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

TEK4500

07.09.2022

Håkon Jacobsen

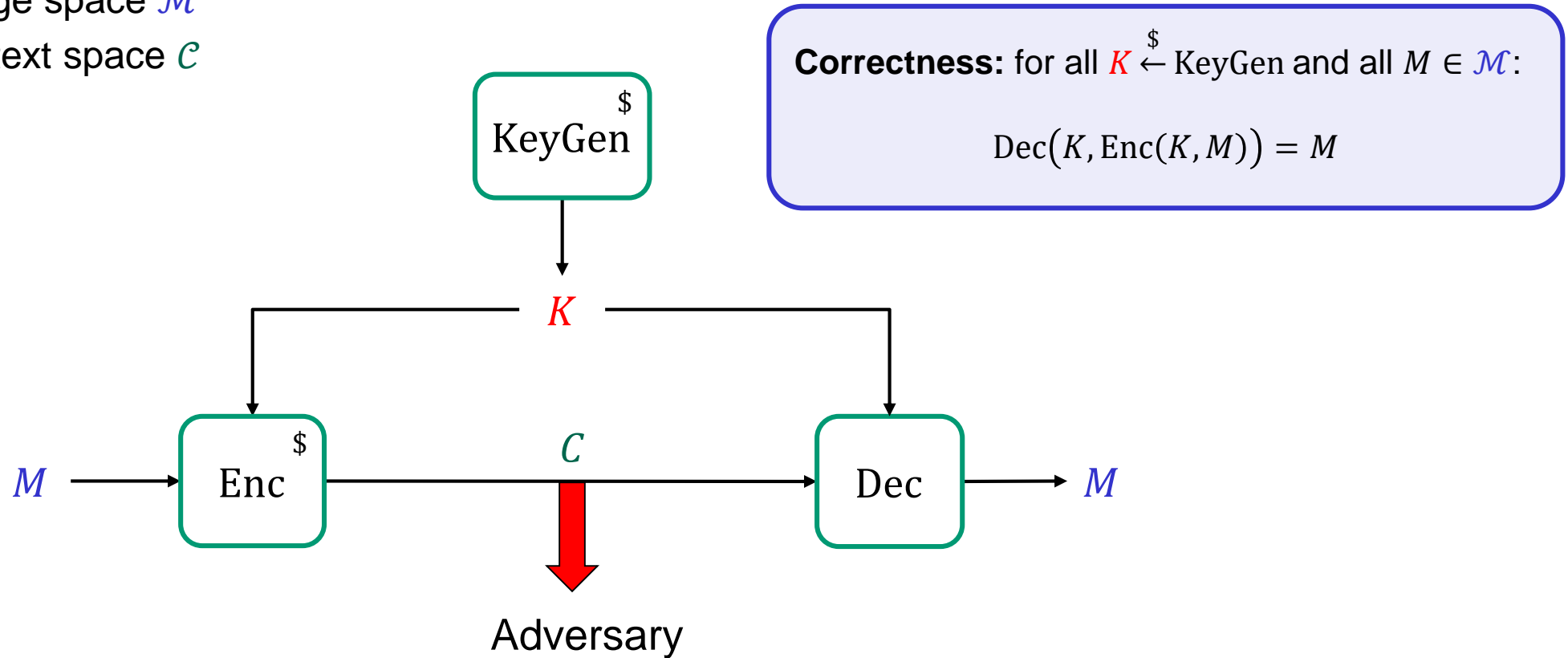
hakon.jacobsen@its.uio.no

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}



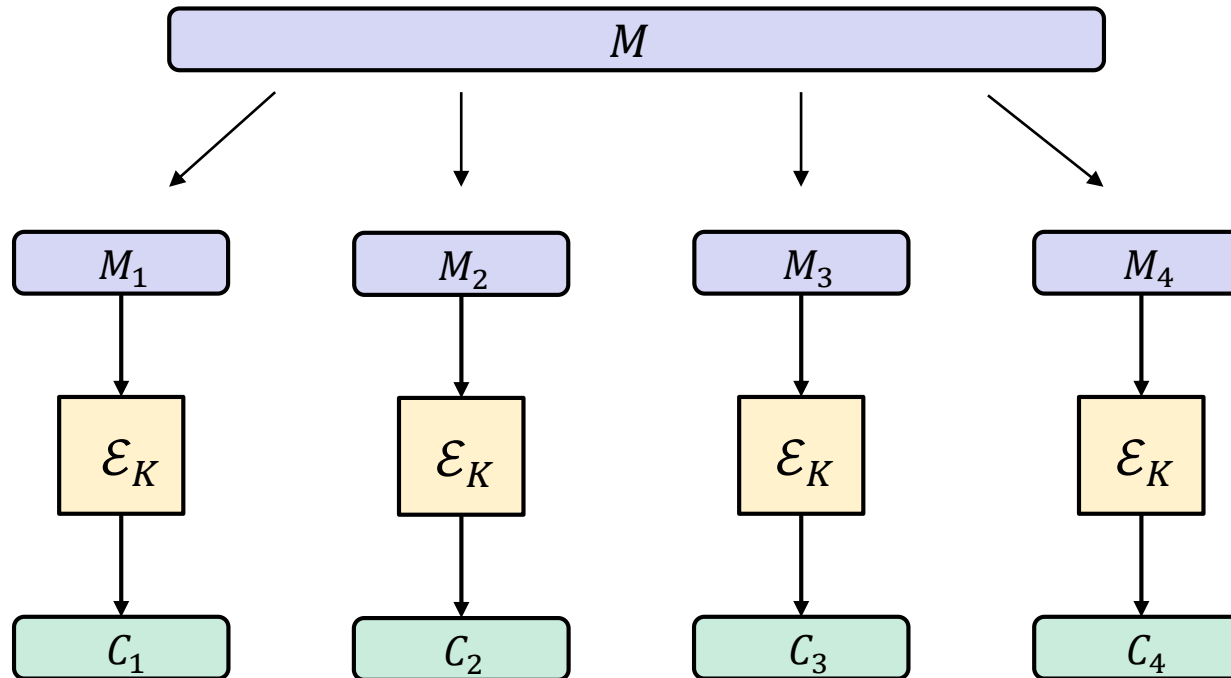
- KeyGen and Enc may be randomized (\$), but Dec must be deterministic

