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

TEK4500

11.09.2024

Håkon Jacobsen

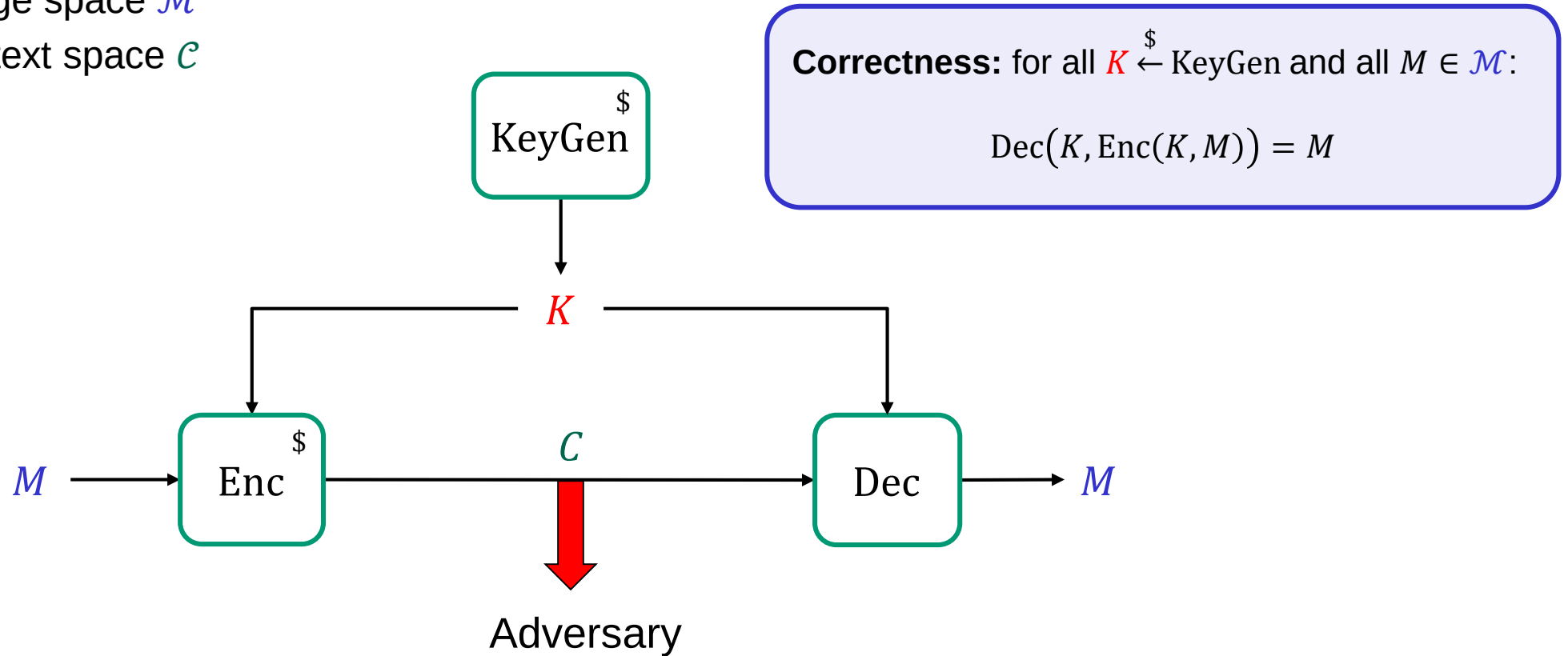
hakon.jacobsen@its.uio.no

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 $\Sigma = (\text{KeyGen}, \text{Enc}, \text{Dec})$
 - Key space $\mathcal{K}$
 - Message space $\mathcal{M}$
 - Ciphertext space $\mathcal{C}$



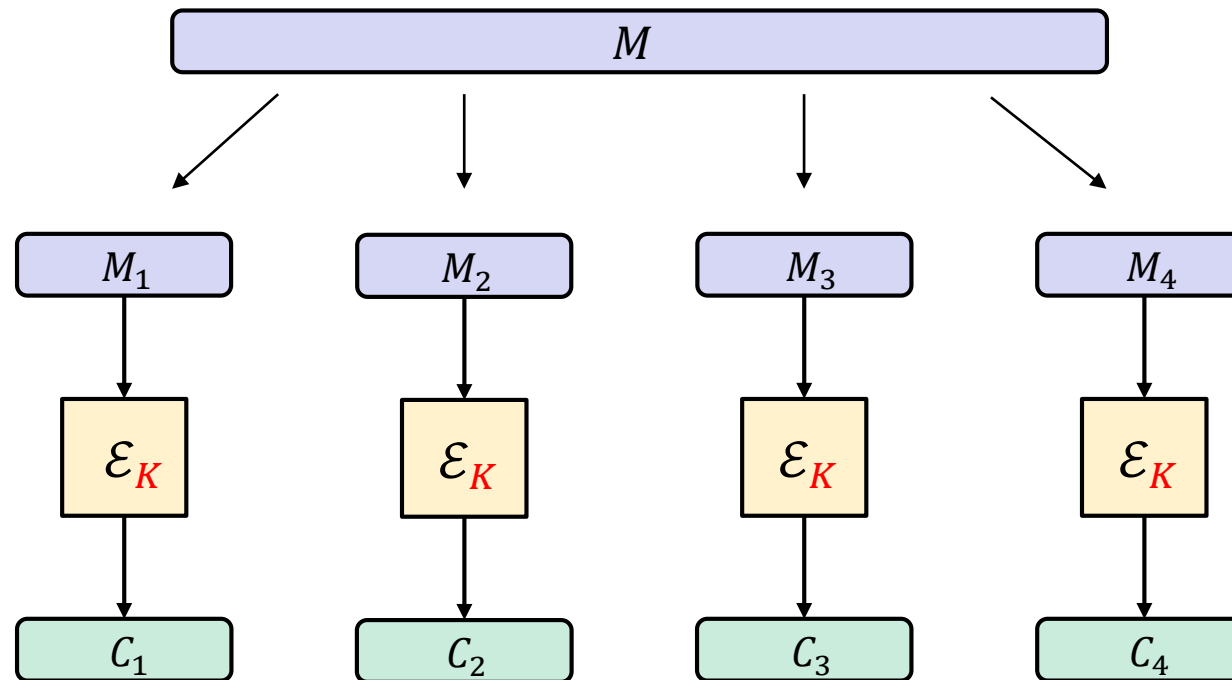
- KeyGen and Enc may be randomized (\$), but Dec must be deterministic

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 $E_K(X_1), E_K(X_2), E_K(X_3) \dots$
 - **P3:** Should be hard to obtain X from $E_K(X)$
 - **P4:** Should be hard to obtain *any* X_i from $E_K(X_1), E_K(X_2), E_K(X_3) \dots$
 - **P5:** Should be hard to learn any *bit* of X from $E_K(X)$
 - **P6:** Should be hard to detect *repetitions* among $X_1, X_2, \dots$ from $E_K(X_1), E_K(X_2), \dots$
 - **P7:** ...
- Not possible for block ciphers!
- 

