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

TEK4500

08.09.2021

Håkon Jacobsen

hakon.jacobsen@its.uio.no

Basic goals of cryptography

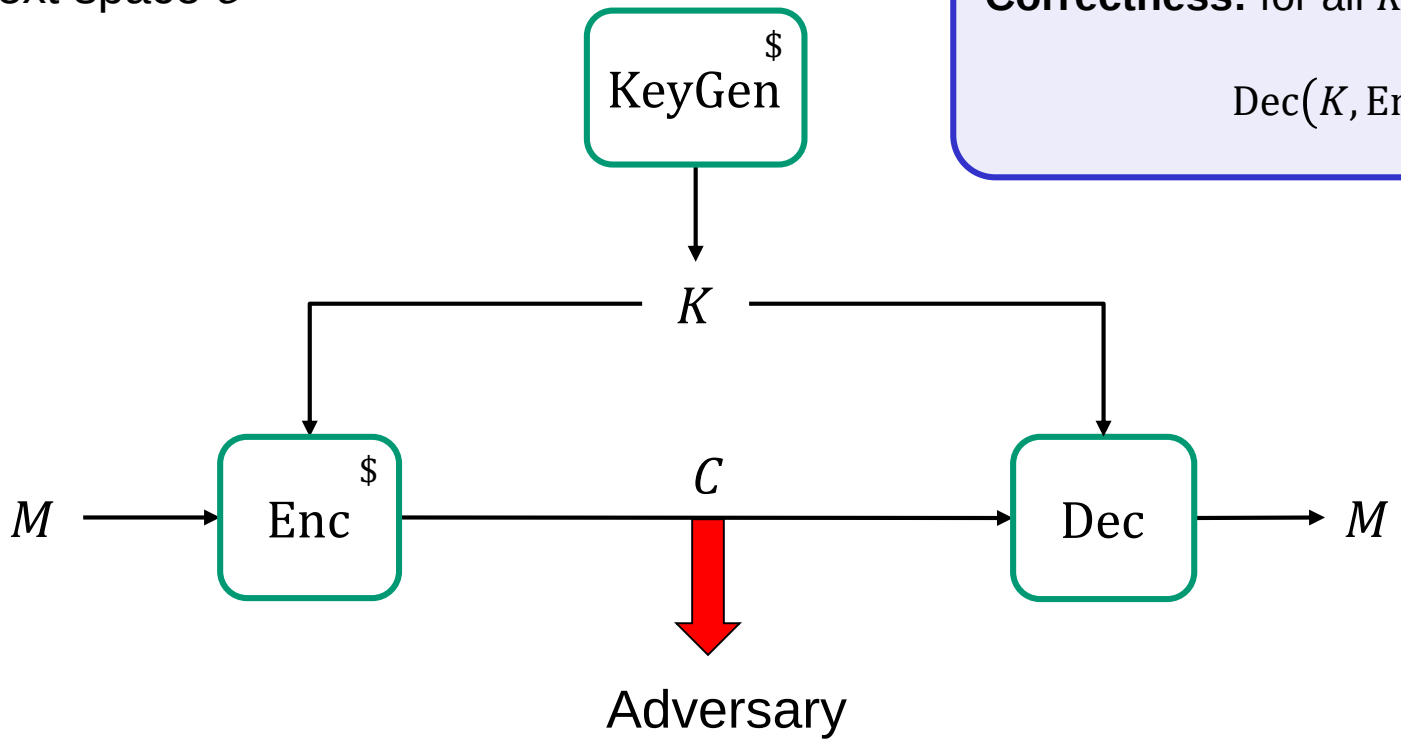
	Message privacy	**Message integrity / authentication**
Symmetric keys	Symmetric encryption	Message authentication codes (MAC)
Asymmetric keys	Asymmetric encryption (a.k.a. public-key encryption)	Digital signatures

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

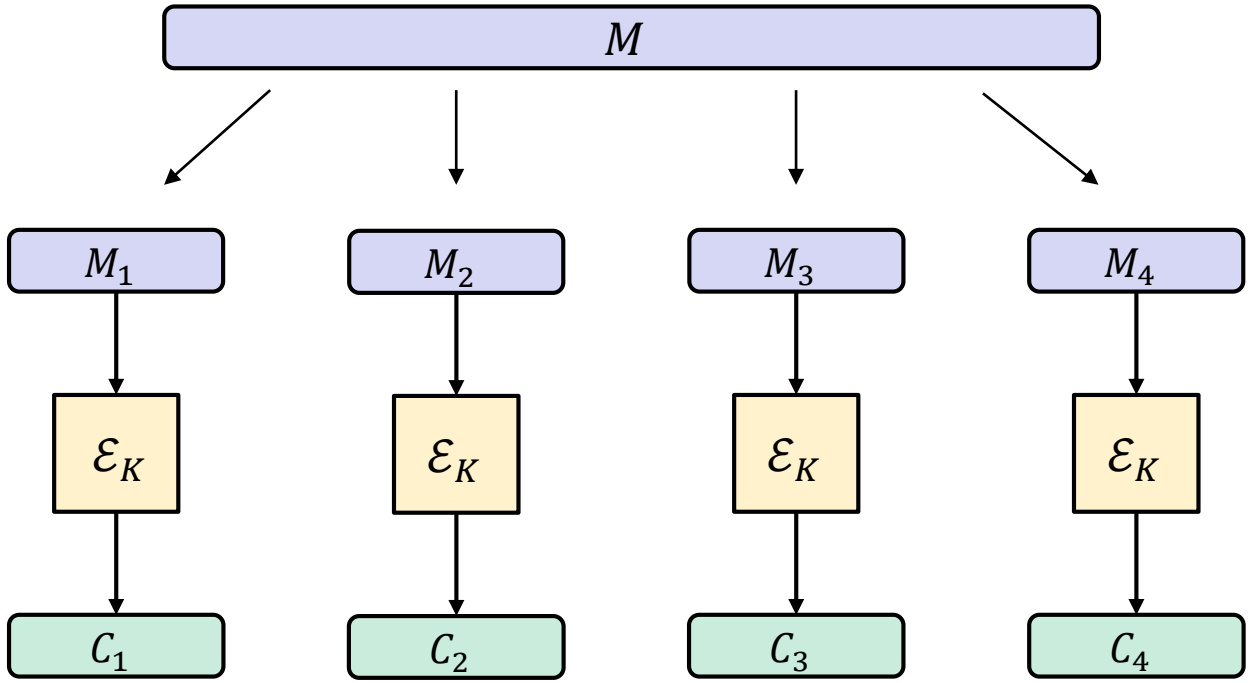
- When is an encryption scheme *secure*?

- 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:** …

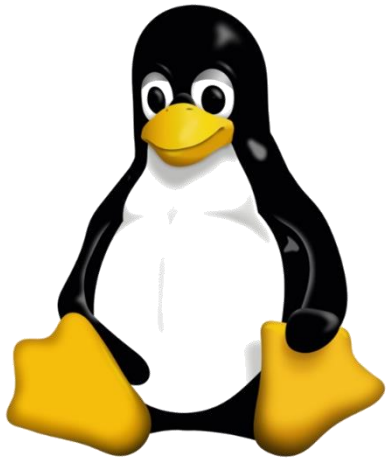
Electronic Code Book (ECB) mode

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

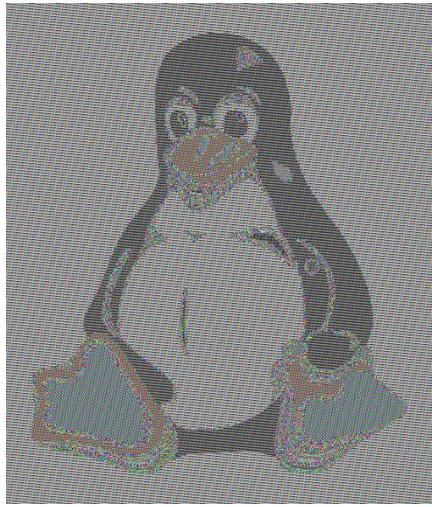


ECB problem

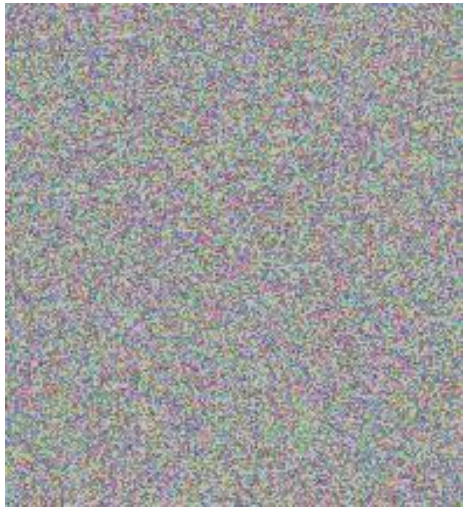
Plaintext



ECB encrypted



Properly encrypted



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

Modern cryptography – idea

- Computational ~~**Perfect**~~ **privacy:** for any $M_0, M_1 \in \mathcal{M}$ and any $C \in \mathcal{C}$:

$$\Pr[\mathcal{E}_K(M_0) = C] \not\approx \Pr[\mathcal{E}_K(M_1) = C]$$

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

- 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

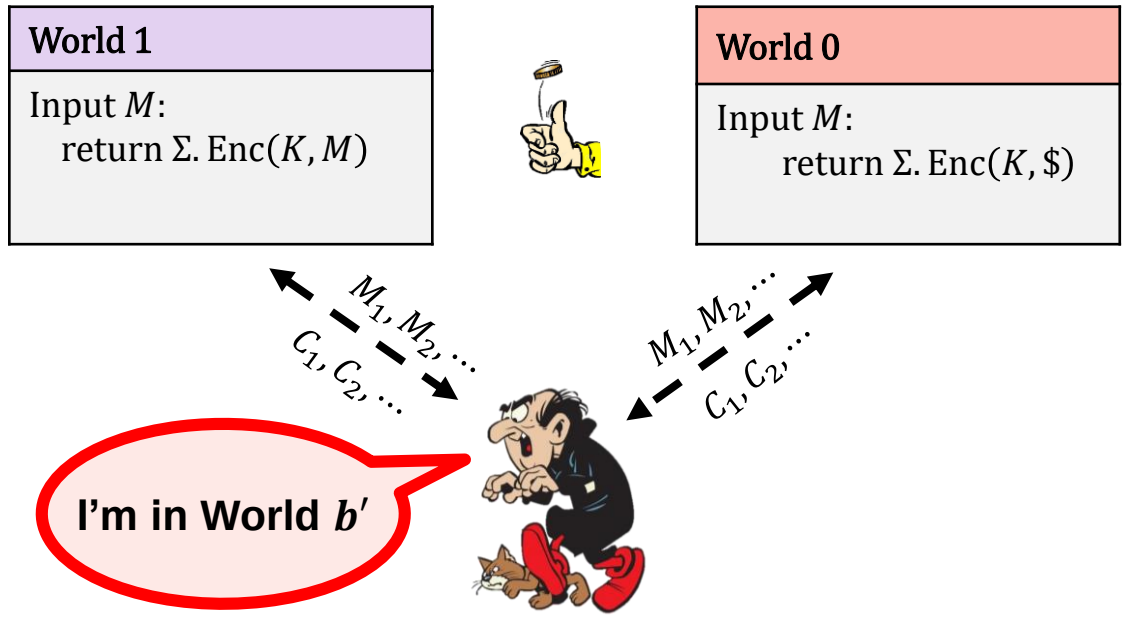
$\mathbf{Exp}_{\Sigma}^{\text{ind-cpa}}(A)$

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

$\mathcal{E}(M)$

---

1. $R \xleftarrow{\$} \{0,1\}^{|M|}$
2. $C_0 \leftarrow \Sigma.\text{Enc}(K, R)$
3. $C_1 \leftarrow \Sigma.\text{Enc}(K, M)$
4. **return** C_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** $b' \stackrel{?}{=} b$

$\mathcal{E}(M$

3.

4. **return** c_b

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

World 1

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

World 0

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

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

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

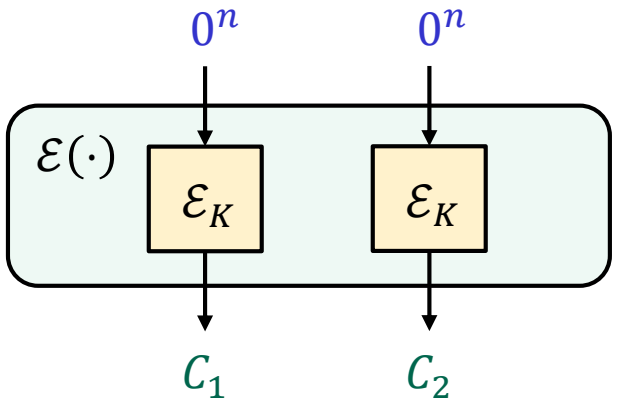
Definition: The **IND-CPA advantage** of an adversary A is

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

Example: IND-CPA insecurity of ECB mode

Adversary A

1. Query $\mathcal{E}(\cdot)$ on $0^n||0^n$
2. Receive back $C = C_1||C_2$
3. if $C_1 = C_2$ output 1
4. else, output 0



$\mathbf{Exp}^{\text{ind-cpa}}_{\text{ECB}[\mathcal{E}]}(A)$

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

$\mathcal{E}(M)$

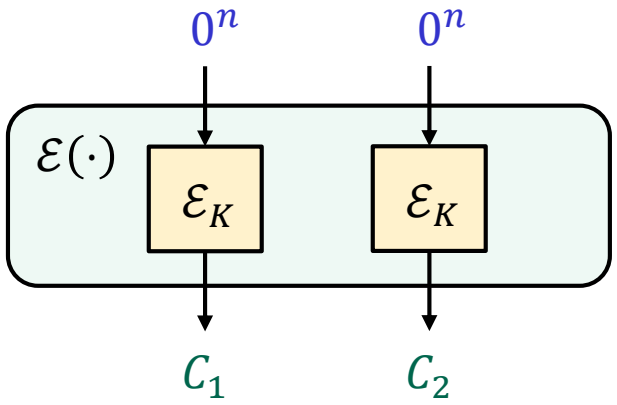
---

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

Example: IND-CPA insecurity of ECB mode

Adversary A

1. Query $\mathcal{E}(\cdot)$ on $0^n||0^n$
2. Receive back $C = C_1||C_2$
3. if $C_1 = C_2$ output 1
4. else, output 0



$\mathbf{Exp}^{\text{ind-cpa}}_{\text{ECB}[\mathcal{E}]}(A)$

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

$\mathcal{E}(M)$

---

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

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

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

$$= (\Pr[\,C_1 \neq C_2 \mid b = 0\,] + \Pr[\,C_1 = C_2 \mid b = 1\,]) \cdot 1/2$$

$$= (\Pr[\,C_1 \neq C_2 \mid b = 0\,] + \quad 1 \quad) \cdot 1/2$$

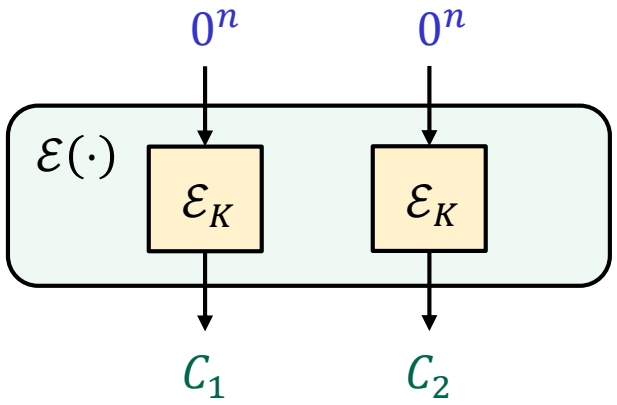
$$= (1 - \Pr[\,C_1 = C_2 \mid b = 0\,] + \quad 1 \quad) \cdot 1/2$$

$$= 1 - \frac{1}{2} \cdot \Pr[\,C_1 = C_2 \mid b = 0\,] = 1 - \frac{1}{2} \cdot \frac{1}{2^n} = 1 - \frac{1}{2^{n+1}}$$

Example: IND-CPA insecurity of ECB mode

Adversary A

1. Query $\mathcal{E}(\cdot)$ on $0^n||0^n$
2. Receive back $C = C_1||C_2$
3. if $C_1 = C_2$ output 1
4. else, output 0



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

$\mathbf{Exp}^{\text{ind-cpa}}_{\text{ECB}[\mathcal{E}]}(A)$

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

$\mathcal{E}(M)$

---

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

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

Consequences of the definition

- An IND-CPA secure scheme *cannot* be deterministic

- 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 $Y_1, Y_2, \ldots$
  -
  - But does it give us *all* the properties we want? I.e., is IND-CPA the "master property"?

Semantic security

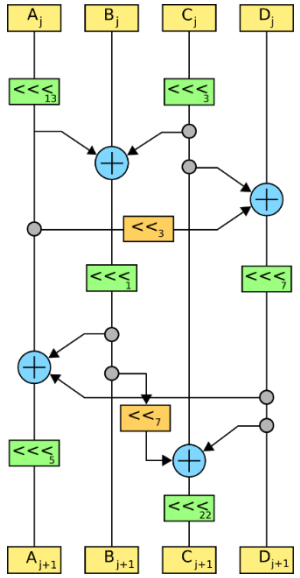
- The conceptually "right" definition
- High level idea: an encryption scheme is **semantically secure** if by observing a ciphertext C the adversary learns *nothing* about the plaintext (except its length)
- Harder to formalize; IND-CPA easier to work with

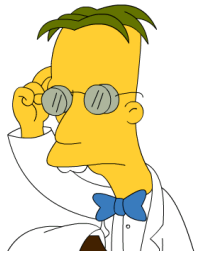
Theorem: (Goldwasser & Micali '83)