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:** ...

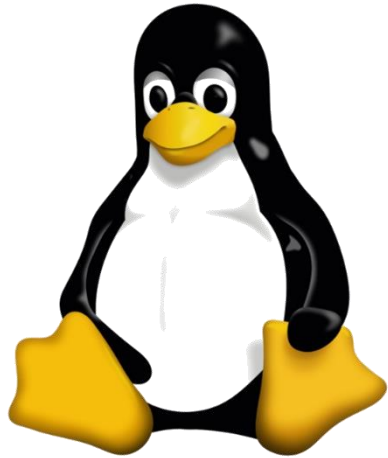
Electronic Code Book (ECB) mode

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

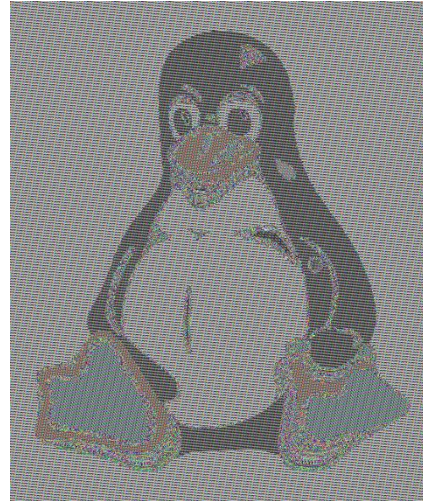


ECB problem

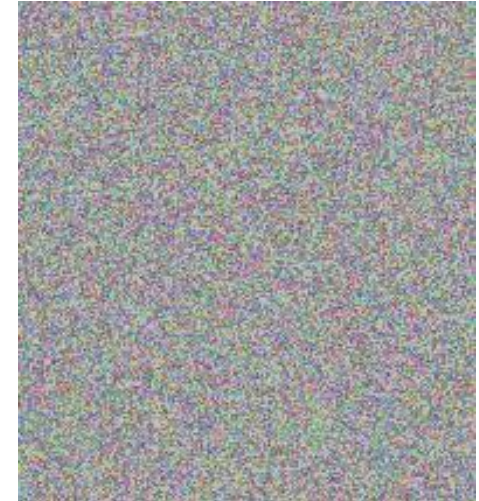
Plaintext



ECB encrypted



Properly encrypted



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

Perfect privacy

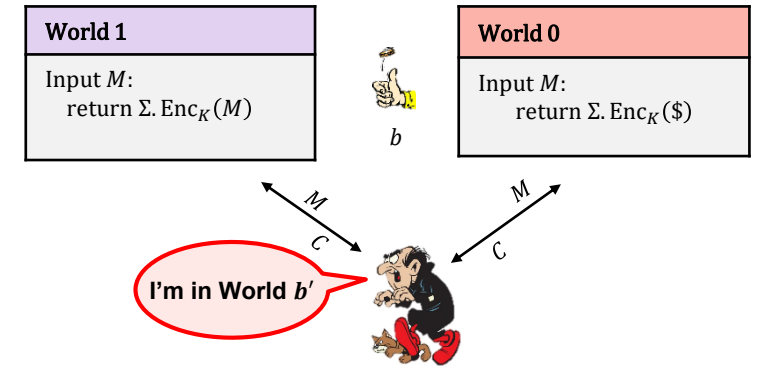
computational

- ~~One-time perfect privacy:~~

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

resource bounded

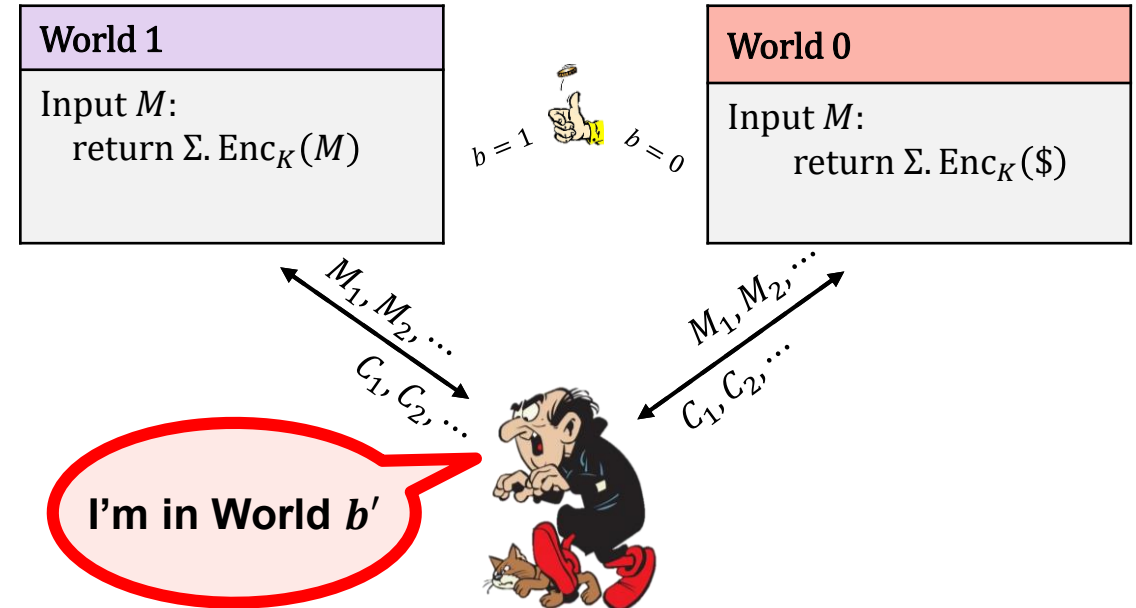
- Security holds for *any* adversary (~~no limit on resource usage~~)
- Very strict requirements:
 - ~~Keys need to be as long as message~~...want keys to be short ✓
 - ~~Key can only be used for one message~~...want to encrypt many messages ✓



