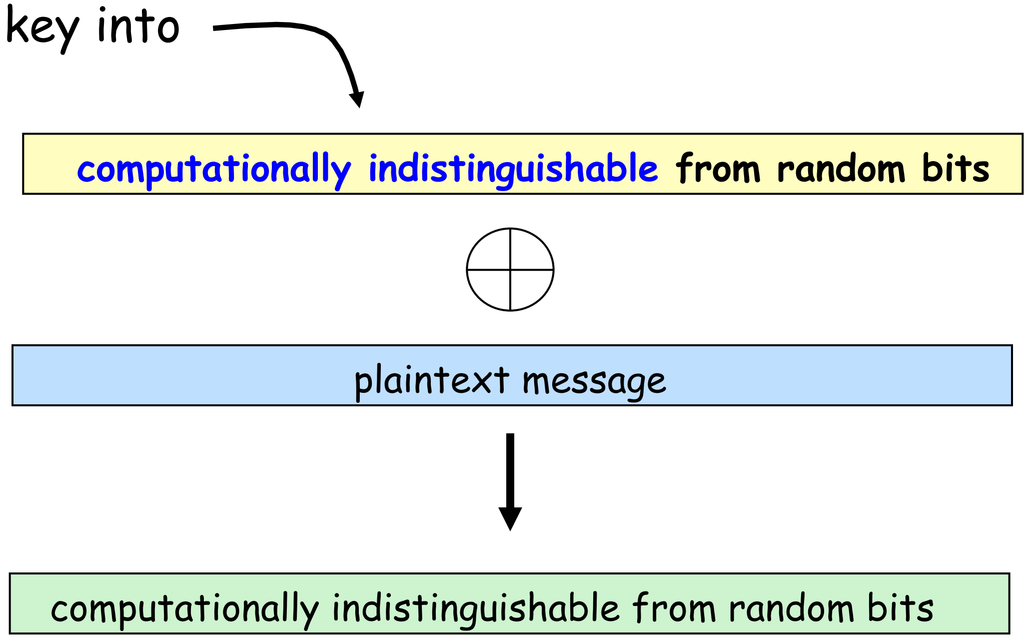
There does exist one “perfect” encryption scheme: **One Time Pad**



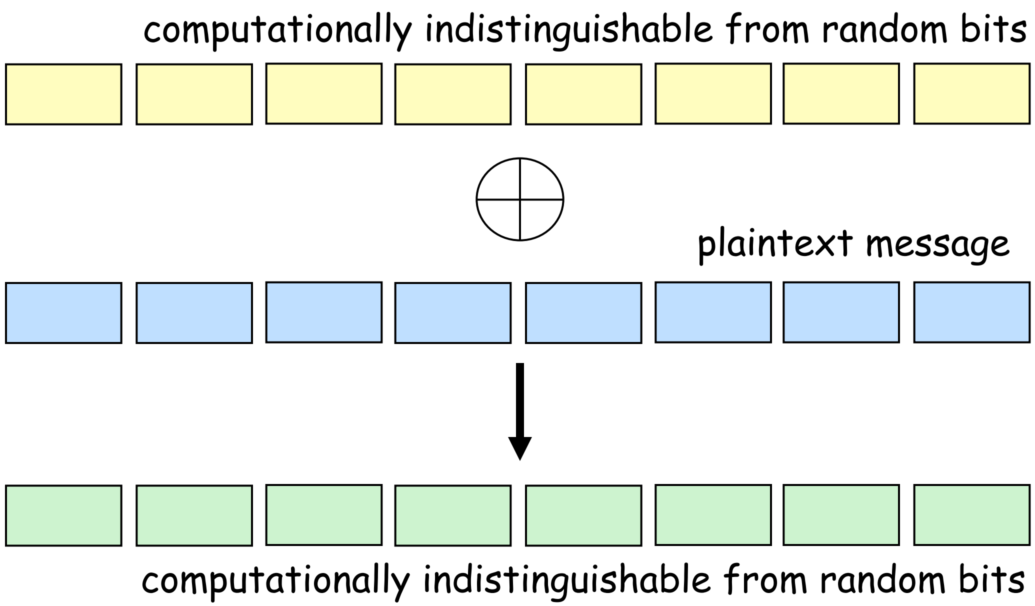
Sadly, requires a stream of random bits as long as the length of all messages you want to send.

Approximating One-Time Pad

Perhaps we can turn a short secret key into



Intuitively, making small blocks of “random-looking” bits should be easier (at least, not harder) than making a long string all at once



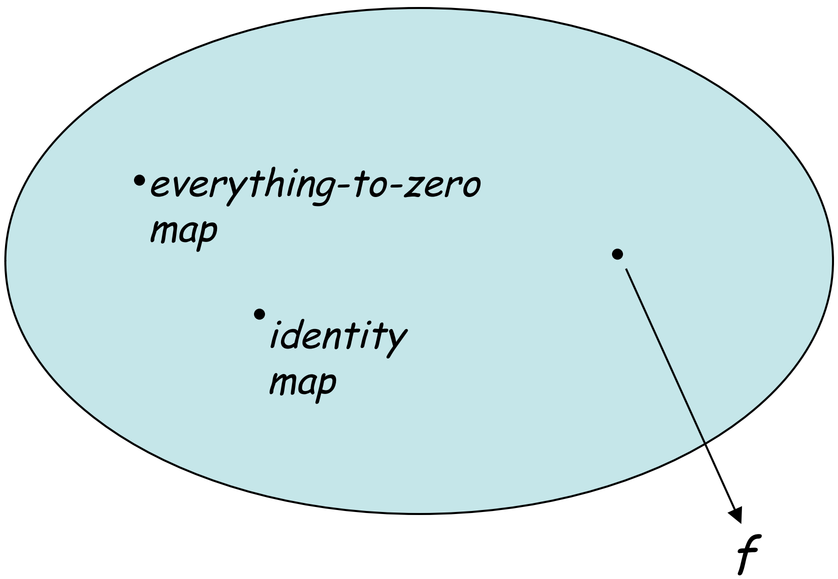
So we need a function that outputs small blocks of “random looking” bits

Consider the set $\mathrm{Func}(n,n) = \{f\colon \{0,1\}^n \to \{0,1\}^n\}$,
the "family" of all functions mapping n-bit strings to n-bit strings

Consider the set $\mathrm{Func}(n,n) = \{f\colon \{0,1\}^n \to \{0,1\}^n\}$,
the “family” of all functions mapping n-bit strings to n-bit strings

Two equivalent viewpoints on picking a “random function”

1. Sampling an element of $\mathrm{Func}(n,n)$

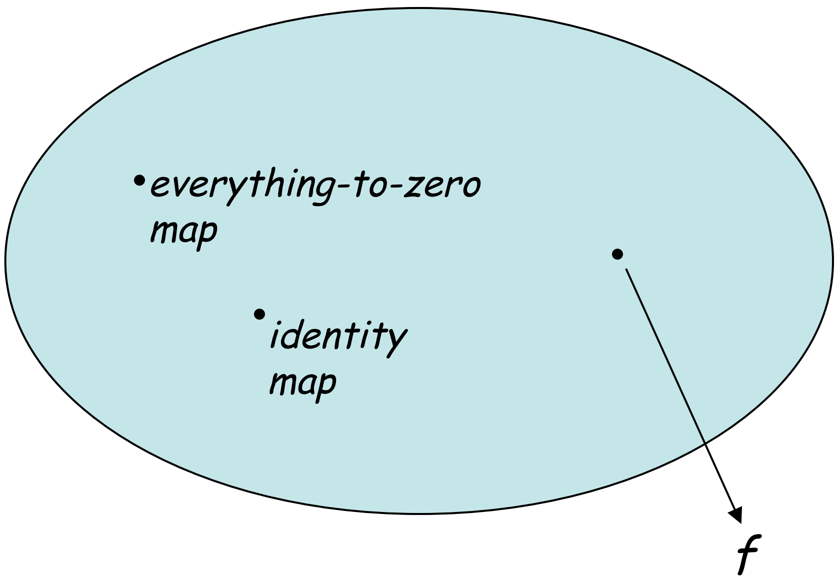


Consider the set $\mathrm{Func}(n,n) = \{f\colon \{0,1\}^n \to \{0,1\}^n\}$, the "family" of all functions mapping n-bit strings to n-bit strings

---

Two equivalent viewpoints on picking a "random function"

1. Sampling an element of $\mathrm{Func}(n,n)$



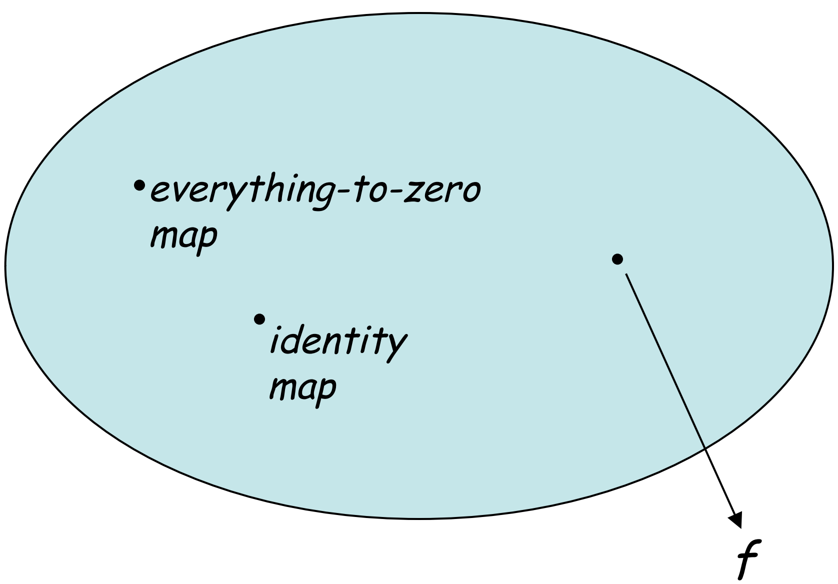
It's not hard to see that

$$\forall X, Y \in \{0,1\}^n,\ \Pr\left(f(X) = Y\right) = \frac{(2^n)^{2^n - 1}}{(2^n)^{2^n}}$$
$$= 1/2^n$$

Consider the set $\mathrm{Func}(n,n) = \{f\colon \{0,1\}^n \to \{0,1\}^n\}$,
the "family" of all functions mapping n-bit strings to n-bit strings

Two equivalent viewpoints on picking a "random function"

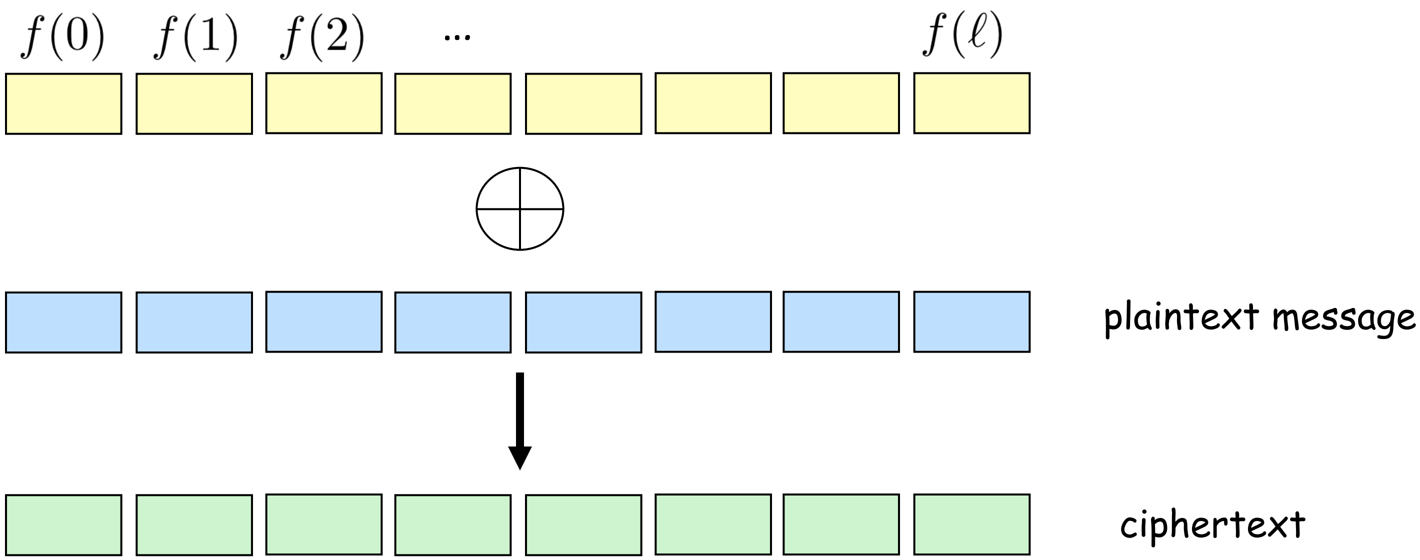
1. Sampling an element of $\mathrm{Func}(n,n)$



2. fill in the function table "lazily"

00…00	111010110…110101
00…01	10000010…100111
00…10	00000010…011111
	⋮
11…10	1011111111…100111
11…11	010101110…100111

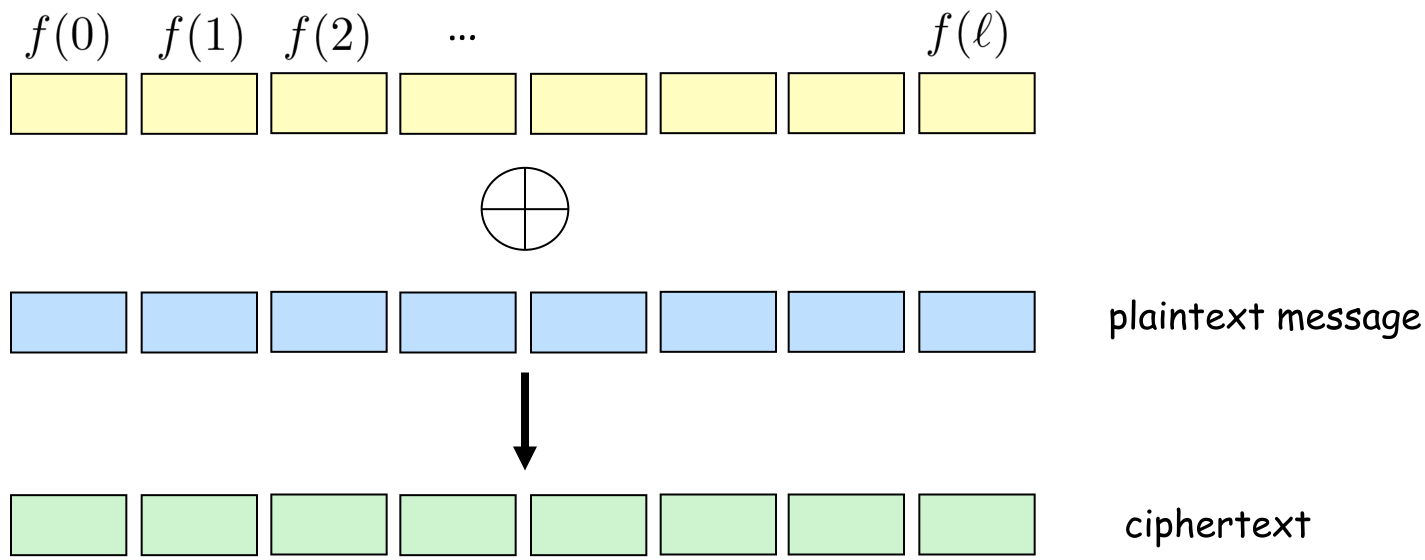
Imagine we could sample $f \xleftarrow{\$} \mathrm{Func}(n, n)$ and then encrypt via…



… we get one-time pad! But there's still a catch.

(What is the size of the key
for this encryption scheme?)

Imagine we could sample $f \xleftarrow{\$} \mathrm{Func}(n, n)$ and then encrypt via…



… we get one-time pad! But there's still a catch.

$\log_2 \left((2^n)^{2^n} \right) = n2^n$ bits of key

Pseudorandom Functions (PRFs)

Let $F: \mathcal{K} \times \{0,1\}^n \rightarrow \{0,1\}^n$ be viewed as a "keyed" function family

$\mathbf{Exp}_F^{\mathrm{prf}}(A)$:

$K \stackrel{\$}{\leftarrow} \mathcal{K}$

$f \stackrel{\$}{\leftarrow} \mathrm{Func}(n,n)$

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

$b' \stackrel{\$}{\leftarrow} A^{\mathcal{O}(\cdot)}$

If $b' = b$ then Return 1

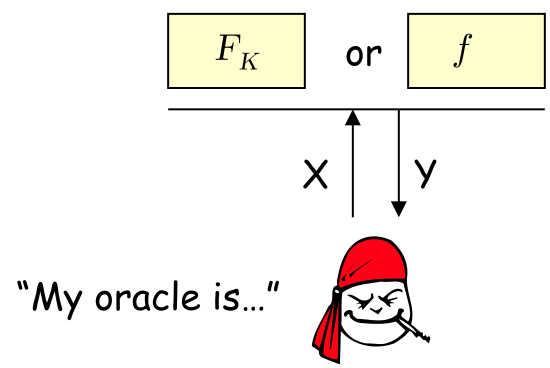
Return 0

Oracle $\mathcal{O}(X)$:

If $b = 0$ then Return $f(X)$

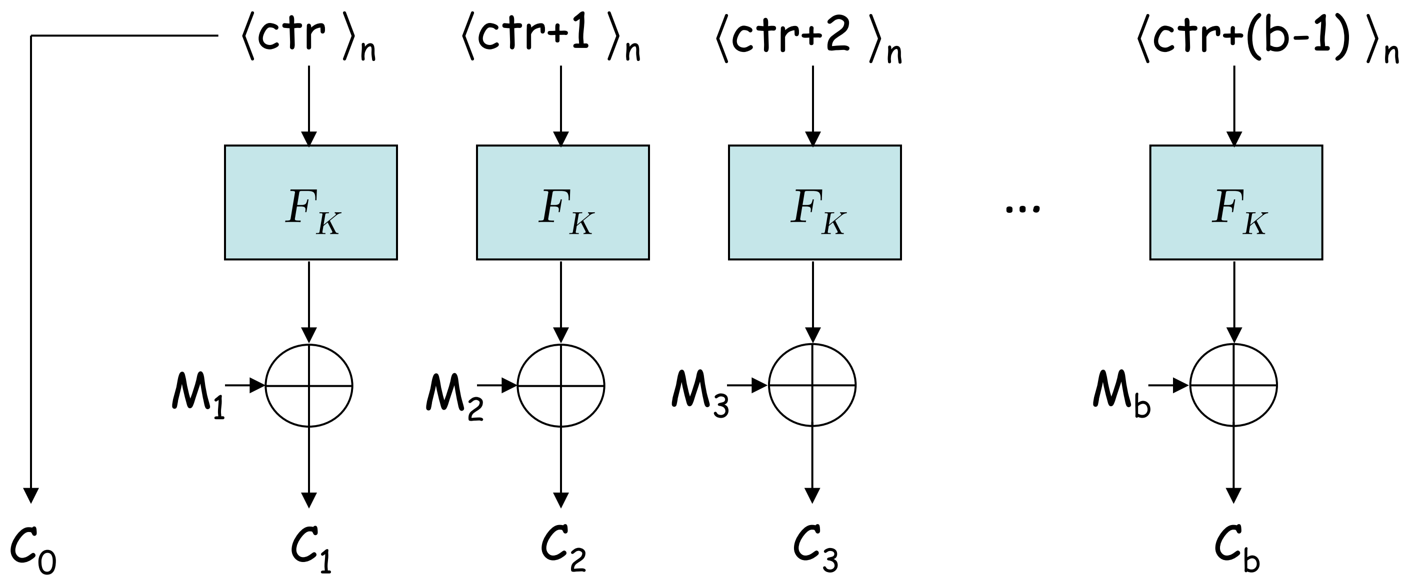
Return $F_K(X)$

$$\mathbf{Adv}_F^{\mathrm{prf}}(A) = 2\Pr(\mathbf{Exp}_F^{\mathrm{prf}}(A) = 1) - 1$$