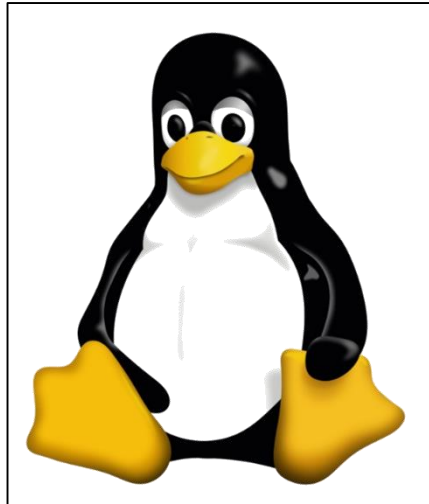
Electronic Code Book (ECB) mode

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

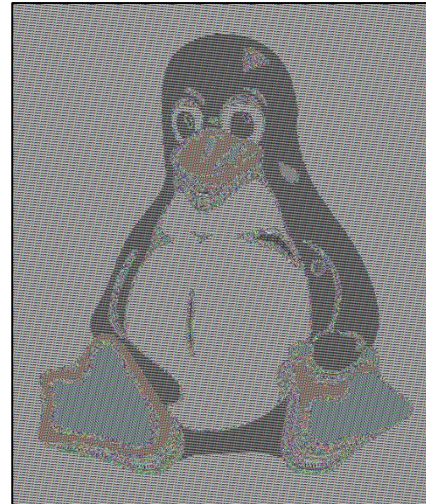


ECB problem

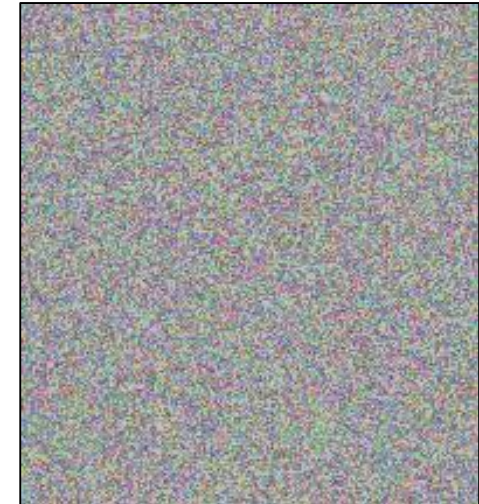
Plaintext



ECB encrypted



Properly encrypted



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

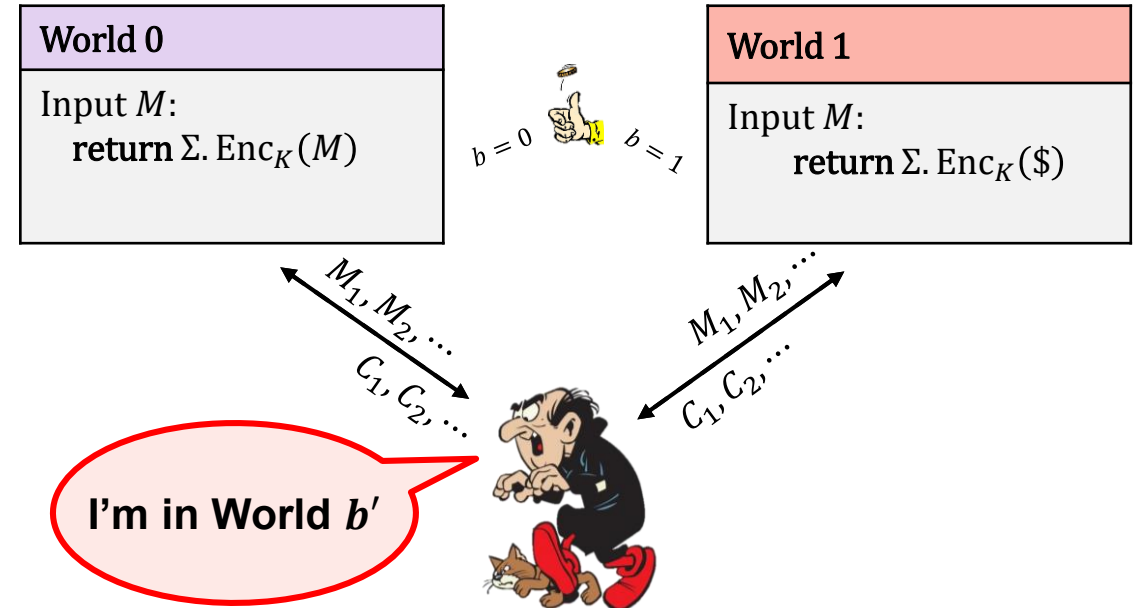
IND-CPA – indistinguishability against chosen-plaintext attacks

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

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. $C_0 \leftarrow \Sigma.\text{Enc}(K, M)$
3. $C_1 \leftarrow \Sigma.\text{Enc}(K, R)$
4. **return** C_b



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

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

IND-CPA – indistinguishability against chosen-plaintext attacks

$\text{Exp}_{\Sigma}^{\text{ind-cpa}}(A)$	
1.	$b \xleftarrow{\$} \{0,1\}$
2.	$K \xleftarrow{\$} \Sigma.\text{KeyGen}$
3.	b'
4.	
$\mathcal{E}(M)$	
1.	$R \xleftarrow{\$} \{0,1\}^{ M }$
2.	$C_0 \leftarrow \Sigma.\text{Enc}(K, M)$
3.	$C_1 \leftarrow \Sigma.\text{Enc}(K, R)$
4.	return C_b

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

World 0

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



World 1

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

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

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

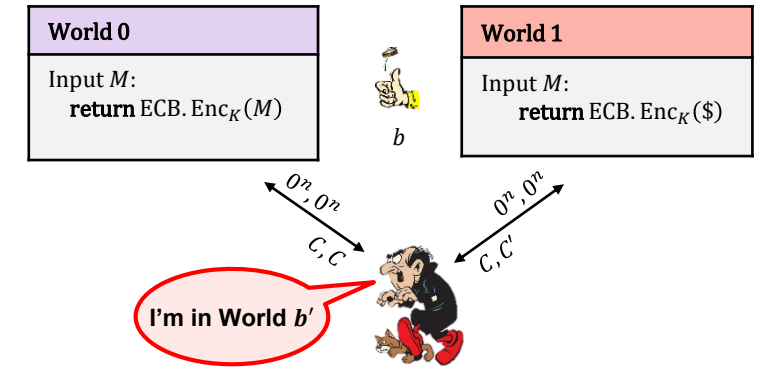
Definition: The **IND-CPA advantage** of an adversary A is

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

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 $b' = 1$



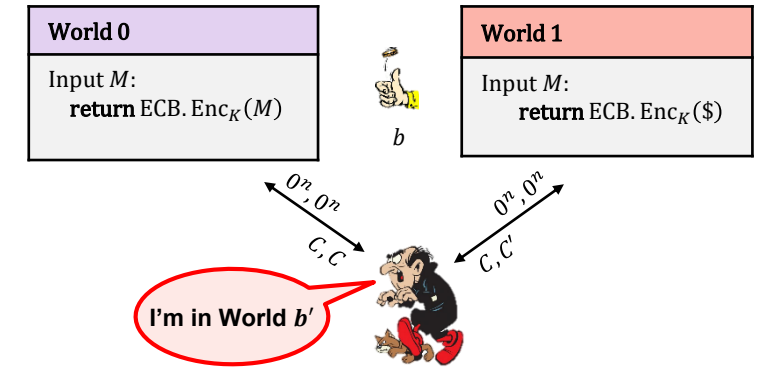
$$\begin{aligned}\Pr\left[\mathbf{Exp}_{\text{ECB}}^{\text{ind-cpa}}(A) \Rightarrow \text{true}\right] &= \Pr[b' = b] \\ &= \Pr[b' = 0 \mid b = 0] \cdot 1/2 + \Pr[b' = 1 \mid b = 1] \cdot 1/2 \\ &= \Pr[C = C' \mid b = 0] \cdot 1/2 + (1 - \Pr[b' = 0 \mid b = 1]) \cdot 1/2 \\ &= 1/2 + (1 - \Pr[C = C' \mid b = 1]) \cdot 1/2 \\ &= 1/2 + (1 - 2^{-n}) \cdot 1/2 \\ &= 1 - \frac{1}{2^{n+1}}\end{aligned}$$

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 $b' = 1$

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



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

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 $Y_1, Y_2, \dots$ 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 $Y_1, Y_2, \dots$ 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 $X_1, X_2, \dots$ from $Y_1, Y_2, \dots$
 - **P7:** ...
- But does it give us *all* the properties we want? I.e., is IND-CPA the "master property"?