IND-CPA – indistinguishability against chosen-plaintext attacks

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

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



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

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

IND-CPA – indistinguishability against chosen-plaintext attacks

Exp_Σ^{ind-cpa}(A)

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

$\mathcal{E}(M)$

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

- 3.
4. **return** c_p

World 1

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



World 0

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

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

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

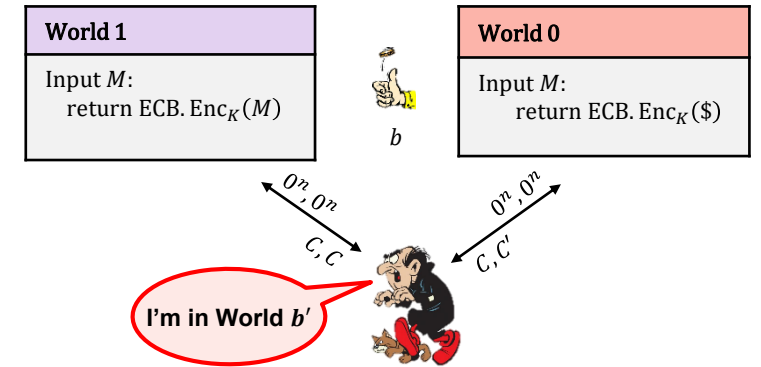
Definition: The **IND-CPA advantage** of an adversary A is

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

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 1
4. else, output 0

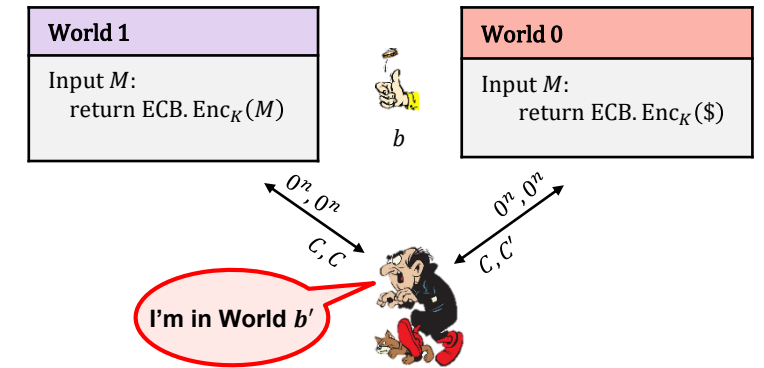


$$\begin{aligned}
 \Pr[\mathbf{Exp}_{\text{ECB}}^{\text{ind-cpa}}(A) \Rightarrow \text{true}] &= \Pr[b' = b] \\
 &= \Pr[b' = 1 \mid b = 1] \cdot 1/2 + \Pr[b' = 0 \mid b = 0] \cdot 1/2 \\
 &= \Pr[C = C' \mid b = 1] \cdot 1/2 + (1 - \Pr[b' = 1 \mid b = 0]) \cdot 1/2 \\
 &= 1/2 + (1 - \Pr[C = C' \mid b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

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 1
4.	else, output 0

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



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

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, \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

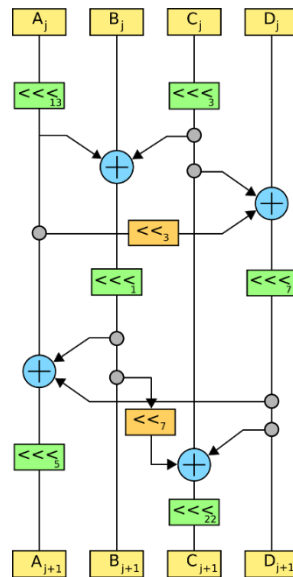
- The conceptually "right" definition
- High level idea: an encryption scheme is **semantically secure** if by observing a ciphertext C the adversary learns *nothing* about the plaintext (except its length)
- Harder to formalize; IND-CPA easier to work with

Theorem: (Goldwasser & Micali '83)