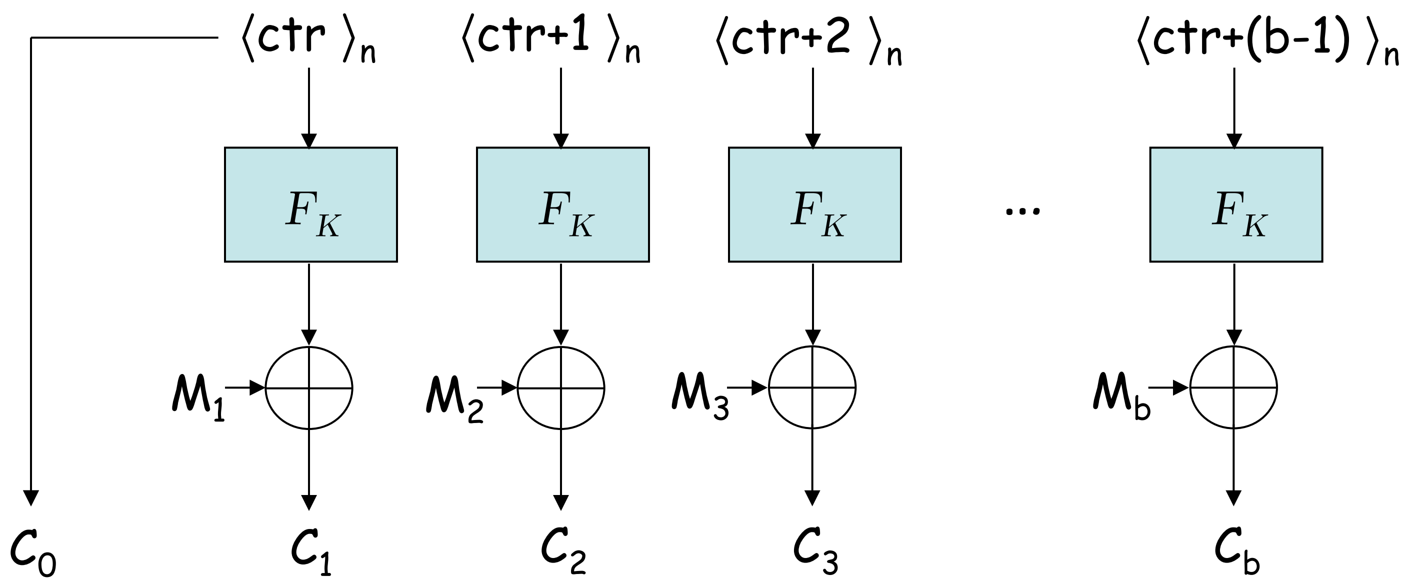
Counter-mode (CTR) encryption over a function family F

Initialization: $K \stackrel{\$}{\leftarrow} \mathcal{K}$; $\mathrm{ctr} \leftarrow 0$



For the next message, $\mathrm{ctr} \leftarrow \mathrm{ctr} + b$

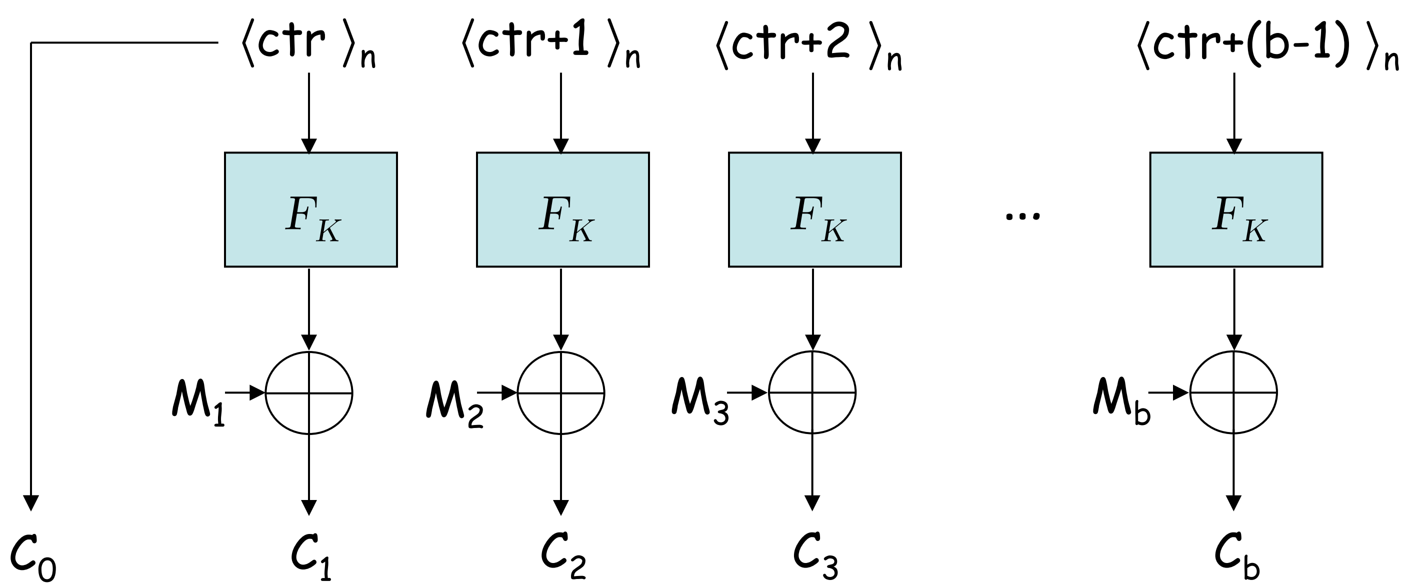
<u>Claim</u>: If $F: \mathcal{K} \times \{0,1\}^n \rightarrow \{0,1\}^n$ is a secure PRF, then $\mathrm{CTR}[F] = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ (counter-mode over F) is IND-CPA secure.



Claim: If $F : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ is a secure PRF, then $\mathrm{CTR}[F] = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ (counter-mode over F) is IND-CPA secure.

Proof idea: break the proof into two steps

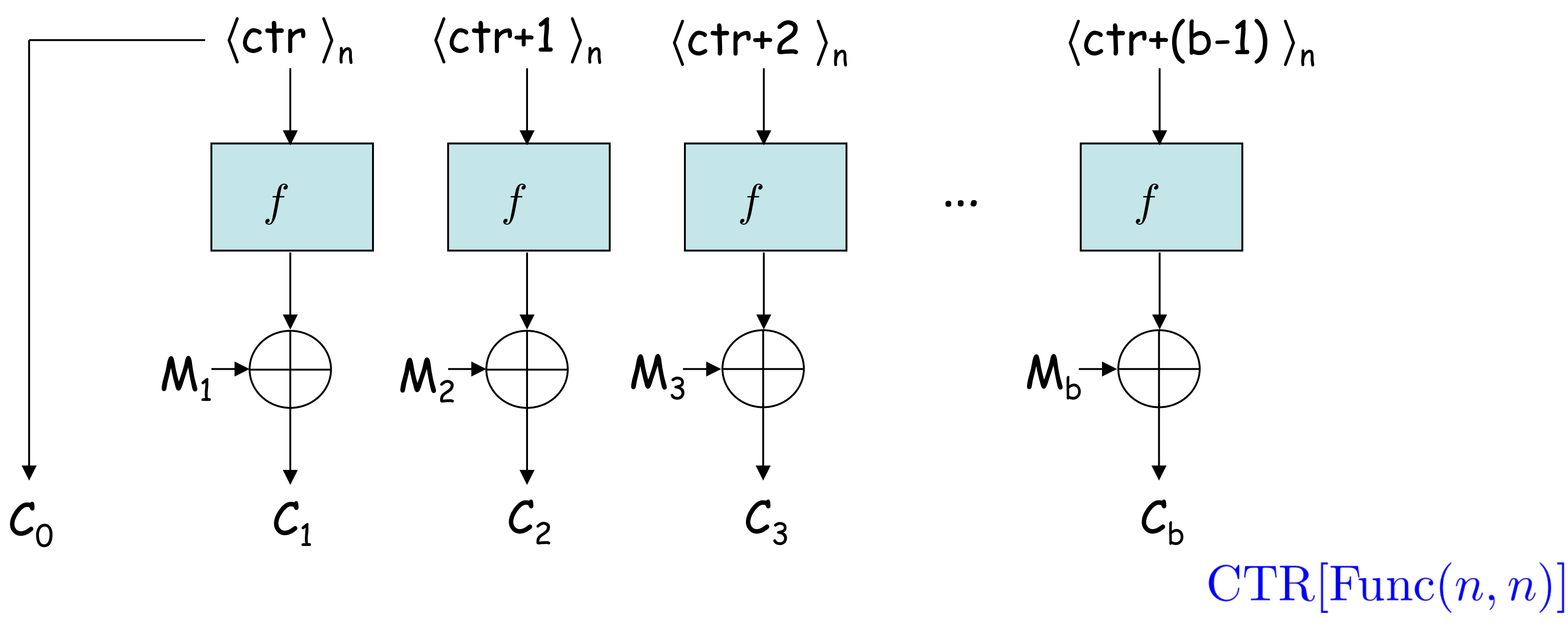
1. replace F_K with a random function f, and argue that any adversary that can detect this can "break" PRF-security of F



Claim: If $F: \mathcal{K} \times \{0,1\}^n \rightarrow \{0,1\}^n$ is a secure PRF, then $\mathrm{CTR}[F] = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ (counter-mode over F) is IND-CPA secure.

Proof idea: break the proof into two steps

1. replace F_K with a random function f, and argue that any adversary that can detect this can "break" PRF-security of F



Claim: If $F: \mathcal{K} \times \{0,1\}^n \rightarrow \{0,1\}^n$ is a secure PRF, then $\mathrm{CTR}[F] = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ (counter-mode over F) is IND-CPA secure.

Proof idea: break the proof into two steps

1. replace F_K with a random function f, and argue that any adversary that can detect this can "break" PRF-security of F

2. analyze IND-CPA security of $\mathrm{CTR}[\mathrm{Func}(n,n)]$

$$\mathrm{Adv}^{\text{ind-cpa}}_{\mathrm{CTR[F]}}(A) \leq \mathrm{Adv}^{\text{ind-cpa}}_{\mathrm{CTR[Func(n,n)]}}(A) + \mathrm{Adv}^{\mathrm{prf}}_{\mathrm{F}}(B)$$

(for reference)

$\underline{\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[F]}(A)\text{:}}$

$K \xleftarrow{\$} \mathcal{K}$
$d \xleftarrow{\$} \{0,1\}$
$d' \xleftarrow{\$} A^{\mathcal{O}(\cdot,\cdot)}$
If $d' = d$ then Return 1
Return 0

$\underline{\text{Oracle } \mathcal{O}(M_0, M_1)\text{:}}$
If $d = 0$ then Return $\mathcal{E}_K(M_0)$
Return $\mathcal{E}_K(M_1)$

$$\mathbf{Adv}^{\text{ind-cpa}}_{\text{CTR}[F]}(A) = 2\Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[F]}(A) = 1) - 1$$

$\underline{\mathbf{Exp}^{\text{prf}}_{F}(B)\text{:}}$

$K \xleftarrow{\$} \mathcal{K}$
$f \xleftarrow{\$} \text{Func}(n, n)$
$b \xleftarrow{\$} \{0,1\}$
$b' \xleftarrow{\$} B^{\mathcal{O}(\cdot)}$
If $b' = b$ then Return 1
Return 0

$\underline{\text{Oracle } \mathcal{O}(X)\text{:}}$
If $b = 0$ then Return $f(X)$
Return $F_K(X)$

$$\mathbf{Adv}^{\text{prf}}_{F}(B) = 2\Pr(\mathbf{Exp}^{\text{prf}}_{F}(B) = 1) - 1$$

$$\text{Adv}^{\text{ind-cpa}}_{\text{CTR[F]}}(A) \le \text{Adv}^{\text{ind-cpa}}_{\text{CTR[Func(n,n)]}}(A) + \text{Adv}^{\text{prf}}_{\text{F}}(B)$$

$$\frac{1}{2}\mathbf{Adv}^{\text{ind-cpa}}_{\text{CTR}[F]}(A) + \frac{1}{2} \quad = \quad \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[F]}(A) = 1)$$

So, we start with
an IND-CPA adversary
that gains some
IND-CPA advantage
in attacking CTR[F]

$$\frac{1}{2}\mathbf{Adv}^{\text{ind-cpa}}_{\text{CTR}[F]}(A) + \frac{1}{2} = \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[F]}(A) = 1)$$

$$= \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[F]}(A) = 1) - \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[\text{Func}(n,n)]}(A) = 1)$$

$$+ \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[\text{Func}(n,n)]}(A) = 1)$$

Now we add a "useful"
version of 0 to the right side

$$\begin{aligned}\frac{1}{2}\mathbf{Adv}^{\text{ind-cpa}}_{\text{CTR}[F]}(A)+\frac{1}{2} &= \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[F]}(A)=1)\\ &= \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[F]}(A)=1)-\Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[\text{Func}(n,n)]}(A)=1)\\ &\quad+\Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[\text{Func}(n,n)]}(A)=1)\end{aligned}$$

$$\begin{aligned}\frac{1}{2}\mathbf{Adv}^{\text{ind-cpa}}_{\text{CTR}[F]}(A) + \frac{1}{2} &= \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[F]}(A) = 1) \\ &= \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[F]}(A) = 1) - \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[\text{Func}(n,n)]}(A) = 1) \\ &\quad + \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[\text{Func}(n,n)]}(A) = 1)\end{aligned}$$

I claim that:

$$\Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[F]}(A) = 1) - \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[\text{Func}(n,n)]}(A) = 1) = \mathbf{Adv}^{\text{prf}}_{F}(B)$$

$$\begin{aligned} \frac{1}{2}\mathbf{Adv}^{\text{ind-cpa}}_{\mathrm{CTR}[F]}(A) + \frac{1}{2} &= \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\mathrm{CTR}[F]}(A) = 1) \\ &= \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\mathrm{CTR}[F]}(A) = 1) - \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\mathrm{CTR}[\mathrm{Func}(n,n)]}(A) = 1) \\ &\quad + \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\mathrm{CTR}[\mathrm{Func}(n,n)]}(A) = 1) \end{aligned}$$

I claim that:

$$\Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\mathrm{CTR}[F]}(A) = 1) - \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\mathrm{CTR}[\mathrm{Func}(n,n)]}(A) = 1) = \mathbf{Adv}^{\mathrm{prf}}_{F}(B)$$

<u>Adversary $B^{g(\cdot)}$:</u>

$d \xleftarrow{\$} \{0,1\}$
Run A
When A asks (M_0, M_1) to its oracle:
  Simulate encryption of M_d using calls to oracle g
  Respond with resulting ctxt C
When A halts with output bit d':
  If $d' = d$ Then Return 1
  Else Return 0

$$\frac{1}{2}\mathbf{Adv}^{\text{ind-cpa}}_{\text{CTR}[F]}(A) + \frac{1}{2} = \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[F]}(A) = 1)$$

$$= \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[F]}(A) = 1) - \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[\text{Func}(n,n)]}(A) = 1)$$

$$+ \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[\text{Func}(n,n)]}(A) = 1)$$

I claim that:

$$\Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[F]}(A) = 1) - \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[\text{Func}(n,n)]}(A) = 1) = \mathbf{Adv}^{\text{prf}}_{F}(B)$$

If PRF bit b=1:

B simulates IND-CPA experiment for $CTR[F]$, And outputs 1 if A guesses the bit

Adversary $B^{g(\cdot)}$:

$d \xleftarrow{\$} \{0,1\}$
Run A
When A asks (M_0, M_1) to its oracle:
  Simulate encryption of M_d using calls to oracle g
  Respond with resulting ctxt C
When A halts with output bit d':
  If $d' = d$ Then Return 1
  Else Return 0

$$\frac{1}{2}\mathbf{Adv}^{\text{ind-cpa}}_{\text{CTR}[F]}(A) + \frac{1}{2} = \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[F]}(A) = 1)$$
$$= \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[F]}(A) = 1) - \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[\text{Func}(n,n)]}(A) = 1)$$
$$+ \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[\text{Func}(n,n)]}(A) = 1)$$

I claim that:

$$\Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[F]}(A) = 1) - \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[\text{Func}(n,n)]}(A) = 1) = \mathbf{Adv}^{\text{prf}}_{F}(B)$$

If PRF bit b=1:

B simulates IND-CPA experiment for $CTR[F]$, And outputs 1 if A guesses the bit

If PRF bit b=0:

B simulates IND-CPA experiment for $CTR[Func(n,n)]$, And outputs 1 if A guesses the bit

Adversary $B^{g(\cdot)}$:

$d \xleftarrow{\$} \{0,1\}$
Run A
When A asks (M_0, M_1) to its oracle:
  Simulate encryption of M_d using calls to oracle g
  Respond with resulting ctxt C
When A halts with output bit d':
  If $d' = d$ Then Return 1
  Else Return 0

$$\begin{aligned}\frac{1}{2}\mathbf{Adv}^{\text{ind-cpa}}_{\text{CTR}[F]}(A)+\frac{1}{2} &= \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[F]}(A)=1)\\ &= \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[F]}(A)=1)-\Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[\text{Func}(n,n)]}(A)=1)\\ &\quad +\Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[\text{Func}(n,n)]}(A)=1)\end{aligned}$$

I claim that:

$$\Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[F]}(A)=1)-\Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[\text{Func}(n,n)]}(A)=1)=\mathbf{Adv}^{\text{prf}}_{F}(B)$$

If PRF bit b=1:

B simulates IND-CPA experiment for $CTR[F]$, And outputs 1 if A guesses the bit

$$\begin{aligned}\Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[F]}(A)=1) &= \Pr(\mathbf{Exp}^{\text{prf}}_{F}(B)=1 \mid b=1)\\ \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[\text{Func}(n,n)]}(A)=1) &= \Pr(\mathbf{Exp}^{\text{prf}}_{F}(B)=0 \mid b=0)\\ &= 1-\Pr(\mathbf{Exp}^{\text{prf}}_{F}(B)=1 \mid b=0)\end{aligned}$$

If PRF bit b=0:

B simulates IND-CPA experiment for $CTR[Func(n,n)]$, And outputs 1 if A guesses the bit

$$
\begin{aligned}
\frac{1}{2}\mathbf{Adv}^{\text{ind-cpa}}_{\text{CTR}[F]}(A) + \frac{1}{2} &= \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[F]}(A) = 1) \\
&= \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[F]}(A) = 1) - \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[\text{Func}(n,n)]}(A) = 1) \\
&\quad + \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[\text{Func}(n,n)]}(A) = 1)
\end{aligned}
$$

I claim that:

$$
\Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[F]}(A) = 1) - \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[\text{Func}(n,n)]}(A) = 1) = \mathbf{Adv}^{\text{prf}}_{F}(B)
$$

$$
\begin{aligned}
\Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[F]}(A) = 1) &= \Pr(\mathbf{Exp}^{\text{prf}}_{F}(B) = 1 \mid b = 1) \\
\Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[\text{Func}(n,n)]}(A) = 1) &= \Pr(\mathbf{Exp}^{\text{prf}}_{F}(B) = 0 \mid b = 0) \\
&= 1 - \Pr(\mathbf{Exp}^{\text{prf}}_{F}(B) = 1 \mid b = 0)
\end{aligned}
$$

