Lecture 3 – Symmetric encryption, IND-CPA, CTR, CBC

TEK4500

13.09.2023

Håkon Jacobsen

hakon.jacobsen@its.uio.no

Basic goals of cryptography

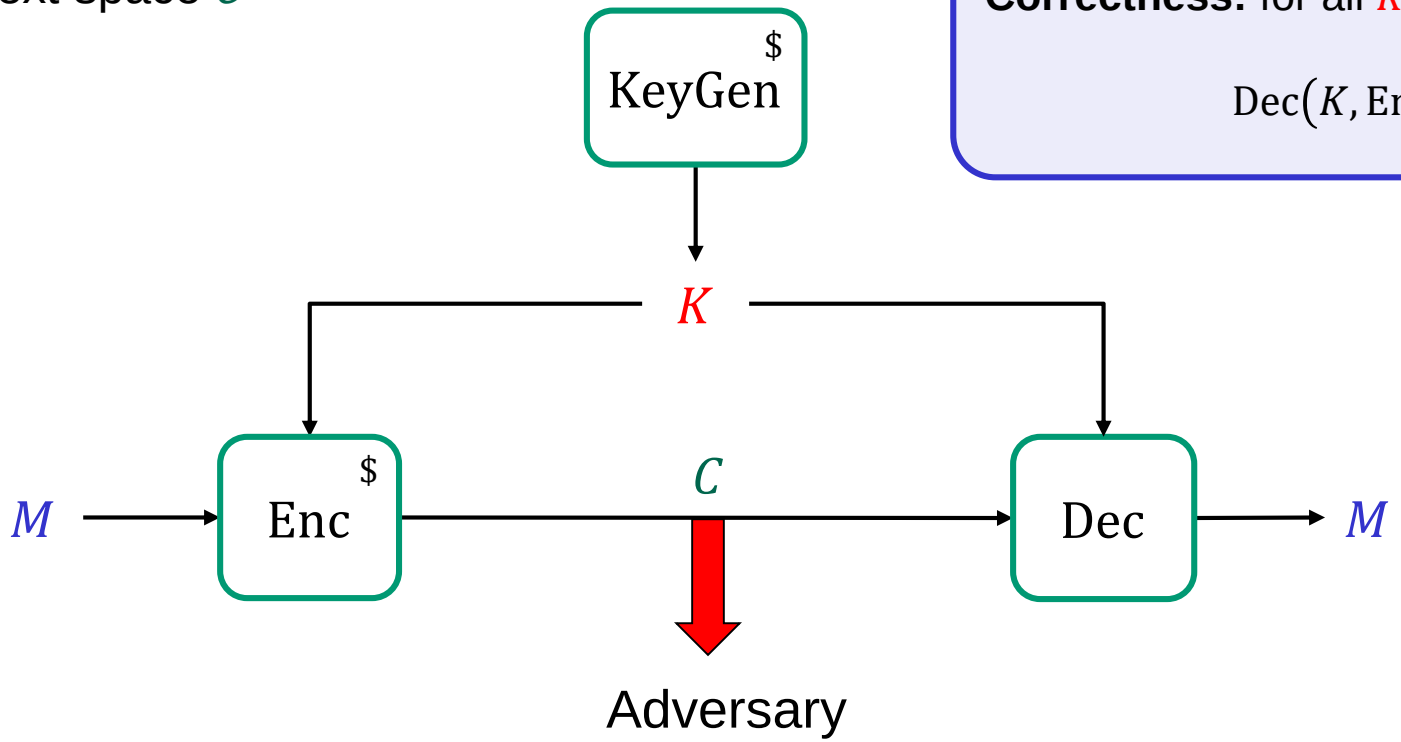
	Message privacy	**Message integrity / authentication**
Symmetric keys	Symmetric encryption	Message authentication codes (MAC)
Asymmetric keys	Asymmetric encryption (a.k.a. public-key encryption)	Digital signatures

Encryption schemes – syntax

- A **symmetric encryption scheme** is a triple of algorithms $\Sigma = (\mathrm{KeyGen}, \mathrm{Enc}, \mathrm{Dec})$
  - Key space $\mathcal{K}$
  - Message space $\mathcal{M}$
  - Ciphertext space $\mathcal{C}$

Correctness: for all $K \xleftarrow{\$} \mathrm{KeyGen}$ and all $M \in \mathcal{M}$:

$$\mathrm{Dec}\big(K, \mathrm{Enc}(K, M)\big) = M$$



- KeyGen and Enc may be randomized ($), but Dec must be deterministic

Symmetric encryption – security definition

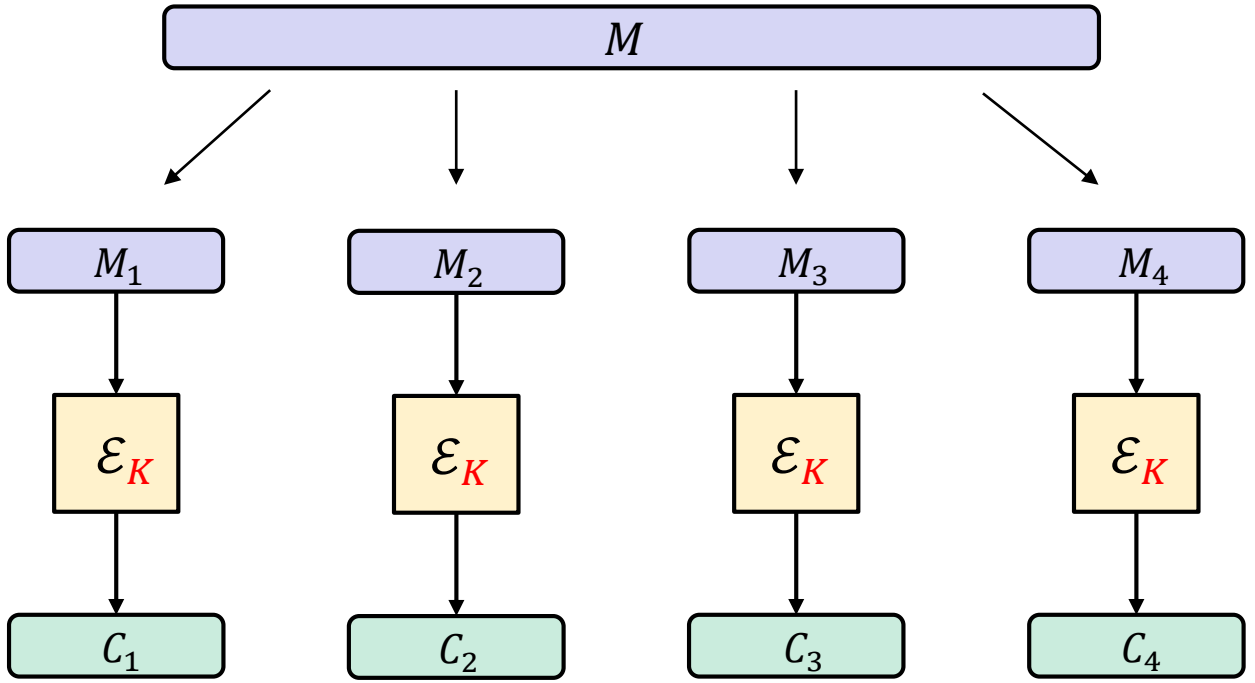
- When is an encryption scheme *secure*?

- Some suggestions:

  - **P1:** Should be hard to obtain K from $E_K(X)$ for secret K
  - **P2:** Should be hard to obtain K from $E_K(X_1), E_K(X_2), E_K(X_3)$ ...
  - **P3:** Should be hard to obtain X from $E_K(X)$
  - **P4:** Should be hard to obtain *any* X_i from $E_K(X_1), E_K(X_2), E_K(X_3)$ ...
  - **P5:** Should be hard to learn any *bit* of X from $E_K(X)$
  - **P6:** Should be hard to detect *repetitions* among X_1, X_2, ... from $E_K(X_1), E_K(X_2)$, ...
  - **P7:** …

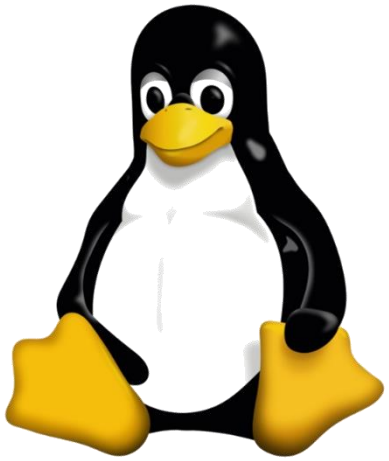
Electronic Code Book (ECB) mode

Block cipher: $\mathcal{E} : \mathcal{K} \times \{0,1\}^n \rightarrow \{0,1\}^n$

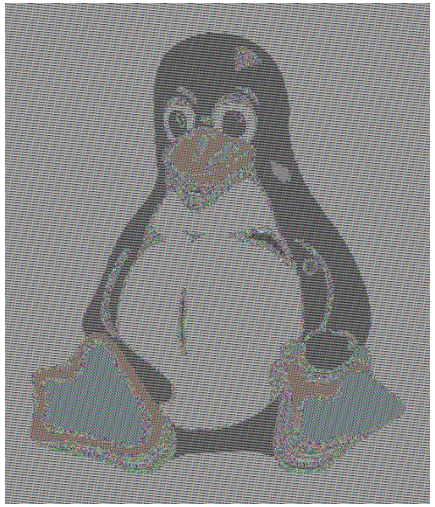


ECB problem

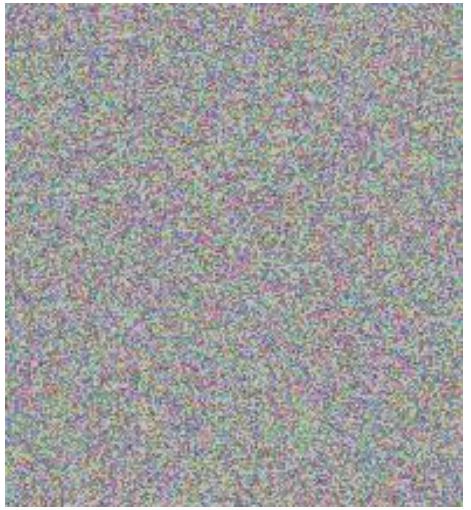
Plaintext



ECB encrypted



Properly encrypted

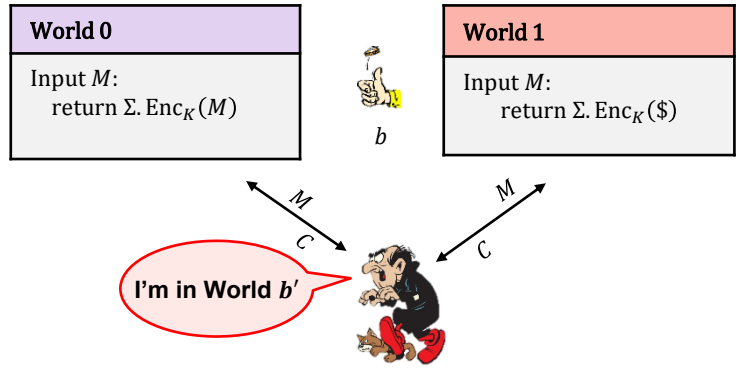


- **Problem:** $M_1 = M_2 \implies C_1 = C_2$
- **Example:** $\mathcal{M} = \{\text{Yes}, \text{No}\}$ $\mathcal{M} = \{\text{Buy}, \text{Sell}\}$ $\mathcal{M} = \{\text{Launch}, \text{Don't launch}\}$