Semantic security

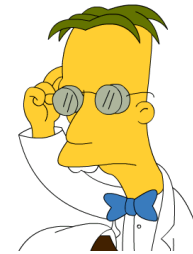
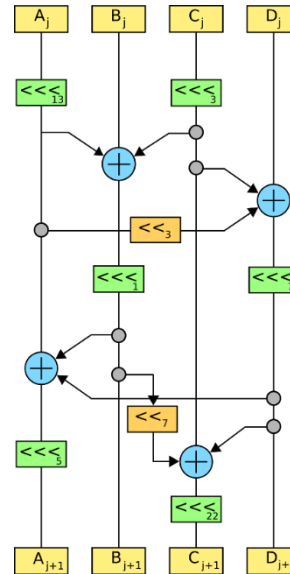
- The conceptually "right" definition
- High level idea: an encryption scheme is **semantically secure** if by observing a ciphertext C the adversary learns *nothing* about the plaintext (except its length)
- Harder to formalize; IND-CPA easier to work with

Theorem: (Goldwasser & Micali '83)

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

Length-leaking attacks

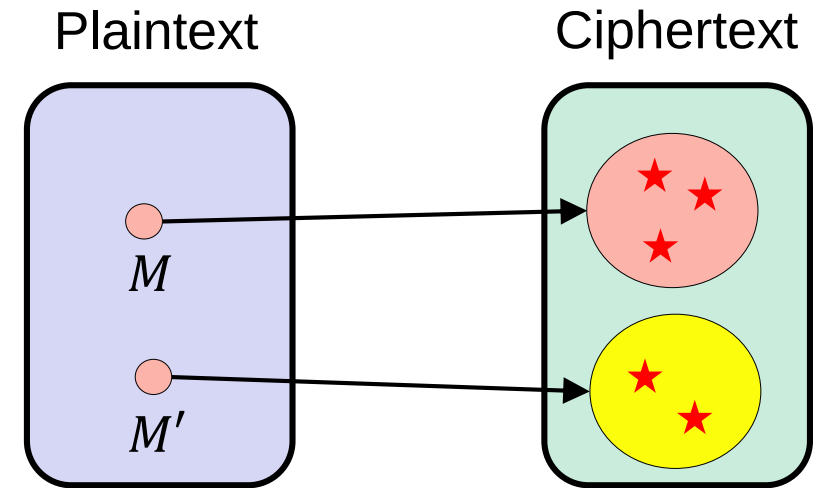
- Wikipedia pages
 - Each page has a unique size
- Google maps
 - World regions have unique "fingerprints" based on length of data (based on map tiles)
- Variable-bitrate encoding
 - Can e.g., fingerprint movies streamed over Netflix
- To combat length-leaking attacks: message padding
 - Can be expensive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



**Constructing symmetric
encryption schemes**

How to achieve non-deterministic encryption?

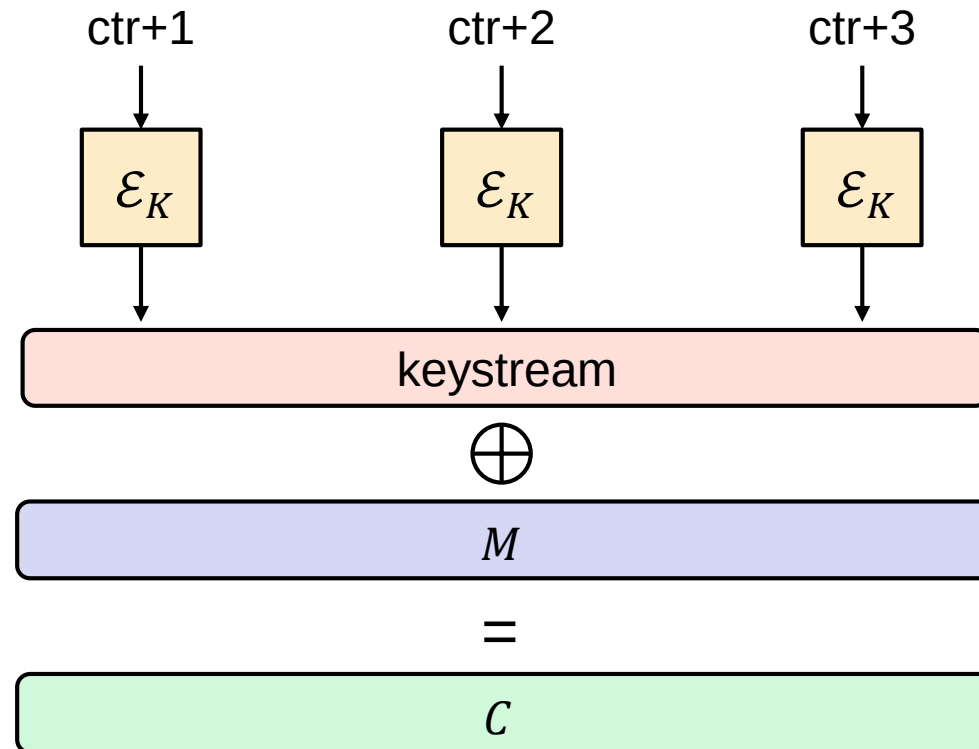
- Randomized encryption
 - Coins flipped internally by the algorithm
- Nonce-based encryption
 - Encryption scheme itself is deterministic
 - Non-determinism injected from the outside