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

Length-leaking attacks

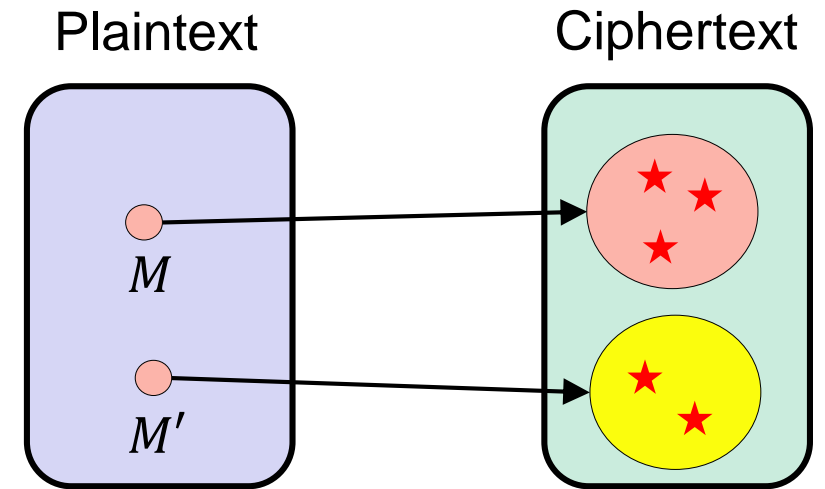
- Wikipedia pages
 - Each page has a unique size
- Google maps
 - World regions have unique "fingerprints" based on length of data (based on map tiles)
- Variable-bitrate encoding
 - Can e.g., fingerprint movies streamed over Netflix
- To combat length-leaking attacks: message padding
 - Can be expensive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



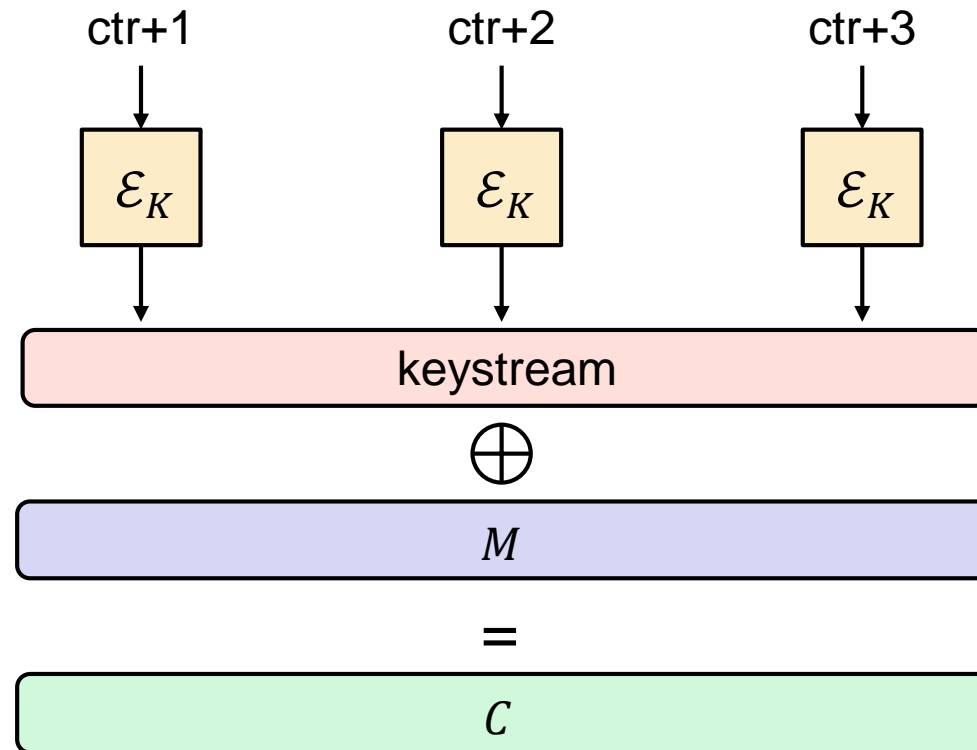
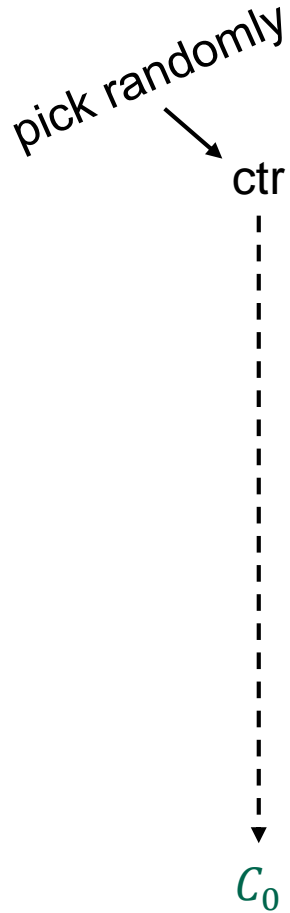
Constructing symmetric encryption schemes

How to achieve non-deterministic encryption?