Perfect privacy

- computational
  ~~One-time perfect~~ **privacy:**

$$\Pr[b' = b] = \frac{1}{2} \pm \varepsilon$$



- Security holds for *any* adversary (~~no limit on resource usage~~)

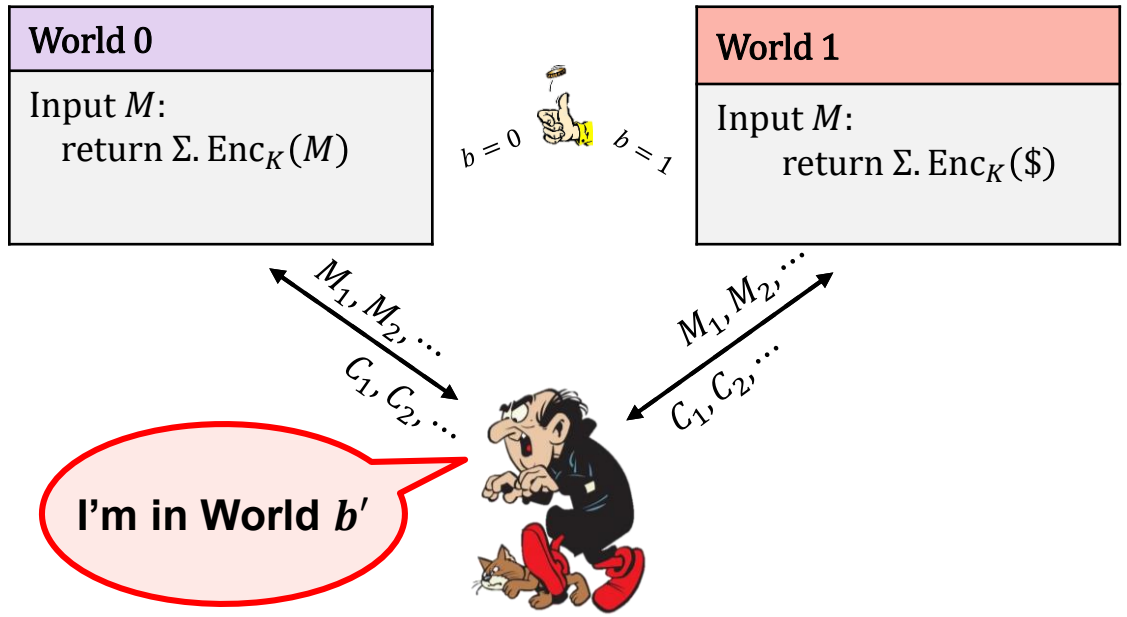
resource bounded

- Very strict requirements:
  - ~~Keys need to be as long as message~~…want keys to be short ✓
  - ~~Key can only be used for one message~~…want to encrypt many messages ✓

IND-CPA – indistinguishability against chosen-plaintext attacks

$\mathbf{Exp}_{\Sigma}^{\text{ind-cpa}}(A)$

1. $b \xleftarrow{\$} \{0,1\}$
2. $K \xleftarrow{\$} \Sigma.\text{KeyGen}$
3. $b' \leftarrow A^{\mathcal{E}(\cdot)}$
4. **return** $b' \stackrel{?}{=} b$



Definition: The **IND-CPA advantage** of an adversary A is

$$\mathbf{Adv}_{\Sigma}^{\text{ind-cpa}}(A) = \left|2 \cdot \Pr\left[\mathbf{Exp}_{\Sigma}^{\text{ind-cpa}}(A) \Rightarrow \text{true}\right] - 1\right|$$

IND-CPA – indistinguishability against chosen-plaintext attacks

$\mathbf{Exp}_{\Sigma}^{\text{ind-cpa}}(A)$

1. $b \xleftarrow{\$} \{0,1\}$
2. $K \xleftarrow{\$} \Sigma.\text{KeyGen}$
3. $b' \leftarrow A^{\mathcal{E}(\cdot)}$
4. **return** $b' \stackrel{?}{=} b$

$\mathcal{E}(M$

2.
3. C
4. **return** C_b

Intuition: Σ is **IND-CPA secure** if $\mathbf{Adv}_{\Sigma}^{\text{ind-cpa}}(A)$ is "small" for all "reasonable" A

World 0

Input M:
return $\Sigma.\text{Enc}_K(M)$

World 1

Input M:
return $\Sigma.\text{Enc}_K(\$)$

$\mathbf{Adv}_{\Sigma}^{\text{ind-cpa}}(A) \approx 1 \implies$ adversary is doing well

$\mathbf{Adv}_{\Sigma}^{\text{ind-cpa}}(A) \approx 0 \implies$ adversary is doing poorly

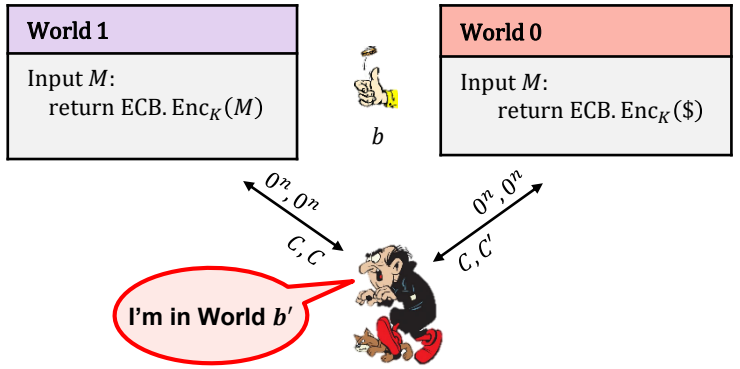
n: The **IND-CPA advantage** of an adversary A is

$$\mathbf{Adv}_{\Sigma}^{\text{ind-cpa}}(A) = \left|2 \cdot \Pr\left[\mathbf{Exp}_{\Sigma}^{\text{ind-cpa}}(A) \Rightarrow \text{true}\right] - 1\right|$$

Example: IND-CPA insecurity of ECB mode

Adversary A

1. Query $\mathcal{E}(\cdot)$ on 0^n twice
2. Receive back C and C'
3. if $C = C'$ output $b' = 0$
4. else, output $b' = 1$



$$\Pr\left[\mathbf{Exp}^{\text{ind-cpa}}_{\text{ECB}}(A) \Rightarrow \text{true}\right] = \Pr[b' = b]$$

$$= \Pr[\, b' = 0 \mid b = 0\,] \cdot 1/2 \;+\; \Pr[\, b' = 1 \mid b = 1\,] \cdot 1/2$$

$$= \Pr[\, C = C' \mid b = 0\,] \cdot 1/2 \;+\; (1 - \Pr[\, b' = 0 \mid b = 1\,]) \cdot 1/2$$

$$= 1/2 \;+\; (1 - \Pr[\, C = C' \mid b = 1\,]) \cdot 1/2$$

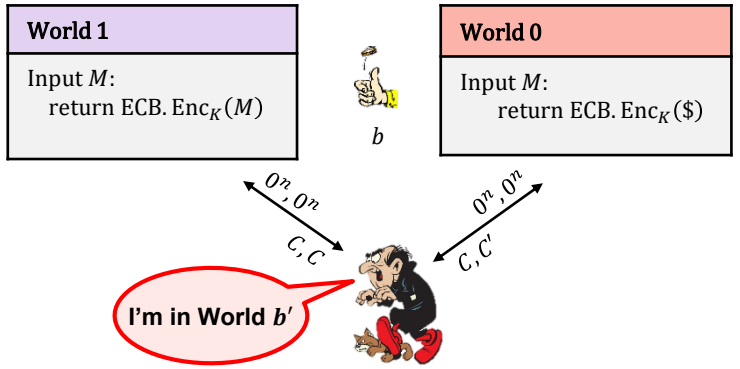
$$= 1/2 \;+\; (1 - 2^{-n}) \cdot 1/2$$

$$= 1 - \frac{1}{2^{n+1}}$$

Example: IND-CPA insecurity of ECB mode

Adversary A

1. Query $\mathcal{E}(\cdot)$ on 0^n twice
2. Receive back C and C'
3. if $C = C'$ output $b' = 0$
4. else, output $b' = 1$



$$\Pr\left[\mathbf{Exp}^{\text{ind-cpa}}_{\text{ECB}}(A) \Rightarrow \text{true}\right] = 1 - \frac{1}{2^{n+1}}$$

$$\mathbf{Adv}^{\text{ind-cpa}}_{\text{ECB}}(A) = \left|2 \cdot \Pr\left[\mathbf{Exp}^{\text{ind-cpa}}_{\Sigma}(A) \Rightarrow \text{true}\right] - 1\right| = \left|2 \cdot \left(1 - \frac{1}{2^{n+1}}\right) - 1\right| = 1 - \frac{1}{2^n} \approx 1$$

Consequences of the definition

- *No* deterministic encryption scheme can be IND-CPA

- IND-CPA security implies other properties that we want:
  - **P1:** Should be hard to obtain K from $Y \leftarrow E_K(X)$ for secret K
  - **P2:** Should be hard to obtain K from $Y_1, Y_2, \ldots$ where $Y_i \leftarrow E_K(X_i)$
  - **P3:** Should be hard to obtain X from $Y \leftarrow E_K(X)$
  - **P4:** Should be hard to obtain *any* X_i from $Y_1, Y_2, \ldots$ where $Y_i \leftarrow E_K(X_i)$
  - **P5:** Should be hard to learn *any* bit of X from $Y \leftarrow E_K(X)$
  - **P6:** Should be hard to detect *repetitions* among $X_1, X_2, \ldots$ from $Y_1, Y_2, \ldots$
  - **P7:** …

- But does it give us *all* the properties we want? I.e., is IND-CPA the "master property"?