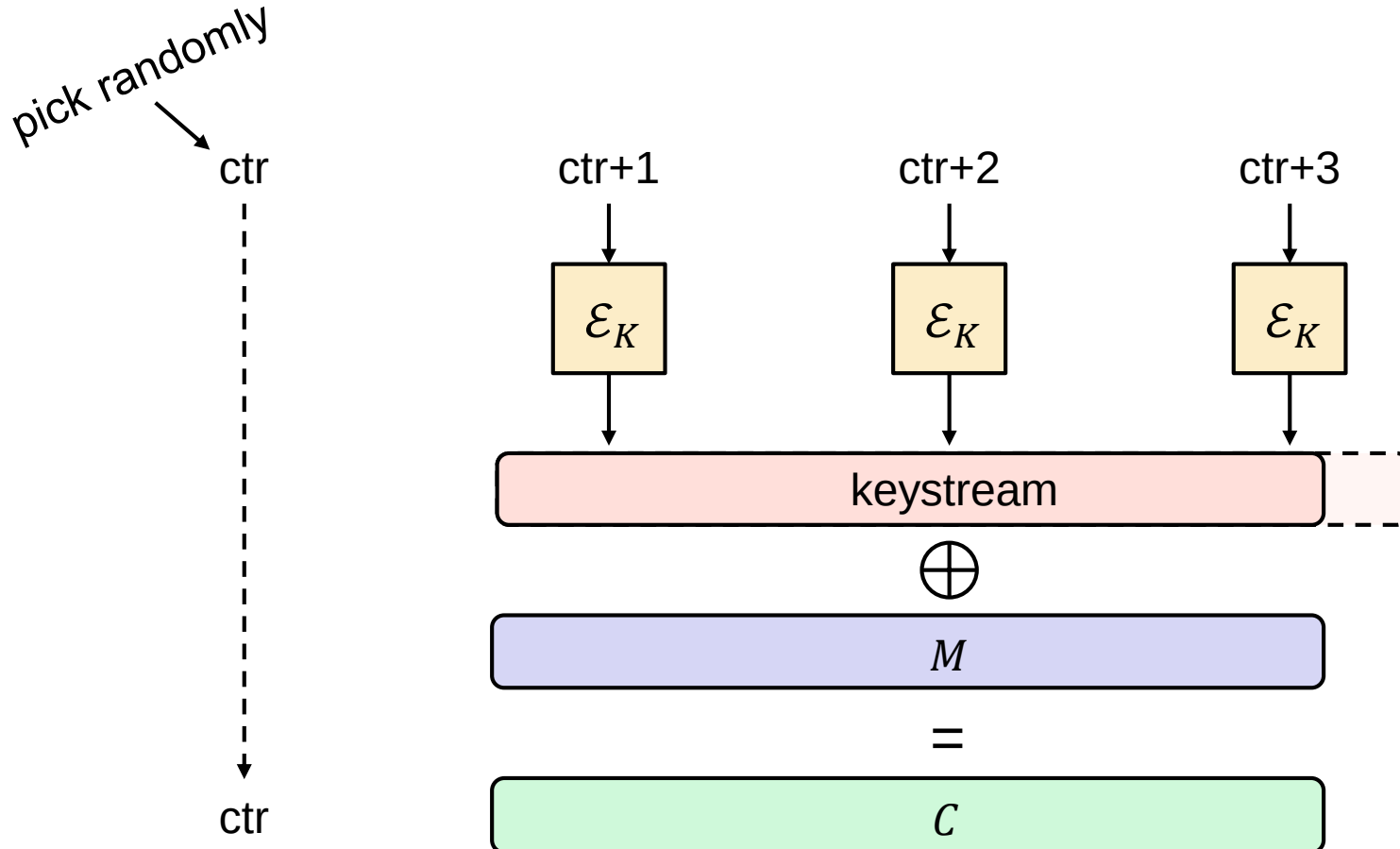
CTR\$ mode

pick randomly
↓
ctr

ctr

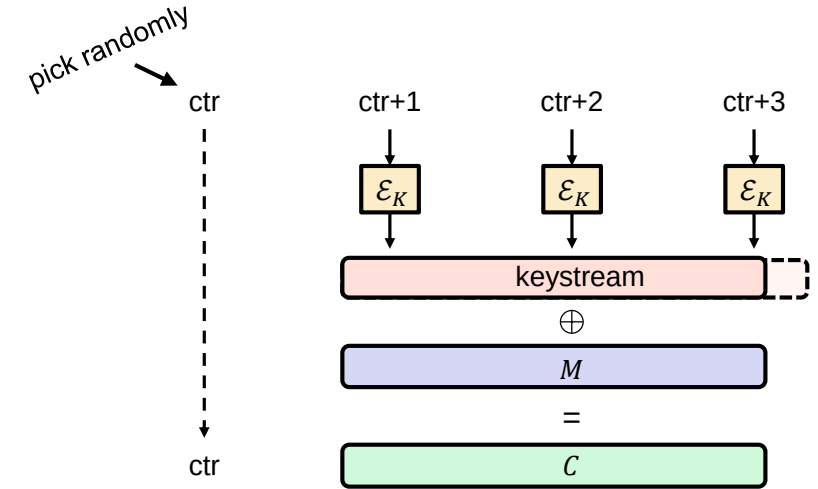


CTR\$ mode



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):

F is a secure PRF $\Rightarrow$ CTR\$ is IND-CPA secure.

Security of CTR\$

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

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

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 makes at most q queries (each of ℓ blocks), there is a PRF-adversary B such that

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

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

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

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

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

Example: AES-CTR\$

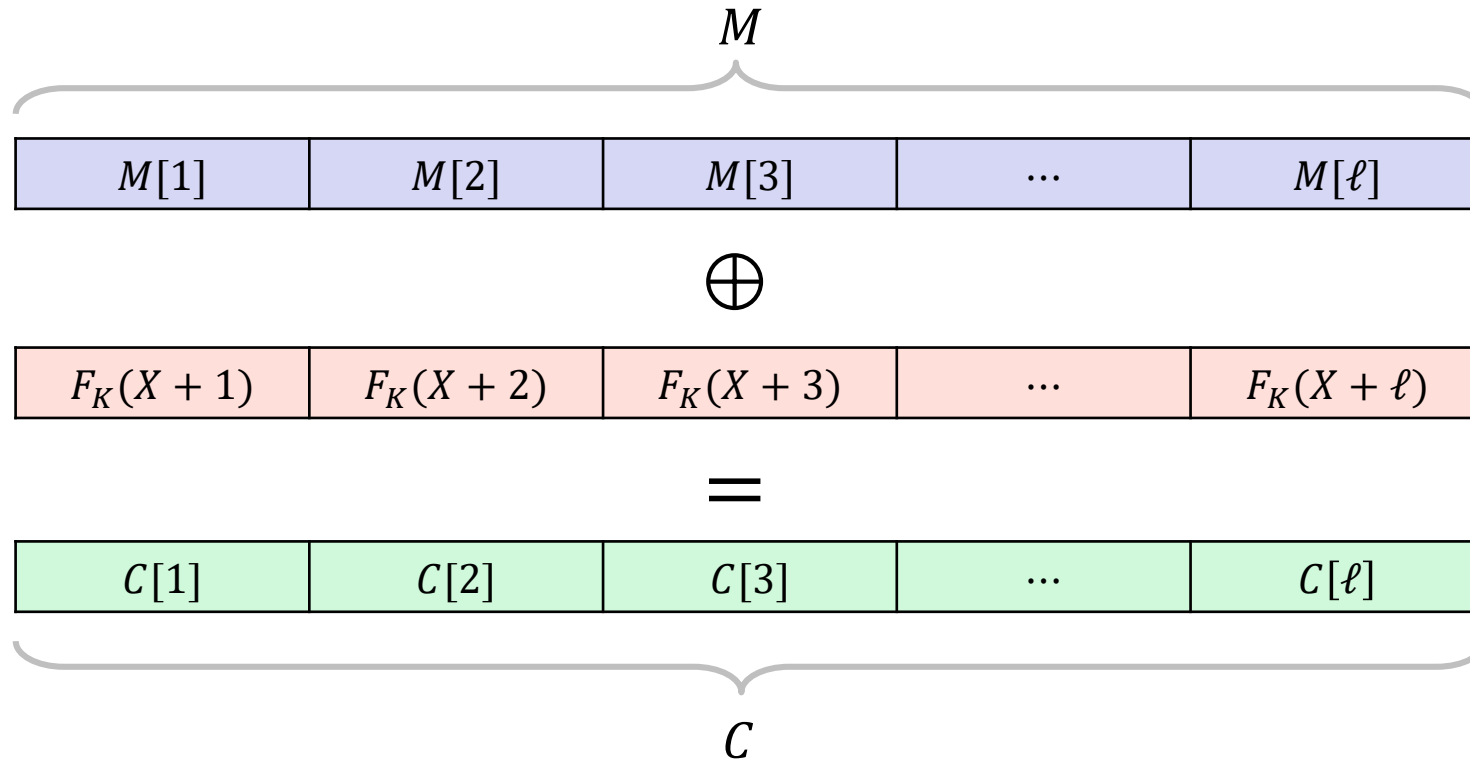
$$\left. \begin{array}{l} n = 128 \\ \ell = 2^6 \approx 1 \text{ kB} \\ q = 2^{40} \end{array} \right\} \approx 70 \text{ TB}$$

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

Security of CTR\$ – proof

Theorem: For any A ... there is B such that

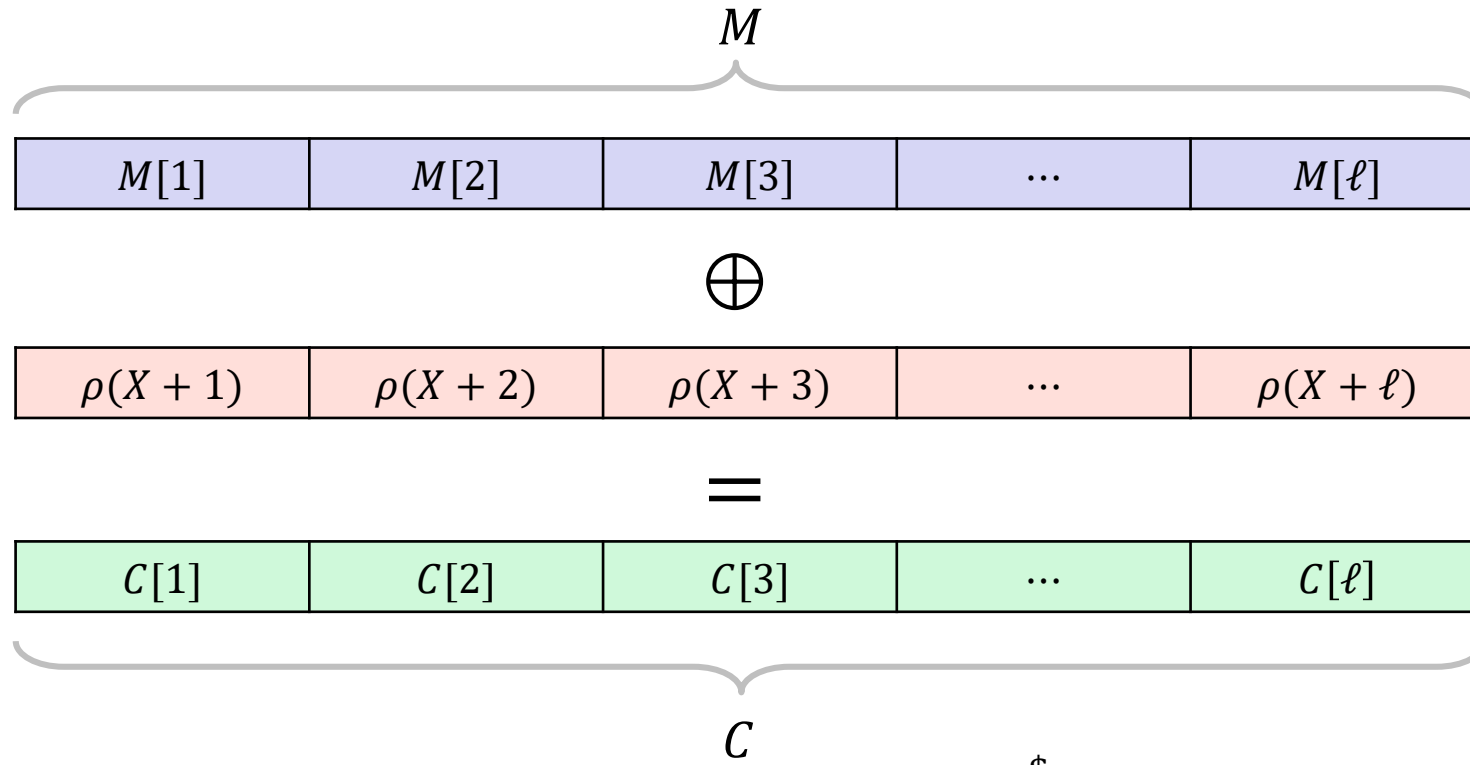
$$\mathbf{Adv}_{\text{CTR\$}}^{\text{ind-cpa}}(A) \leq \mathbf{Adv}_F^{\text{prf}}(B) + \frac{q^2 \ell}{2^n}$$