So by subtracting:

$$
\begin{aligned}
&\Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[F]}(A) = 1) - \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[\text{Func}(n,n)]}(A) = 1) \\
&\quad = \Pr(\mathbf{Exp}^{\text{prf}}_{F}(B) = 1 \mid b = 1) + \Pr(\mathbf{Exp}^{\text{prf}}_{F}(B) = 1 \mid b = 0) - 1 \\
&\quad = 2\Pr(\mathbf{Exp}^{\text{prf}}_{F}(B) = 1) - 1 \\
&\quad = \mathbf{Adv}^{\text{prf}}_{F}(B)
\end{aligned}
$$

$$
\begin{aligned}
\frac{1}{2}\mathbf{Adv}^{\text{ind-cpa}}_{\mathrm{CTR}[F]}(A) + \frac{1}{2} &= \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\mathrm{CTR}[F]}(A) = 1) \\
&= \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\mathrm{CTR}[F]}(A) = 1) - \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\mathrm{CTR}[\mathrm{Func}(n,n)]}(A) = 1) \\
&\quad + \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\mathrm{CTR}[\mathrm{Func}(n,n)]}(A) = 1) \\
&= \mathbf{Adv}^{\text{prf}}_{F}(B) + \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\mathrm{CTR}[\mathrm{Func}(n,n)]}(A) = 1)
\end{aligned}
$$

$$
\begin{aligned}
\frac{1}{2}\mathbf{Adv}^{\text{ind-cpa}}_{\mathrm{CTR}[F]}(A) + \frac{1}{2} &= \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\mathrm{CTR}[F]}(A) = 1) \\
&= \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\mathrm{CTR}[F]}(A) = 1) - \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\mathrm{CTR}[\mathrm{Func}(n,n)]}(A) = 1) \\
&\quad + \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\mathrm{CTR}[\mathrm{Func}(n,n)]}(A) = 1)
\end{aligned}
$$

$$
= \mathbf{Adv}^{\text{prf}}_{F}(B) + \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\mathrm{CTR}[\mathrm{Func}(n,n)]}(A) = 1)
$$

$$
\begin{aligned}
\mathbf{Adv}^{\text{ind-cpa}}_{\mathrm{CTR}[F]}(A) &= 2\mathbf{Adv}^{\text{prf}}_{F}(B) + 2\Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\mathrm{CTR}[\mathrm{Func}(n,n)]}(A) = 1) - 1 \\
&= 2\mathbf{Adv}^{\text{prf}}_{F}(B) + \mathbf{Adv}^{\text{ind-cpa}}_{\mathrm{CTR}[\mathrm{Func}(n,n)]}(A)
\end{aligned}
$$

$$\begin{aligned}
\frac{1}{2}\mathbf{Adv}^{\text{ind-cpa}}_{\text{CTR}[F]}(A) + \frac{1}{2} &= \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[F]}(A) = 1) \\
&= \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[F]}(A) = 1) - \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[\text{Func}(n,n)]}(A) = 1) \\
&\quad + \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[\text{Func}(n,n)]}(A) = 1) \\
&= \mathbf{Adv}^{\text{prf}}_{F}(B) + \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[\text{Func}(n,n)]}(A) = 1)
\end{aligned}$$

$$\begin{aligned}
\mathbf{Adv}^{\text{ind-cpa}}_{\text{CTR}[F]}(A) &= 2\mathbf{Adv}^{\text{prf}}_{F}(B) + 2\Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[\text{Func}(n,n)]}(A) = 1) - 1 \\
&= 2\mathbf{Adv}^{\text{prf}}_{F}(B) + \mathbf{Adv}^{\text{ind-cpa}}_{\text{CTR}[\text{Func}(n,n)]}(A)
\end{aligned}$$

I claim: $\Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR}[\text{Func}(n,n)]}(A) = 1) \le \frac{1}{2} \quad \Rightarrow \mathbf{Adv}^{\text{ind-cpa}}_{\text{CTR}[\text{Func}(n,n)]}(A) \le 0$

Proof sketch: all ciphertexts are independent of the IND-CPA experiment bit!
So probability of guessing the bit is at most 1/2

$$
\begin{aligned}
\frac{1}{2}\mathbf{Adv}^{\text{ind-cpa}}_{\mathrm{CTR}[F]}(A) + \frac{1}{2} \quad &= \quad \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\mathrm{CTR}[F]}(A) = 1) \\
&= \quad \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\mathrm{CTR}[F]}(A) = 1) - \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\mathrm{CTR}[\mathrm{Func}(n,n)]}(A) = 1) \\
&\qquad + \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\mathrm{CTR}[\mathrm{Func}(n,n)]}(A) = 1)
\end{aligned}
$$

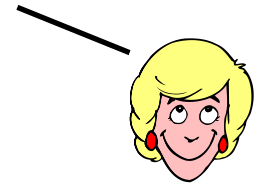
$$
= \mathbf{Adv}^{\text{prf}}_{F}(B) + \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\mathrm{CTR}[\mathrm{Func}(n,n)]}(A) = 1)
$$

$$
\begin{aligned}
\mathbf{Adv}^{\text{ind-cpa}}_{\mathrm{CTR}[F]}(A) &= 2\mathbf{Adv}^{\text{prf}}_{F}(B) + 2\Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\mathrm{CTR}[\mathrm{Func}(n,n)]}(A) = 1) - 1 \\
&= 2\mathbf{Adv}^{\text{prf}}_{F}(B) + \mathbf{Adv}^{\text{ind-cpa}}_{\mathrm{CTR}[\mathrm{Func}(n,n)]}(A)
\end{aligned}
$$

$$
\mathbf{Adv}^{\text{ind-cpa}}_{\mathrm{CTR}[F]}(A) \leq 2\mathbf{Adv}^{\text{prf}}_{F}(B)
$$

And we're done.

Wait… blockciphers are not function families,
they are permutation families

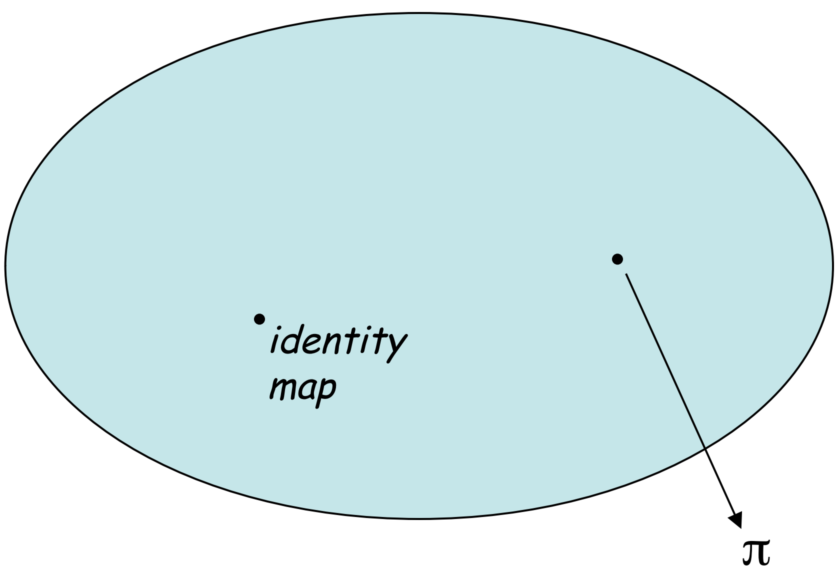


How does $\mathrm{Adv}^{\mathrm{ind\text{-}cpa}}_{\mathrm{CTR[F]}}(A)$ relate to $\mathrm{Adv}^{\mathrm{ind\text{-}cpa}}_{\mathrm{CTR[AES]}}(A)$?

Consider the set $\mathrm{Perm}(n) = \{\pi \colon \{0,1\}^n \to \{0,1\}^n\}$,
the "family" of all permutations over n-bit strings

Two equivalent viewpoints on picking a "random permutation"

1. Sampling an element of $\mathrm{Perm}(n)$



2. fill in the permutation table "lazily"

00…00	111010110…110101
00…01	10000010…100111
00…10	00000010…011111
	⋮
11…10	1011111111…100111
11…11	010101110…100111

Pseudorandom Permutations (PRPs)

Let $E\colon \mathcal{K} \times \{0,1\}^n \rightarrow \{0,1\}^n$ be viewed as a "keyed" function family

$\underline{\mathbf{Exp}_F^{\mathrm{prp}}(A)}$:

$K \stackrel{\$}{\leftarrow} \mathcal{K}$

$\pi \stackrel{\$}{\leftarrow} \mathrm{Perm}(n)$

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

$b' \stackrel{\$}{\leftarrow} A^{\mathcal{O}(\cdot)}$

If $b' = b$ then Return 1

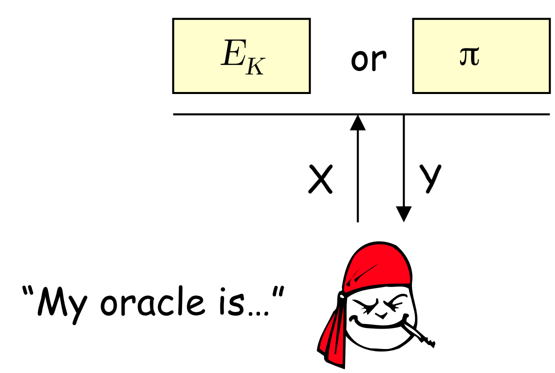
Return 0

$\underline{\text{Oracle } \mathcal{O}(X)}$:

If $b = 0$ then Return $\pi(X)$

Return $E_K(X)$

$$\mathbf{Adv}_F^{\mathrm{prp}}(A) = 2\Pr(\mathbf{Exp}_F^{\mathrm{prp}}(A) = 1) - 1$$



The PRP-PRF Switching Lemma

Let $E\colon \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ be viewed as a "keyed" function family

Let A be an adversary, asking q queries to its single oracle. Then

$$\left|\mathbf{Adv}_E^{\mathrm{prp}}(A) - \mathbf{Adv}_E^{\mathrm{prf}}(A)\right| \le \frac{0.5q^2}{2^n}$$

The PRP-PRF Switching Lemma

Let $E\colon \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ be viewed as a "keyed" function family

Let A be an adversary, asking q queries to its single oracle. Then

$$\left|\mathbf{Adv}_E^{\mathrm{prp}}(A) - \mathbf{Adv}_E^{\mathrm{prf}}(A)\right| \leq \frac{0.5q^2}{2^n}$$

So, for example,

$$\mathbf{Adv}_{\mathrm{CTR}[AES]}^{\mathrm{ind\text{-}cpa}}(A) \leq 2\mathbf{Adv}_{AES}^{\mathrm{prf}}(B)$$

$$\leq 2\mathbf{Adv}_{AES}^{\mathrm{prp}}(B) + \frac{q^2}{2^n}$$

$\underline{\mathbf{Exp}_F^{\mathrm{prp}}(A)}$:

$K \xleftarrow{\$} \mathcal{K}$

$\pi \xleftarrow{\$} \mathrm{Perm}(n)$

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

$b' \xleftarrow{\$} A^{\mathcal{O}(\cdot)}$

If $b' = b$ then Return 1

Return 0

$\underline{\text{Oracle } \mathcal{O}(X)}$:

If $b = 0$ then Return $\pi(X)$

Return $F_K(X)$

$$\mathbf{Adv}_F^{\mathrm{prp}}(A) = 2\Pr(\mathbf{Exp}_F^{\mathrm{prp}}(A) = 1) - 1$$

$\underline{\mathbf{Exp}_F^{\mathrm{prf}}(A)}$:

$K \xleftarrow{\$} \mathcal{K}$

$f \xleftarrow{\$} \mathrm{Func}(n,n)$

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

$b' \xleftarrow{\$} A^{\mathcal{O}(\cdot)}$

If $b' = b$ then Return 1

Return 0

$\underline{\text{Oracle } \mathcal{O}(X)}$:

If $b = 0$ then Return $f(X)$

Return $F_K(X)$

$$\mathbf{Adv}_F^{\mathrm{prf}}(A) = 2\Pr(\mathbf{Exp}_F^{\mathrm{prf}}(A) = 1) - 1$$

$$\left|\mathbf{Adv}_F^{\mathrm{prp}}(A) - \mathbf{Adv}_F^{\mathrm{prf}}(A)\right| \le \Pr\left(A^{f(\cdot)} \Rightarrow 1\right) - \Pr\left(A^{\pi(\cdot)} \Rightarrow 1\right) \le \frac{0.5q^2}{2^n}$$

Requires care, but the reason for the "birthday term" is obvious!

$\underline{G0(A):}$

$b' \xleftarrow{\$} A^{\mathcal{O}(\cdot)}$

Return b'

$\underline{\text{Oracle } \mathcal{O}(X):}$

$Y \xleftarrow{\$} \{0,1\}^n$

If $Y \in \text{Range}(\mathtt{P})$

  $\text{bad} \leftarrow \mathsf{true}$

  $Y \xleftarrow{\$} \overline{\text{Range}(\mathtt{P})}$

$\mathtt{P}[X] \leftarrow Y$

Return Y

all values already assigned as outputs of the oracle

all values still free to be assigned as outputs

$\underline{G1(A):}$

$b' \xleftarrow{\$} A^{\mathcal{O}(\cdot)}$

Return b'

$\underline{\text{Oracle } \mathcal{O}(X):}$

$Y \xleftarrow{\$} \{0,1\}^n$

If $Y \in \text{Range}(\mathtt{P})$

  $\text{bad} \leftarrow \mathsf{true}$

$\mathtt{P}[X] \leftarrow Y$

Return Y

$\underline{G0(A)}$:	$\underline{G1(A)}$:
$b' \xleftarrow{\$} A^{\mathcal{O}(\cdot)}$	$b' \xleftarrow{\$} A^{\mathcal{O}(\cdot)}$
Return b'	Return b'
$\underline{\text{Oracle } \mathcal{O}(X)}$:	$\underline{\text{Oracle } \mathcal{O}(X)}$:
$Y \xleftarrow{\$} \{0,1\}^n$	$Y \xleftarrow{\$} \{0,1\}^n$
If $Y \in \text{Range}(\texttt{P})$	If $Y \in \text{Range}(\texttt{P})$
$\text{bad} \leftarrow \textsf{true}$	$\text{bad} \leftarrow \textsf{true}$
$Y \xleftarrow{\$} \overline{\text{Range}(\texttt{P})}$	
$\texttt{P}[X] \leftarrow Y$	$\texttt{P}[X] \leftarrow Y$
Return Y	Return Y

$$\Pr(A^f \Rightarrow 1) - \Pr(A^\pi \Rightarrow 1) = \Pr(G1(A) \Rightarrow 1) - \Pr(G0(A) \Rightarrow 1)$$

$G0(A)$:

$b' \xleftarrow{\$} A^{\mathcal{O}(\cdot)}$

Return b'

Oracle $\mathcal{O}(X)$:

$Y \xleftarrow{\$} \{0,1\}^n$

If $Y \in \text{Range}(\texttt{P})$

  $\text{bad} \leftarrow \textsf{true}$

  $Y \xleftarrow{\$} \overline{\text{Range}(\texttt{P})}$

$\texttt{P}[X] \leftarrow Y$

Return Y

$G1(A)$:

$b' \xleftarrow{\$} A^{\mathcal{O}(\cdot)}$

Return b'

Oracle $\mathcal{O}(X)$:

$Y \xleftarrow{\$} \{0,1\}^n$

If $Y \in \text{Range}(\texttt{P})$

  $\text{bad} \leftarrow \textsf{true}$

$\texttt{P}[X] \leftarrow Y$

Return Y

$$\Pr(A^f \Rightarrow 1) - \Pr(A^\pi \Rightarrow 1) = \Pr(G1(A) \Rightarrow 1) - \Pr(G0(A) \Rightarrow 1)$$
$$\leq \Pr(G1(A) : \text{bad} = \textsf{true})$$

Fundamental lemma of game-playing (Bellare, Rogaway)

$\underline{G0(A):}$

$b' \xleftarrow{\$} A^{\mathcal{O}(\cdot)}$
Return b'

$\underline{\text{Oracle } \mathcal{O}(X):}$

$Y \xleftarrow{\$} \{0,1\}^n$
If $Y \in \text{Range}(\mathtt{P})$
  $\text{bad} \leftarrow \mathsf{true}$
  $Y \xleftarrow{\$} \overline{\text{Range}(\mathtt{P})}$
$\mathtt{P}[X] \leftarrow Y$
Return Y

$\underline{G1(A):}$

$b' \xleftarrow{\$} A^{\mathcal{O}(\cdot)}$
Return b'

$\underline{\text{Oracle } \mathcal{O}(X):}$

$Y \xleftarrow{\$} \{0,1\}^n$
If $Y \in \text{Range}(\mathtt{P})$
  $\text{bad} \leftarrow \mathsf{true}$
$\mathtt{P}[X] \leftarrow Y$
Return Y

$$\Pr(A^f \Rightarrow 1) - \Pr(A^\pi \Rightarrow 1) = \Pr(G1(A) \Rightarrow 1) - \Pr(G0(A) \Rightarrow 1)$$

$$\leq \Pr(G1(A)\colon \text{bad} = \mathsf{true})$$

Fundamental lemma of game-playing (Bellare, Rogaway)

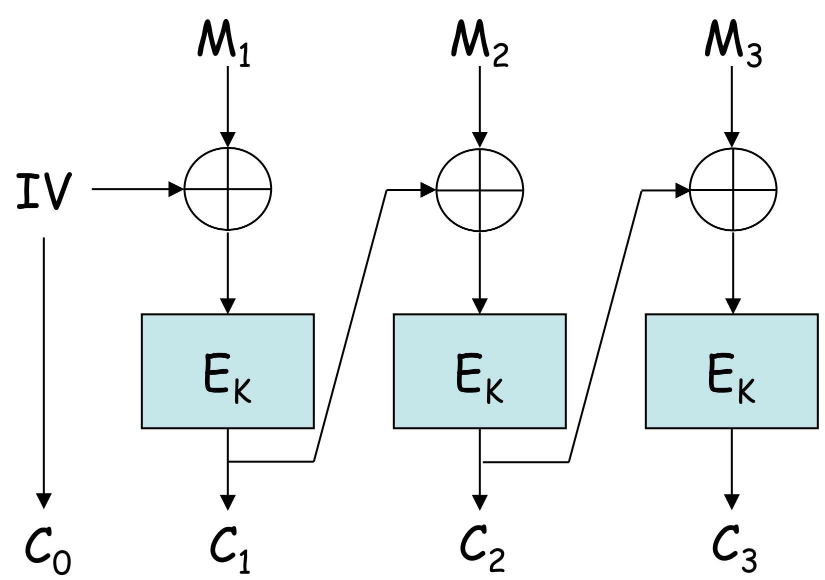
$$\leq \frac{0}{2^n} + \frac{1}{2^n} + \cdots + \frac{q-1}{2^n}$$

union bound

$$\leq \frac{0.5q^2}{2^n}$$

What about cipher-block-chaining (CBC) mode?

CBC mode appears in IPSec, SSH, TLS, …



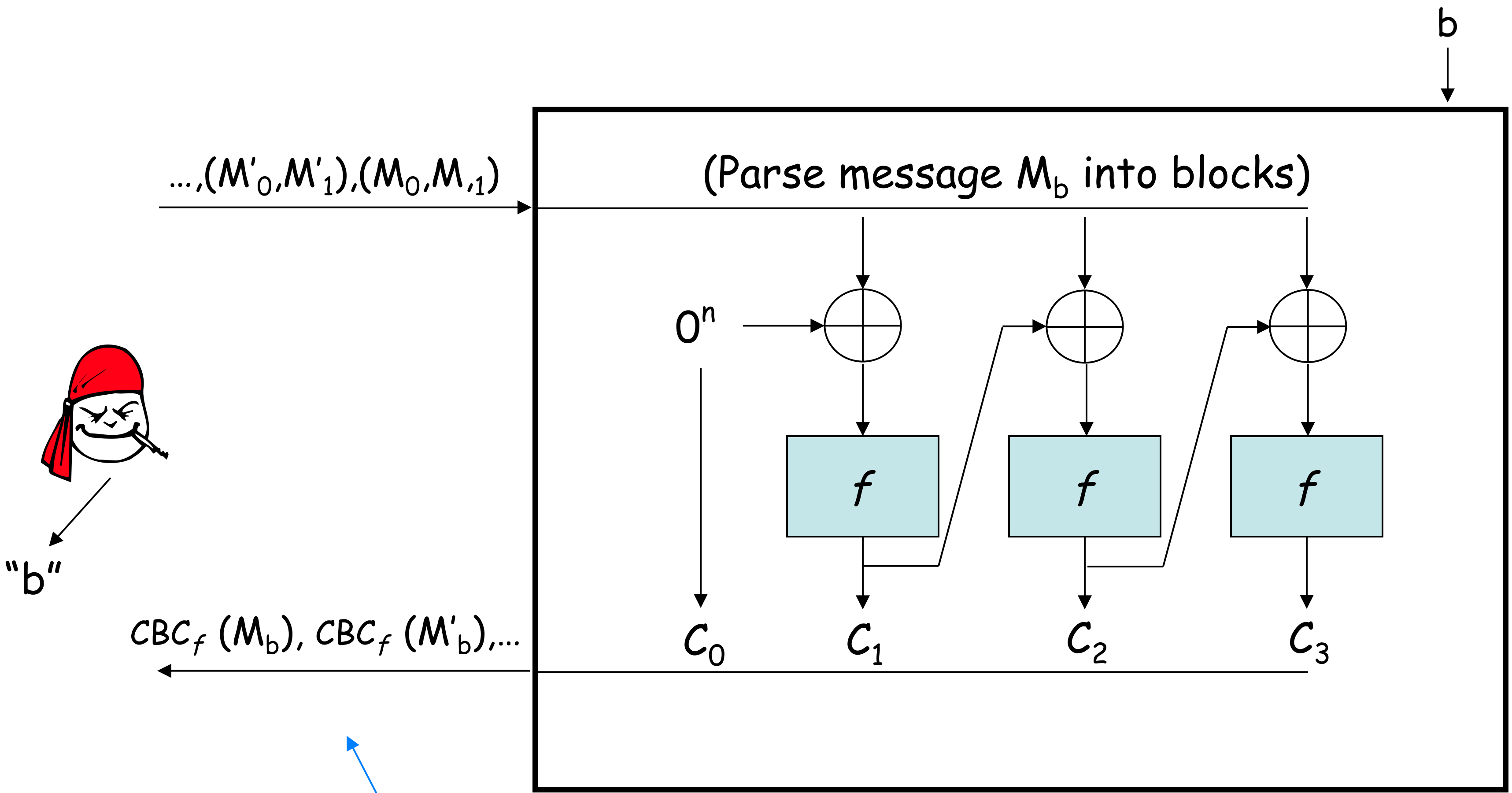
How to handle the IV?