JOURNAL OF COMPUTER AND SYSTEM SCIENCES 28, 270–299 (1984)

Probabilistic Encryption*

SHAFI GOLDWASSER AND SILVIO MICALI

Laboratory of Computer Science, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139

Received February 3, 1983; revised November 8, 1983

A new probabilistic model of data encryption is introduced. For this model, under suitable complexity assumptions, it is proved that extracting *any information* about the cleartext from the cyphertext is hard on the average for an adversary with polynomially bounded computational resources. The proof holds for any message space with any probability distribution. The first implementation of this model is presented. The security of this implementation is proved under the intractability assumption of deciding Quadratic Residuosity modulo composite numbers whose factorization is unknown.

1. INTRODUCTION

This paper proposes an encryption scheme that possesses the following property:

Whatever is efficiently computable about the cleartext given the cyphertext, is also efficiently computable without the cyphertext.

Semantic security

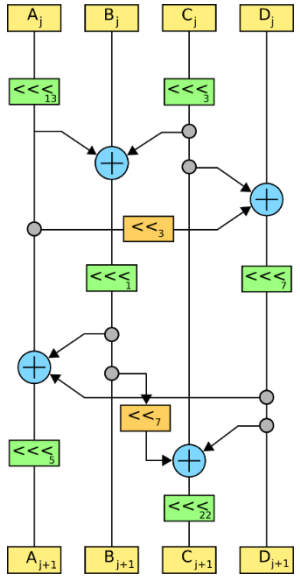
- The conceptually "right" definition
- High level idea: an encryption scheme is **semantically secure** if by observing a ciphertext C the adversary learns *nothing* about the plaintext (except its length)
- Harder to formalize; IND-CPA easier to work with

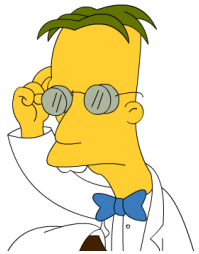
Theorem: (Goldwasser & Micali '83)

An encryption scheme Σ is IND-CPA secure $\Leftrightarrow$ Σ is semantically secure.

Length-leaking attacks

- Wikipedia pages
  - Each page has a unique size
- Google maps
  - World regions have unique "fingerprints" based on length of data (based on map tiles)
- Variable-bitrate encoding
  - Can e.g., fingerprint movies streamed over Netflix
- To combat length-leaking attacks: message padding
  - Can be expensive
  - Supported in TLS, but seldom used
  - Used by TOR



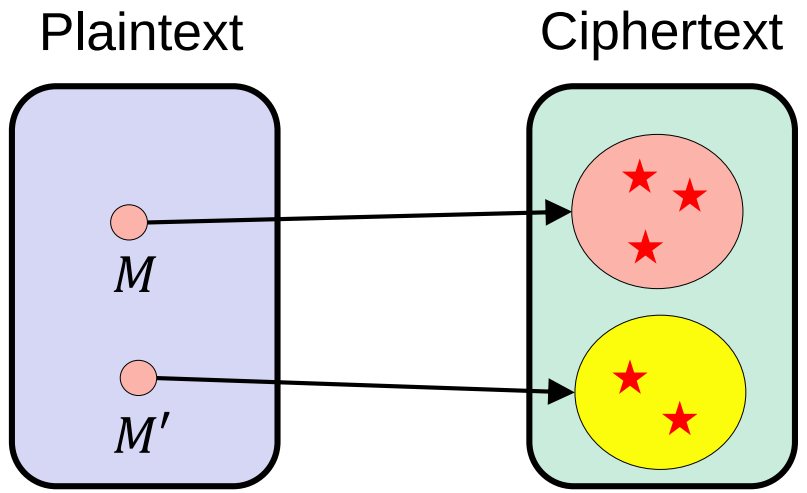


Constructing symmetric encryption schemes

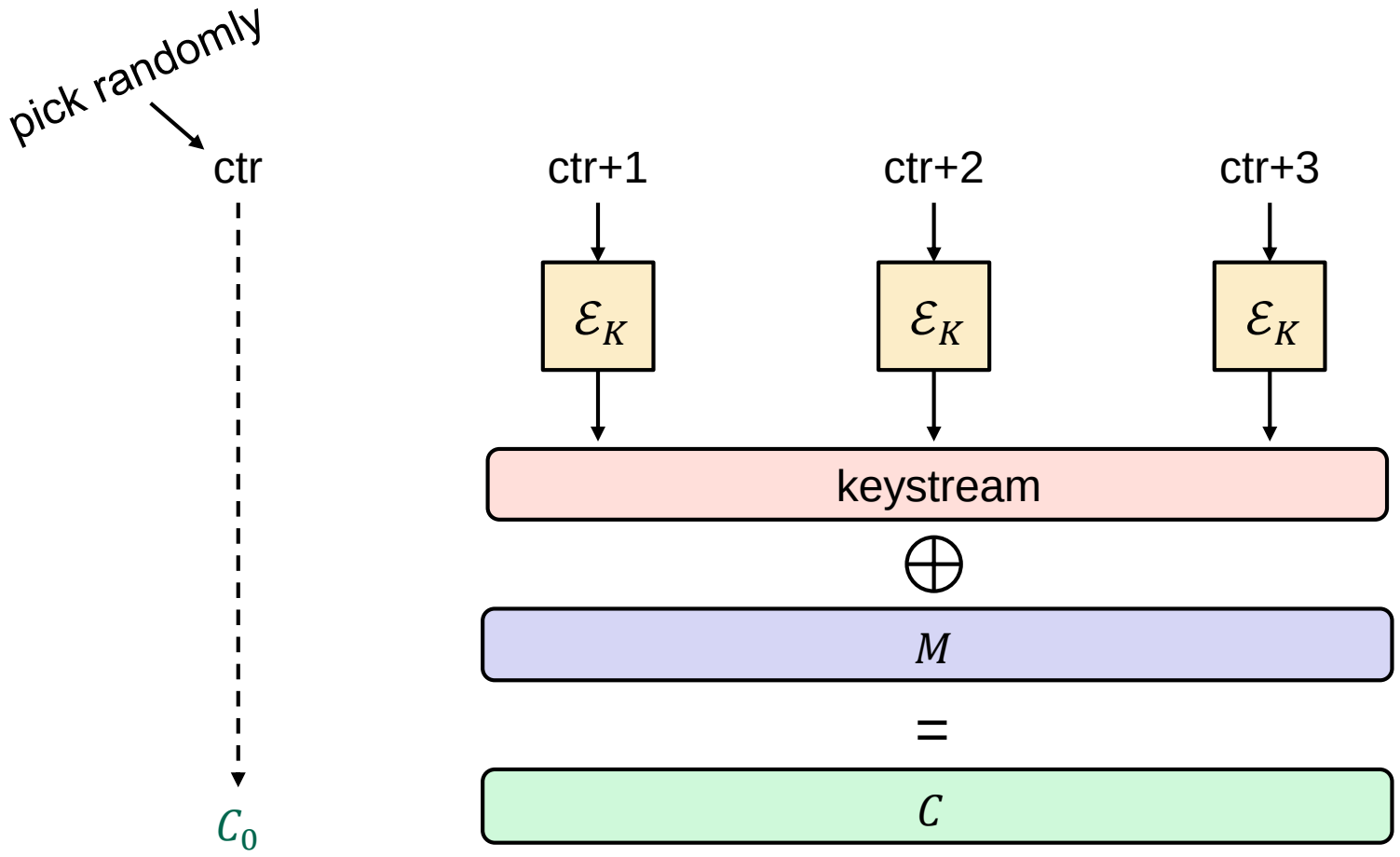
How to achieve non-deterministic encryption?

- Randomized encryption
  - Coins flipped internally by the algorithm

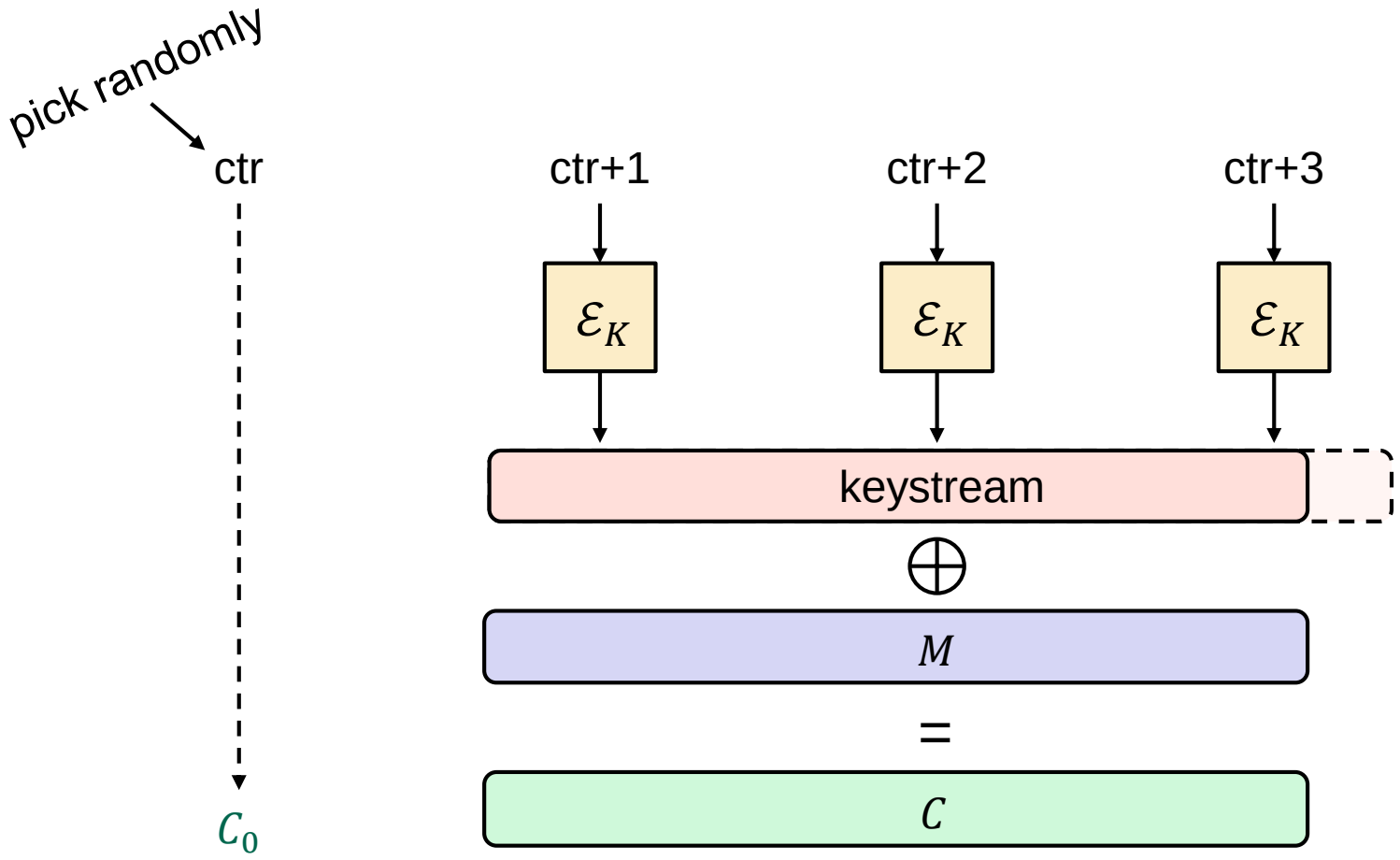
- Nonce-based encryption
  - Encryption scheme itself is deterministic
  - Non-determinism injected from the outside