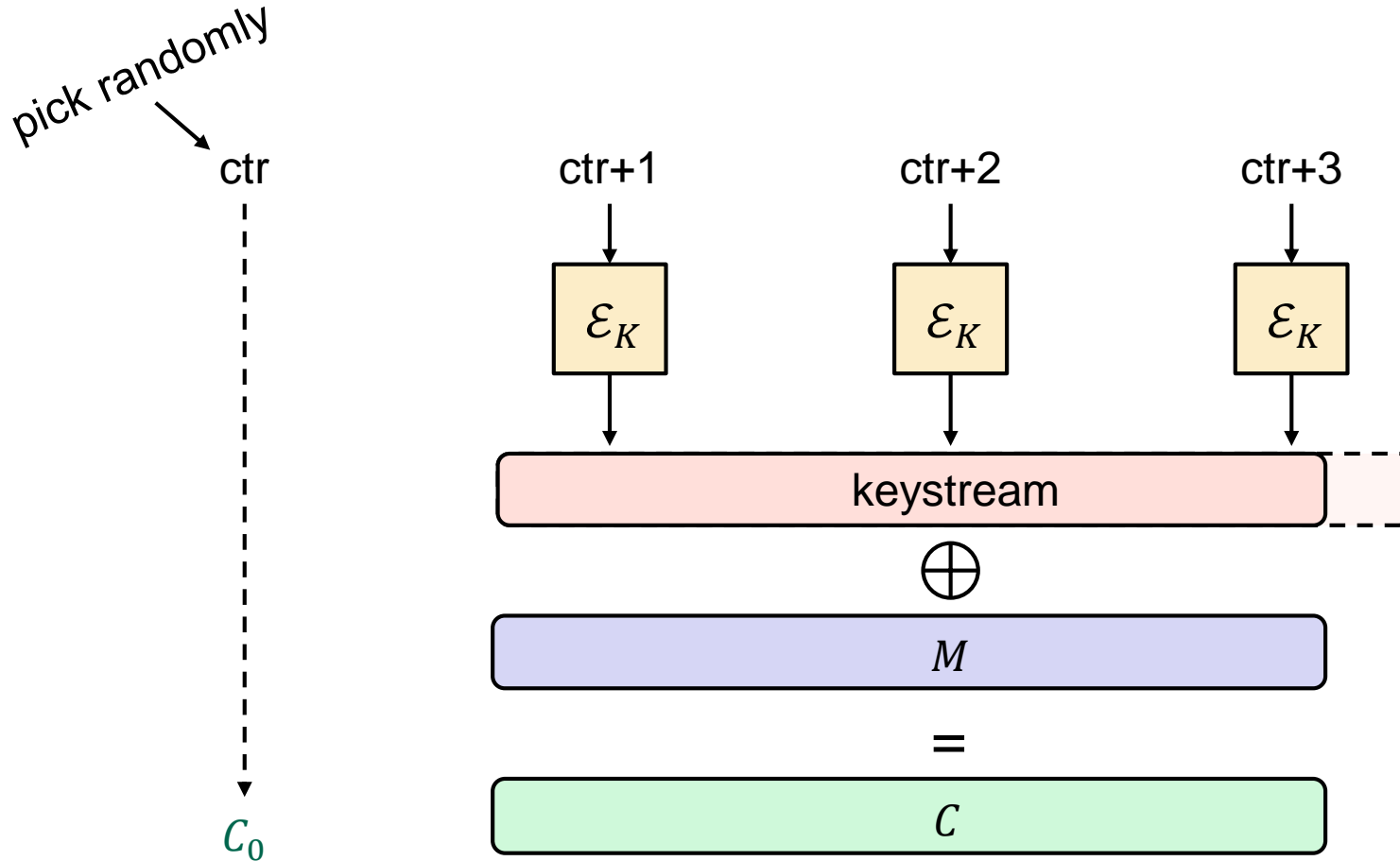
- Randomized encryption
 - Coins flipped internally by the algorithm
- Nonce-based encryption
 - Encryption scheme itself is deterministic
 - Non-determinism injected from the outside



CTR\$ mode

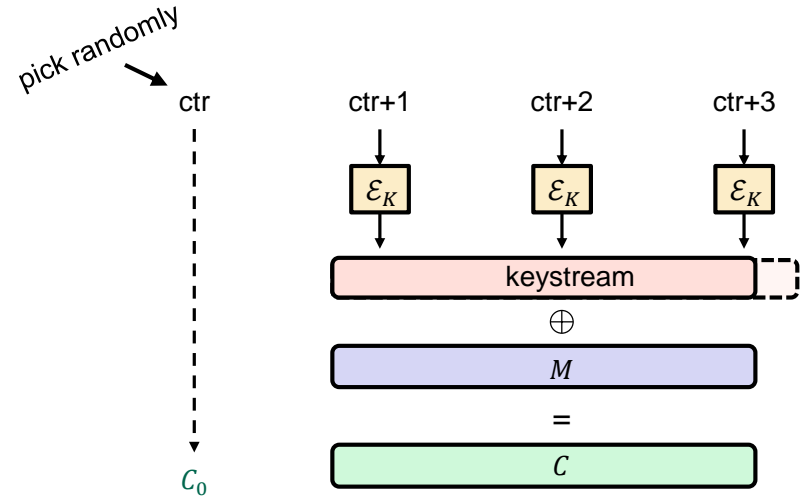


CTR\$ mode



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\$

Logic 101

$$A \Rightarrow B$$

is equivalent to:

$$\bar{A} \Leftarrow \bar{B}$$

Theorem (idea):

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

\Leftrightarrow equivalent!

Theorem (idea):

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

Security of CTR\$

Theorem (idea):

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

Proof idea:

- CTR\$[F] not IND-CPA secure \Rightarrow there exists adversary A with good advantage $\mathbf{Adv}_{\text{CTR}\$[F]}^{\text{ind-cpa}}(A)$
- Can use A to create a *new* adversary B that has good advantage $\mathbf{Adv}_F^{\text{prf}}(B)$ against F
 $\Rightarrow F$ is not a secure PRF!