Fixed IV?

Counter IV?

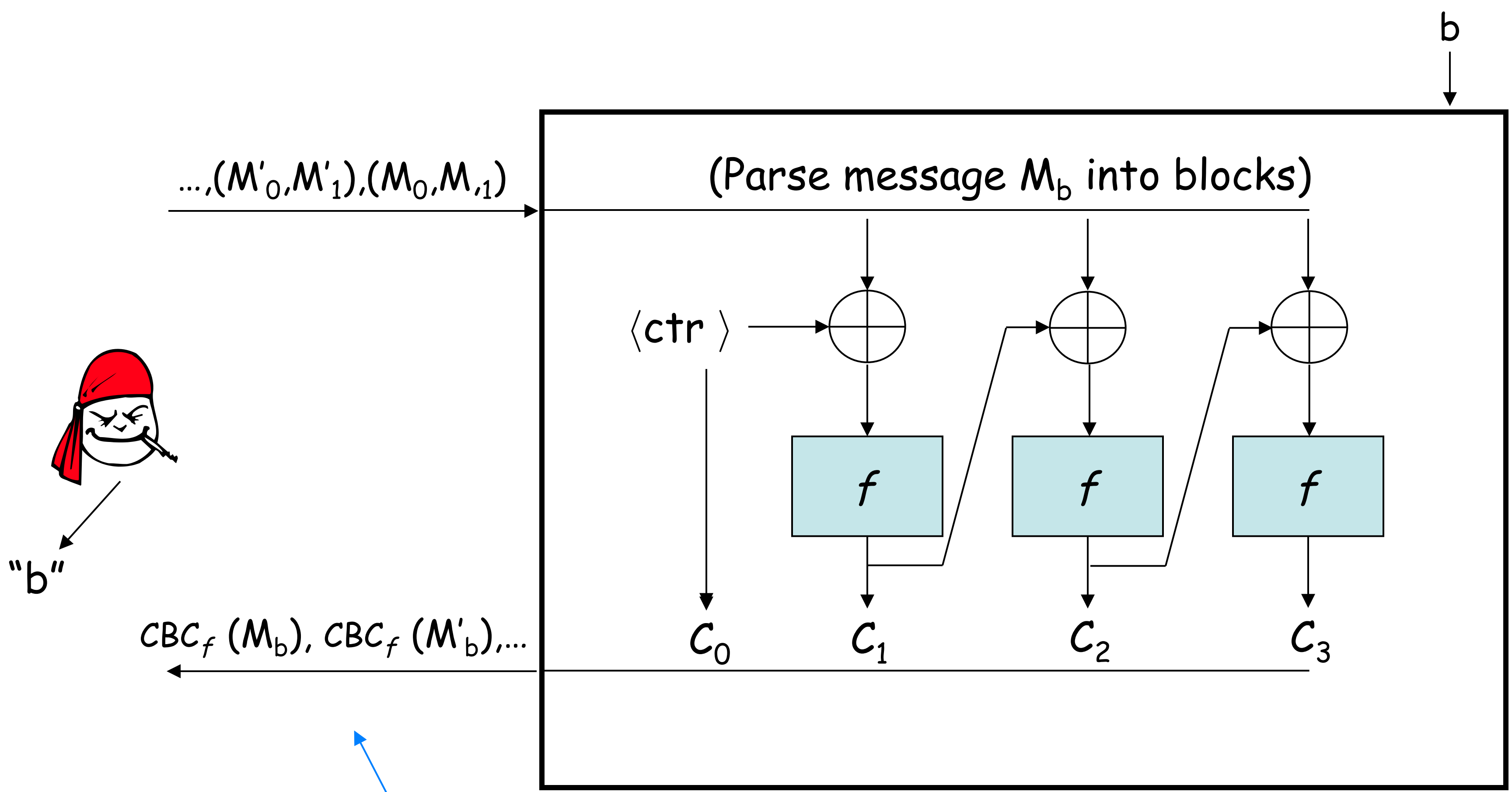
Random IV?

CBC with a fixed IV



Can the adversary easily guess the bit?

CBC with a counter IV



Can the adversary easily guess the bit?

Claim: If $F: \mathcal{K} \times \{0,1\}^n \rightarrow \{0,1\}^n$ is a secure PRF, then $\mathrm{CBC\$}[F]$ (CBC-mode, with a random IV, over F) is IND-CPA secure.

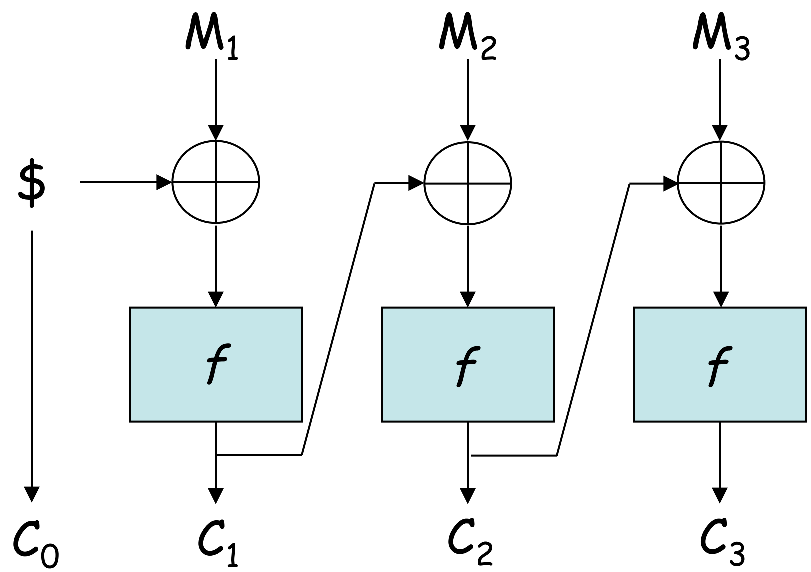
Proof idea: break the proof into two steps

1. replace F_K with a random function f, and argue that any adversary that can detect this, can "break" PRF-security of F

2. analyze IND-CPA security of $\mathrm{CBC\$}[\mathrm{Func}(n,n)]$

$$\begin{aligned}\mathbf{Adv}^{\text{ind-cpa}}_{\mathrm{CBC\$}[F]}(A) &\leq \mathbf{Adv}^{\text{ind-cpa}}_{\mathrm{CBC\$}[\mathrm{Func}(n,n)]}(A) + \mathbf{Adv}^{\text{prf}}_{F}(A) \\ &\leq \frac{0.5(\mu/n)^2}{2^n} + \mathbf{Adv}^{\text{prf}}_{F}(A)\end{aligned}$$

(Proof Sketch)

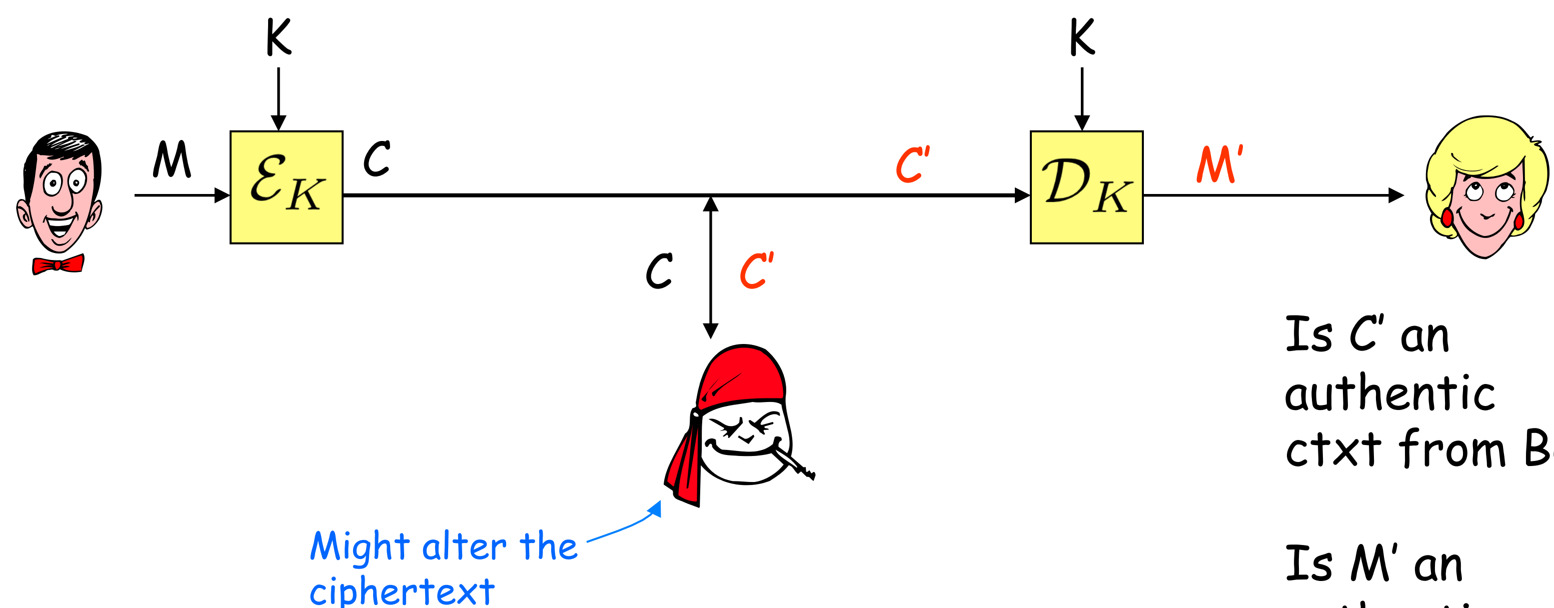


Until *f* is called on the same value twice, the ciphertext blocks are *random and independent* of the message blocks.

There are μ/n chances for an *f*-domain "collision"

Privacy? ✓ What about authenticity?

Authenticity: Alice wants to be **sure** she's received Bob's message

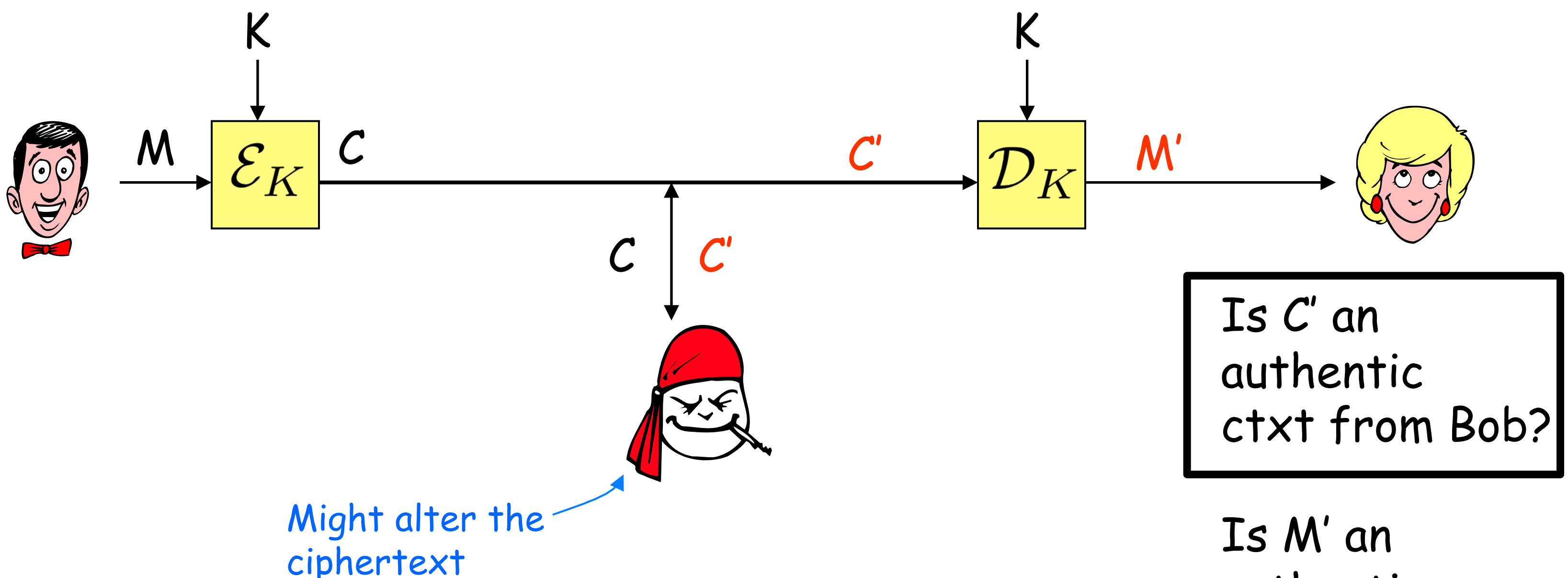


Is C' an authentic ctxt from Bob?

Is M' an authentic ptxt from Bob?

Privacy? ✓ What about authenticity?

Authenticity: Alice wants to be **sure** she's received Bob's message



Is M' an authentic ptxt from Bob?

First of all, we need a syntactic addition

(New primitive, new syntax!)

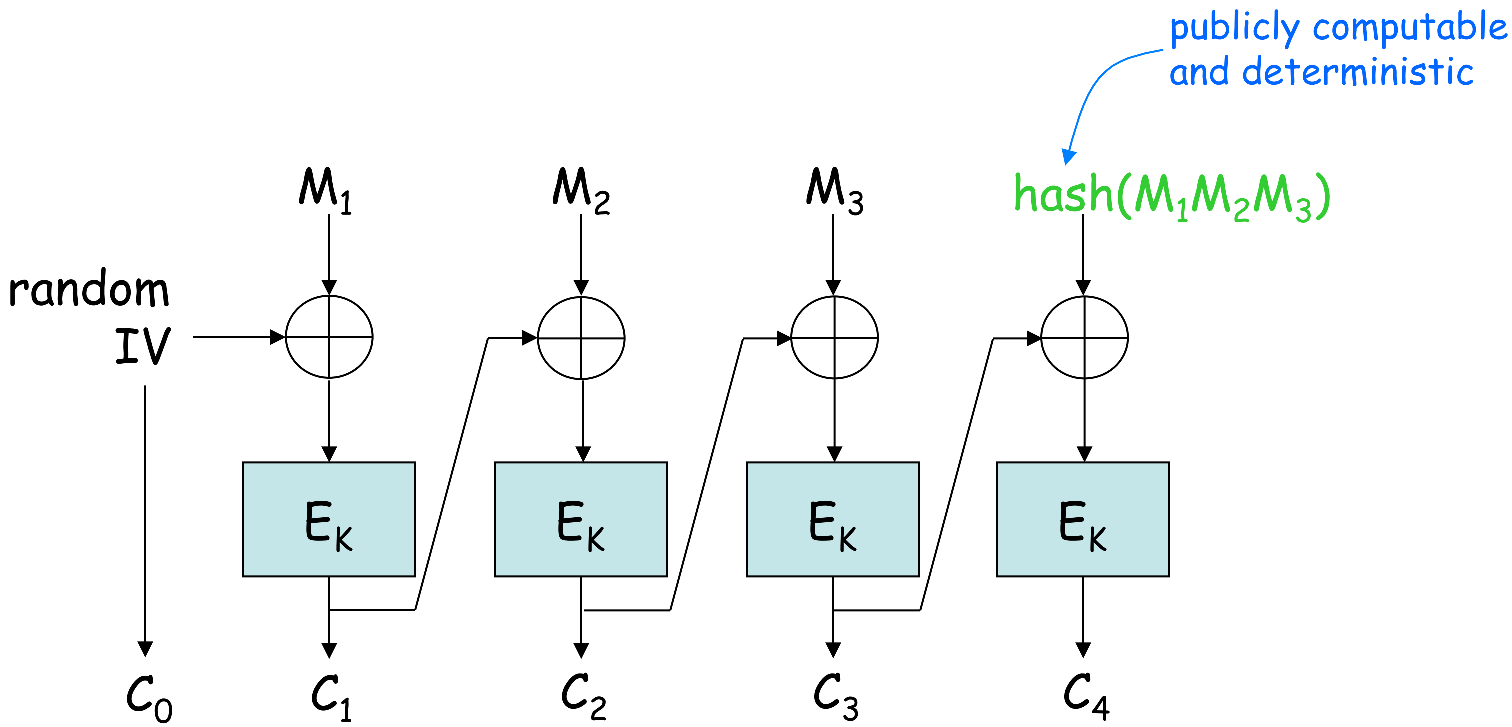
Key-generation algorithm $\mathcal{K}$ samples from a set of the same name

Encryption algorithm $\mathcal{E}: \mathcal{K} \times \{0,1\}^* \rightarrow \{0,1\}^* \cup \{\perp\}$

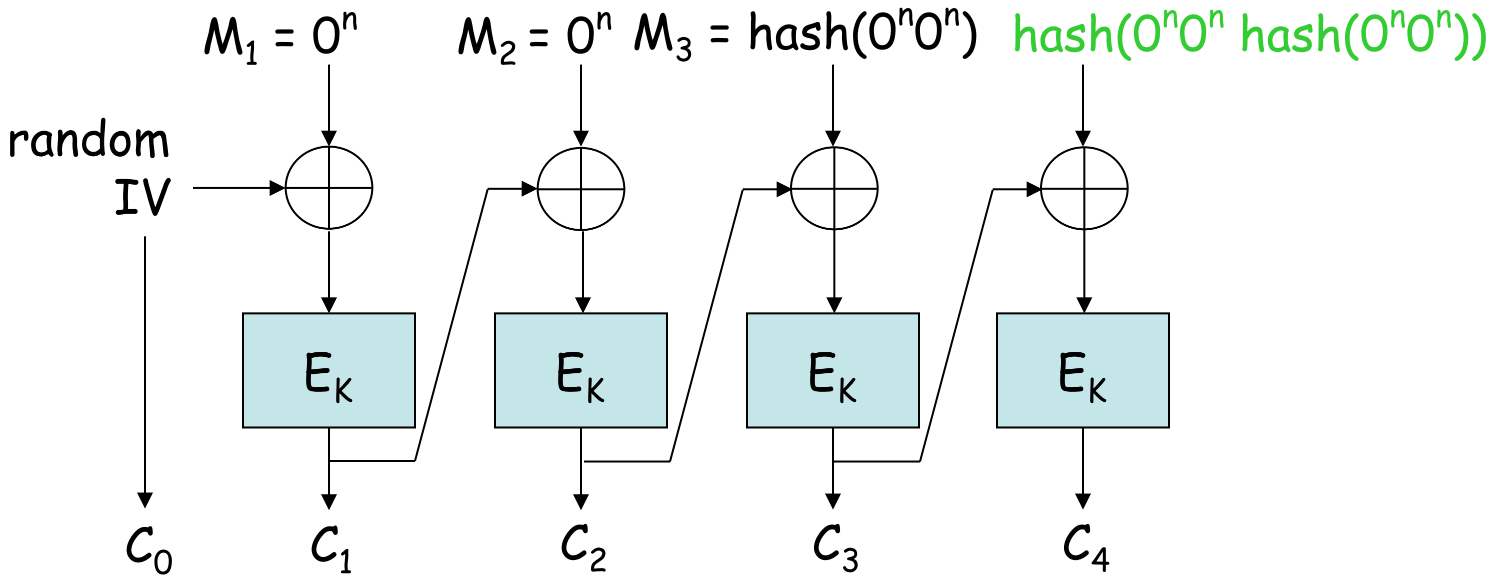
Decryption algorithm $\mathcal{D}: \mathcal{K} \times \{0,1\}^* \rightarrow \{0,1\}^* \cup \{\perp\}$

Decryption now has the ability to "complain"

Folklore idea: add "redundancy" to encryption



Decryption: just like CBC, except return $\perp$ if hash doesn't match



Can you forge an authentic ciphertext?