CTR$ mode

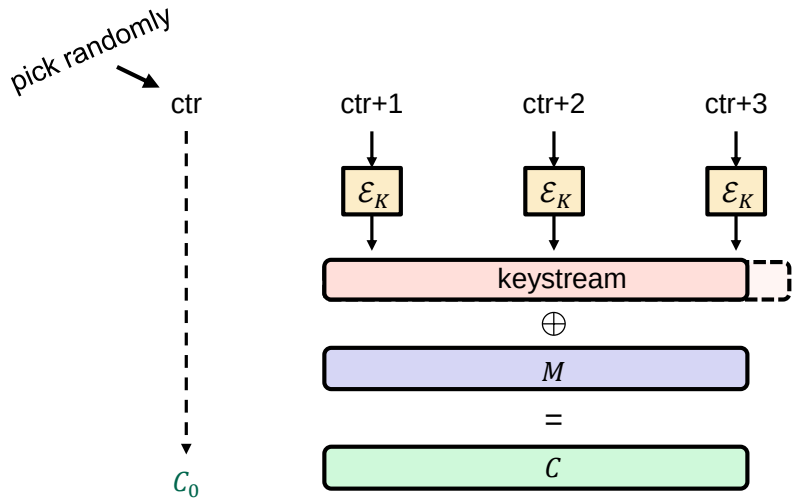

pick randomly
ctr
C_0
ctr+1
ctr+2
ctr+3
$\mathcal{E}_K$
$\mathcal{E}_K$
$\mathcal{E}_K$
keystream
M
=
C

CTR$ mode


pick randomly
ctr
C_0
ctr+1
ctr+2
ctr+3
$\mathcal{E}_K$
$\mathcal{E}_K$
$\mathcal{E}_K$
keystream
M
=
C

CTR properties

- Fully parallelizable
- Inverse direction of $\mathcal{E}_K$ not needed
  - Can use a PRF instead of a PRP
- Keystream can be generated in advance
- No padding needed for messages not a multiple of block length
- What about security?



Modern approach to cryptography

- Trying to make cryptography more a **science** than an **art**
- Focus on **formal definitions** of security (and insecurity)
- Clearly stated **assumptions**
- Analysis supported by mathematical **proofs**

Security of CTR$

Theorem (idea):

If F is a secure PRF then CTR$ is IND-CPA secure.

Logic 101

$A \Rightarrow B$

is *equivalent to:*

$\overline{A} \Leftarrow \overline{B}$

⇕ equivalent!

Theorem (idea):

If CTR$ is *not* IND-CPA secure then F is *not* a secure PRF.

Security of CTR$

Theorem (actual): For *any* IND-CPA adversary A against CTR$ that runs in time t_A and asks at most q queries (each of ℓ blocks), there is a PRF-adversary B such that

$$\mathbf{Adv}^{\text{ind-cpa}}_{\text{CTR\$}}(A) \leq \mathbf{Adv}^{\text{prf}}_{F}(B) + \frac{q^2\ell}{2^n}$$

where B runs in time $t_B = t_A + O(n \cdot q\ell)$ and asks at most $q_B = q\ell$ PRF-queries.

Security of CTR$

Theorem (actual): For *any* IND-CPA adversary A against CTR$ that runs in time t_A and asks at most q queries (each of ℓ blocks), there is a PRF-adversary B such that

$$\mathbf{Adv}^{\text{ind-cpa}}_{\text{CTR\$}}(A) \le \mathbf{Adv}^{\text{prf}}_{F}(B) + \frac{q^2\ell}{2^n}$$

where B runs in time $t_B = t_A + O(n \cdot q\ell)$ and asks at most $q_B = q\ell$ PRF-queries.

F secure PRF $\Rightarrow \mathbf{Adv}^{\text{prf}}_{F}(B) \approx 0$

$\Rightarrow \mathbf{Adv}^{\text{ind-cpa}}_{\text{CTR\$}}(A) \le \frac{q^2\ell}{2^n}$

$\Rightarrow \mathbf{Adv}^{\text{ind-cpa}}_{\text{CTR\$}}(A) \approx 0 \qquad (q^2\ell \ll 2^n)$

$\Rightarrow$ CTR$ is IND-CPA secure!

Example: AES-CTR$

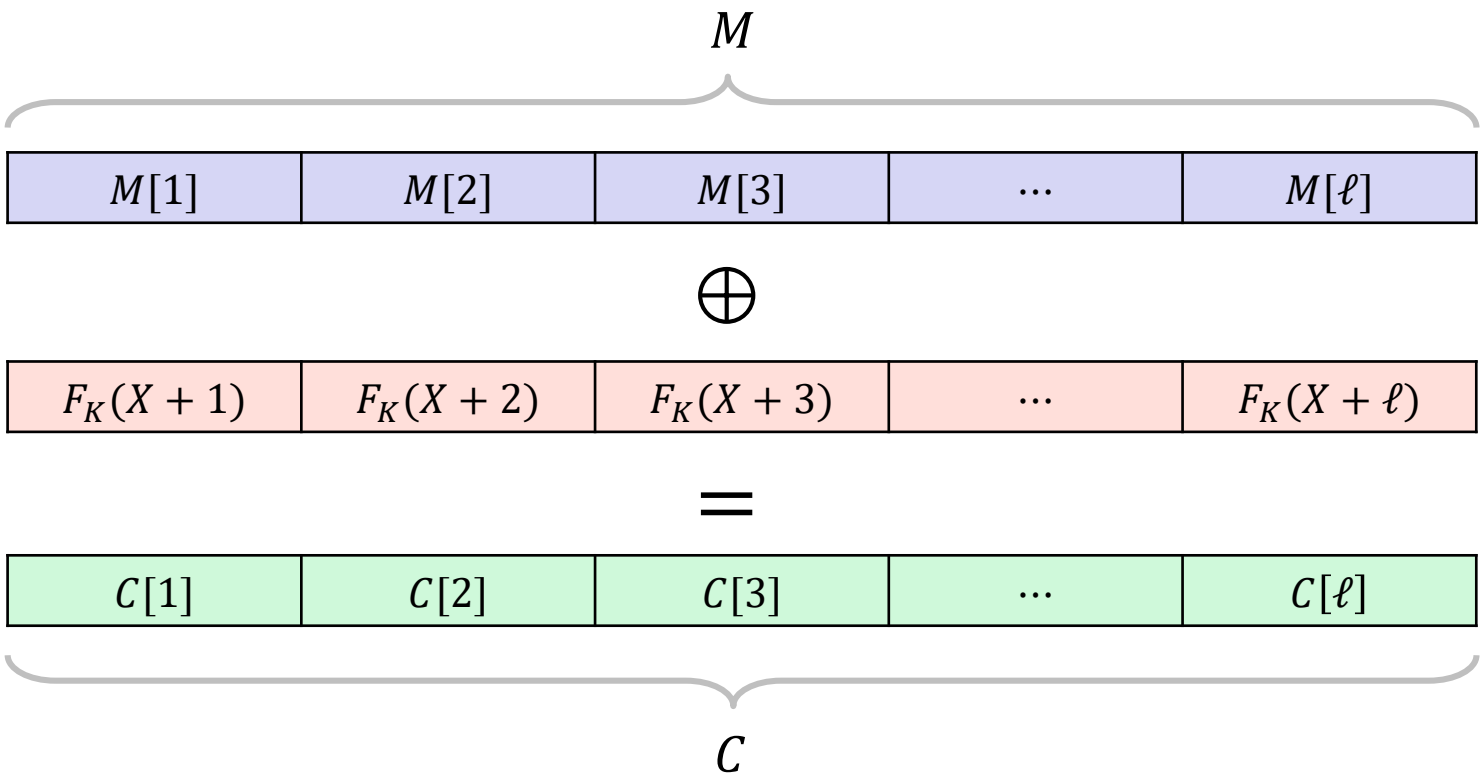
$n = 128$
$\ell = 2^6 \approx 1$ kB
$q = 2^{40}$
$\}\ \approx 70$ TB

$$\mathbf{Adv}^{\text{ind-cpa}}_{\text{AES-CTR\$}}(A) \le \frac{(2^{40})^2 \cdot 2^6}{2^{128}} = \frac{2^{86}}{2^{128}} = \frac{1}{2^{42}}$$

Security of CTR$ – proof idea

Theorem: For *any* A … there is B such that

$$\mathbf{Adv}^{\text{ind-cpa}}_{\text{CTR\$}}(A) \le \mathbf{Adv}^{\text{prf}}_{F}(B) + \frac{q^2\ell}{2^n}$$



$\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR\$}}(A)$

1. $b \xleftarrow{\$} \{0,1\}$
2. $K \xleftarrow{\$} \text{CTR\$.KeyGen}$
3. $b' \leftarrow A^{\mathcal{E}(\cdot)}$
4. **return** $b' \stackrel{?}{=} b$