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

Length-leaking attacks

- 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



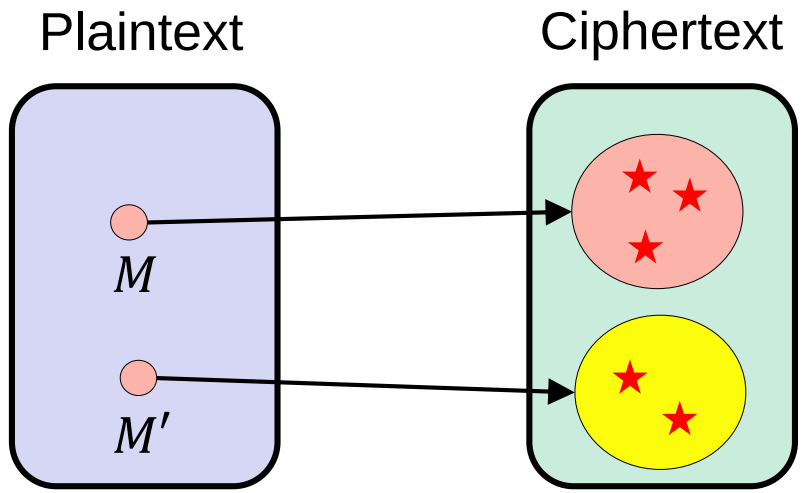


Constructing symmetric encryption schemes

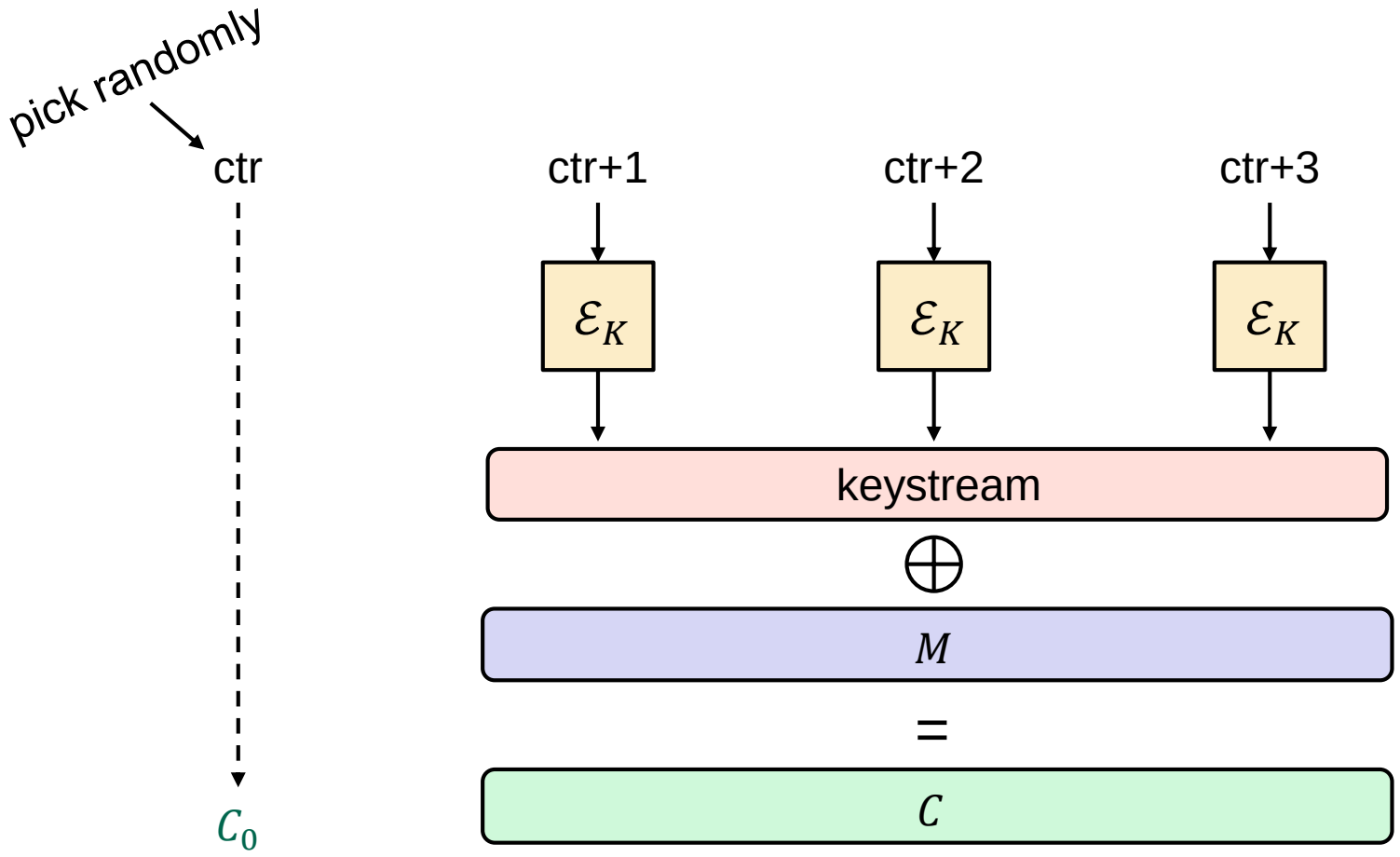
How to achieve non-deterministic encryption?

- Randomized encryption
  - Coins flipped internally by the algorithm

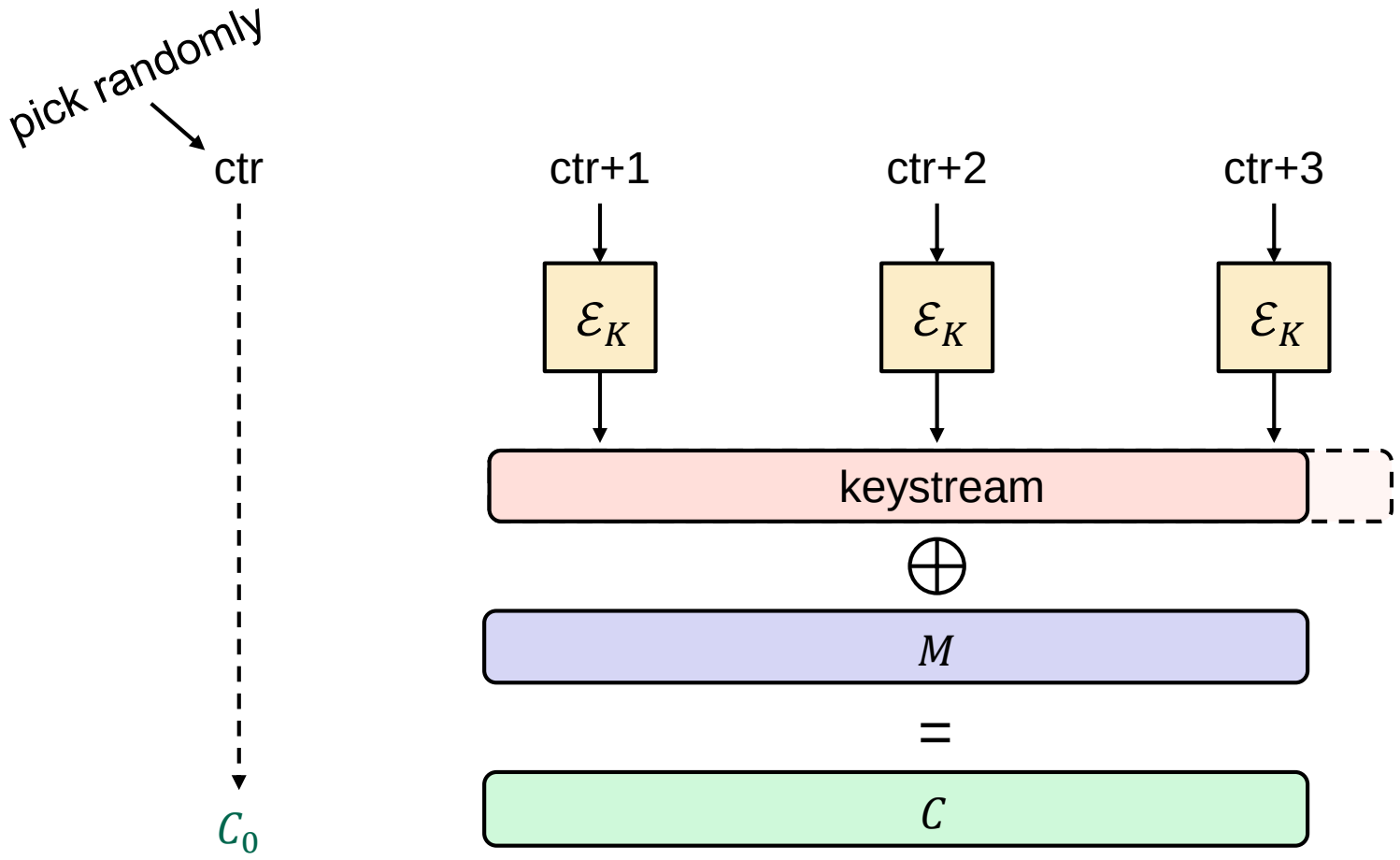
- Nonce-based encryption
  - Encryption scheme itself is deterministic
  - Non-determinism injected from the outside



CTR$ mode

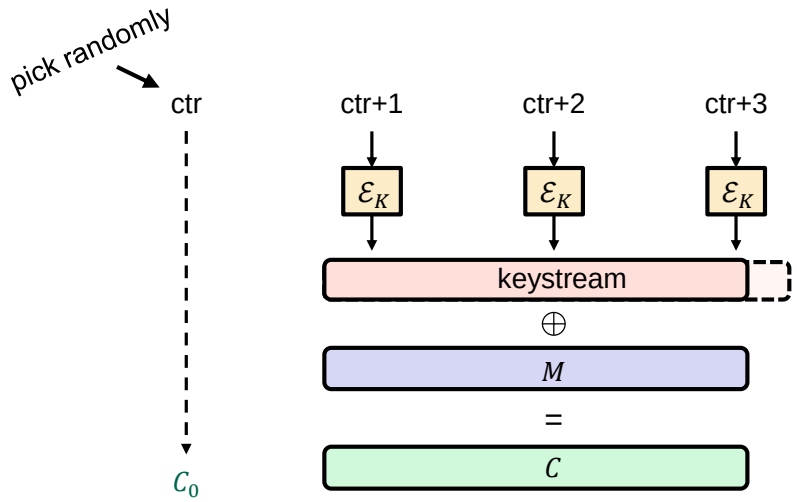

pick randomly
ctr
C_0
ctr+1
ctr+2
ctr+3
$\mathcal{E}_K$
$\mathcal{E}_K$
$\mathcal{E}_K$
keystream
M
=
C

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
- Key stream 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$

Logic 101

$A \Rightarrow B$

is *equivalent to:*

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

Theorem (idea):

If $F: \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ is a *secure* PRF then $\mathrm{CTR\$}[F]$ is *IND-CPA secure*.