Security of CTR\$ – proof

Theorem: For any A ... there is B such that

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

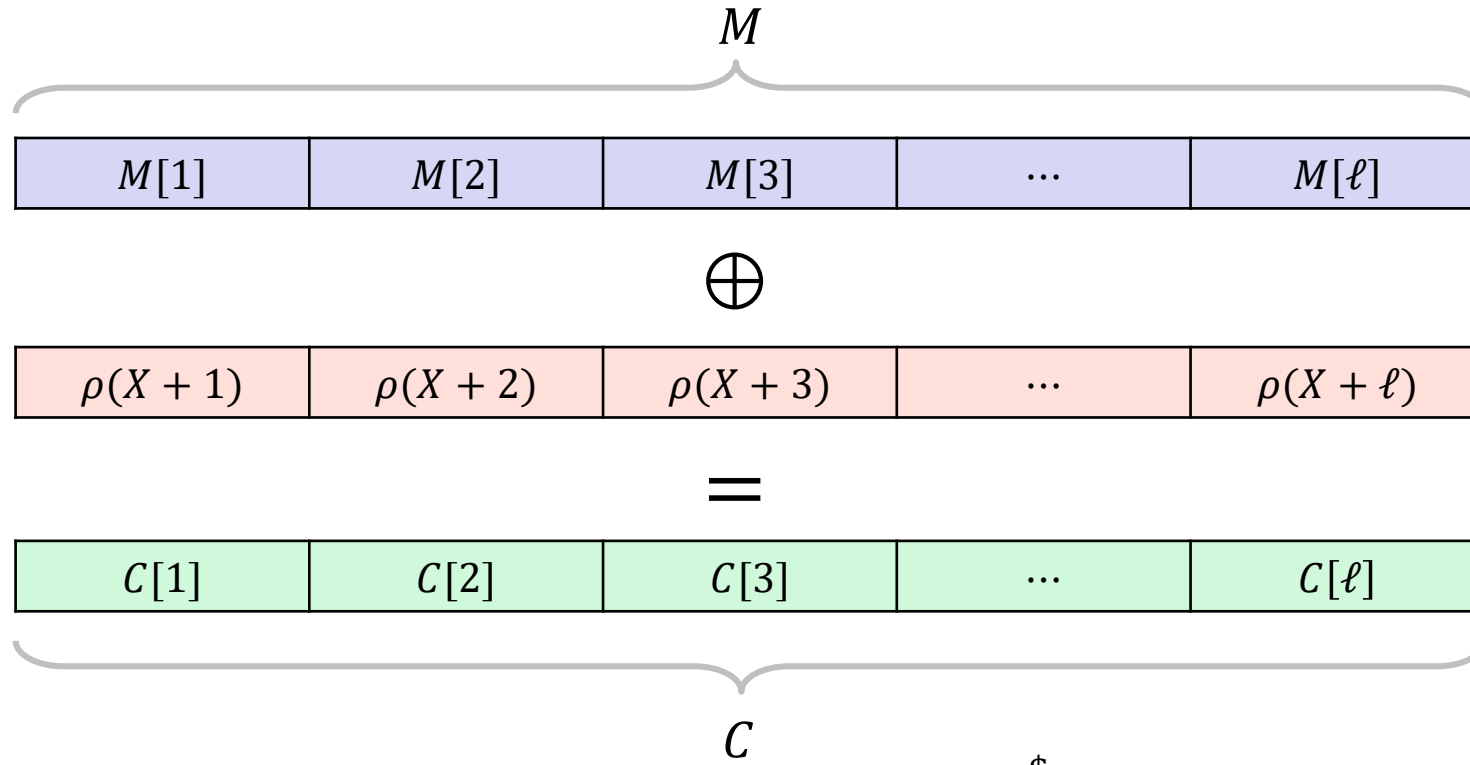


$\rho \stackrel{\$}{\leftarrow} \text{Func}[n, n] \approx F_K$ by PRF-security

Security of CTR\$ – proof

Theorem: For any A ... there is B such that

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



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

Security of CTR\$ – proof

$$0^{\ell n} \xrightarrow{\varepsilon(\cdot)} X_1 || C_1 : \quad X_1 \quad X_1 + 1 \quad \boxed{X_1 + 2} \quad \dots \quad X_1 + \ell$$

$$0^{\ell n} \xrightarrow{\varepsilon(\cdot)} X_2 || C_2 : \quad X_2 \quad X_2 + 1 \quad X_2 + 2 \quad \dots \quad X_2 + \ell$$

$$0^{\ell n} \xrightarrow{\varepsilon(\cdot)} X_q || C_q : \quad X_q \quad \boxed{X_q + 1} \quad X_q + 2 \quad \dots \quad X_q + \ell$$

$$\oplus$$

$$\text{OTP} \rightarrow \begin{array}{|c|c|c|c|c|} \hline \rho(X+1) & \rho(X+2) & \rho(X+3) & \dots & \rho(X+\ell) \\ \hline \end{array}$$

Event Coll:

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

$$\Rightarrow \quad C_i[j] = C_{i'}[j'] = (\tilde{K} \oplus 0^n)$$

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

$$\dots \quad M[\ell]$$

$$\dots \quad C[\ell]$$

Func[n, n] $\approx F_K$ by PRF-security

Security of CTR\$ – proof



$$\begin{aligned}\Pr[\text{Coll}] &= \Pr[\text{Coll}_1 \vee \text{Coll}_2 \vee \dots \vee \text{Coll}_q] \\ &\leq \Pr[\text{Coll}_1] + \Pr[\text{Coll}_2] + \dots + \Pr[\text{Coll}_q] \\ &\leq 0\end{aligned}$$

Security of CTR\$ – proof



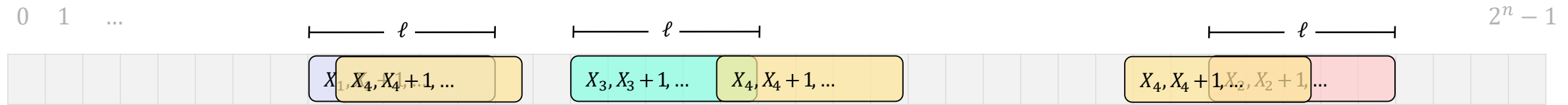
$$\begin{aligned}
 \Pr[\text{Coll}] &= \Pr[\text{Coll}_1 \vee \text{Coll}_2 \vee \dots \vee \text{Coll}_q] \\
 &\leq \Pr[\text{Coll}_1] + \Pr[\text{Coll}_2] + \dots + \Pr[\text{Coll}_q] \\
 &\leq 0 + \frac{2\ell}{2^n}
 \end{aligned}$$

Security of CTR\$ – proof



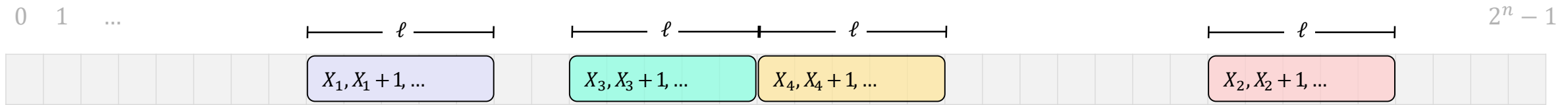
$$\begin{aligned}
 \Pr[\text{Coll}] &= \Pr[\text{Coll}_1 \vee \text{Coll}_2 \vee \dots \vee \text{Coll}_q] \\
 &\leq \Pr[\text{Coll}_1] + \Pr[\text{Coll}_2] + \dots + \Pr[\text{Coll}_q] \\
 &\leq 0 + \frac{2\ell}{2^n} + \frac{2 \cdot 2\ell}{2^n}
 \end{aligned}$$