$\mathcal{E}(M)$

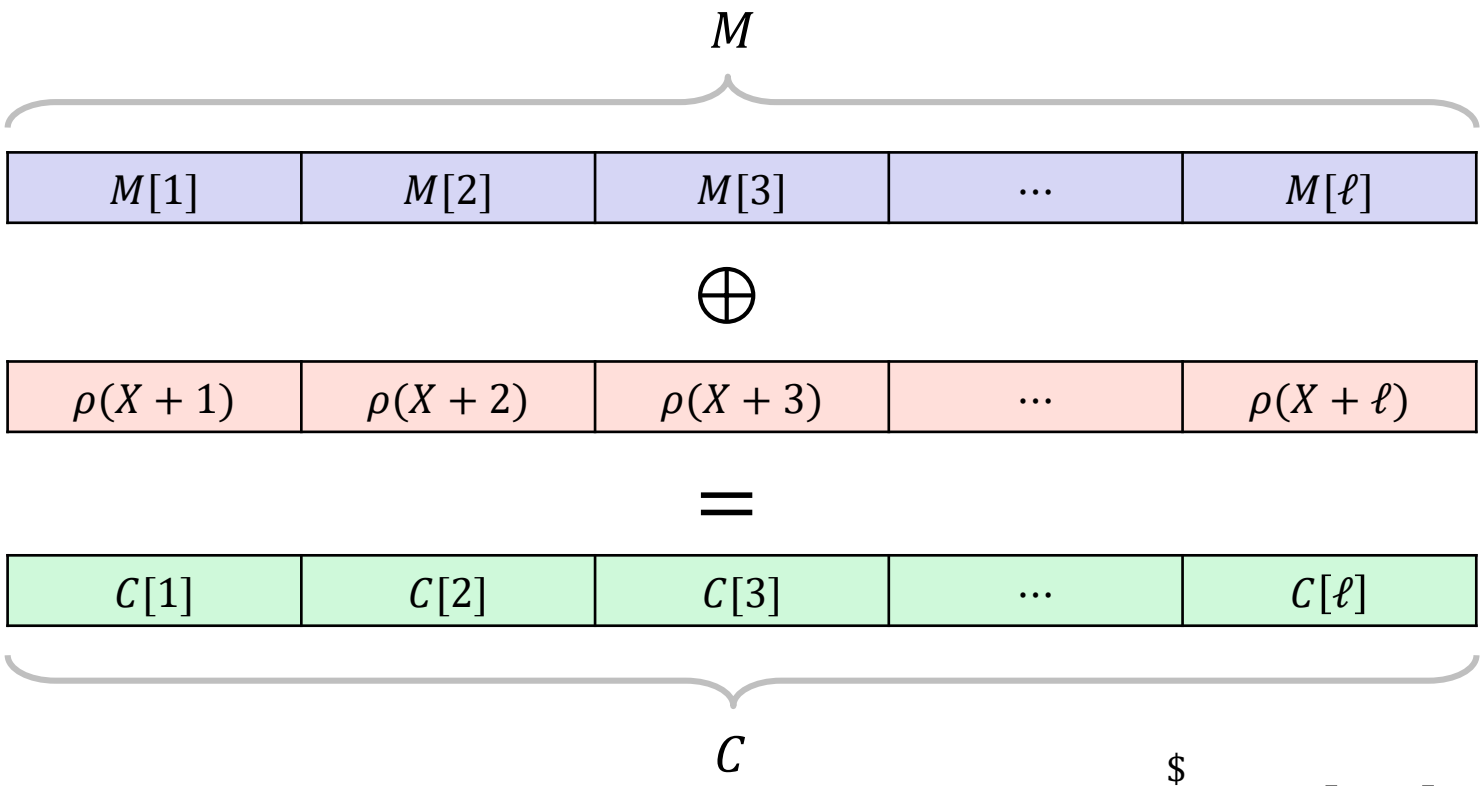
---

1. $R \xleftarrow{\$} \{0,1\}^{|M|}$
2. $C_0 \leftarrow \text{CTR\$.Enc}(K, M)$
3. $C_1 \leftarrow \text{CTR\$.Enc}(K, R)$
4. **return** C_b

Security of CTR$ – proof idea

Theorem: For *any* A … there is B such that

$$\mathbf{Adv}^{\text{ind-cpa}}_{\text{CTR\$}}(A) \le \mathbf{Adv}^{\text{prf}}_{F}(B) + \frac{q^2\ell}{2^n}$$



$\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR\$}}(A)$

1. $b \xleftarrow{\$} \{0,1\}$
2. $K \xleftarrow{\$} \text{CTR\$.KeyGen}$
3. $b' \leftarrow A^{\mathcal{E}(\cdot)}$
4. **return** $b' \stackrel{?}{=} b$

$\mathcal{E}(M)$

---

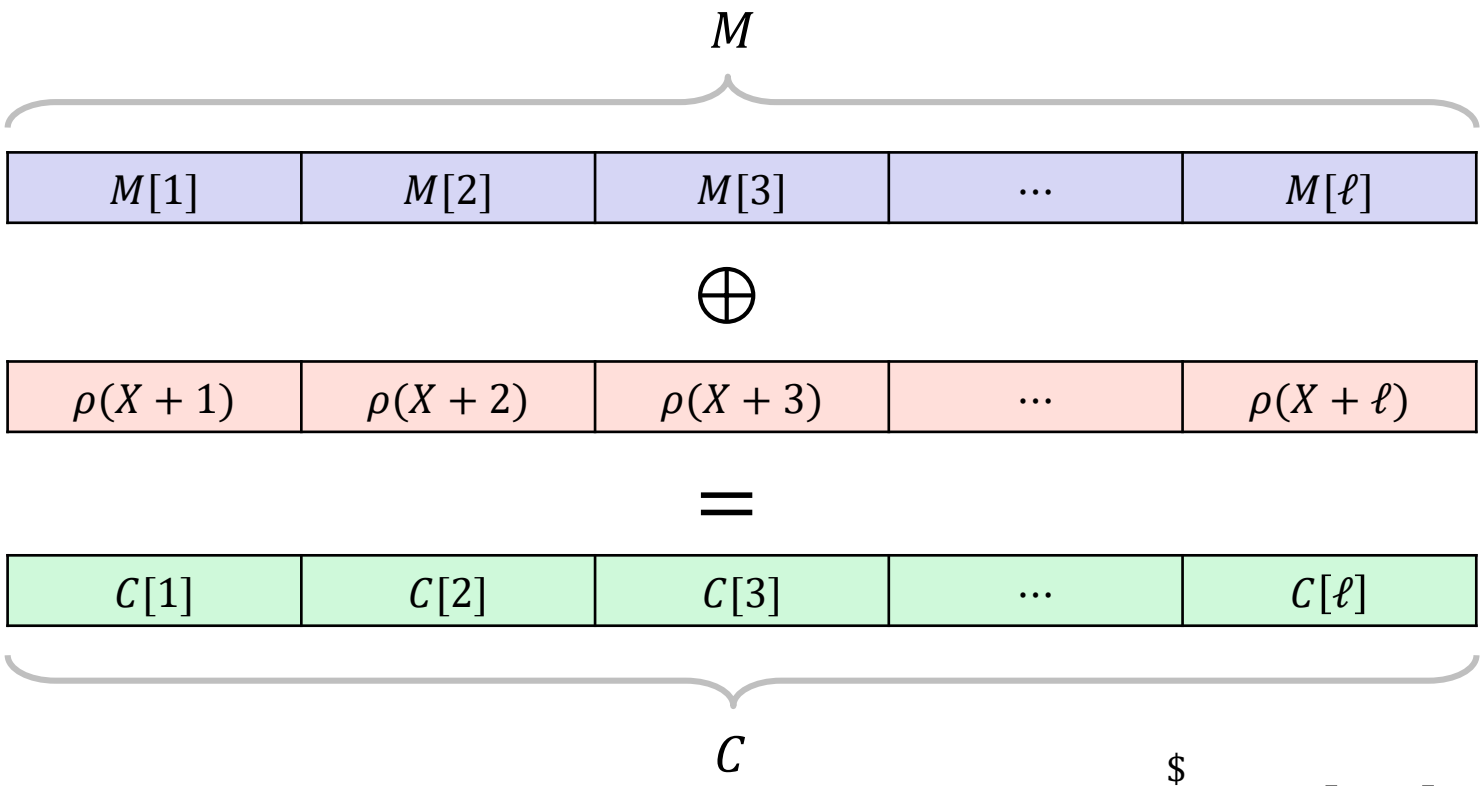
1. $R \xleftarrow{\$} \{0,1\}^{|M|}$
2. $C_0 \leftarrow \text{CTR\$.Enc}(K, M)$
3. $C_1 \leftarrow \text{CTR\$.Enc}(K, R)$
4. **return** C_b

$\rho \xleftarrow{\$} \text{Func}[n,n] \approx F_K$ by PRF-security

Security of CTR$ – proof idea

Theorem: For *any* A … there is B such that

$$\mathbf{Adv}^{\text{ind-cpa}}_{\text{CTR\$}}(A) \le \mathbf{Adv}^{\text{prf}}_{F}(B) + \frac{q^2\ell}{2^n}$$



$\text{Exp}^{\text{ind-cpa}}_{\text{CTR\$}}(A)$

1. $b \xleftarrow{\$} \{0,1\}$
2. $K \xleftarrow{\$} \text{CTR\$.KeyGen}$
3. $b' \leftarrow A^{\mathcal{E}(\cdot)}$
4. **return** $b' \stackrel{?}{=} b$

$\mathcal{E}(M)$

---

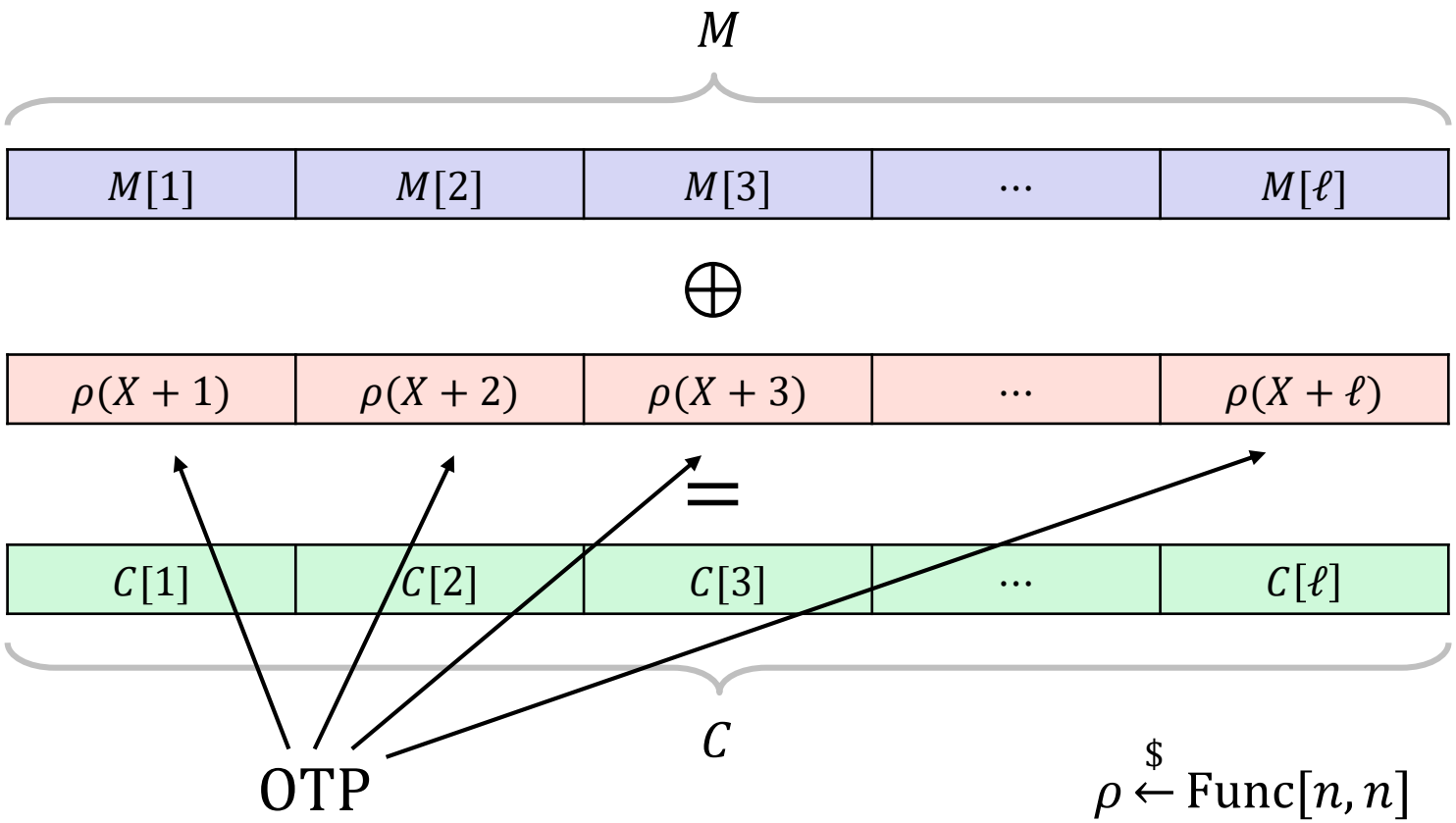
1. $R \xleftarrow{\$} \{0,1\}^{|M|}$
2. $C_0 \leftarrow \text{CTR\$.Enc}(K, M)$
3. $C_1 \leftarrow \text{CTR\$.Enc}(K, R)$
4. **return** C_b