Security of CTR\$

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

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

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

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

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

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

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

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

Example: $\text{CTR}\$[\text{AES}]$

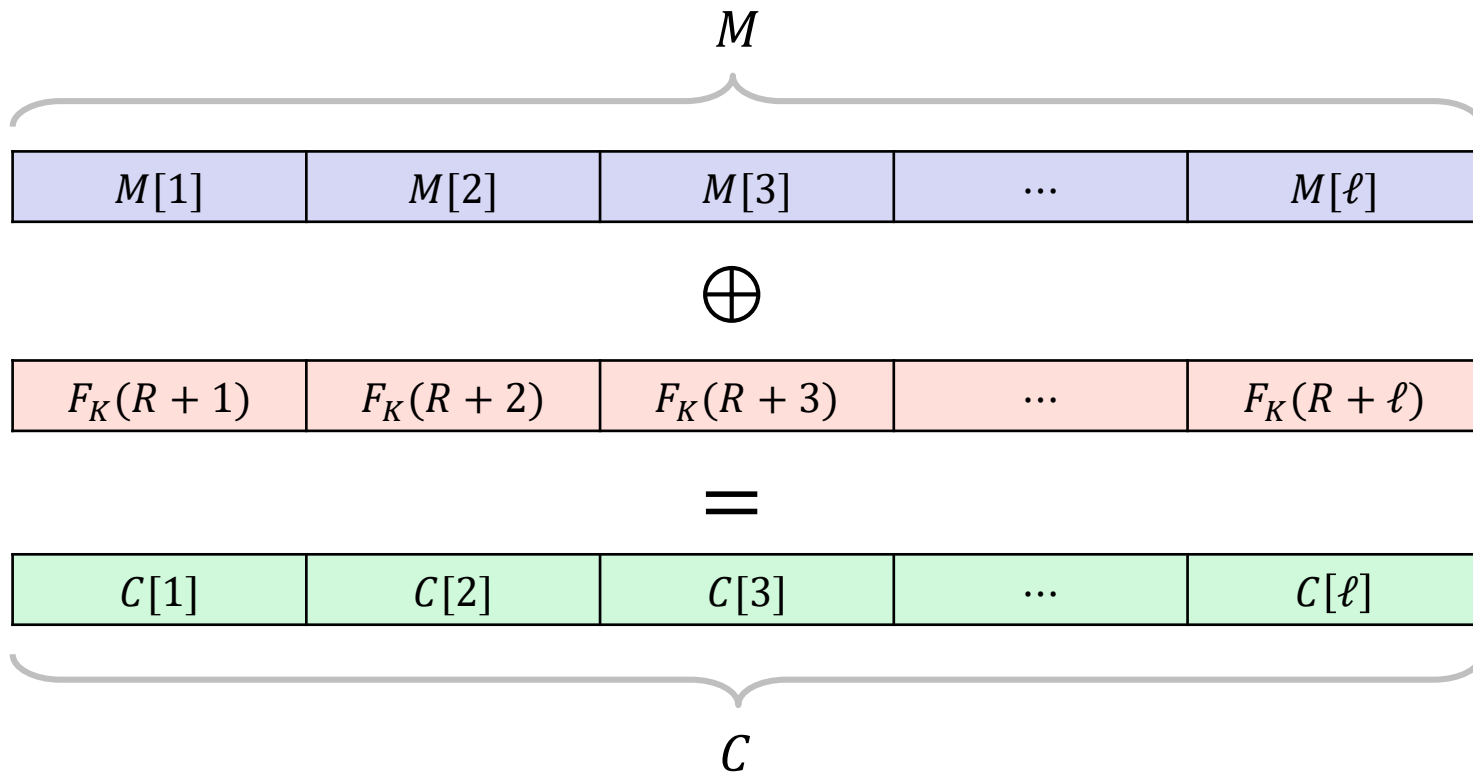
$$\left. \begin{array}{l} n = 128 \\ \ell = 2^6 \approx 1 \text{ kB} \\ q = 2^{40} \end{array} \right\} \approx 70 \text{ TB}$$