⇕ equivalent!

Theorem (idea):

If $\mathrm{CTR\$}[F]$ is *not* IND-CPA secure then F is *not* a secure PRF.

Security of CTR$

Theorem (idea):

If $\mathrm{CTR\$}[F]$ is *not* IND-CPA secure then F is *not* a secure PRF.

Proof idea:

- $\mathrm{CTR\$}[F]$ not IND-CPA secure $\Longrightarrow$ there exists adversary A with good advantage $\mathbf{Adv}^{\mathrm{ind-cpa}}_{\mathrm{CTR\$}[F]}(A)$

- Can use A to create a *new* adversary B that has good advantage $\mathbf{Adv}^{\mathrm{prf}}_{F}(B)$ against F

  $\Longrightarrow F$ is not a secure PRF!

Security of CTR$

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

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

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 $\mathrm{CTR\$}[F]$ that runs in time t_A and asks at most q queries (each of ℓ blocks), there is a PRF-adversary B such that

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

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

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

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

$\Rightarrow \mathrm{CTR\$}[F]$ is IND-CPA secure!

Example: AES-128

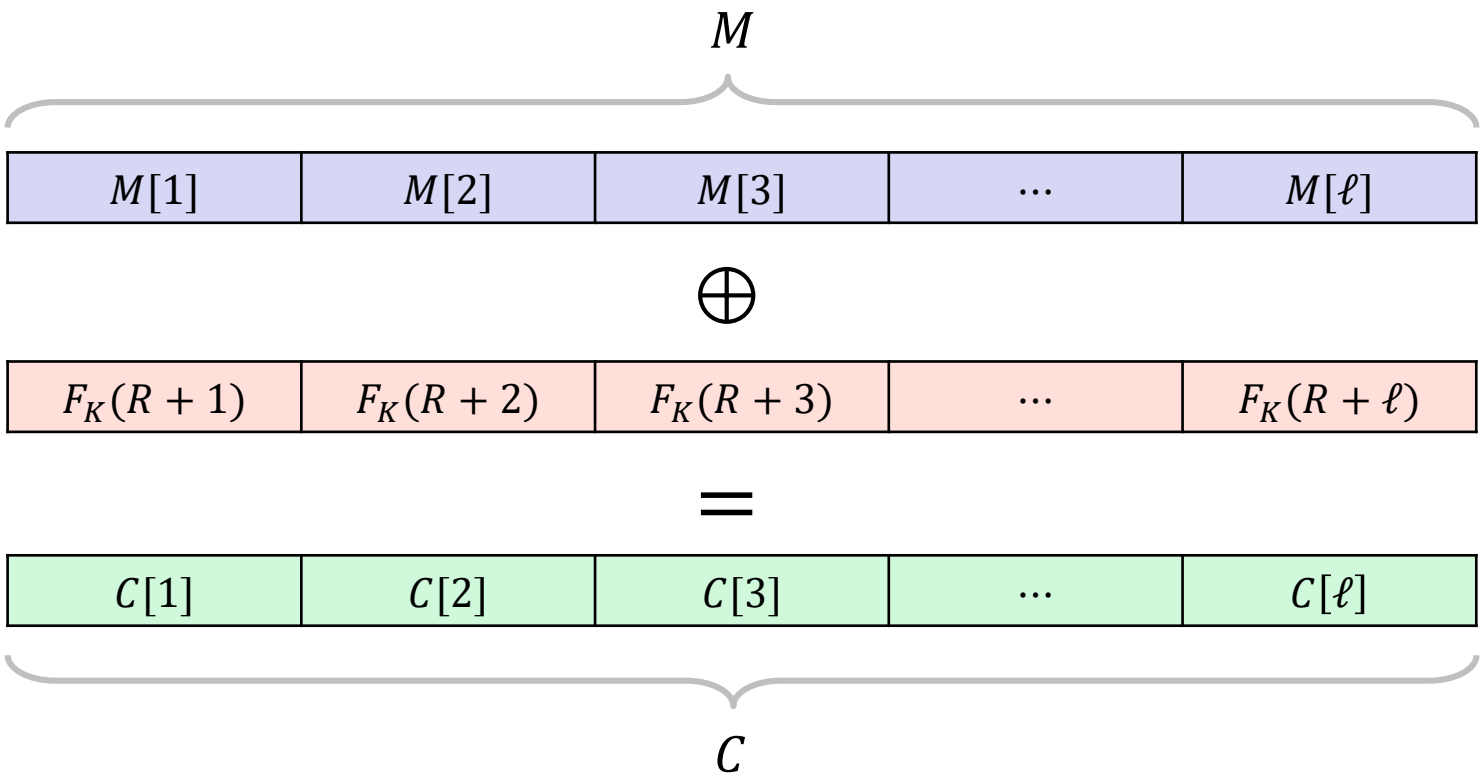
$n = 128$
$\ell = 2^6 \approx 1$ kB
$q = 2^{40}$
} ≈ 70 TB