$\rho \xleftarrow{\$} \text{Func}[n,n] \approx F_K$ by PRF-security

Security of CTR$ – proof idea

Theorem: For *any* A … there is B such that

$$\mathbf{Adv}^{\text{ind-cpa}}_{\text{CTR\$}}(A) \le \mathbf{Adv}^{\text{prf}}_{F}(B) + \frac{q^2\ell}{2^n}$$



$\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR\$}}(A)$

1. $b \xleftarrow{\$} \{0,1\}$
2. $K \xleftarrow{\$} \text{CTR\$.KeyGen}$
3. $b' \leftarrow A^{\mathcal{E}(\cdot)}$
4. **return** $b' \stackrel{?}{=} b$

$\mathcal{E}(M)$

---

1. $R \xleftarrow{\$} \{0,1\}^{|M|}$
2. $C_0 \leftarrow \text{CTR\$.Enc}(K, M)$
3. $C_1 \leftarrow \text{CTR\$.Enc}(K, R)$
4. **return** C_b

$\rho \xleftarrow{\$} \text{Func}[n,n] \approx F_K$ by PRF-security

Security of CTR$ – proof idea

Thec

$$M_1 \xrightarrow{\mathcal{E}(\cdot)} X_1||C_1 : \quad X_1 \quad X_1+1 \quad X_1+2 \quad \cdots \quad X_1+\ell$$

$$M_2 \xrightarrow{\mathcal{E}(\cdot)} X_2||C_2 : \quad X_2 \quad X_2+1 \quad X_2+2 \quad \cdots \quad X_2+\ell$$

$$\vdots \qquad\qquad \vdots$$

$$M_q \xrightarrow{\mathcal{E}(\cdot)} X_q||C_q : \quad X_q \quad X_q+1 \quad X_q+2 \quad \cdots \quad X_q+\ell$$

$\rho(X+1)$	$\rho(X+2)$	$\rho(X+3)$	$\cdots$	$\rho(X+\ell)$

Event Coll:

$$X_i + j = X_{i'} + j' \implies \rho(X_i + j) = \rho(X_{i'} + j') = \tilde{K}$$

$$\implies C_i[j] \oplus C_i[j'] = \left(\tilde{K} \oplus M_i[j]\right) \oplus \left(\tilde{K} \oplus M_{i'}[j']\right) = M_i[j] \oplus M_{i'}[j']$$

$\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR\$}}(A)$

1. $b \xleftarrow{\$} \{0,1\}$
2. $K \xleftarrow{\$} \text{CTR\$.KeyGen}$
3. $b' \leftarrow A^{\mathcal{E}(\cdot)}$
4. **return** $b' \stackrel{?}{=} b$

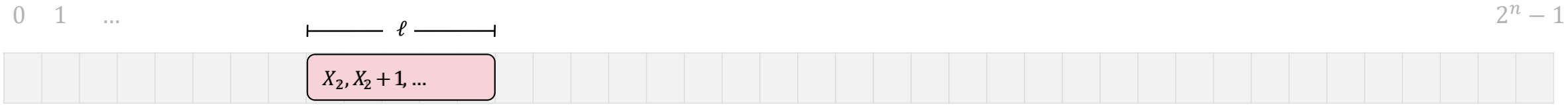
$\mathcal{E}(M)$

---

1. $R \xleftarrow{\$} \{0,1\}^{|M|}$
2. $C_0 \xleftarrow{\$} \{0,1\}^{|M|}$
3. $C_1 \xleftarrow{\$} \{0,1\}^{|M|}$
4. **return** C_b

- by PRF-security

Security of CTR$ – proof idea

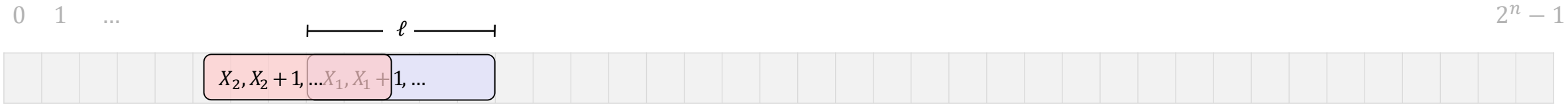


$$\Pr[\text{Coll}] = \Pr\left[\text{Coll}_1 \vee \text{Coll}_2 \vee \cdots \vee \text{Coll}_q\right]$$

$$\leq \Pr[\text{Coll}_1] + \Pr[\text{Coll}_2] + \cdots + \Pr\left[\text{Coll}_q\right]$$

$$\leq \quad 0$$

Security of CTR$ – proof idea

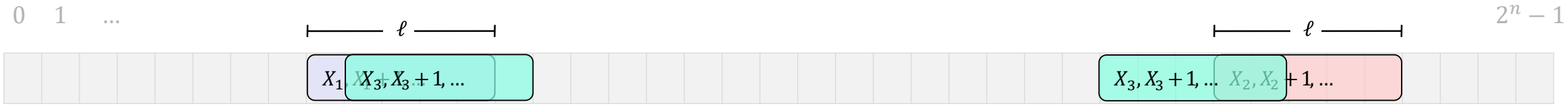


$$\Pr[\text{Coll}] = \Pr\left[\text{Coll}_1 \vee \text{Coll}_2 \vee \cdots \vee \text{Coll}_q\right]$$

$$\leq \Pr[\text{Coll}_1] + \Pr[\text{Coll}_2] + \cdots + \Pr\left[\text{Coll}_q\right]$$

$$\leq \quad 0 \quad + \frac{2\ell}{2^n}$$

Security of CTR$ – proof idea

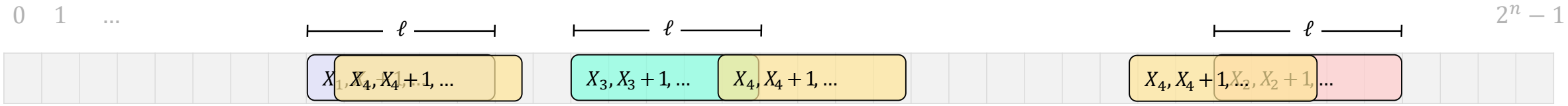


$$\Pr[\text{Coll}] = \Pr\left[\text{Coll}_1 \vee \text{Coll}_2 \vee \cdots \vee \text{Coll}_q\right]$$

$$\leq \Pr[\text{Coll}_1] + \Pr[\text{Coll}_2] + \cdots + \Pr\left[\text{Coll}_q\right]$$

$$\leq \quad 0 \quad + \frac{2\ell}{2^n} \quad + \frac{2 \cdot 2\ell}{2^n}$$

Security of CTR$ – proof idea

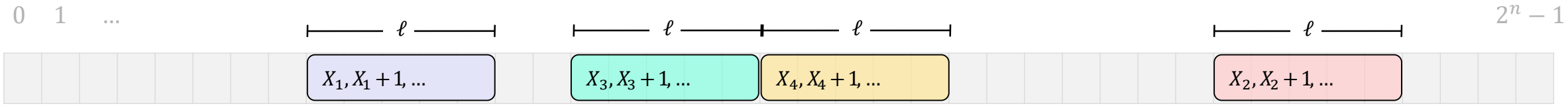


$$\Pr[\text{Coll}] = \Pr\left[\text{Coll}_1 \vee \text{Coll}_2 \vee \cdots \vee \text{Coll}_q\right]$$

$$\leq \Pr[\text{Coll}_1] + \Pr[\text{Coll}_2] + \cdots + \Pr\left[\text{Coll}_q\right]$$

$$\leq \quad 0 \quad + \frac{2\ell}{2^n} + \frac{2 \cdot 2\ell}{2^n} + \frac{3 \cdot 2\ell}{2^n}$$