$C_0\ C_1\ C_2\ C_3$ decrypts properly,
and so is "authentic" by the
if-it-decrypts-the-authentic measure…

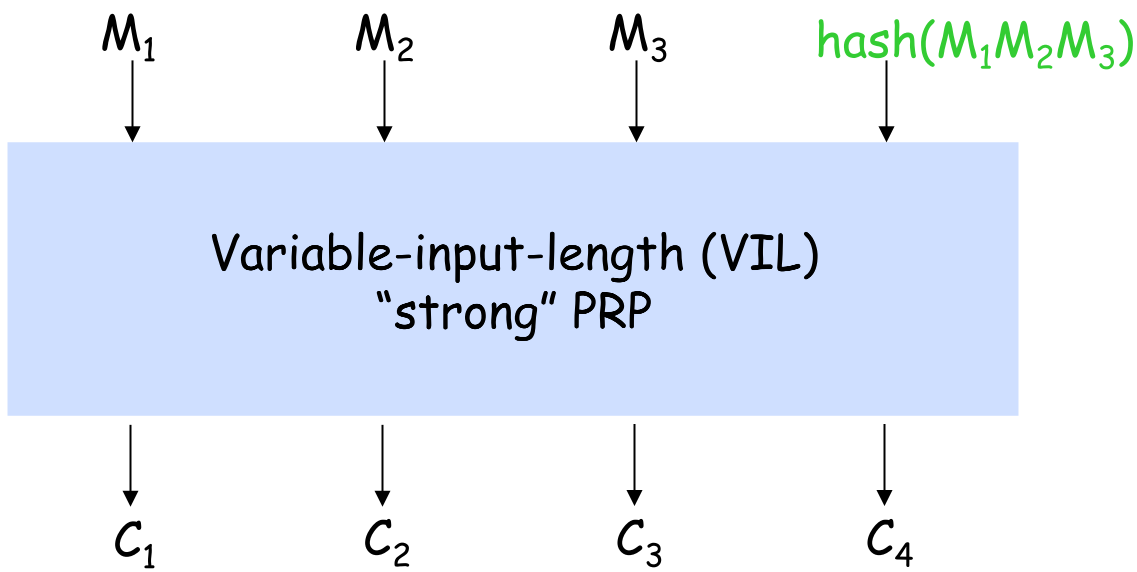
So what's wrong?

It's not CBC-mode is "bad", it's just that traditional encryption schemes have been designed to provide

PRIVACY ONLY

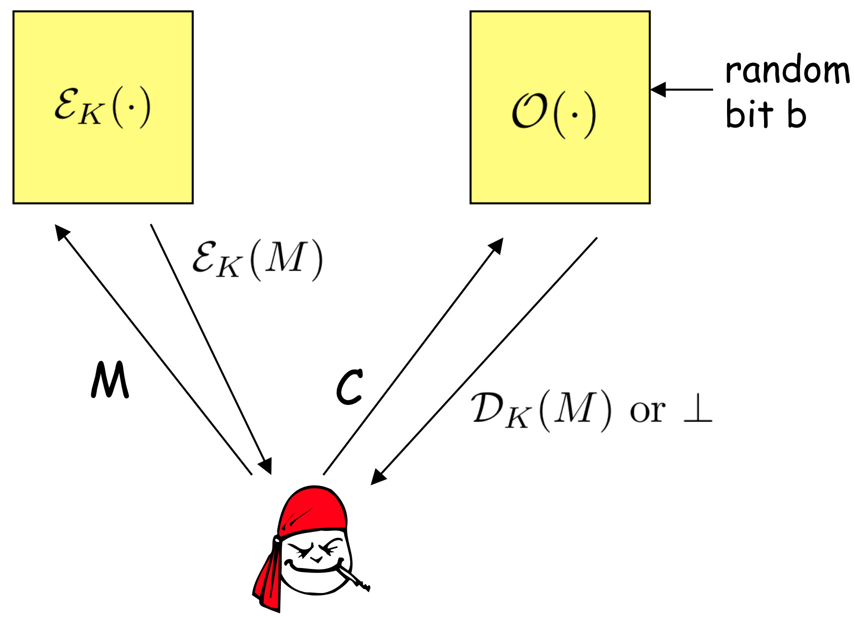
(

This *can* be made to work… (more later)



)

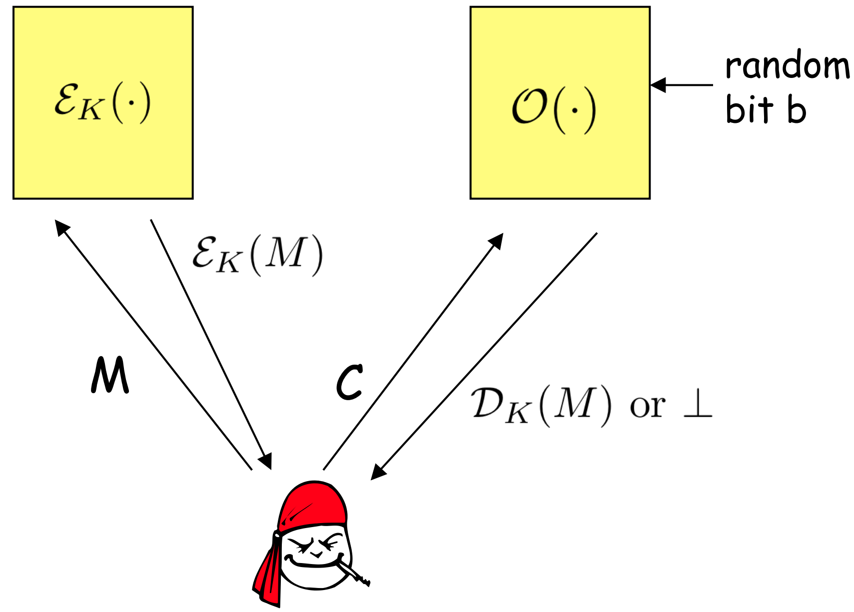
A notion of "authenticity": Integrity of Ciphertexts (INT-CTXT)



A notion of "authenticity": Integrity of Ciphertexts (INT-CTXT)

$\underline{\mathbf{Exp}_{\Pi}^{\text{int-ctxt}}(A)}$:
$K \xleftarrow{\$} \mathcal{K}$
$b \xleftarrow{\$} \{0,1\}$
$b' \xleftarrow{\$} A^{\mathcal{E}_K(\cdot),\mathcal{O}(\cdot)}$
If $b' = b$ then Return 1
Return 0

$\underline{\text{Oracle } \mathcal{O}(C)}$:
If $b = 0$ then Return $\perp$
Return $\mathcal{D}_K(C)$



$$\mathbf{Adv}_{\Pi}^{\text{int-ctxt}}(A) = 2\Pr(\mathbf{Exp}_{\Pi}^{\text{int-ctxt}}(A) = 1) - 1$$

Adversarial "resources":
the number of oracle queries, q_e, q_d
the total length in bits of the queries, μ_e, μ_d
the time-complexity of the adversary, t

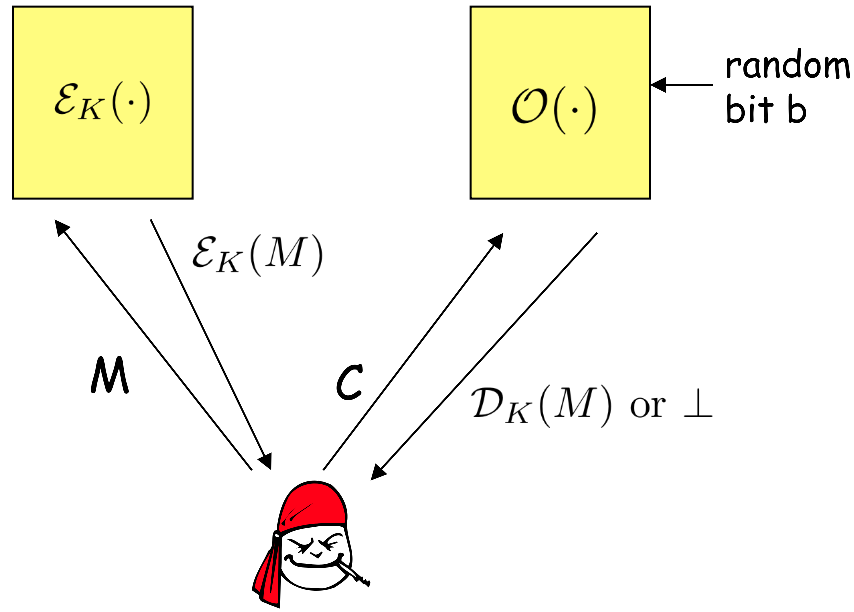
A notion of "authenticity": Integrity of Ciphertexts (INT-CTXT)

$\underline{\mathbf{Exp}^{\text{int-ctxt}}_{\Pi}(A)\text{:}}$

$K \stackrel{\$}{\leftarrow} \mathcal{K}$
$b \stackrel{\$}{\leftarrow} \{0,1\}$
$b' \stackrel{\$}{\leftarrow} A^{\mathcal{E}_K(\cdot),\mathcal{O}(\cdot)}$
If $b' = b$ then Return 1
Return 0

$\underline{\text{Oracle } \mathcal{O}(C)\text{:}}$

If $b = 0$ then Return $\perp$
Return $\mathcal{D}_K(C)$



$$\mathbf{Adv}^{\text{int-ctxt}}_{\Pi}(A) = 2\Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\Pi}(A) = 1) - 1$$

To prevent "trivial wins" of the game, adversary is forbidden to ask C of the right oracle if C was returned by the left oracle

Building a simple INT-CTXT secure encryption scheme

Let $F : \mathcal{K} \times \{0,1\}^* \to \{0,1\}^n$ be a function family.

Define an encryption scheme $\Pi[\ F\ ]$ as follows:

$$\mathcal{E}_K(M) = M \parallel F_K(M)$$

$$\mathcal{D}_K(X \parallel T) = \begin{cases} X & \text{if } F_K(X) = T \\ \perp & \text{otherwise} \end{cases}$$

Claim: if $F: \mathcal{K} \times \{0,1\}^* \to \{0,1\}^n$ is a secure PRF, then $\Pi[F]$ is an INT-CTXT secure encryption scheme

---

Proof idea: break the proof into two steps

1. replace F_K with a random function f, and argue that any adversary that can detect this can "break" PRF-security of F

2. analyze INT-CTXT security of $\Pi[\mathrm{Func}(*, n)]$

$$\mathbf{Adv}^{\text{int-ctxt}}_{\Pi[F]}(A) = 2\mathbf{Adv}^{\text{prf}}_{F}(B) + \frac{q_d}{2^n}$$

$$
\begin{aligned}
\frac{1}{2}\mathbf{Adv}^{\text{int-ctxt}}_{\Pi[F]}(A) + \frac{1}{2} &= \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\Pi[F]}(A) = 1) \\
&= \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\Pi[F]}(A) = 1) - \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\Pi[\text{Func}(*,n)]}(A) = 1) \\
&\qquad + \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\Pi[\text{Func}(*,n)]}(A) = 1) \\
&\leq \mathbf{Adv}^{\text{prf}}_{F}(B) + \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\Pi[\text{Func}(*,n)]}(A) = 1)
\end{aligned}
$$

$$
\begin{aligned}
\frac{1}{2}\mathbf{Adv}^{\text{int-ctxt}}_{\Pi[F]}(A) + \frac{1}{2} &= \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\Pi[F]}(A) = 1) \\
&= \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\Pi[F]}(A) = 1) - \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\Pi[\text{Func}(*,n)]}(A) = 1) \\
&\qquad + \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\Pi[\text{Func}(*,n)]}(A) = 1) \\
&\leq \mathbf{Adv}^{\text{prf}}_{F}(B) + \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\Pi[\text{Func}(*,n)]}(A) = 1)
\end{aligned}
$$

Adversary $B^{g(\cdot)}$:

Run A When A asks M to its left oracle:
  Respond with $M \parallel g(M)$
When A asks $X \parallel T$ to its right oracle:
  Respond with X if $g(X) = T$; else $\perp$
When A halts with output bit b:
  Return b

If the bit b in the PRF experiment is 1 (resp. 0), then B simulates the INT-CTXT experiment for $\Pi[F]$ (resp. $\Pi[Func(*,n)]$)

$$
\begin{aligned}
\frac{1}{2}\mathbf{Adv}^{\text{int-ctxt}}_{\Pi[F]}(A) + \frac{1}{2} &= \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\Pi[F]}(A) = 1) \\
&= \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\Pi[F]}(A) = 1) - \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\Pi[\text{Func}(*,n)]}(A) = 1) \\
&\qquad + \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\Pi[\text{Func}(*,n)]}(A) = 1) \\
&\leq \mathbf{Adv}^{\text{prf}}_{F}(B) + \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\Pi[\text{Func}(*,n)]}(A) = 1) \\
\text{Hence,} & \\
\mathbf{Adv}^{\text{int-ctxt}}_{\Pi[F]}(A) &\leq 2\mathbf{Adv}^{\text{prf}}_{F}(B) + 2\Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\Pi[\text{Func}(*,n)]}(A) = 1) - 1 \\
&= 2\mathbf{Adv}^{\text{prf}}_{F}(B) + \mathbf{Adv}^{\text{int-ctxt}}_{\Pi[\text{Func}(*,n)]}(A)
\end{aligned}
$$

Consider $\Pi[\mathrm{Func}(*, n)]$

f is a random function

$$\mathcal{E}_K(M) = M \parallel f(M)$$

$$\mathcal{D}_K(X \parallel T) = \begin{cases} X & \text{if } f(X) = T \\ \perp & \text{otherwise} \end{cases}$$

Consider $\Pi[\mathrm{Func}(*, n)]$

f is a random function

$$\mathcal{E}_K(M) = M \parallel f(M)$$

$$\mathcal{D}_K(X \parallel T) = \begin{cases} X & \text{if } f(X) = T \\ \perp & \text{otherwise} \end{cases}$$

Decryption cases

0. (X, T) old: not allowed

(i.e. T not the tag previously returned with X)

1. X old, T "new": returns $\perp$ because f is deterministic

Consider $\Pi[\mathrm{Func}(*, n)]$

f is a random function

$$\mathcal{E}_K(M) = M \parallel f(M)$$

$$\mathcal{D}_K(X \parallel T) = \begin{cases} X & \text{if } f(X) = T \\ \perp & \text{otherwise} \end{cases}$$

Decryption cases

0. (X, T) old: not allowed

(i.e. T not the tag previously returned with X)

1. X old, T "new": returns $\perp$ because f is deterministic

2. X new, T old: f(x) uniformly random, $\Pr(f(X) = T) = 2^{-n}$

Consider $\Pi[\mathrm{Func}(*, n)]$

f is a random function

$$\mathcal{E}_K(M) = M \parallel f(M)$$

$$\mathcal{D}_K(X \parallel T) = \begin{cases} X & \text{if } f(X) = T \\ \perp & \text{otherwise} \end{cases}$$

Decryption cases

0. (X, T) old: not allowed

(i.e. T not the tag previously returned with X)

1. X old, T "new": returns $\perp$ because f is deterministic

2. X new, T old: f(x) uniformly random, $\Pr(f(X) = T) = 2^{-n}$

3. X new, T new: f(x) uniformly random, $\Pr(f(X) = T) = 2^{-n}$

$$
\begin{aligned}
\frac{1}{2}\mathbf{Adv}^{\text{int-ctxt}}_{\Pi[F]}(A) + \frac{1}{2} &= \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\Pi[F]}(A) = 1) \\
&= \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\Pi[F]}(A) = 1) - \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\Pi[\text{Func}(*,n)]}(A) = 1) \\
&\qquad + \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\Pi[\text{Func}(*,n)]}(A) = 1) \\
&\leq \mathbf{Adv}^{\text{prf}}_{F}(B) + \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\Pi[\text{Func}(*,n)]}(A) = 1) \\
\text{Hence,} & \\
\mathbf{Adv}^{\text{int-ctxt}}_{\Pi[F]}(A) &\leq 2\mathbf{Adv}^{\text{prf}}_{F}(B) + 2\Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\Pi[\text{Func}(*,n)]}(A) = 1) - 1 \\
&= 2\mathbf{Adv}^{\text{prf}}_{F}(B) + \mathbf{Adv}^{\text{int-ctxt}}_{\Pi[\text{Func}(*,n)]}(A) \\
&\leq 2\mathbf{Adv}^{\text{prf}}_{F}(B) + \frac{q_d}{2^n}
\end{aligned}
$$

Adding IND-CPA…

Let $F\colon \mathcal{K}_F \times \{0,1\}^* \to \{0,1\}^n$ be a function family.