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

Security of CTR$ – proof idea

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

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



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

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

$\mathcal{E}(M)$

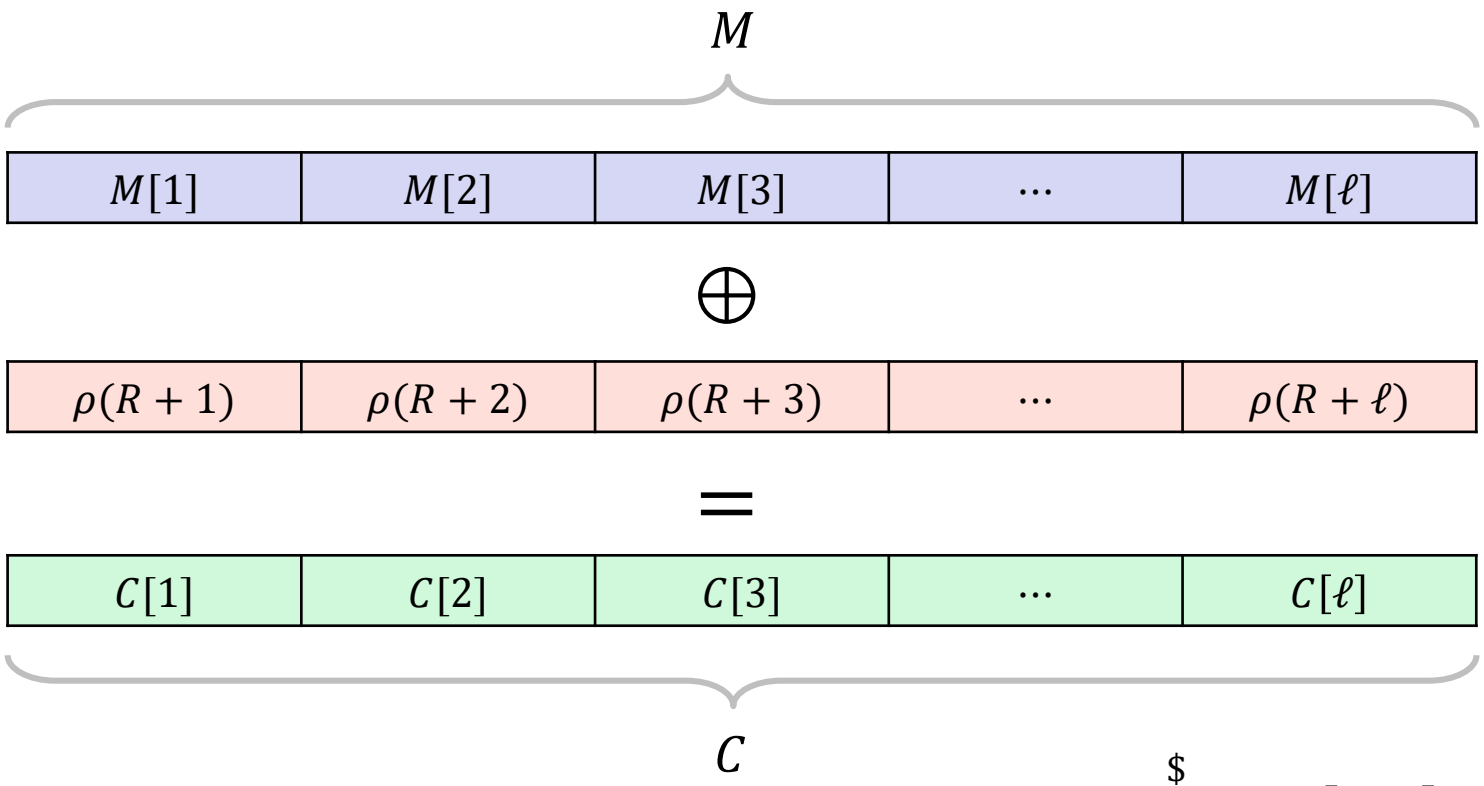
---

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

Security of CTR$ – proof idea

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

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



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

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

$\mathcal{E}(M)$

---

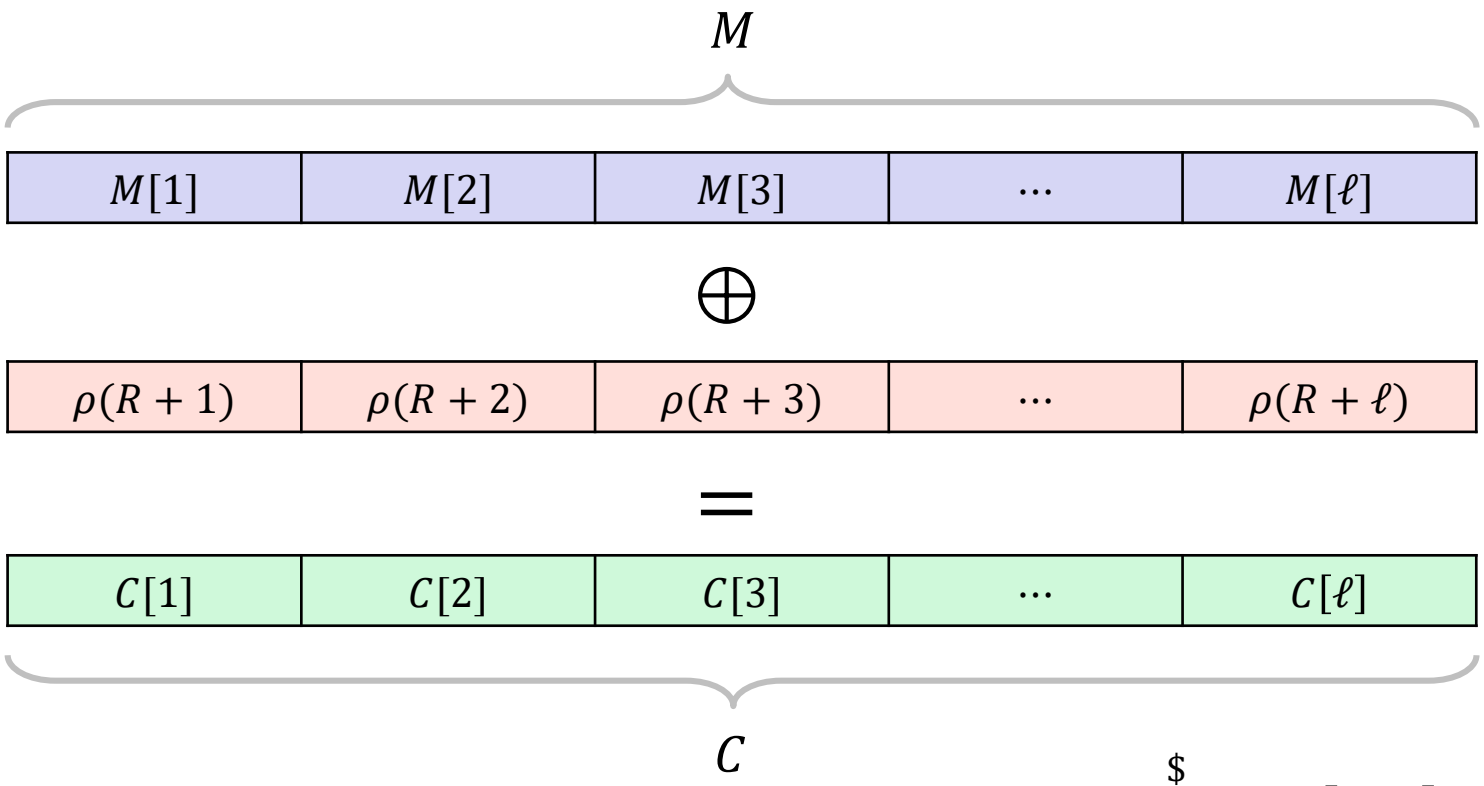
1. $U \xleftarrow{\$} \{0,1\}^{|M|}$
2. $C_0 \leftarrow \text{CTR\$.Enc}(K, U)$
3. $C_1 \leftarrow \text{CTR\$.Enc}(K, M)$
4. **return** C_b

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

Security of CTR$ – proof idea

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

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



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

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

$\mathcal{E}(M)$

---

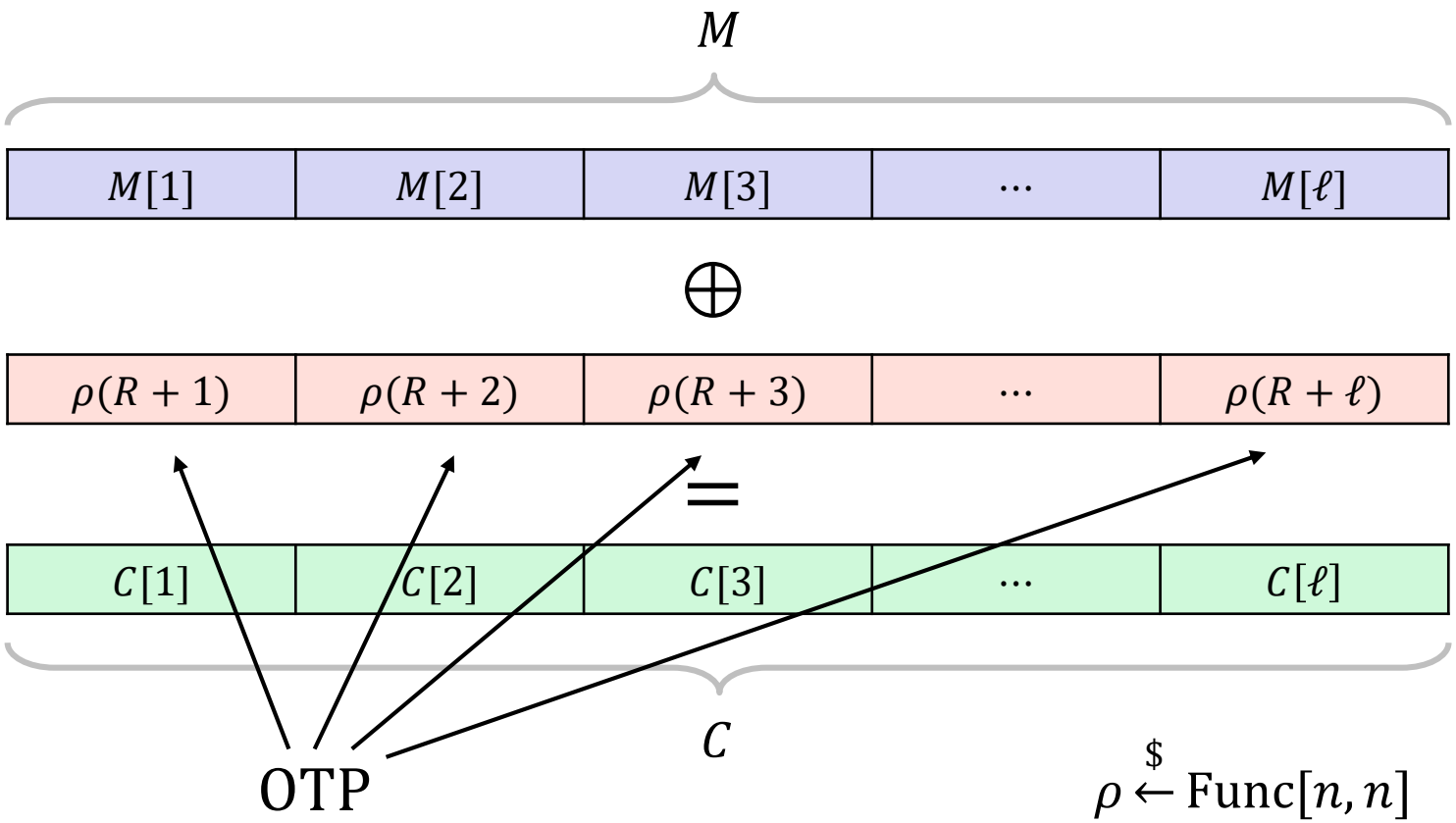
1. $U \xleftarrow{\$} \{0,1\}^{|M|}$
2. $C_0 \leftarrow \text{CTR\$.Enc}(K, U)$
3. $C_1 \leftarrow \text{CTR\$.Enc}(K, M)$
4. **return** C_b