Security of CTR$ – proof idea



$$\Pr[\text{Coll}] = \Pr\left[\text{Coll}_1 \vee \text{Coll}_2 \vee \cdots \vee \text{Coll}_q\right]$$

$$\leq \Pr[\text{Coll}_1] + \Pr[\text{Coll}_2] + \cdots + \Pr\left[\text{Coll}_q\right]$$

$$\leq \quad 0 \quad + \frac{2\ell}{2^n} + \frac{2 \cdot 2\ell}{2^n} + \frac{3 \cdot 2\ell}{2^n} + \cdots + \frac{(q-1) \cdot 2\ell}{2^n}$$

$$= \frac{2\ell}{2^n} \cdot \left(1 + 2 + 3 + \cdots + (q-1)\right)$$

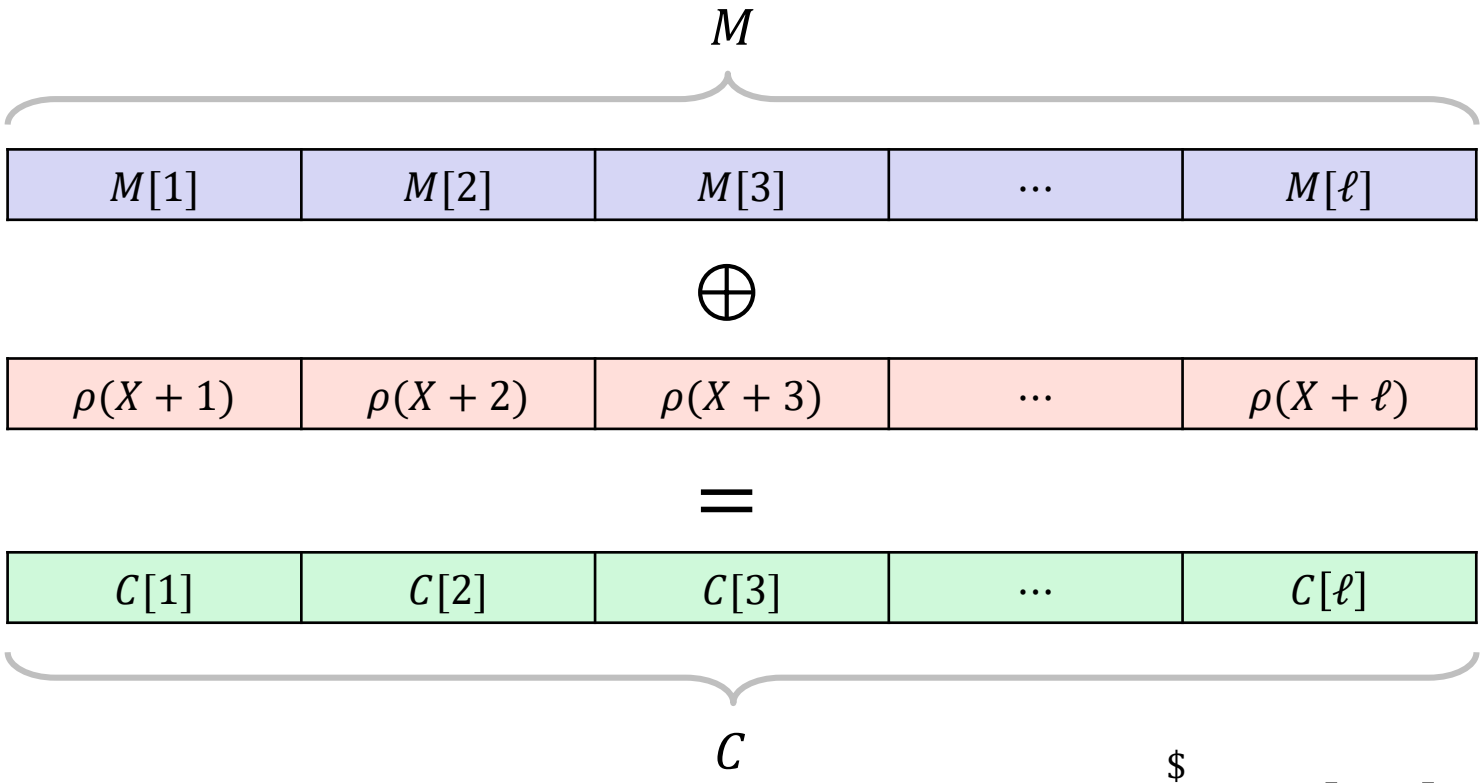
$$\frac{q(q-1)}{2}$$

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

Security of CTR$ – proof idea

Theorem: For *any* A … there is B such that

$$\mathbf{Adv}^{\text{ind-cpa}}_{\text{CTR\$}}(A) \le \mathbf{Adv}^{\text{prf}}_{F}(B) + \frac{q^2\ell}{2^n}$$



$\mathbf{Exp}^{\text{ind-cpa}}_{\text{CTR\$}}(A)$

1. $b \xleftarrow{\$} \{0,1\}$
2. $K \xleftarrow{\$} \text{CTR\$.KeyGen}$
3. $b' \leftarrow A^{\mathcal{E}(\cdot)}$
4. **return** $b' \stackrel{?}{=} b$

$\mathcal{E}(M)$

---

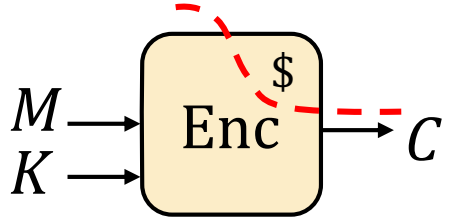
1. $R \xleftarrow{\$} \{0,1\}^{|M|}$
2. $C_0 \xleftarrow{\$} \{0,1\}^{|M|}$
3. $C_1 \xleftarrow{\$} \{0,1\}^{|M|}$
4. **return** C_b

$\rho \xleftarrow{\$} \text{Func}[n,n] \approx F_K$ by PRF-security

Nonce-based encryption

$$\text{Enc} : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C}$$

$$\text{Enc}(K, M) = \text{Enc}_K(M)$$

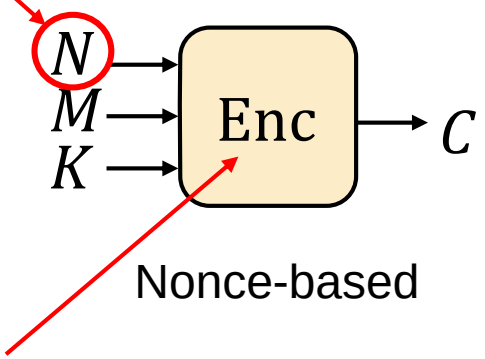


Randomized

"number used once" = Nonce

$$\text{Enc} : \mathcal{K} \times \mathcal{N} \times \mathcal{M} \rightarrow \mathcal{C}$$

$$\text{Enc}(K, N, M) = \text{Enc}_K(N, M) = \text{Enc}_K^N(M)$$



Nonce-based

Deterministic

How to create the nonce?

- Randomly (also called IV-based)
- Counter
- Combination

CTR$ vs. (nonce-based) CTR

Probabilistic

$\text{CTR\$}.\text{Enc}(K, M)$

1. $\text{ctr} \xleftarrow{\$} \{0,1\}^n$
2. $C_0 \leftarrow \text{ctr}$
3. **for** $i = 1, \ldots, \ell$ **do**
4. $\quad C_i \leftarrow \mathcal{E}_K(\text{ctr} + i) \oplus M_i$
5. **return** $C_0 || C_1 || \cdots || C_\ell$

vs.

Nonce-based

$\text{CTR}.\text{Enc}(K, N, M)$

1. $\text{ctr} \leftarrow N$
2. $C_0 \leftarrow \text{ctr}$
3. **for** $i = 1, \ldots, \ell$ **do**
4. $\quad C_i \leftarrow \mathcal{E}_K(\text{ctr} + i) \oplus M_i$
5. **return** $C_0 || C_1 || \cdots || C_\ell$

Nonce-based CTR – IND-CPA security

Theorem (CTR$): For *any* IND-CPA adversary A against CTR$ that runs in time t_A and asks at most q queries (each of ℓ blocks), there is a PRF-adversary B such that

$$\mathbf{Adv}^{\text{ind-cpa}}_{\text{CTR\$}}(A) \leq \mathbf{Adv}^{\text{prf}}_{F}(B) + \frac{q^2\ell}{2^n}$$

where B runs in time $t_B = t_A + O(n \cdot q\ell)$ and asks at most $q_B = q\ell$ PRF-queries.

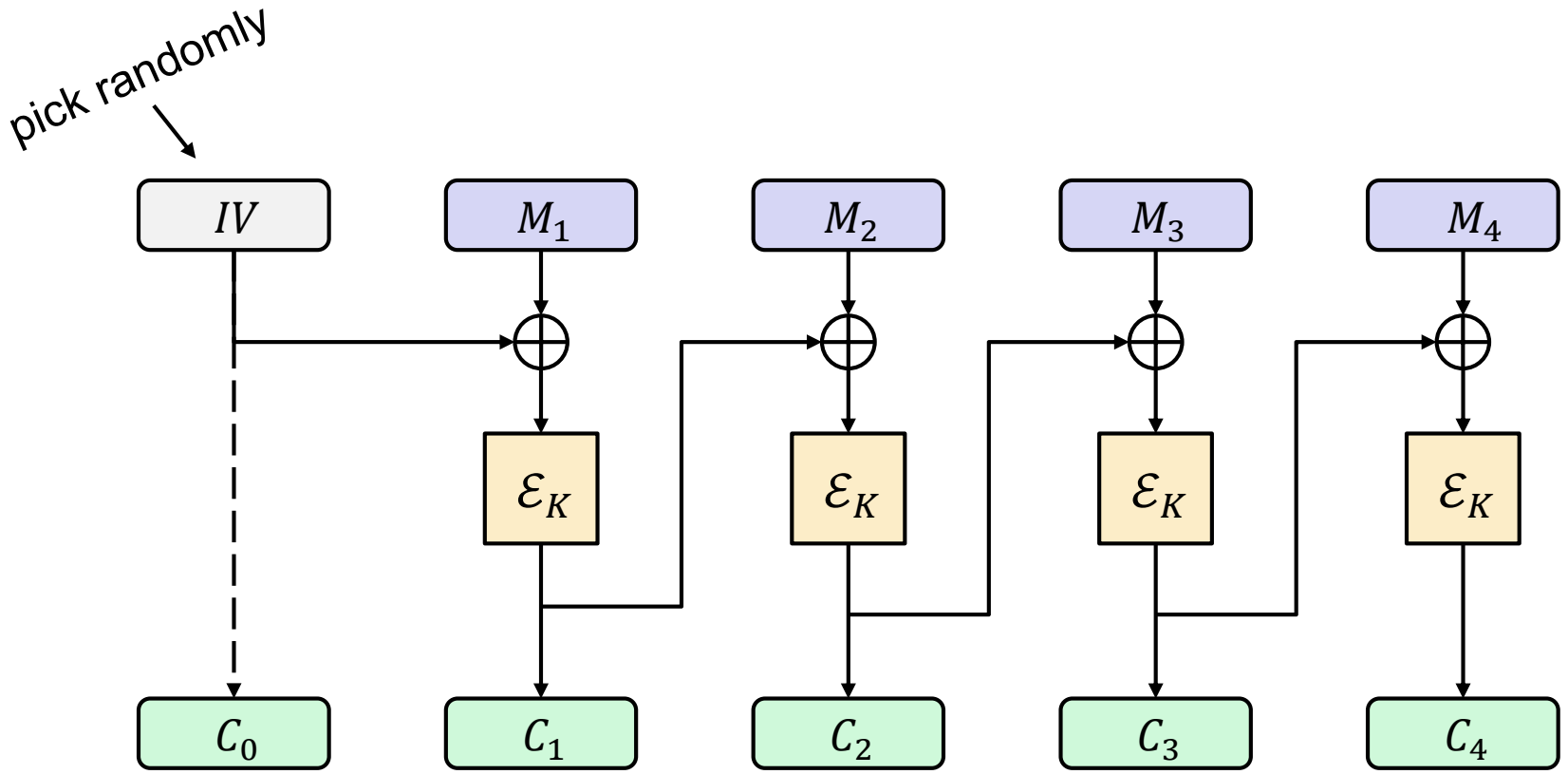
vs.