Let $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be an encryption scheme

Define an encryption scheme $\overline{\Pi} = (\overline{\mathcal{K}}, \overline{\mathcal{E}}, \overline{\mathcal{D}})$ as follows:

$$\overline{\mathcal{K}}: \text{ Return } (K1, K2) \xleftarrow{\$} \mathcal{K} \times \mathcal{K}_F$$

$$\overline{\mathcal{E}}_{K1}(M) = \mathcal{E}_{K1}(M) \parallel F_{K2}(\mathcal{E}_{K1}(M))$$

$$\overline{\mathcal{D}}_{K1,K2}(C \parallel T) = \begin{cases} \mathcal{D}_{K1}(C) & \text{if } F_{K2}(C) = T \\ \perp & \text{otherwise} \end{cases}$$

This is called "Encrypt-then-MAC"

Claim: if $F: \mathcal{K}_F \times \{0,1\}^* \to \{0,1\}^n$ is a secure PRF, and $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is IND-CPA secure, then $\overline{\Pi} = (\overline{\mathcal{K}}, \overline{\mathcal{E}}, \overline{\mathcal{D}})$ is both IND-CPA and INT-CTXT secure

Claim: if $F: \mathcal{K}_F \times \{0,1\}^* \to \{0,1\}^n$ is a secure PRF, and $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is IND-CPA secure, then $\overline{\Pi} = (\overline{\mathcal{K}}, \overline{\mathcal{E}}, \overline{\mathcal{D}})$ is both IND-CPA and INT-CTXT secure

Let's do the easy part first: INT-CTXT

$$
\begin{aligned}
\frac{1}{2}\mathbf{Adv}^{\text{int-ctxt}}_{\overline{\Pi}[F]}(A) + \frac{1}{2} &= \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\overline{\Pi}[F]}(A) = 1) \\
&= \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\overline{\Pi}[F]}(A) = 1) - \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\overline{\Pi}[\text{Func}(*,n)]}(A) = 1) \\
&\quad + \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\overline{\Pi}[\text{Func}(*,n)]}(A) = 1) \\
&\leq \mathbf{Adv}^{\text{prf}}_{F}(B) + \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\overline{\Pi}[\text{Func}(*,n)]}(A) = 1)
\end{aligned}
$$

<u>Claim</u>: if $F: \mathcal{K}_F \times \{0,1\}^* \rightarrow \{0,1\}^n$ is a secure PRF,
and $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is IND-CPA secure, then $\overline{\Pi} = (\overline{\mathcal{K}}, \overline{\mathcal{E}}, \overline{\mathcal{D}})$
is both IND-CPA and INT-CTXT secure

Let's do the easy part first: INT-CTXT

$$\begin{aligned}
\frac{1}{2}\mathbf{Adv}^{\text{int-ctxt}}_{\overline{\Pi}[F]}(A) + \frac{1}{2} &= \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\overline{\Pi}[F]}(A) = 1) \\
&= \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\overline{\Pi}[F]}(A) = 1) - \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\overline{\Pi}[\text{Func}(*,n)]}(A) = 1) \\
&\quad + \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\overline{\Pi}[\text{Func}(*,n)]}(A) = 1) \\
&\leq \mathbf{Adv}^{\text{prf}}_{F}(B) + \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\overline{\Pi}[\text{Func}(*,n)]}(A) = 1)
\end{aligned}$$

<u>Adversary $B^{g(\cdot)}$:</u>

$K1 \xleftarrow{\$} \mathcal{K}$
Run A When A asks M to its left oracle:
    $C \xleftarrow{\$} \mathcal{E}_{K1}(M)$
    Respond with $C \parallel g(C)$
When A asks $X \parallel T$ to its right oracle:
    Respond with $\mathcal{D}_{K1}(X)$ if $g(X) = T$; else $\perp$
When A halts with output bit b:
    Return b

If the bit b in the PRF experiment is 1 (resp. 0), then B simulates the INT-CTXT experiment for $\Pi[F]$ (resp. $\Pi[Func(*,n)]$)

Claim: if $F : \mathcal{K}_F \times \{0,1\}^* \to \{0,1\}^n$ is a secure PRF, and $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is IND-CPA secure, then $\overline{\Pi} = (\overline{\mathcal{K}}, \overline{\mathcal{E}}, \overline{\mathcal{D}})$ is both IND-CPA and INT-CTXT secure

---

Let's do the easy part first: INT-CTXT

$$\begin{aligned}
\frac{1}{2}\mathbf{Adv}^{\text{int-ctxt}}_{\overline{\Pi}[F]}(A) + \frac{1}{2} &= \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\overline{\Pi}[F]}(A) = 1) \\
&= \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\overline{\Pi}[F]}(A) = 1) - \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\overline{\Pi}[\text{Func}(*,n)]}(A) = 1) \\
&\quad + \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\overline{\Pi}[\text{Func}(*,n)]}(A) = 1) \\
&\leq \mathbf{Adv}^{\text{prf}}_F(B) + \Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\overline{\Pi}[\text{Func}(*,n)]}(A) = 1) \\
\text{Hence,} & \\
\mathbf{Adv}^{\text{int-ctxt}}_{\overline{\Pi}[F]}(A) &\leq 2\mathbf{Adv}^{\text{prf}}_F(B) + 2\Pr(\mathbf{Exp}^{\text{int-ctxt}}_{\overline{\Pi}[\text{Func}(*,n)]}(A) = 1) - 1 \\
&= 2\mathbf{Adv}^{\text{prf}}_F(B) + \mathbf{Adv}^{\text{int-ctxt}}_{\overline{\Pi}[\text{Func}(*,n)]}(A) \\
&\leq 2\mathbf{Adv}^{\text{prf}}_F(B) + \frac{q_d}{2^n}
\end{aligned}$$

Claim: if $F: \mathcal{K}_F \times \{0,1\}^* \to \{0,1\}^n$ is a secure PRF, and $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is IND-CPA secure, then $\overline{\Pi} = (\overline{\mathcal{K}}, \overline{\mathcal{E}}, \overline{\mathcal{D}})$ is both IND-CPA and INT-CTXT secure

Now the "new" part: IND-CPA.

But this is even easier! $\overline{\mathcal{E}}_{K1}(M) = \mathcal{E}_{K1}(M) \parallel F_{K2}(\mathcal{E}_{K1}(M))$

$$\begin{aligned}
\frac{1}{2}\mathbf{Adv}^{\text{ind-cpa}}_{\overline{\Pi}[F]}(A) + \frac{1}{2} &= \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\overline{\Pi}[F]}(A) = 1) \\
&= \Pr(\mathbf{Exp}^{\text{ind-cpa}}_{\Pi[F]}(B) = 1) \\
\text{Hence,} & \\
\mathbf{Adv}^{\text{ind-cpa}}_{\overline{\Pi}[F]}(A) &\leq \mathbf{Adv}^{\text{ind-cpa}}_{\Pi[F]}(B)
\end{aligned}$$

Where this reduction B simulates the F_{K2} part of encryption

The three "Generic Composition" authenticated encryption schemes

Encrypt-then-MAC:

$$\overline{\mathcal{E}}_{K1}(M) = \mathcal{E}_{K1}(M) \parallel F_{K2}(\mathcal{E}_{K1}(M))$$

(IPSec)

$$\overline{\mathcal{D}}_{K1,K2}(C \parallel T) = \begin{cases} \mathcal{D}_{K1}(C) & \text{if } F_{K2}(C) = T \\ \perp & \text{otherwise} \end{cases}$$

✓ IND-CPA
✓ INT-CTXT

The three "Generic Composition" authenticated encryption schemes

Encrypt-then-MAC: (IPSec)

✓ IND-CPA
✓ INT-CTXT

$$\overline{\mathcal{E}}_{K1}(M) = \mathcal{E}_{K1}(M) \parallel F_{K2}(\mathcal{E}_{K1}(M))$$

$$\overline{\mathcal{D}}_{K1,K2}(C \parallel T) = \begin{cases} \mathcal{D}_{K1}(C) & \text{if } F_{K2}(C) = T \\ \perp & \text{otherwise} \end{cases}$$

MAC-then-Encrypt: (SSL/TLS)

$$\overline{\mathcal{E}}_{K1,K2}(M) = \mathcal{E}_{K1}(M \parallel F_{K2}(M))$$

$$\overline{\mathcal{D}}_{K1,K2}(C) = \begin{cases} M' \parallel T \leftarrow \mathcal{D}_{K1}(C) \text{ then:} \\ \quad \text{Return } M' \text{ if } F_{K2}(M') = T \\ \quad \text{Return } \perp \text{ otherwise} \end{cases}$$

The three "Generic Composition" authenticated encryption schemes

Encrypt-then-MAC:

$$\overline{\mathcal{E}}_{K1}(M) = \mathcal{E}_{K1}(M) \parallel F_{K2}(\mathcal{E}_{K1}(M))$$

(IPSec)

✓ IND-CPA
✓ INT-CTXT

$$\overline{\mathcal{D}}_{K1,K2}(C \parallel T) = \begin{cases} \mathcal{D}_{K1}(C) & \text{if } F_{K2}(C) = T \\ \perp & \text{otherwise} \end{cases}$$

MAC-then-Encrypt:

$$\overline{\mathcal{E}}_{K1,K2}(M) = \mathcal{E}_{K1}(M \parallel F_{K2}(M))$$

(SSL/TLS)

✓ IND-CPA
✗ INT-CTXT

$$\overline{\mathcal{D}}_{K1,K2}(C) = \begin{cases} M' \parallel T \leftarrow \mathcal{D}_{K1}(C) \text{ then:} \\ \quad \text{Return } M' \text{ if } F_{K2}(M') = T \\ \quad \text{Return } \perp \text{ otherwise} \end{cases}$$

The three "Generic Composition" authenticated encryption schemes

Encrypt-then-MAC: (IPSec)

✓ IND-CPA
✓ INT-CTXT

$$\overline{\mathcal{E}}_{K1}(M) = \mathcal{E}_{K1}(M) \parallel F_{K2}(\mathcal{E}_{K1}(M))$$

$$\overline{\mathcal{D}}_{K1,K2}(C \parallel T) = \begin{cases} \mathcal{D}_{K1}(C) & \text{if } F_{K2}(C) = T \\ \bot & \text{otherwise} \end{cases}$$

MAC-then-Encrypt: (SSL/TLS)

✓ IND-CPA
✗ INT-CTXT

$$\overline{\mathcal{E}}_{K1,K2}(M) = \mathcal{E}_{K1}(M \parallel F_{K2}(M))$$

$$\overline{\mathcal{D}}_{K1,K2}(C) = \begin{cases} M' \parallel T \leftarrow \mathcal{D}_{K1}(C) \text{ then:} \\ \quad \text{Return } M' \text{ if } F_{K2}(M') = T \\ \quad \text{Return } \bot \text{ otherwise} \end{cases}$$

MAC and Encrypt: (SSH)
(or Encrypt and MAC)

$$\overline{\mathcal{E}}_{K1,K2}(M) = \mathcal{E}_{K1}(M) \parallel F_{K2}(M)$$

$$\overline{\mathcal{D}}_{K1,K2}(C \parallel T) = \begin{cases} M' \leftarrow \mathcal{D}_{K1}(C) \text{ then:} \\ \quad \text{Return } M' \text{ if } F_{K2}(M') = T \\ \quad \text{Return } \bot \text{ otherwise} \end{cases}$$

The three "Generic Composition" authenticated encryption schemes

Encrypt-then-MAC: (IPSec)

✓ IND-CPA
✓ INT-CTXT

$$\overline{\mathcal{E}}_{K1}(M) = \mathcal{E}_{K1}(M) \parallel F_{K2}(\mathcal{E}_{K1}(M))$$

$$\overline{\mathcal{D}}_{K1,K2}(C \parallel T) = \begin{cases} \mathcal{D}_{K1}(C) & \text{if } F_{K2}(C) = T \\ \perp & \text{otherwise} \end{cases}$$

MAC-then-Encrypt: (SSL/TLS)

✓ IND-CPA
✗ INT-CTXT

$$\overline{\mathcal{E}}_{K1,K2}(M) = \mathcal{E}_{K1}(M \parallel F_{K2}(M))$$

$$\overline{\mathcal{D}}_{K1,K2}(C) = \begin{cases} M' \parallel T \leftarrow \mathcal{D}_{K1}(C) \text{ then:} \\ \quad \text{Return } M' \text{ if } F_{K2}(M') = T \\ \quad \text{Return } \perp \text{ otherwise} \end{cases}$$

MAC and Encrypt: (SSH)
(or Encrypt and MAC)

✗ IND-CPA
✗ INT-CTXT

$$\overline{\mathcal{E}}_{K1,K2}(M) = \mathcal{E}_{K1}(M) \parallel F_{K2}(M)$$

$$\overline{\mathcal{D}}_{K1,K2}(C \parallel T) = \begin{cases} M' \leftarrow \mathcal{D}_{K1}(C) \text{ then:} \\ \quad \text{Return } M' \text{ if } F_{K2}(M') = T \\ \quad \text{Return } \perp \text{ otherwise} \end{cases}$$

(Bellare, Namprempre)

(Violating INT-CTXT)

Consider $\mathcal{E}_{K1}(X) = 0 \,\|\, \mathcal{E}'_{K1}(X)$

$\mathcal{D}_{K1}(b \,\|\, C) = \mathcal{D}'_{K1}(C)$ which is IND-CPA if $\mathcal{E}'_{K1}(X)$ is...

MAC-then-Encrypt:

✓ IND-CPA

✗ INT-CTXT

$$\overline{\mathcal{E}}_{K1,K2}(M) = \mathcal{E}_{K1}(M \,\|\, F_{K2}(M))$$

$$\overline{\mathcal{D}}_{K1,K2}(C) = \begin{cases} M' \,\|\, T \leftarrow \mathcal{D}_{K1}(C) \text{ then:} \\ \quad \text{Return } M' \text{ if } F_{K2}(M') = T \\ \quad \text{Return } \perp \text{ otherwise} \end{cases}$$

MAC and Encrypt:
(or Encrypt and MAC)

✗ IND-CPA

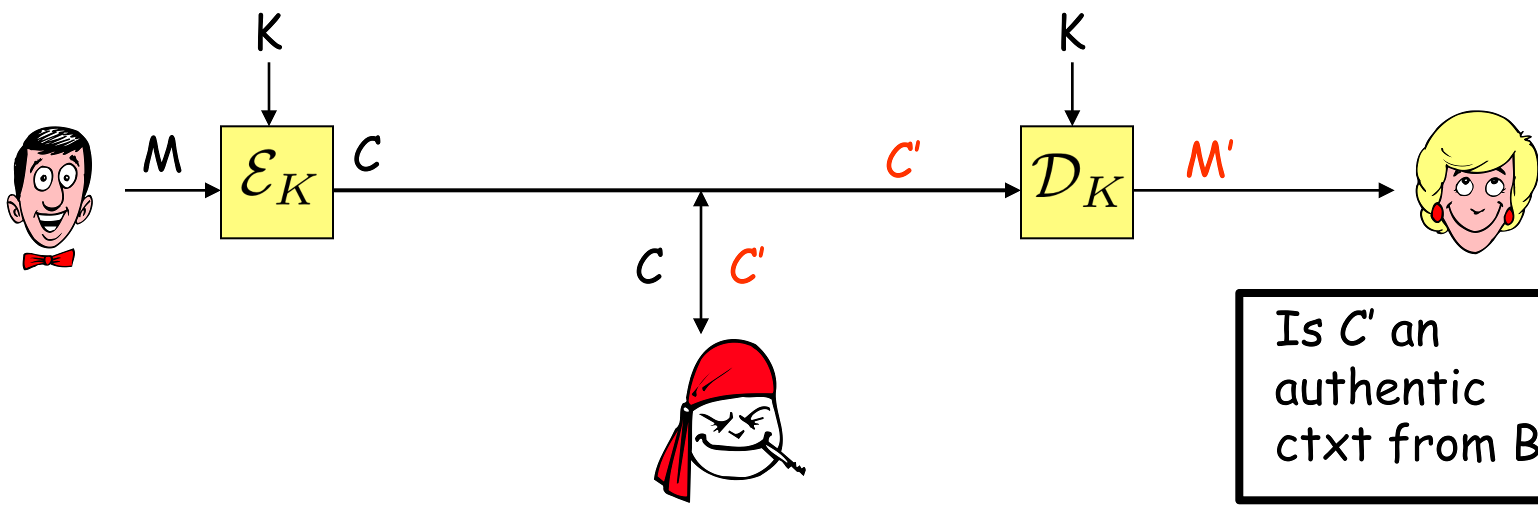
✗ INT-CTXT

$$\overline{\mathcal{E}}_{K1,K2}(M) = \mathcal{E}_{K1}(M) \,\|\, F_{K2}(M)$$

$$\overline{\mathcal{D}}_{K1,K2}(C \,\|\, T) = \begin{cases} M' \leftarrow \mathcal{D}_{K1}(C) \text{ then:} \\ \quad \text{Return } M' \text{ if } F_{K2}(M') = T \\ \quad \text{Return } \perp \text{ otherwise} \end{cases}$$

Privacy? ✓ What about authenticity?

Authenticity: Alice wants to be **sure** she's received Bob's message

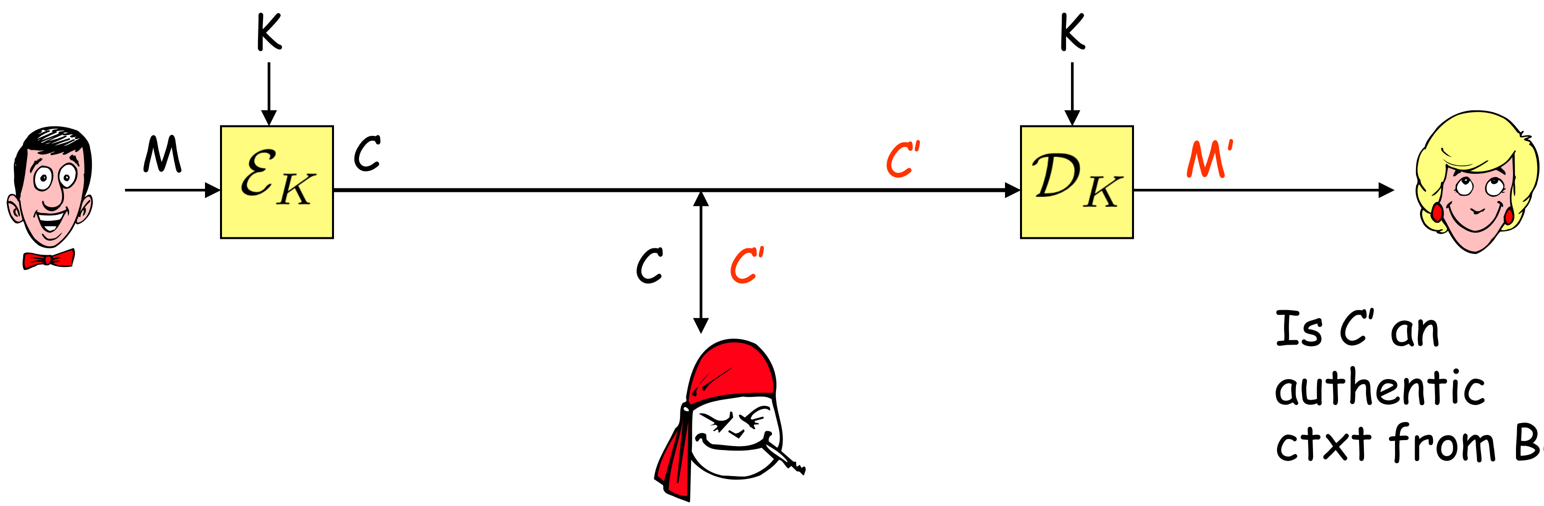


Is C' an authentic ctxt from Bob?

Is M' an authentic ptxt from Bob?

Privacy? ✓ What about authenticity?

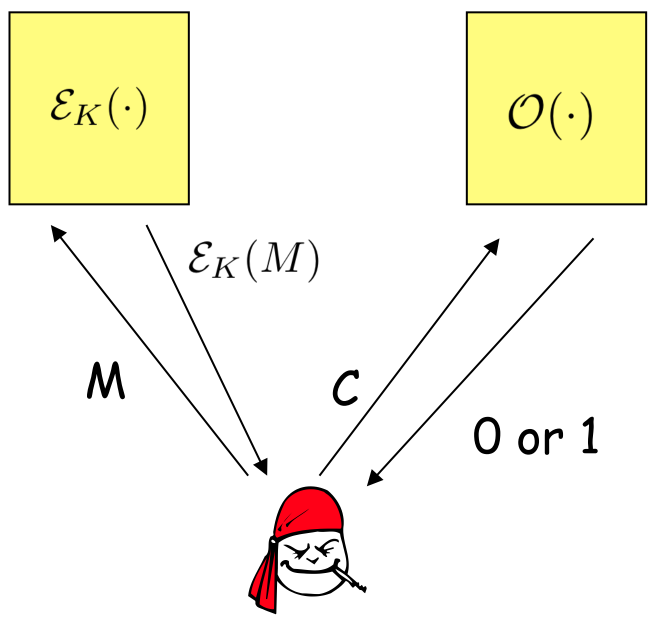
Authenticity: Alice wants to be **sure** she's received Bob's message



Is C' an authentic ctxt from Bob?

Is M' an authentic ptxt from Bob?

Another notion of "authenticity": Integrity of Plaintexts (INT-PTXT)



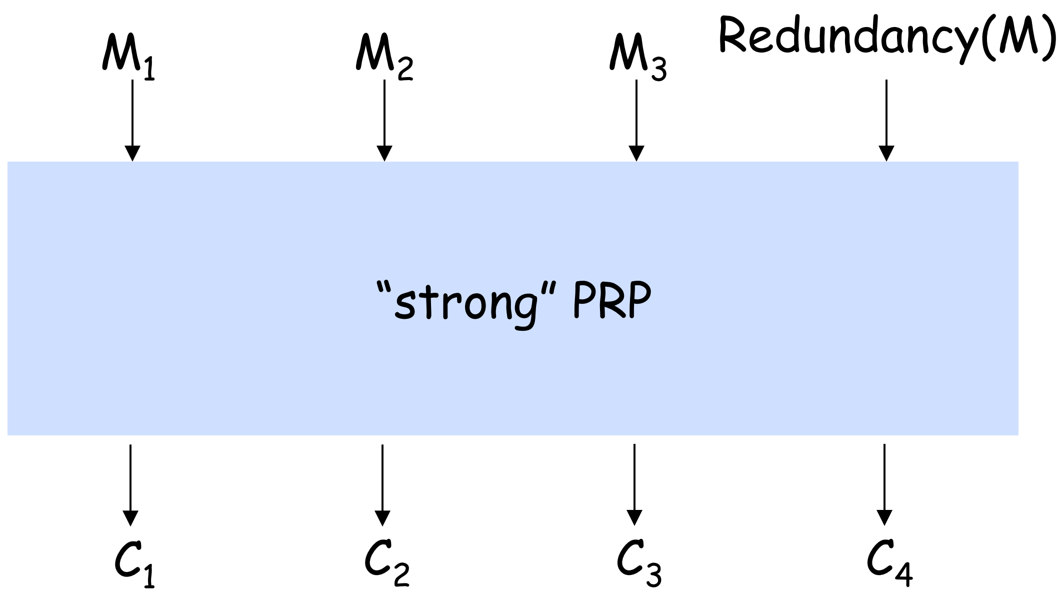
Adversary wins if it asks C such that

1. $\perp \neq M' \leftarrow \mathcal{D}_K(C)$
2. M' never asked to $\mathcal{E}_K(\cdot)$

+ Achieved (generically) by "MAC-then-Encrypt"
- Strictly weaker security goal
- Requires calling applications to be aware of repeated plaintexts
- Efficient schemes achieve INT-CTXT already

Stick with INT-CTXT if possible!