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

Security of CTR$ – proof idea

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

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



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

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

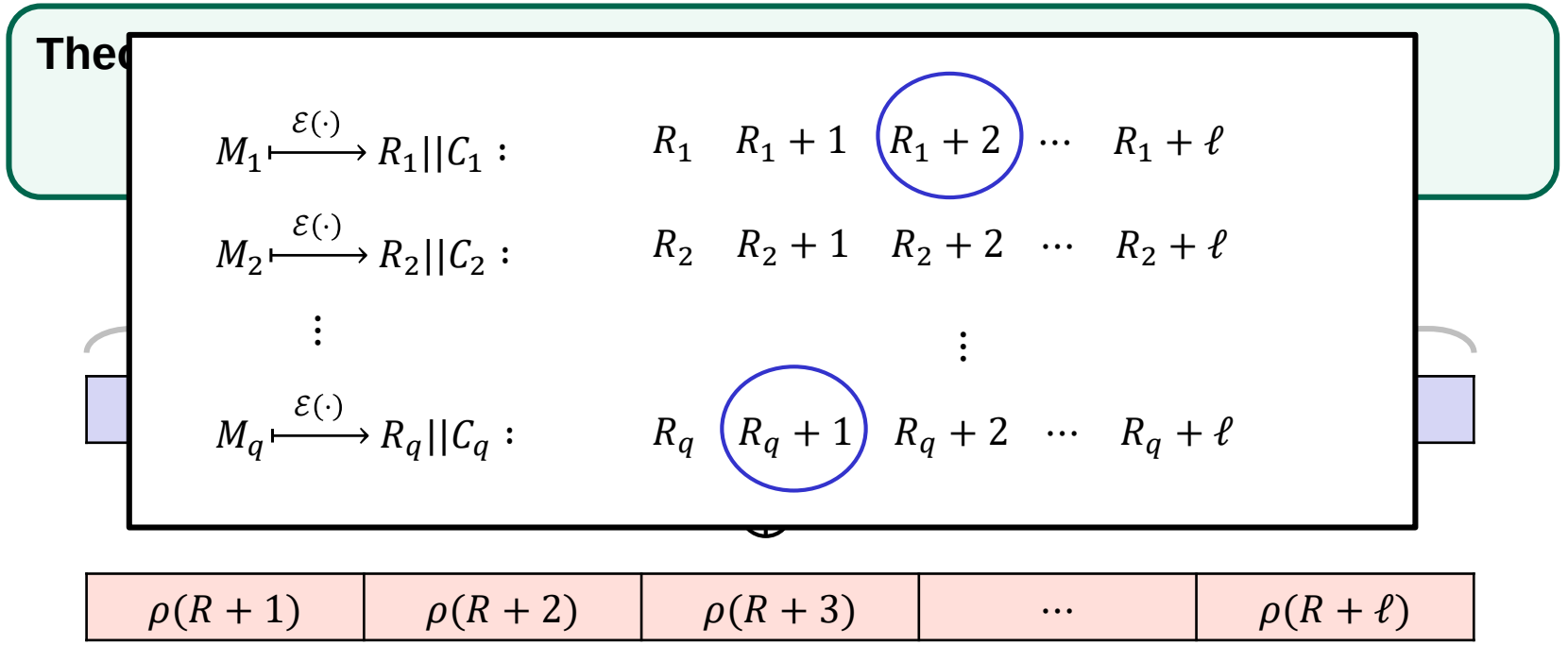
$\mathcal{E}(M)$

---

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

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

Security of CTR$ – proof idea



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

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

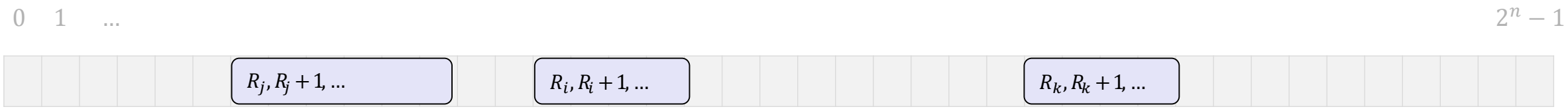
Event Coll:

$$R_i + j = R_{i'} + j' \implies \rho(R_i + j) = \rho(R_{i'} + j') = P$$

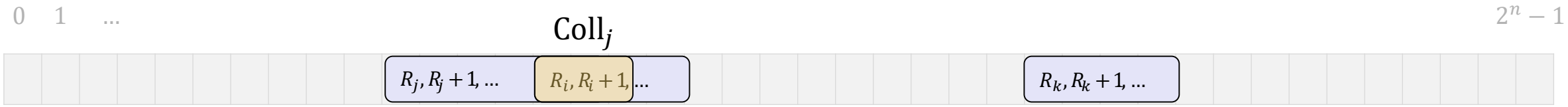
$$\implies C_i[j] \oplus C_i[j'] = (P \oplus M_i[j]) \oplus (P \oplus M_{i'}[j']) = M_i[j] \oplus M_{i'}[j']$$

- by PRF-security

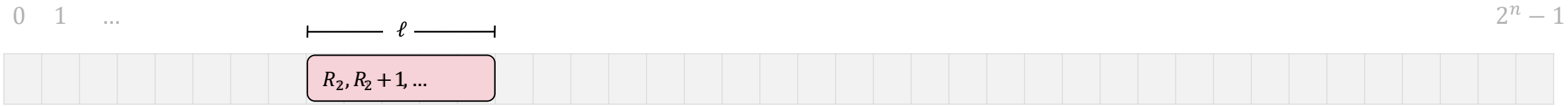
Security of CTR$ – proof idea



Security of CTR$ – proof idea



Security of CTR$ – proof idea

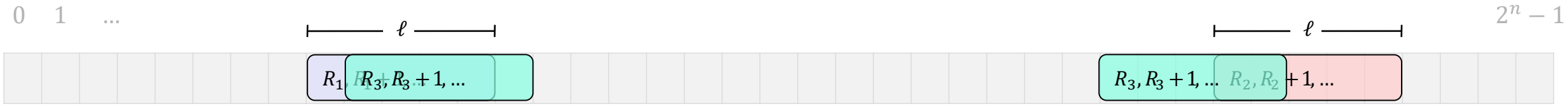


$$\Pr[\text{Coll}] = \Pr\left[\text{Coll}_1 \vee \text{Coll}_2 \vee \cdots \vee \text{Coll}_q\right]$$

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

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

Security of CTR$ – proof idea

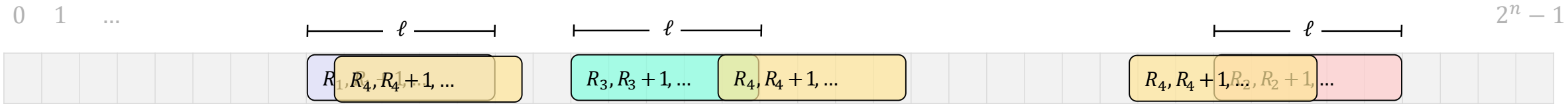


$$\Pr[\text{Coll}] = \Pr\left[\text{Coll}_1 \vee \text{Coll}_2 \vee \cdots \vee \text{Coll}_q\right]$$

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

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

Security of CTR$ – proof idea

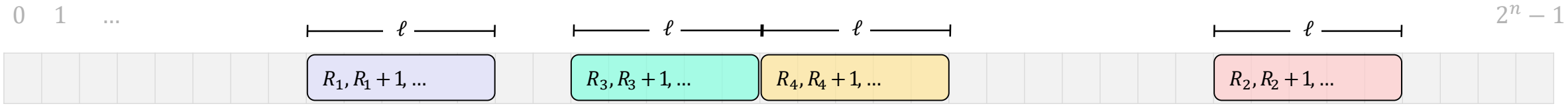


$$\Pr[\text{Coll}] = \Pr\left[\text{Coll}_1 \vee \text{Coll}_2 \vee \cdots \vee \text{Coll}_q\right]$$