Security of CTR\$ – proof



$$\begin{aligned}
 \Pr[\text{Coll}] &= \Pr[\text{Coll}_1 \vee \text{Coll}_2 \vee \dots \vee \text{Coll}_q] \\
 &\leq \Pr[\text{Coll}_1] + \Pr[\text{Coll}_2] + \dots + \Pr[\text{Coll}_q] \\
 &\leq 0 + \frac{2\ell}{2^n} + \frac{2 \cdot 2\ell}{2^n} + \frac{3 \cdot 2\ell}{2^n}
 \end{aligned}$$

Security of CTR\$ – proof



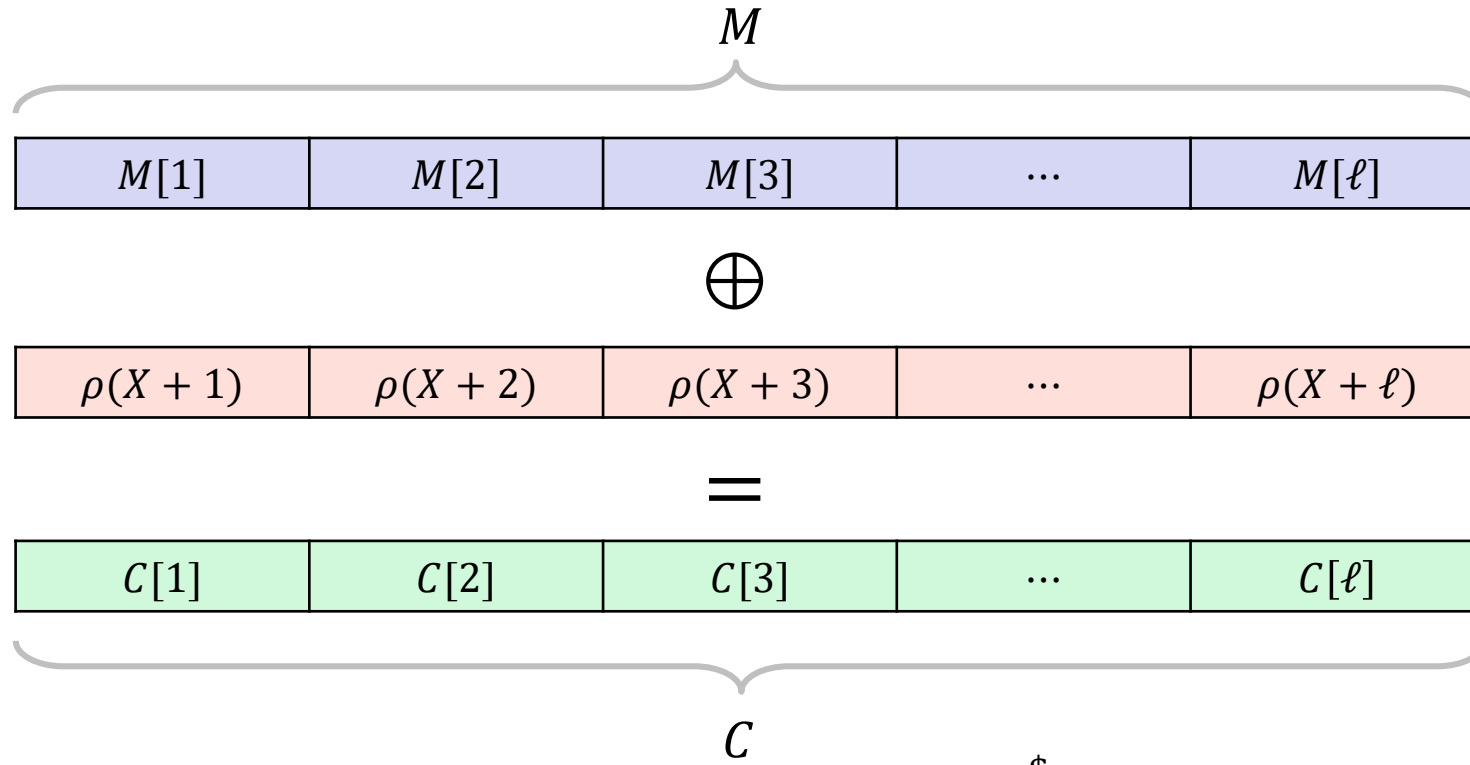
$$\begin{aligned}
 \Pr[\text{Coll}] &= \Pr[\text{Coll}_1 \vee \text{Coll}_2 \vee \dots \vee \text{Coll}_q] \\
 &\leq \Pr[\text{Coll}_1] + \Pr[\text{Coll}_2] + \dots + \Pr[\text{Coll}_q] \\
 &\leq 0 + \frac{2\ell}{2^n} + \frac{2 \cdot 2\ell}{2^n} + \frac{3 \cdot 2\ell}{2^n} + \dots + \frac{(q-1) \cdot 2\ell}{2^n} \\
 &= \frac{2\ell}{2^n} \cdot (1 + 2 + 3 + \dots + (q-1)) \\
 &\leq \frac{q^2 \ell}{2^n}
 \end{aligned}$$

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

Security of CTR\$ – proof

Theorem: For any A ... there is B such that

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



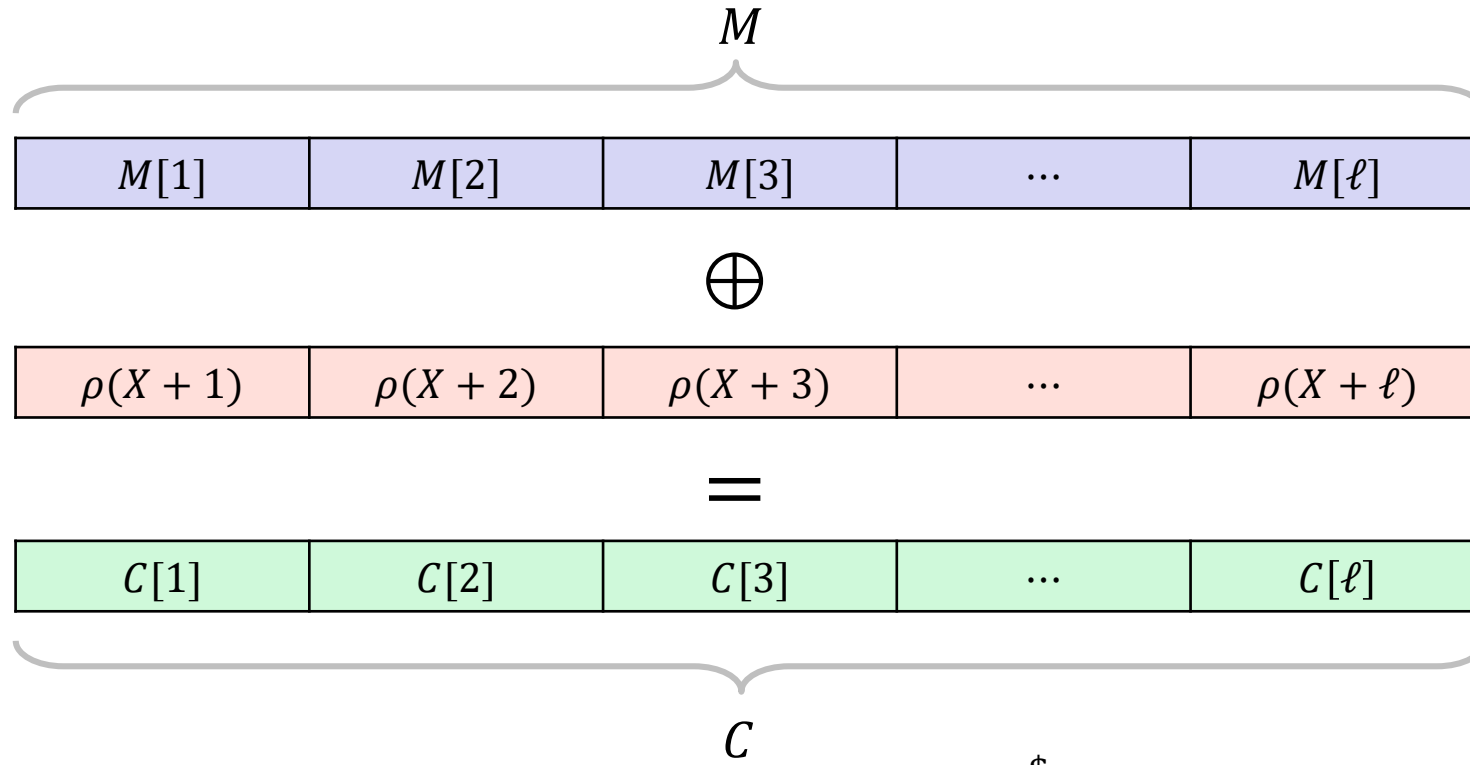
$$\Pr[\text{Coll}] < \frac{q^2 \ell}{2^n}$$