Let's return to this idea



Strong PRPs

Let $E\colon \mathcal{K} \times \{0,1\}^N \to \{0,1\}^N$ be a permutation family

$\underline{\mathbf{Exp}_E^{\mathrm{sprp}}(A)}$:

$K \xleftarrow{\$} \mathcal{K}$

$\pi \xleftarrow{\$} \mathrm{Perm}(N)$

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

$b' \xleftarrow{\$} A^{\mathcal{O}(\cdot),\mathcal{O}^{-1}(\cdot)}$

If $b' = b$ then Return 1

Return 0

$\underline{\text{Oracle } \mathcal{O}(X)}$:

If $b = 1$ Return $E_K(X)$

Else Return $\pi(X)$

$\underline{\text{Oracle } \mathcal{O}^{-1}(Y)}$:

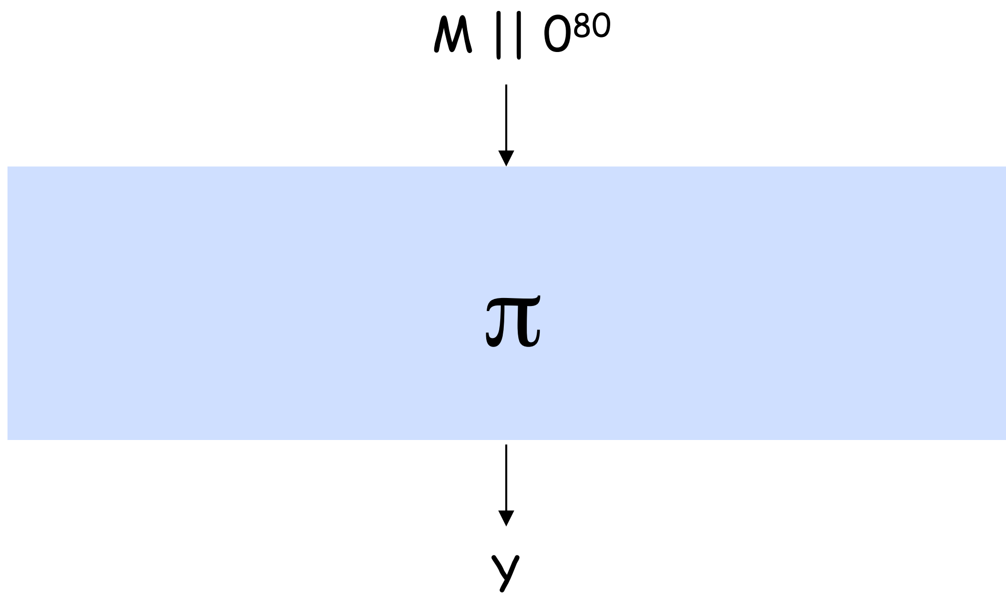
If $b = 1$ Return $E_K^{-1}(Y)$

Else Return $\pi^{-1}(Y)$

$$\mathbf{Adv}_E^{\mathrm{sprp}}(A) = 2\Pr(\mathbf{Exp}_E^{\mathrm{sprp}}(A) = 1) - 1$$

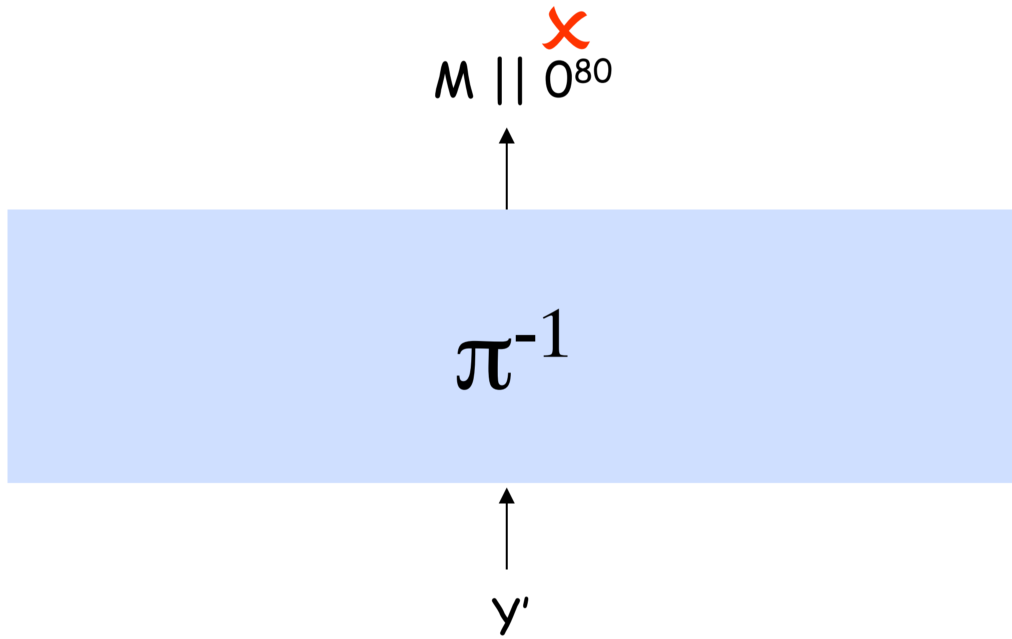
It's easy to extend this to the VIL setting, by considering $E\colon \mathcal{K} \times \mathcal{S} \to \mathcal{S}$, with $\mathcal{S} \subset \{0,1\}^*$, to be length-preserving.

Intuition: if you encrypt new messages, with redundancy…



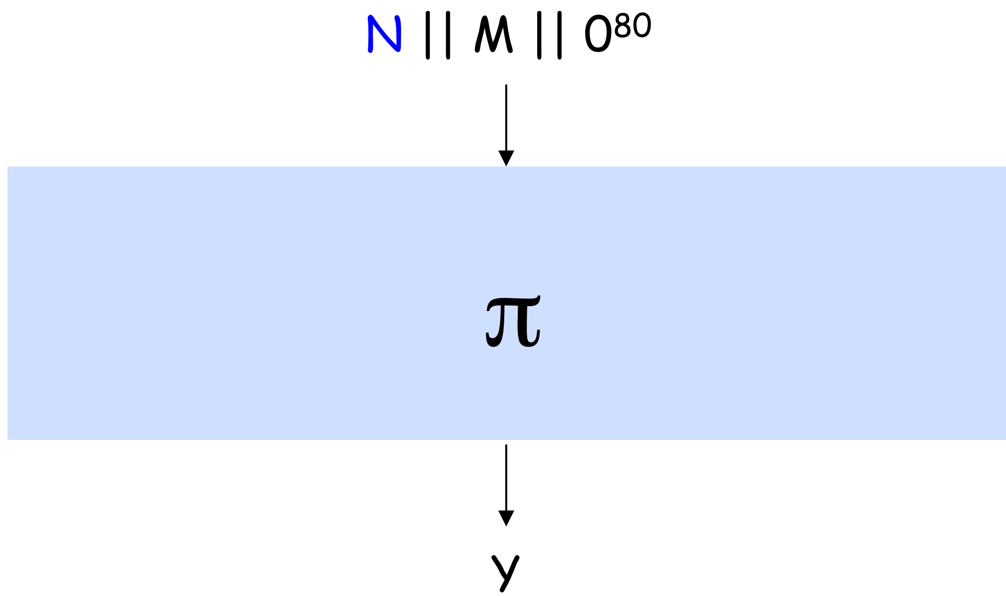
… then outputs look like random bitstrings (subject to permutivity)

Intuition: if you flip any bit of the output and decrypt…



… then "plaintexts" random, and unlikely to have correct redundancy

Of course, we're not guaranteed that messages are new, so we add a per-message "nonce" (number used once)



This is the "Encode-Encipher" paradigm, due to Bellare and Rogaway

New object, new syntax!

A nonce-based encryption scheme is a triple of algorithms

Key-generation algorithm $\mathcal{K}$ samples from a set of the same name

Encryption algorithm $\mathcal{E}\colon \mathcal{N} \times \mathcal{K} \times \{0,1\}^* \to \{0,1\}^* \cup \{\perp\}$

Decryption algorithm $\mathcal{D}\colon \mathcal{N} \times \mathcal{K} \times \{0,1\}^* \to \{0,1\}^* \cup \{\perp\}$

(See Rogaway's
Nonce-Based Encryption Paper)

New object, new syntax!

A nonce-based encryption scheme is a triple of algorithms

Key-generation algorithm $\mathcal{K}$ samples from a set of the same name

Encryption algorithm $\mathcal{E}: \mathcal{N} \times \mathcal{K} \times \{0,1\}^* \rightarrow \{0,1\}^* \cup \{\perp\}$

Decryption algorithm $\mathcal{D}: \mathcal{N} \times \mathcal{K} \times \{0,1\}^* \rightarrow \{0,1\}^* \cup \{\perp\}$

the nonce space

New object, new syntax!

A nonce-based encryption scheme is a triple of algorithms

Key-generation algorithm $\mathcal{K}$ samples from a set of the same name

Encryption algorithm $\mathcal{E}\colon \mathcal{N} \times \mathcal{K} \times \{0,1\}^* \to \{0,1\}^* \cup \{\bot\}$

Deterministic!

$C \leftarrow \mathcal{E}_K^N(M)$

Decryption algorithm $\mathcal{D}\colon \mathcal{N} \times \mathcal{K} \times \{0,1\}^* \to \{0,1\}^* \cup \{\bot\}$

IND-CPA in the nonce-based setting

$\underline{\mathbf{Exp}_{\Pi}^{\text{ind-cpa}}(A):}$
$K \xleftarrow{\$} \mathcal{K}$
$d \xleftarrow{\$} \{0,1\}$
$d' \xleftarrow{\$} A^{\mathcal{O}(\cdot,\cdot,\cdot)}$
If $d' = d$ then Return 1
Return 0

$\underline{\text{Oracle } \mathcal{O}(N, M_0, M_1):}$
If $d = 0$ then Return $\mathcal{E}_K^N(M_0)$
Return $\mathcal{E}_K^N(M_1)$

$$\mathbf{Adv}_{\Pi}^{\text{ind-cpa}}(A) = 2\Pr(\mathbf{Exp}_{\Pi}^{\text{ind-cpa}}(A) = 1) - 1$$

Restrictions:

1. $|M_0| = |M_1|$
2. No nonce-message pair $(N, M_0, \cdot)$ or $(N, \cdot, M_1)$ repeated

"Nonces" are meant to be used once.
An adversary that never repeats a nonce is called "nonce-respecting"

Let's define a nonce-based encryption scheme from an SPRP.

Let $\mathcal{N} = \{0,1\}^{128}$ and let $\mathcal{S} \subset \{0,1\}^*$ contain all strings up to length 128+80+L for some $L > 0$

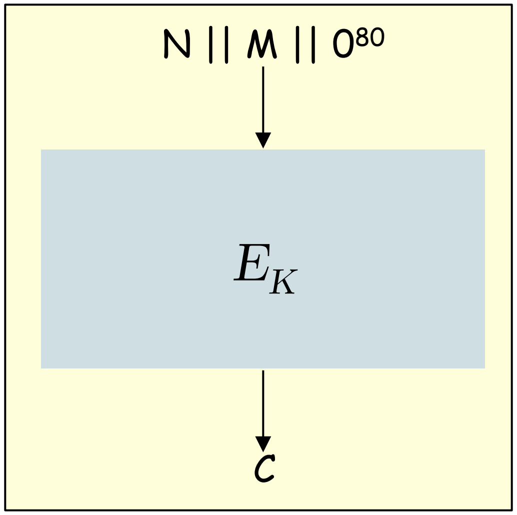
Let's define a nonce-based encryption scheme from an SPRP.

Let $\mathcal{N} = \{0,1\}^{128}$ and let $\mathcal{S} \subset \{0,1\}^*$ contain all strings up to length 128+80+L for some $L > 0$

Let $E\colon \mathcal{K} \times \mathcal{S} \to \mathcal{S}$ be a length-preserving permutation family.

$$\mathcal{E}_K^N(M) \quad = \quad E_K(N \,\|\, M \,\|\, 0^{80})$$

$$\mathcal{D}_K^N(C) \quad : \quad \begin{cases} X \leftarrow E_K^{-1}(C) \\ \text{Parse } X \text{ into } N, M, T \text{ where } |T| = 80 \\ \text{If parse fails, Return } \bot \\ \text{If } T \neq 0^{80} \text{ then Return } \bot \\ \text{Return } M \end{cases}$$



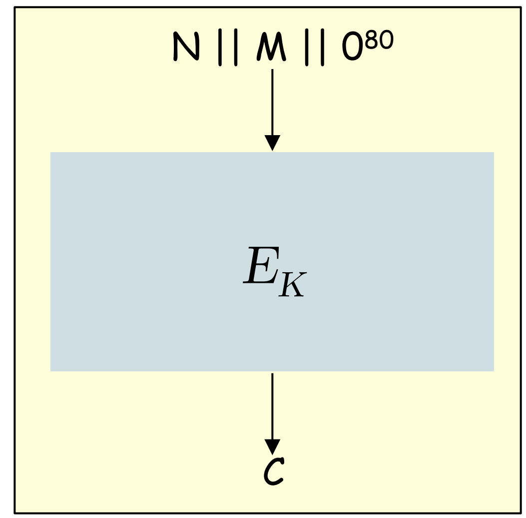
Let's define a nonce-based encryption scheme from an SPRP.

Let $\mathcal{N} = \{0,1\}^{128}$ and let $\mathcal{S} \subset \{0,1\}^*$ contain all strings up to length 128+80+L for some $L > 0$

Let $E\colon \mathcal{K} \times \mathcal{S} \to \mathcal{S}$ be a length-preserving permutation family.

$$\mathcal{E}_K^N(M) = E_K(N \,\|\, M \,\|\, 0^{80})$$

$$\mathcal{D}_K^N(C) : \begin{cases} X \leftarrow E_K^{-1}(C) \\ \text{Parse } X \text{ into } N, M, T \text{ where } |T| = 80 \\ \text{If parse fails, Return } \bot \\ \text{If } T \neq 0^{80} \text{ then Return } \bot \\ \text{Return } M \end{cases}$$

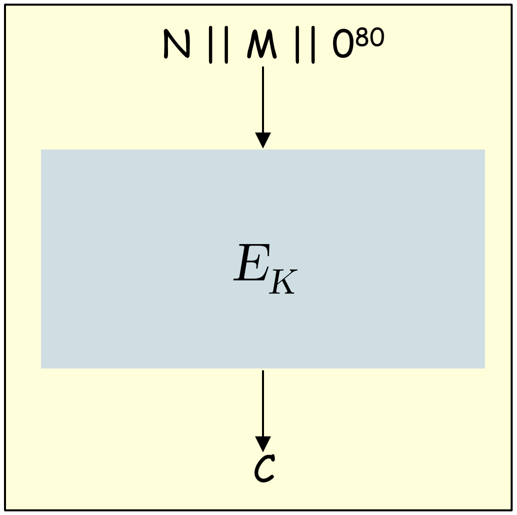


Claim: if $E\colon \mathcal{K} \times \mathcal{S} \to \mathcal{S}$ is a secure SPRP, then this scheme is both (nonce-based) IND-CPA and (nonce-based) INT-CTXT secure

Proof: exercise (you might need a "bi-directional" version of the PRP-PRF switching lemma…)

Proof intuition:

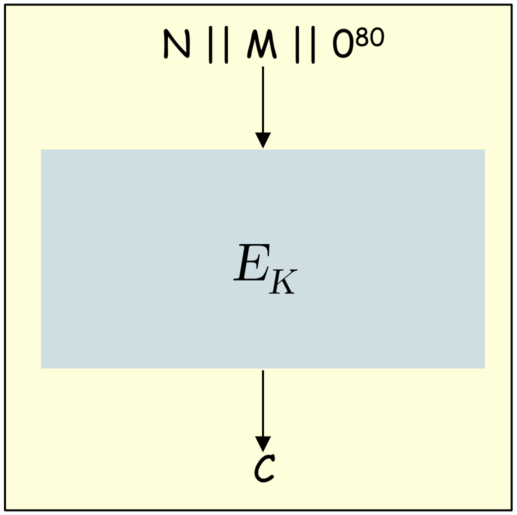
1. Replace $E_K(\cdot), E_K^{-1}(\cdot)$ with $\pi(\cdot), \pi^{-1}(\cdot)$



Proof intuition:

1. Replace $E_K(\cdot), E_K^{-1}(\cdot)$ with $\pi(\cdot), \pi^{-1}(\cdot)$

2. Replace $\pi(\cdot), \pi^{-1}(\cdot)$ with two independent random functions $f1(\cdot), f2(\cdot)$

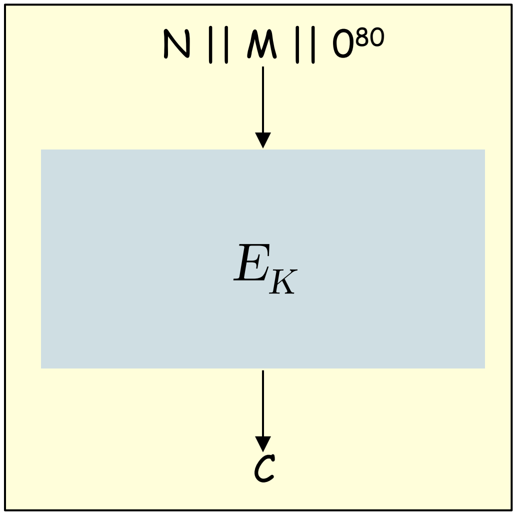


Proof intuition:

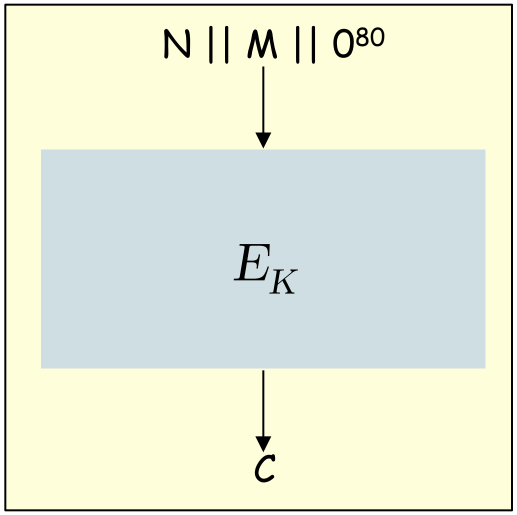
1. Replace $E_K(\cdot), E_K^{-1}(\cdot)$ with $\pi(\cdot), \pi^{-1}(\cdot)$