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

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

Security of CTR$ – proof idea



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

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

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

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

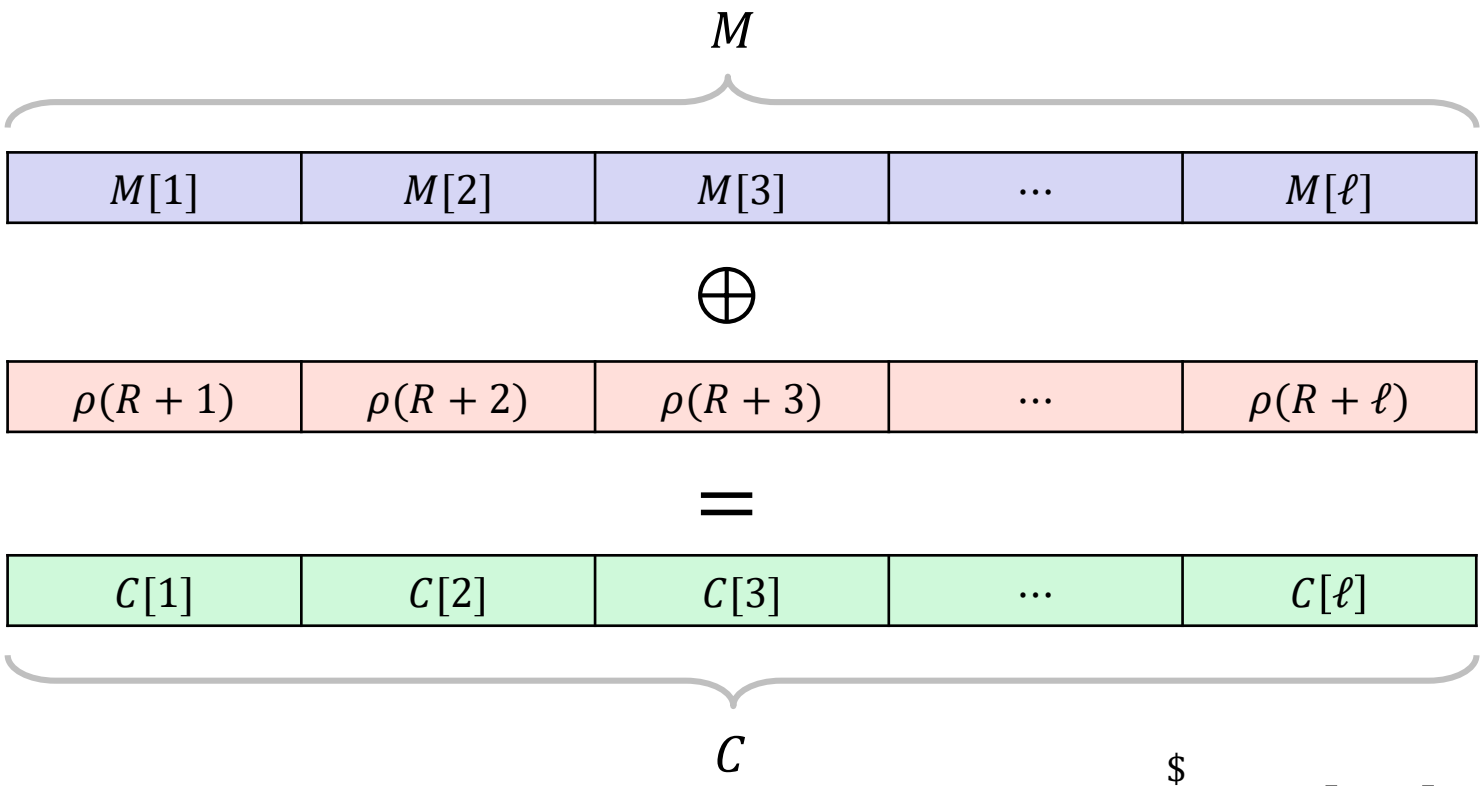
$\frac{q(q-1)}{2}$

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

Security of CTR$ – proof idea

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

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



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

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

$\mathcal{E}(M)$

---

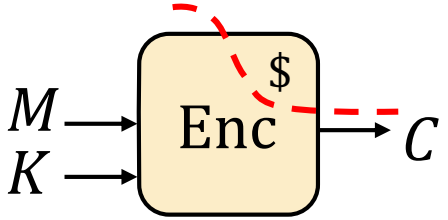
1. $U \xleftarrow{\$} \{0,1\}^{|M|}$
2. $C_0 \xleftarrow{\$} \{0,1\}^{|M|}$
3. $C_1 \xleftarrow{\$} \{0,1\}^{|M|}$
4. **return** C_b

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

Nonce-based encryption

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

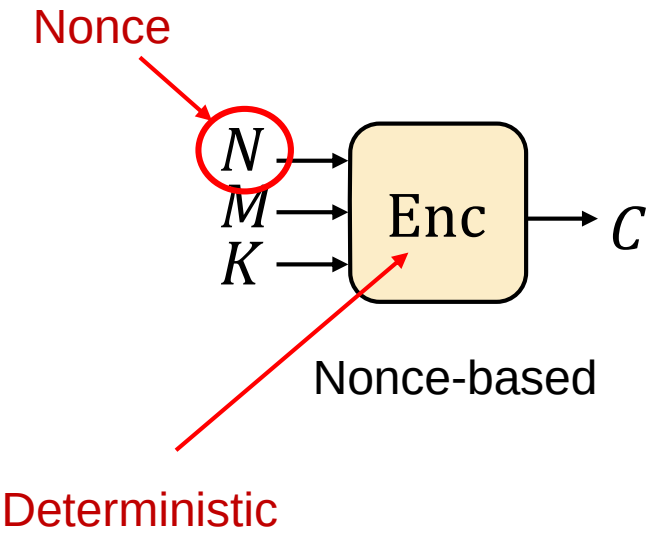
$$\text{Enc}(K, M) = \text{Enc}_K(M)$$



Randomized

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

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



How to create the nonce?

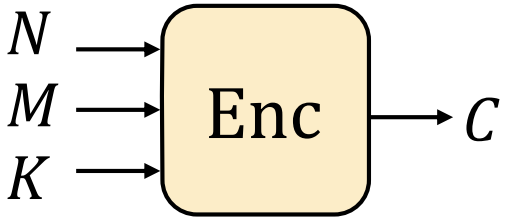
- Randomly (also called IV-based)
- Counter
- Combination

Nonce-based encryption – new syntax

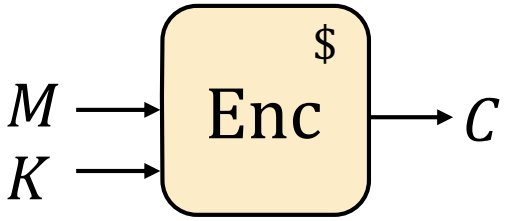
$$\mathrm{Enc} : \mathcal{K} \times \mathcal{N} \times \mathcal{M} \to \mathcal{C}$$

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

Nonce-based



- Enc is now a deterministic *function*
- Non-determinism comes from varying N
- Choose N at random $\Longrightarrow$ recover probabilistic notion



Randomized

CTR$ vs. (nonce-based) CTR

$\mathrm{CTR\$}[\mathcal{E}].\mathrm{Enc}(K, M)$

---

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

VS.

$\mathrm{CTR}[\mathcal{E}].\mathrm{Enc}(K, N, M)$

---

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

Nonce-based CTR – IND-CPA security

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

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

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

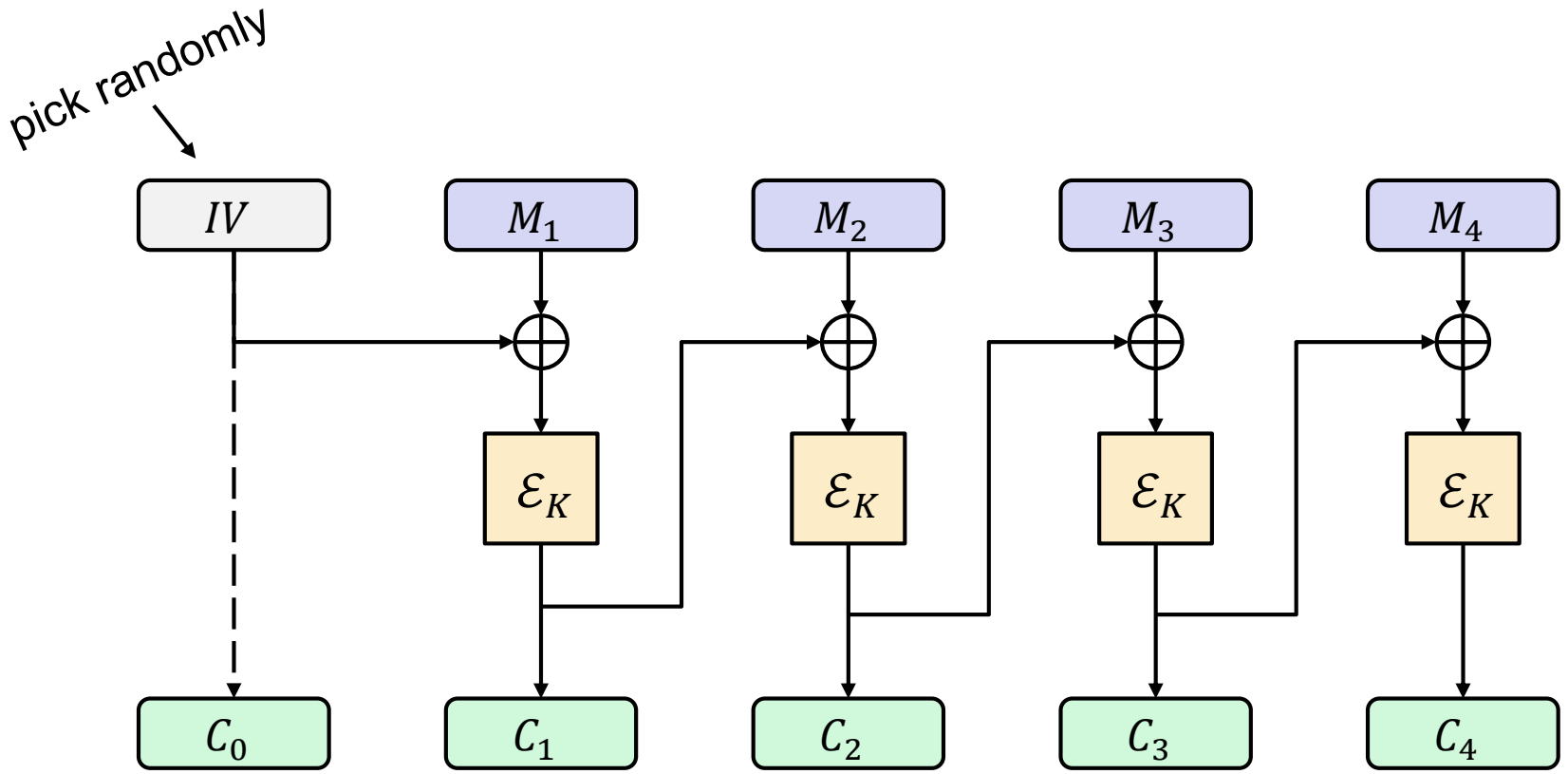
vs.