Theorem (CTR): For *any* IND-CPA adversary A against CTR that runs in time t_A and asks at most q queries (each of ℓ blocks), there is a PRF-adversary B such that

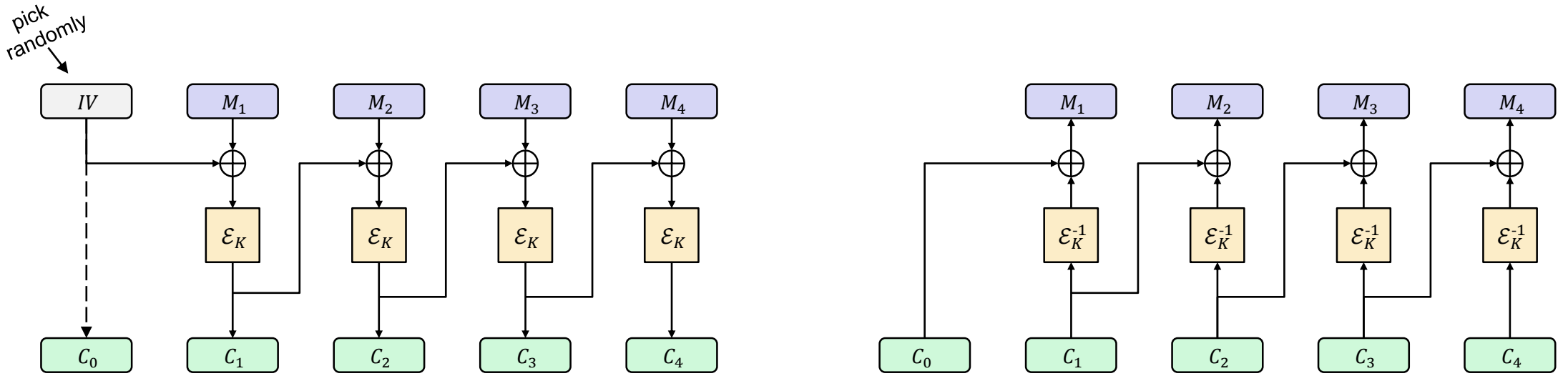
$$\mathbf{Adv}^{\text{ind-cpa}}_{\text{CTR}}(A) \leq \mathbf{Adv}^{\text{prf}}_{F}(B)$$

where B runs in time $t_B = t_A + O(n \cdot q\ell)$ and asks at most $q_B = q\ell$ PRF-queries.

CBC$ – Cipher Block Chaining mode

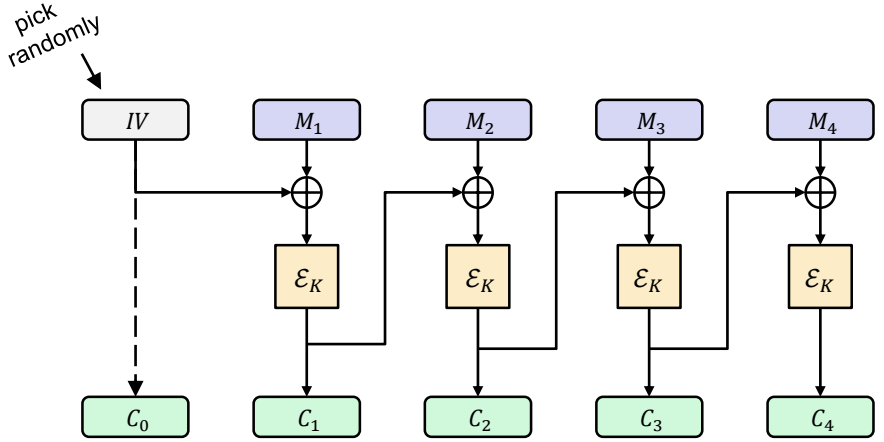


CBC$ – Cipher Block Chaining mode

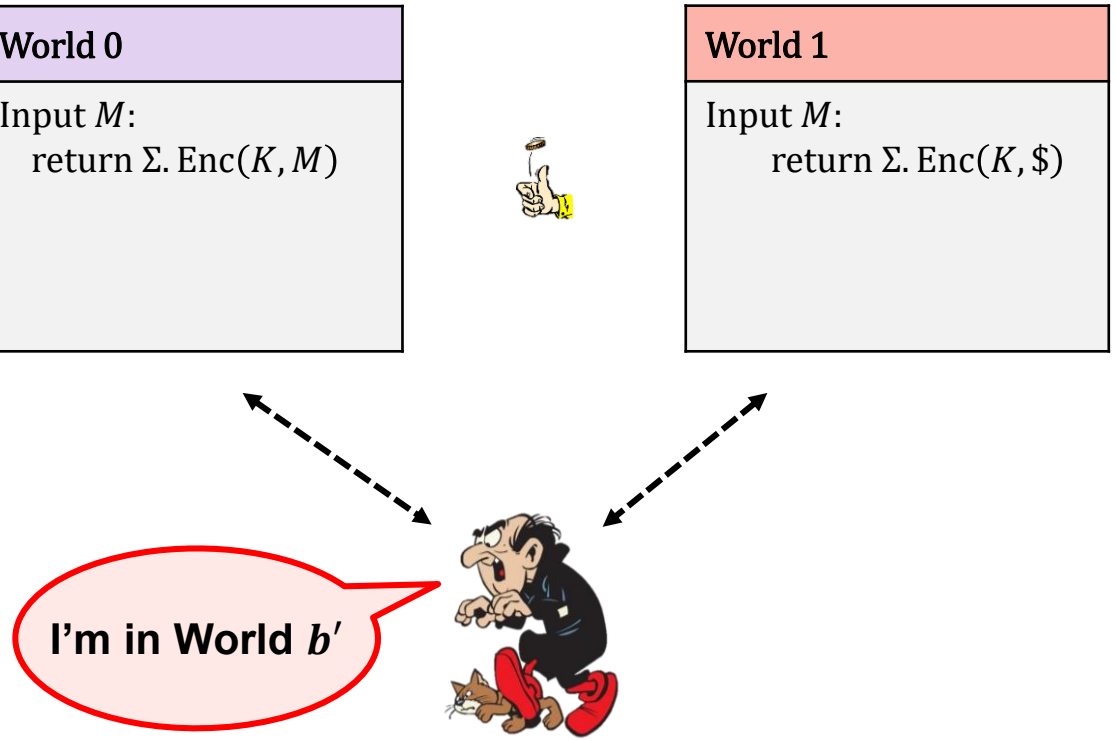


CBC

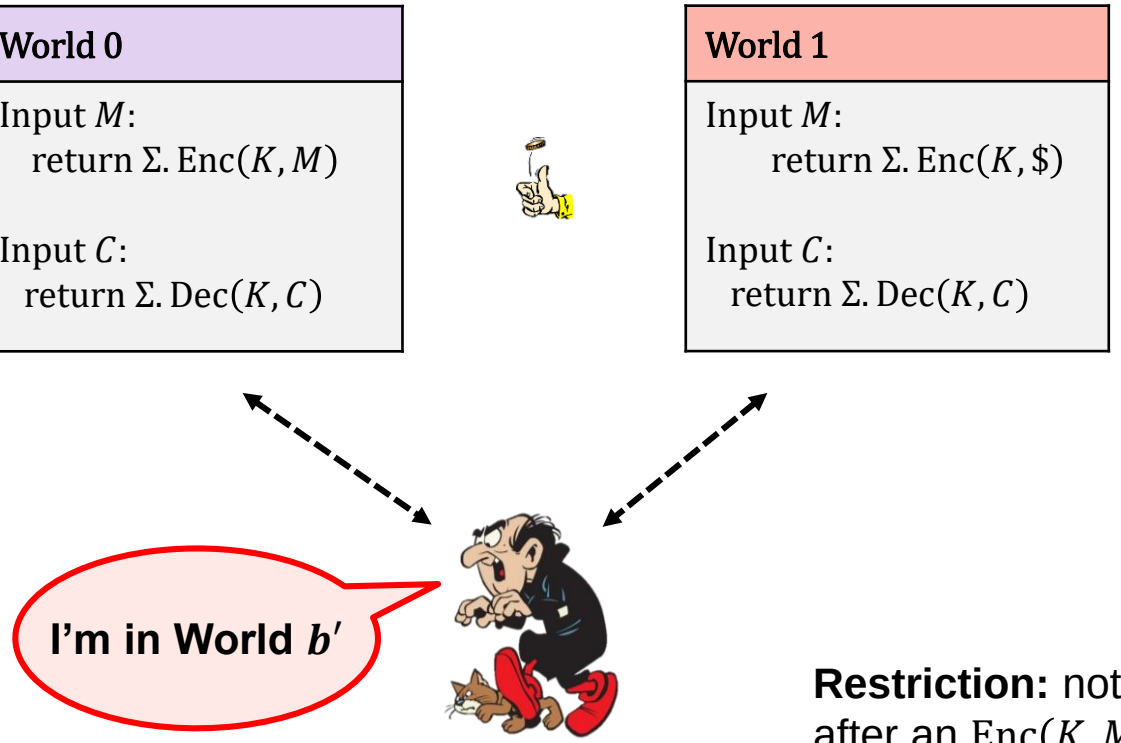
- **Theorem:** IND-CPA secure for *random* IV (assuming $\mathcal{E}$ is a good block cipher)
- Not IND-CPA secure for nonce-based IV
  - (exercise: show this)
- Not parallelizable; cannot precompute values
- Inverse of block cipher needed for decryption
- Padding needed for messages not a multiple of block length
- …historically one of the most used modes-of-operation



IND-CPA – Indistinguishability against chosen-plaintext attacks



IND-CCA – Indistinguishability against chosen-ciphertext attacks



Restriction: not allowed to query $\mathrm{Dec}(K, C)$ after an $\mathrm{Enc}(K, M)$ call returned C

IND-CCA

- None of the schemes we have looked at today are IND-CCA secure
  - Attacks are easy to demonstrate (exercise)
- New techniques are needed
- Next week: message authentication codes