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

Security of CTR\$ – proof idea

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

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



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

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

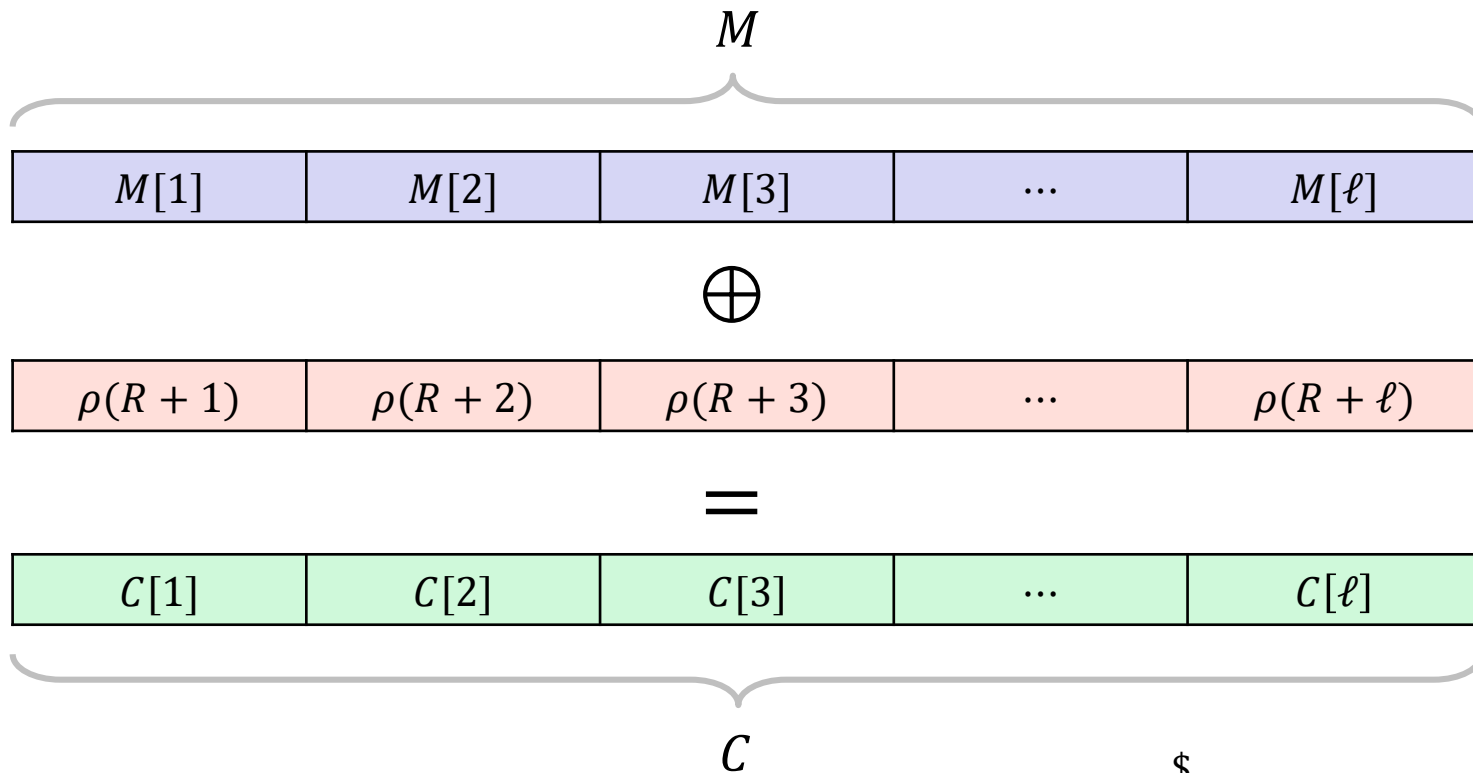
$\mathcal{E}(M)$

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

Security of CTR\$ – proof idea

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

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



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

Exp_{CTR\$}^{ind-cpa}(A)

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

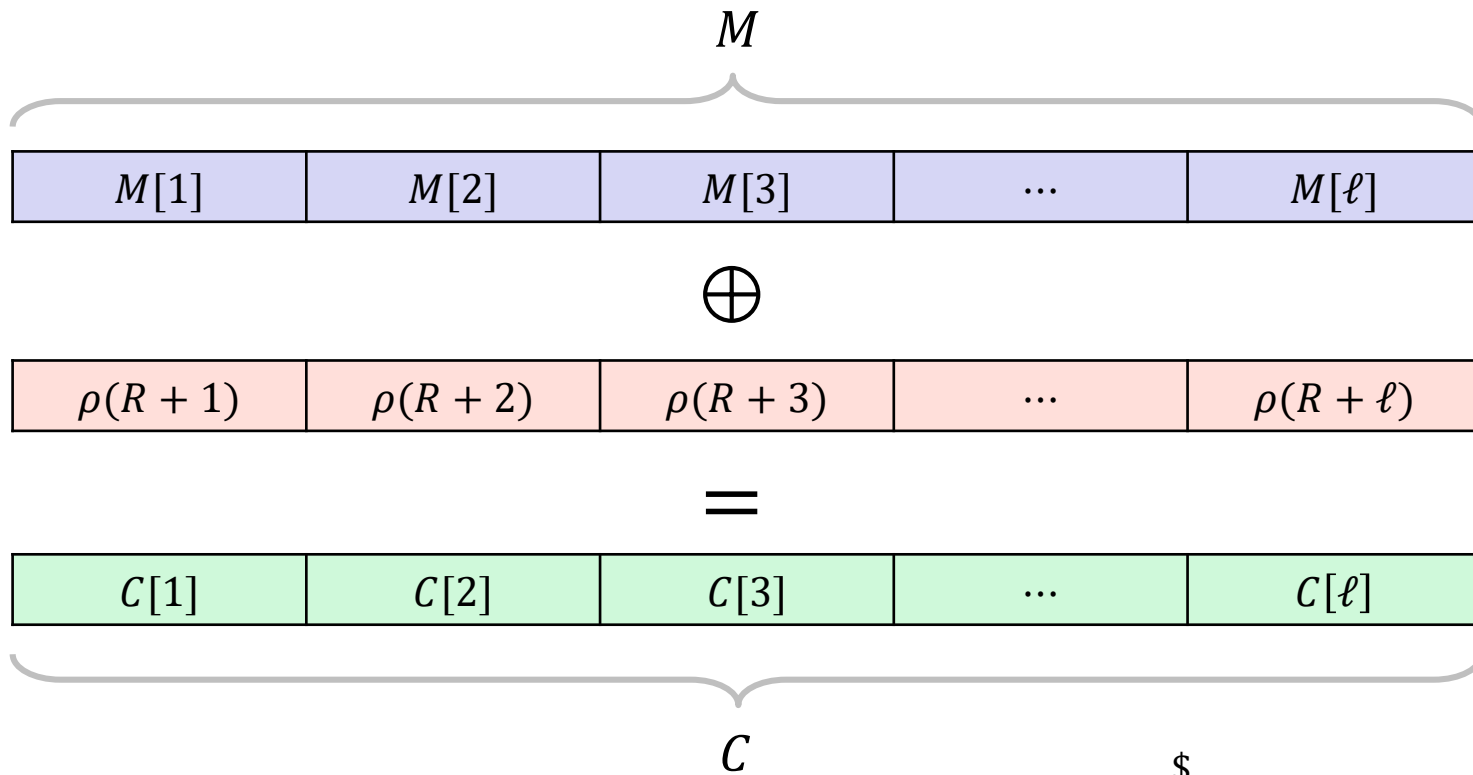
$\mathcal{E}(M)$

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

Security of CTR\$ – proof idea

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

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



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

Exp_{CTR\$}^{ind-cpa}(A)