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

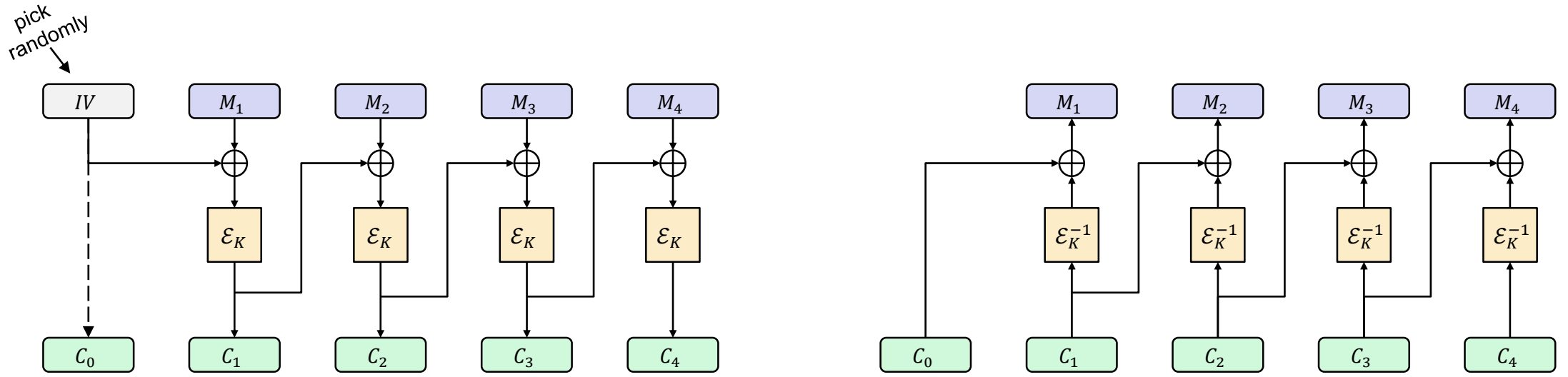
$$\mathbf{Adv}^{\text{ind-cpa}}_{\mathrm{CTR\$}[F]}(A) \leq \mathbf{Adv}^{\text{prf}}_{F}(B) + \frac{q^2\ell}{2^n}$$

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

CBC$ – Cipher Block Chaining mode

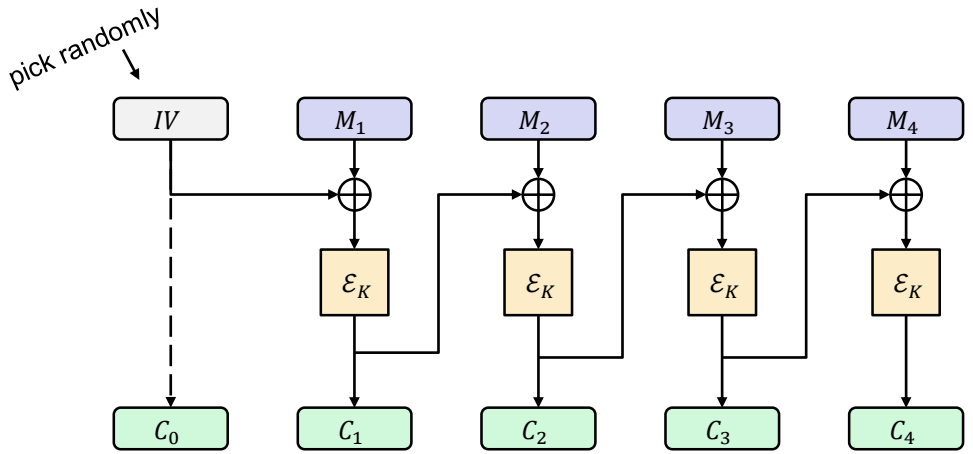


CBC$ – Cipher Block Chaining mode

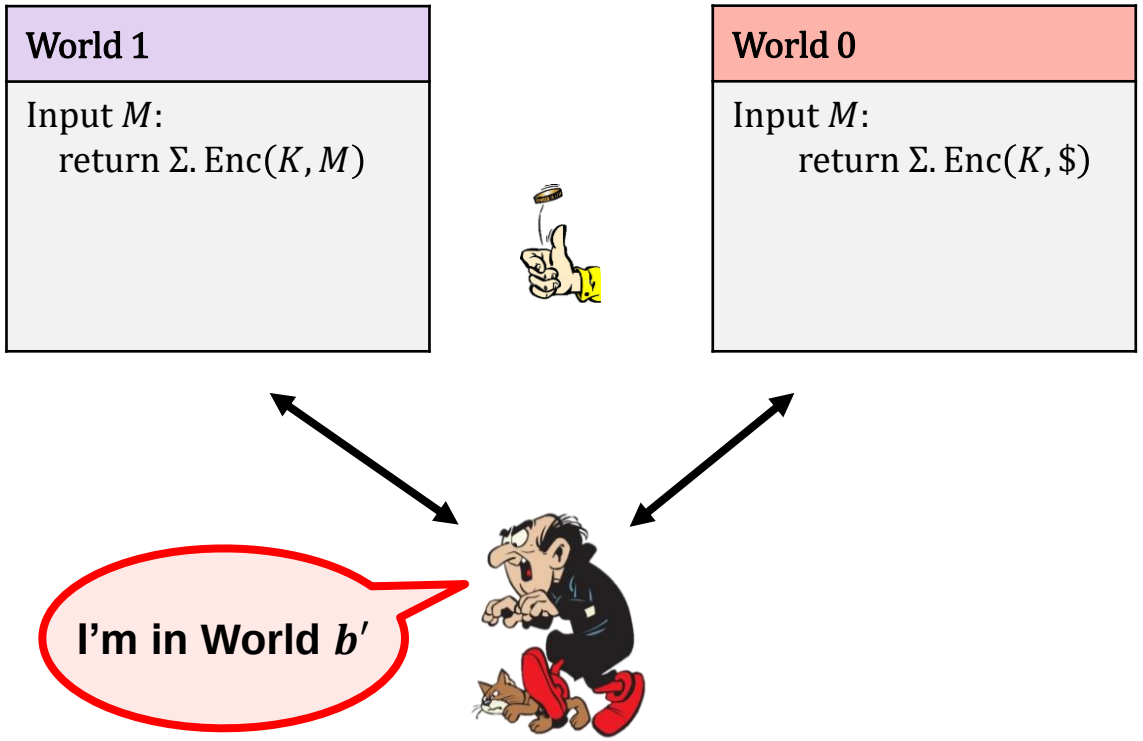


CBC

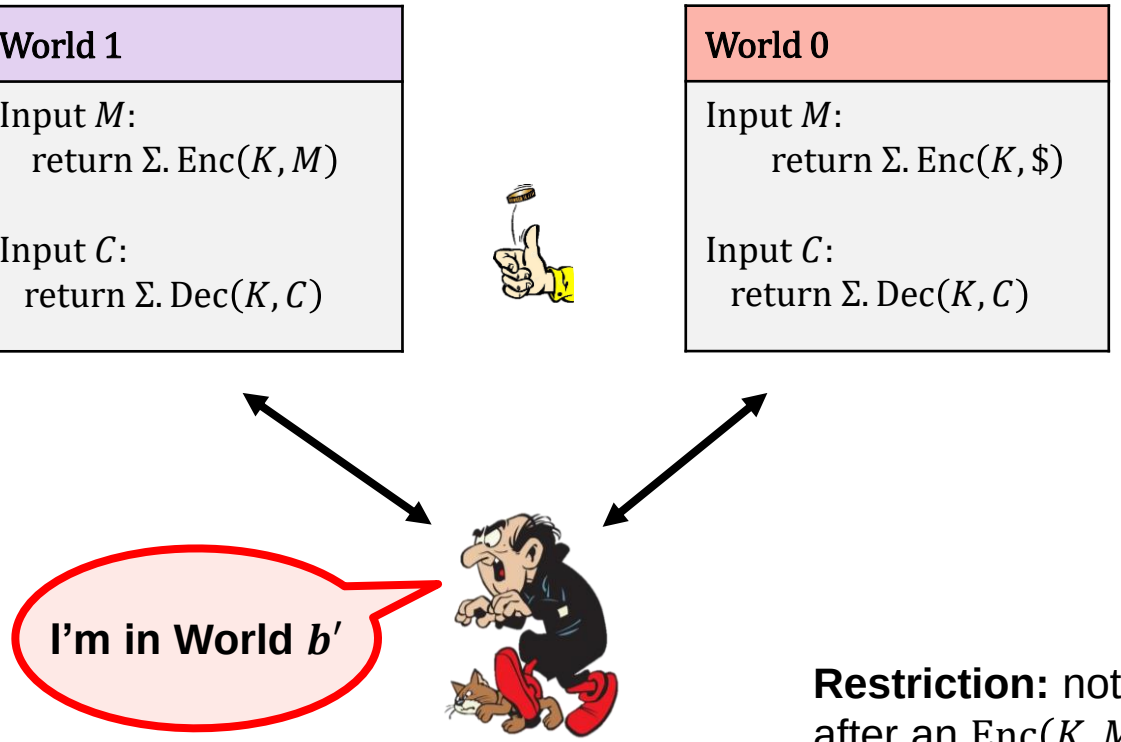
- **Theorem:** IND-CPA secure for *random* IV (assuming $\mathcal{E}$ is a good block cipher)
- Not IND-CPA secure for nonce-based IV
  - (exercise: show this)
- Not parallelizable; cannot precompute values
- Inverse of block cipher $\mathcal{E}$ needed for decryption
- Padding needed for messages not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