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

Security of CTR\$ – proof

Theorem: For any A ... there is B such that

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



$$\Pr[\text{Coll}] < \frac{q^2 \ell}{2^n}$$

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

Nonce-based encryption

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

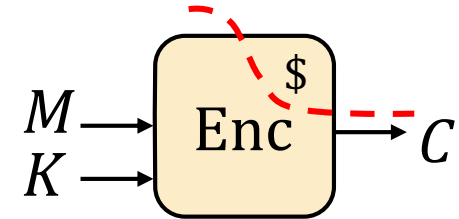
$$\text{Enc}(K, M) = \text{Enc}_K(M)$$

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

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

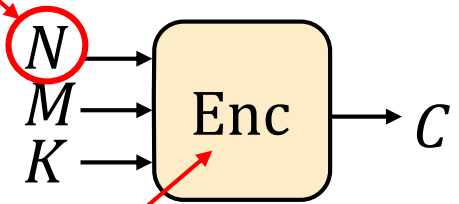
How to create the nonce?

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



Randomized

"number used once" = Nonce



Nonce-based

Deterministic

CTR\$ vs. (nonce-based) CTR

Probabilistic

CTR\$. Enc(K, M)

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

vs.

Nonce-based

CTR. Enc(K, N, M)

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

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

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

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

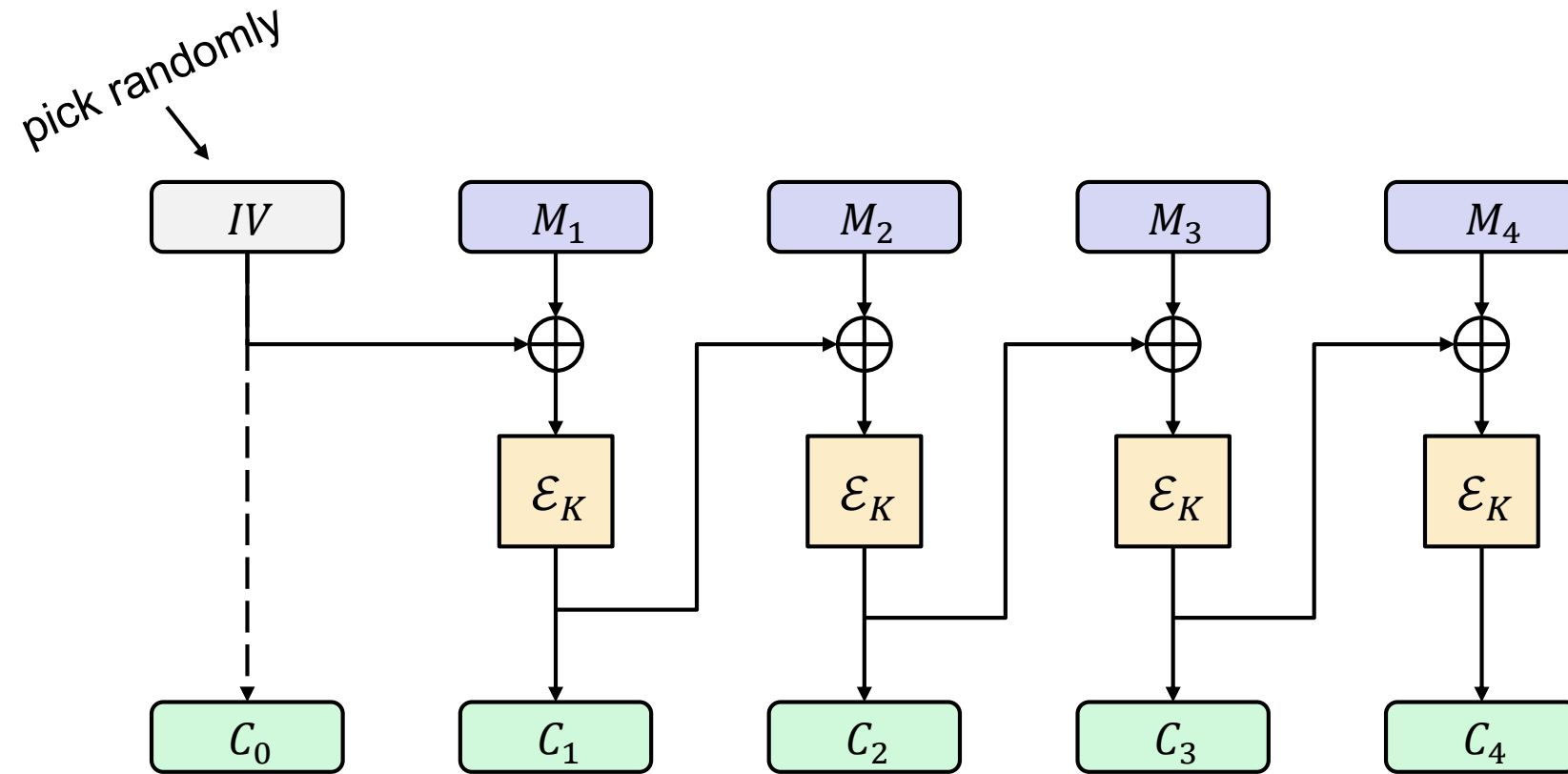
VS.

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

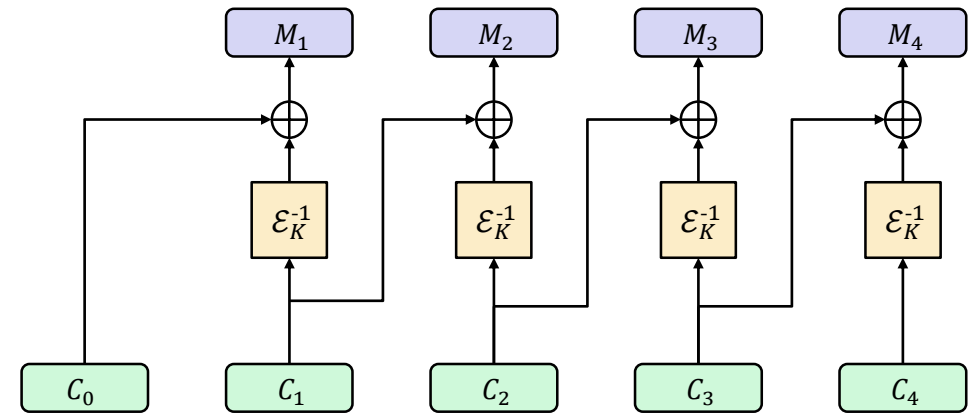
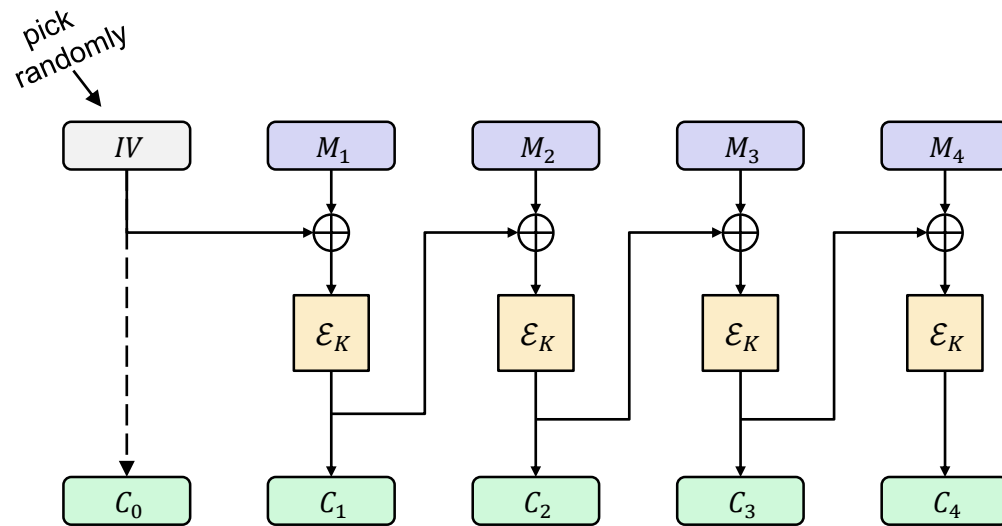
$$\mathbf{Adv}_{\text{CTR}}^{\text{ind-cpa}}(A) \leq \mathbf{Adv}_F^{\text{prf}}(B)$$