2. Replace $\pi(\cdot), \pi^{-1}(\cdot)$ with two independent random functions $f1(\cdot), f2(\cdot)$

3. Now uniform random strings in both "directions" if nonces are respected



What makes this work is that SPRPs are (so of) all-or-nothing objects

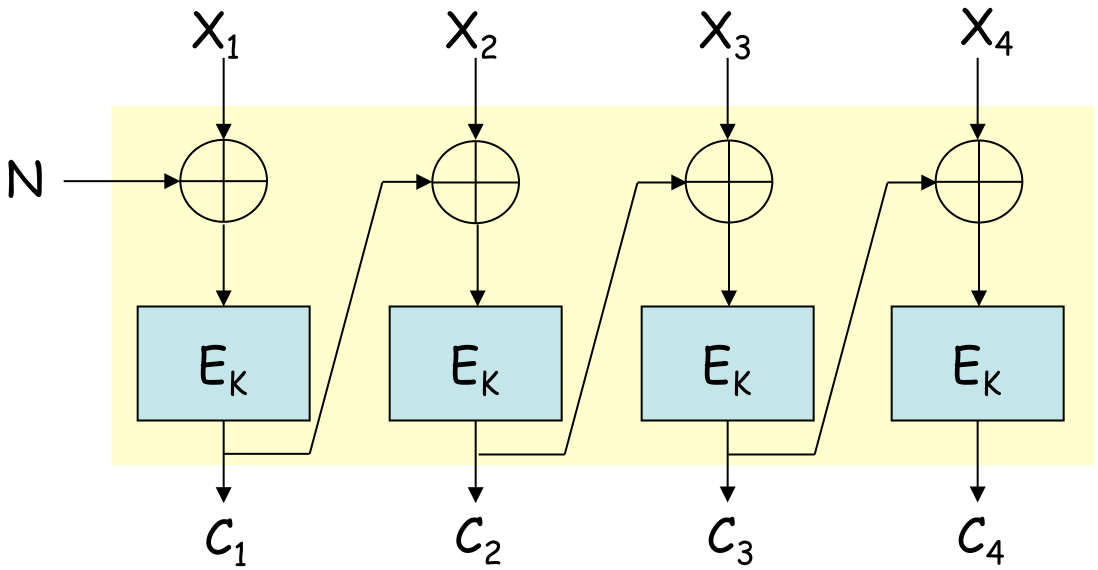


Change any bit of input = randomize entire output

Change any bit of output = randomize entire input

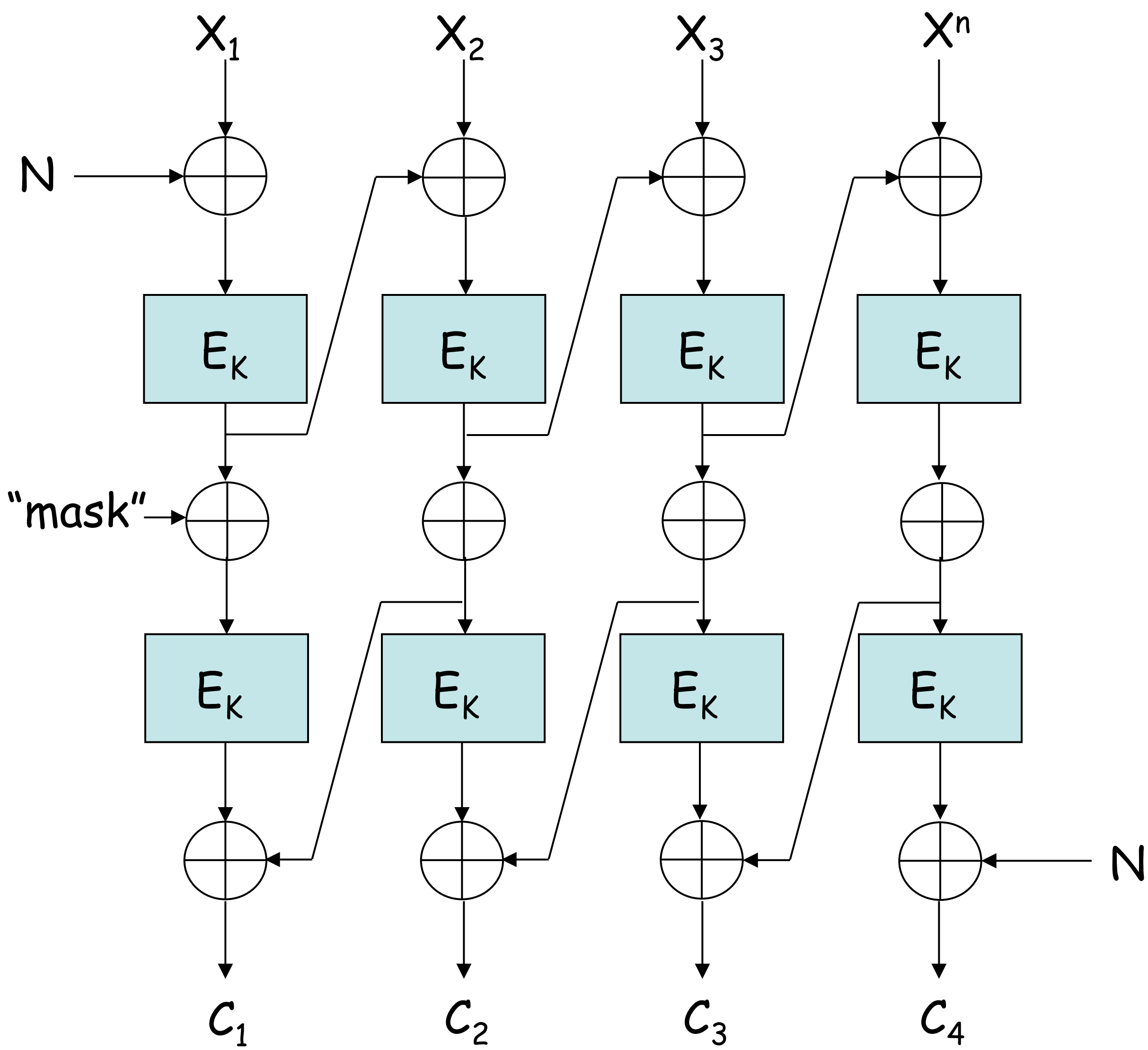
But this comes with a cost:

Loosely, every bit of output (input) must depend on every bit of input (output).



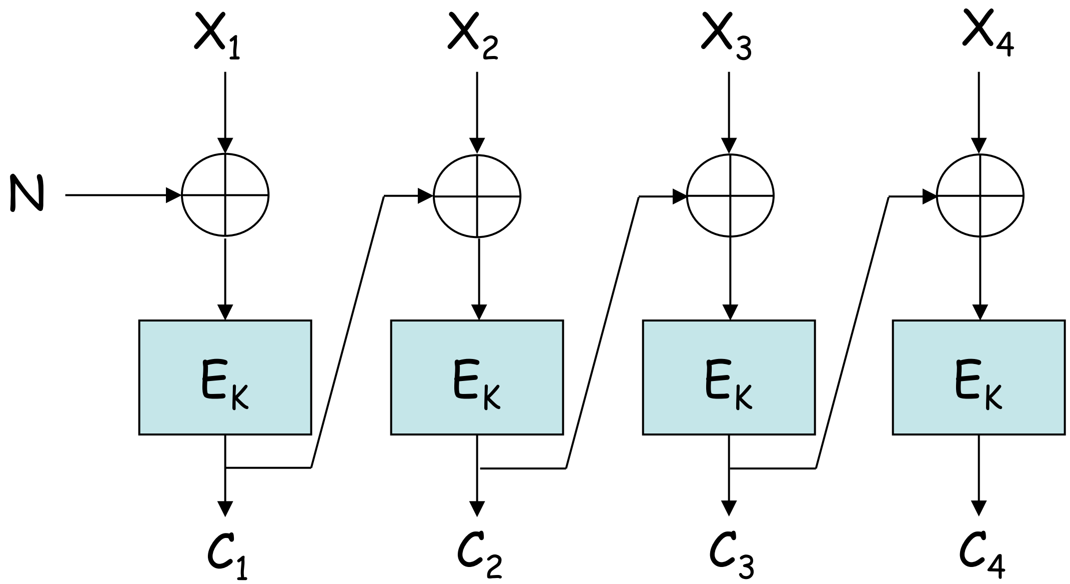
Definitely NOT an SPRP, even if E_K is.

SPRPs generally seem to require two full "cryptographic passes"



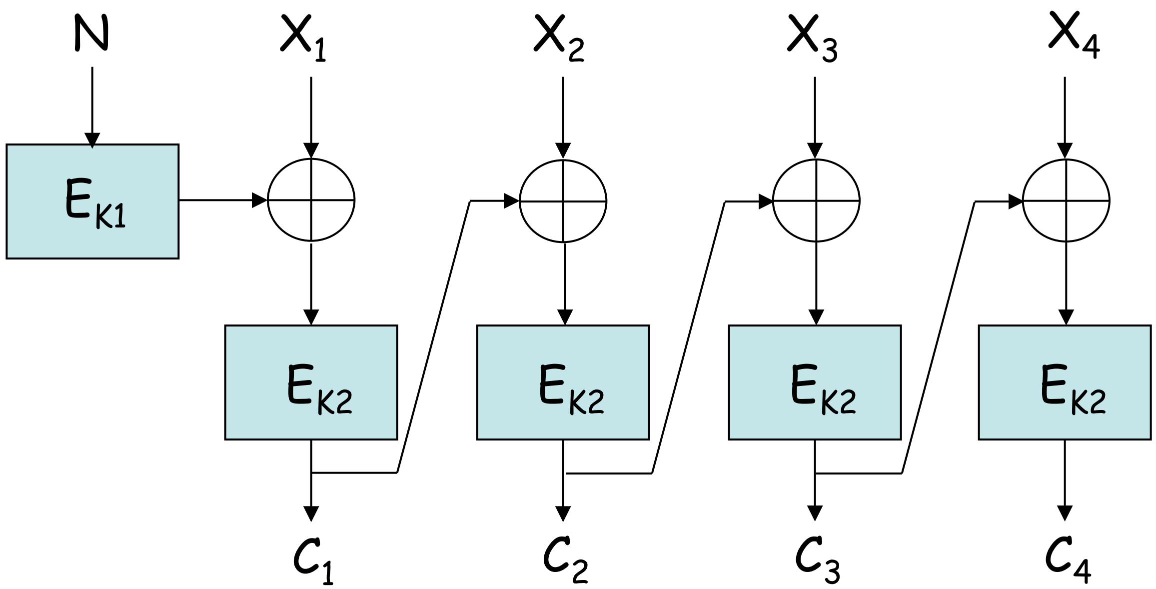
CMC mode
(Halevi and Rogway)

Nonce-based encryption is interesting area



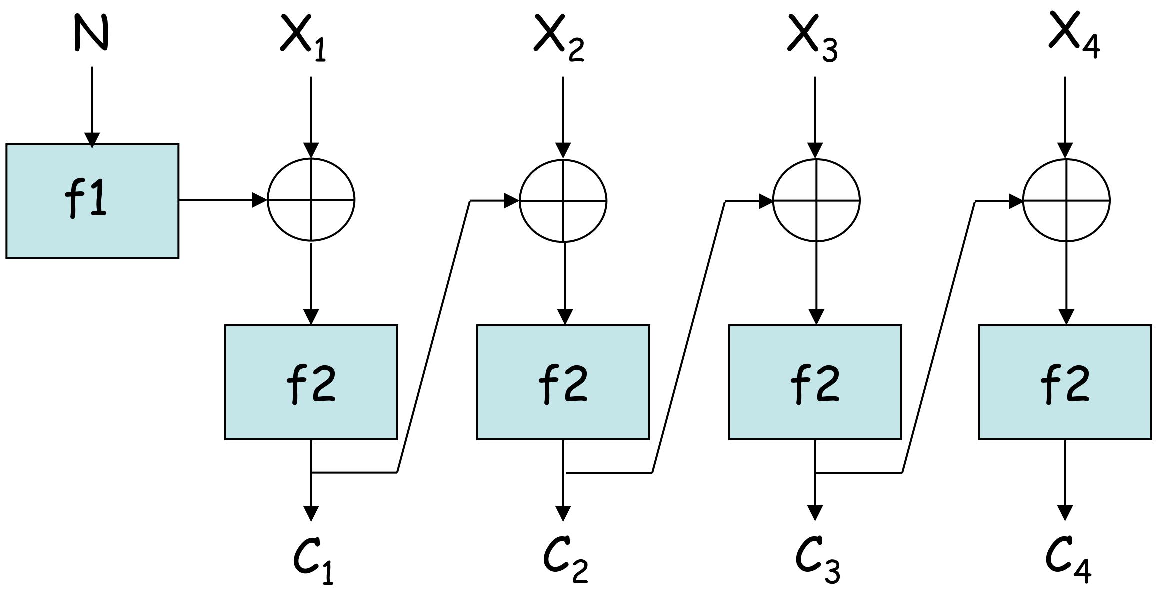
This is not IND-CPA secure in the nonce-based setting, even if nonces are respected.

Nonce-based encryption is interesting area



But this should work…

Nonce-based encryption is interesting area



If f1 and f2 are independent random functions
(so we need E to be a PRF under two random keys)
then all f2 inputs are random…

…what type of bound do you expect?

Yet more: Deterministic AE with "Associated Data" (AEAD)(DAE)

Key-generation algorithm $\mathcal{K}$ samples from a set of the same name

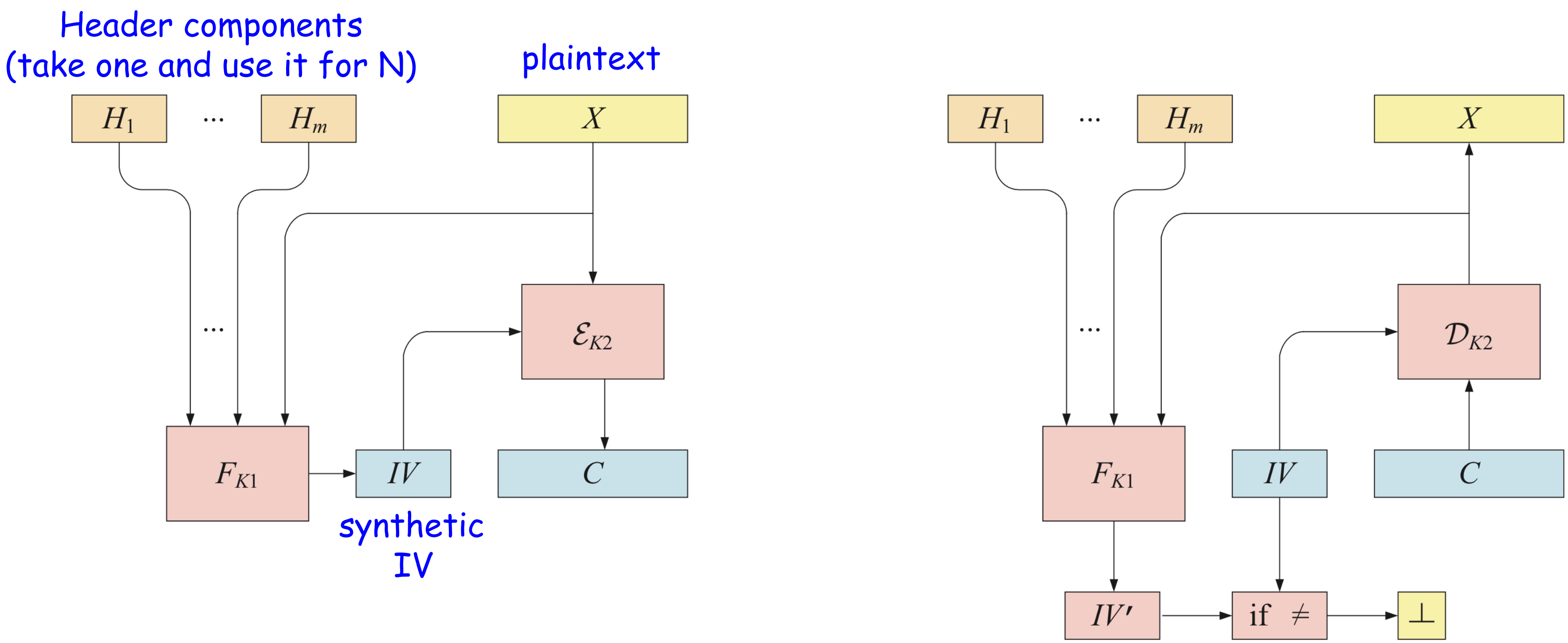
Encryption algorithm $\mathcal{E}\colon (\mathcal{H} \times \mathcal{N}) \times \mathcal{K} \times \{0,1\}^* \to \{0,1\}^* \cup \{\perp\}$

Decryption algorithm $\mathcal{D}\colon (\mathcal{H} \times \mathcal{N}) \times \mathcal{K} \times \{0,1\}^* \to \{0,1\}^* \cup \{\perp\}$

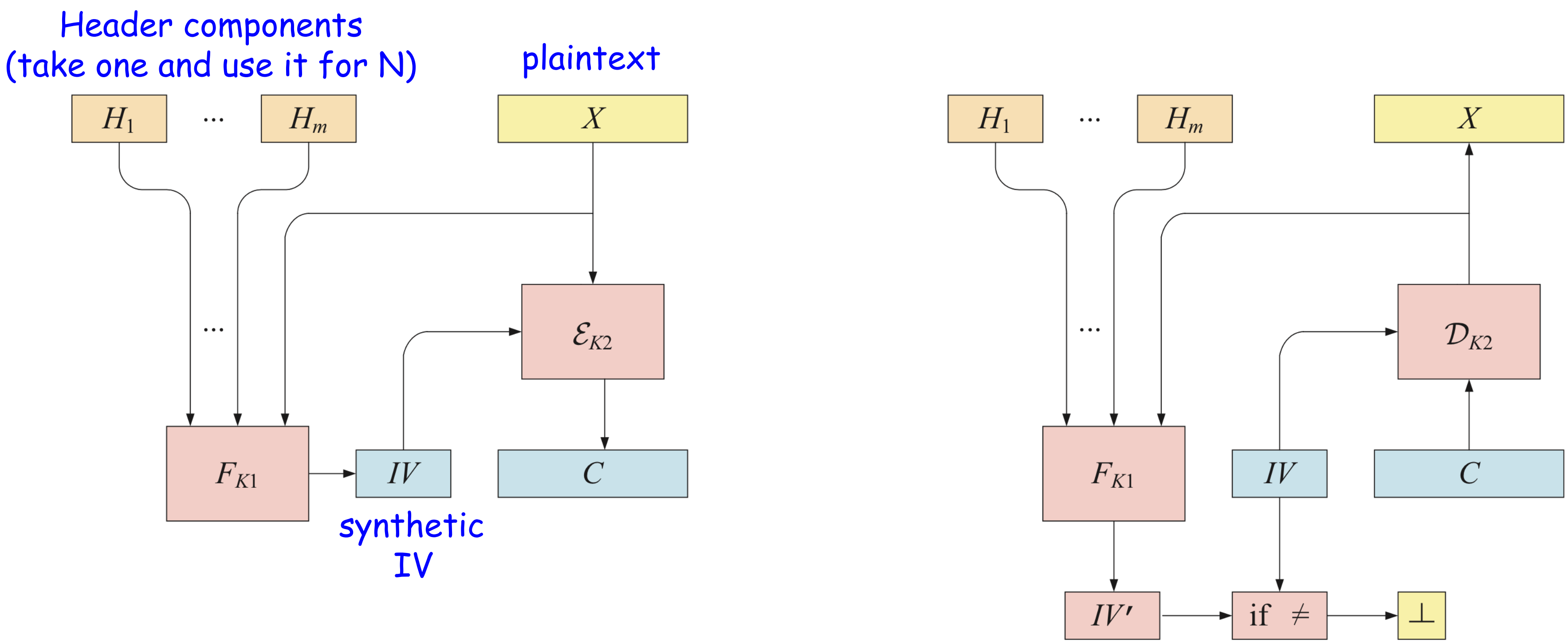
The "header" or "associated data" space

(See Rogaway's AEAD Paper)
(See Rogaway and Shrimpton's "Keywrap" Paper)

Here's one way to build a DAE scheme: SIV mode



Here's one way to build a DAE scheme: SIV mode



If F is a secure PRF, and $\mathcal{E}$ is IND-CPA against nonce-respecting adversaries, then this is a secure DAE scheme (IND-CPA and INT-CTXT)

(also provides "nonce-misuse resistance")

This is NOT the whole story of symmetric encryption!

Many interesting "faces" of symmetric encryption to explore

Message-locked encryption

Format-preserving encryption

Format-transforming encryption

Length-hiding AEAD

"Online" encryption

Key-dependent message encryption

...

Thanks!