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

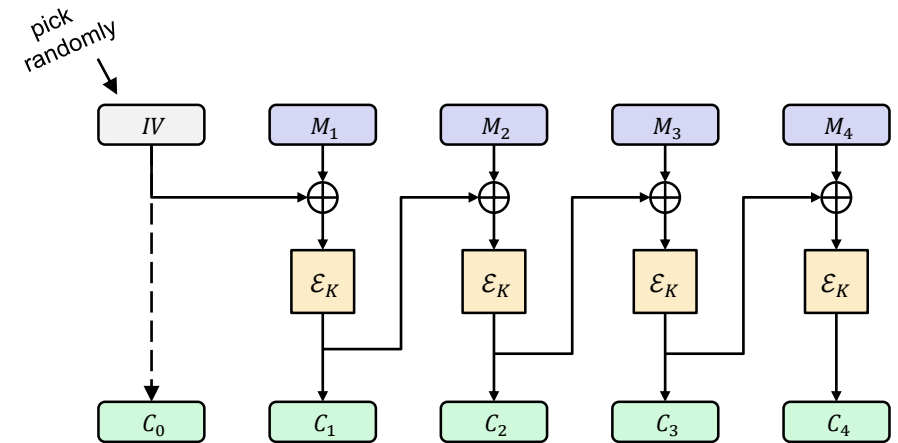


CBC\$ – Cipher Block Chaining mode

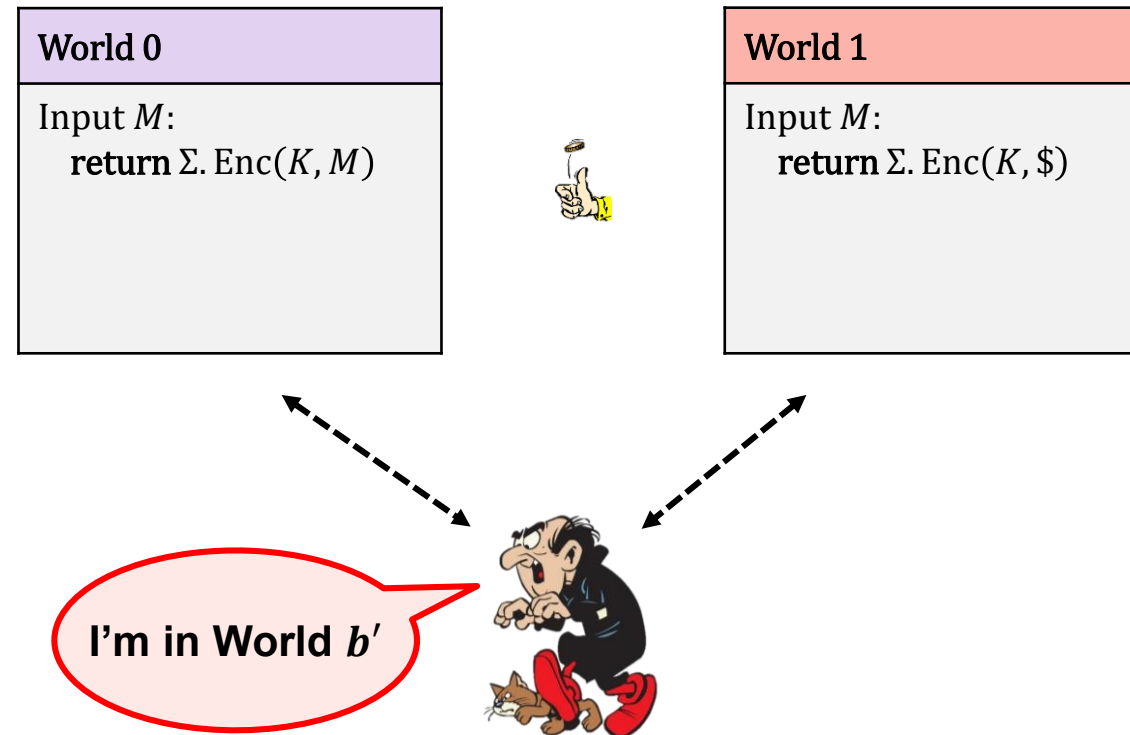


CBC

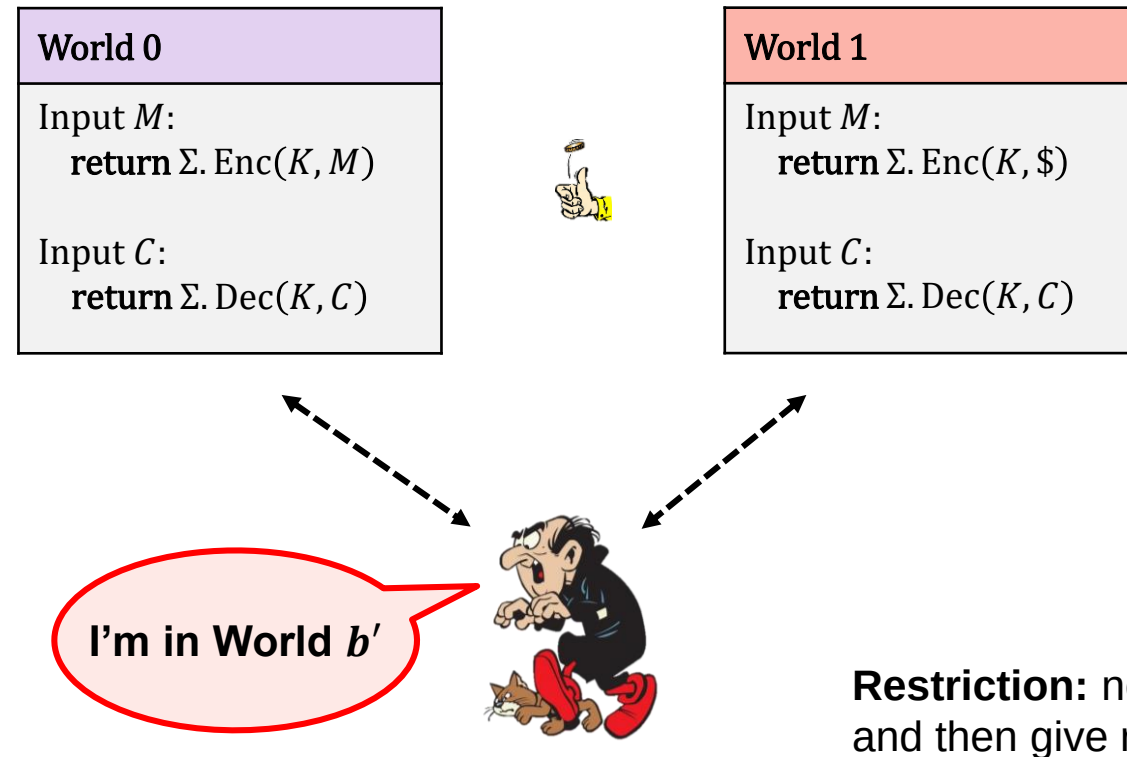
- **Theorem:** IND-CPA secure for *random* IV (assuming $\mathcal{E}$ is a good block cipher)
- Not IND-CPA secure for nonce-based IV
 - (exercise: show this)
- Not parallelizable; cannot precompute values
- Inverse of block cipher needed for decryption
- Padding needed for messages not a multiple of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



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