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

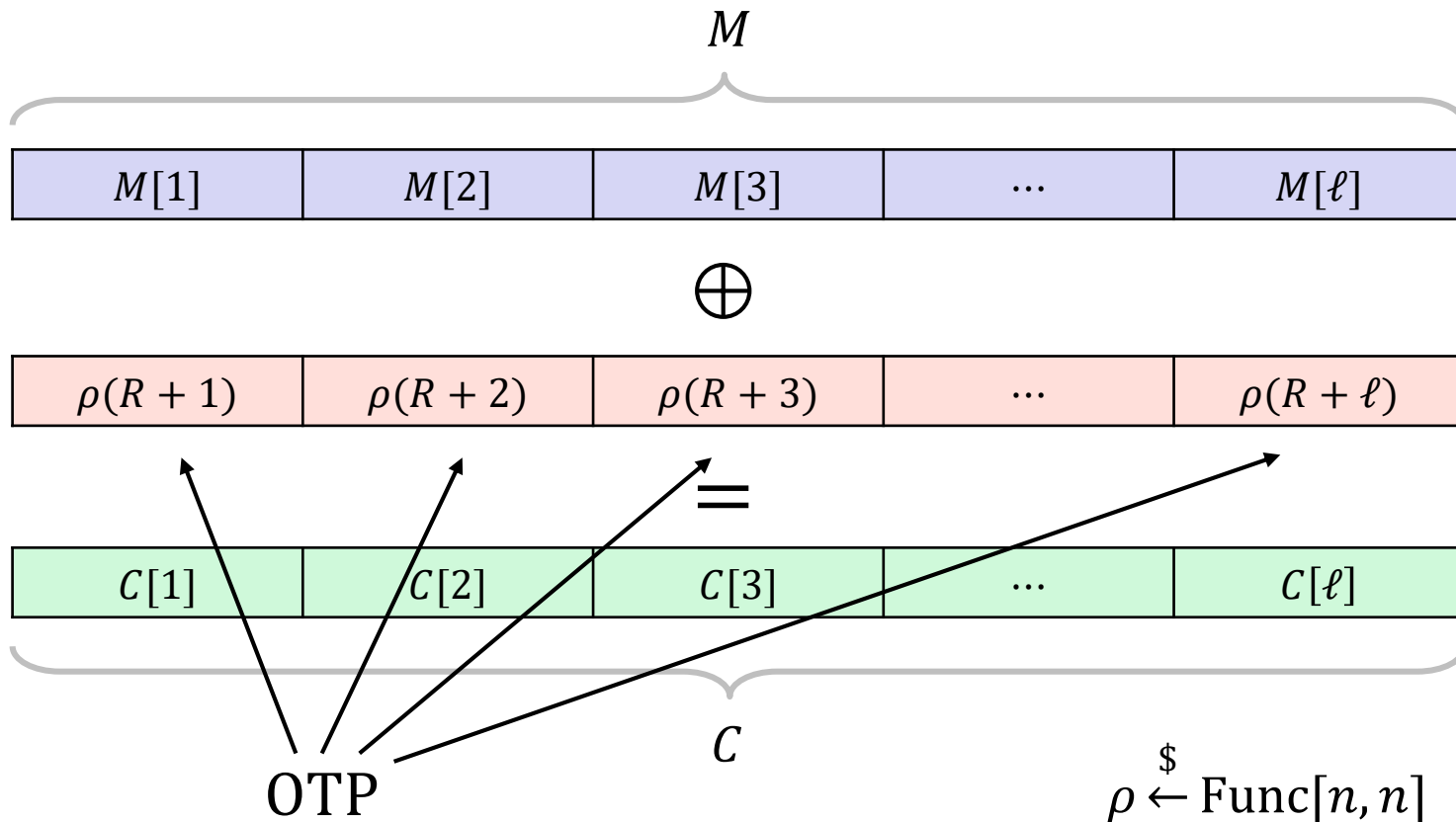
$\mathcal{E}(M)$

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

Security of CTR\$ – proof idea

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

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



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

Exp_{CTR\$}^{ind-cpa}(A)

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

$\mathcal{E}(M)$

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

Security of CTR\$ – proof idea

Theorem

$$\begin{array}{l}
 M_1 \xrightarrow{\mathcal{E}(\cdot)} R_1 || C_1 : \quad R_1 \quad R_1 + 1 \quad \textcircled{R_1 + 2} \quad \dots \quad R_1 + \ell \\
 M_2 \xrightarrow{\mathcal{E}(\cdot)} R_2 || C_2 : \quad R_2 \quad R_2 + 1 \quad R_2 + 2 \quad \dots \quad R_2 + \ell \\
 \vdots \\
 M_q \xrightarrow{\mathcal{E}(\cdot)} R_q || C_q : \quad R_q \quad \textcircled{R_q + 1} \quad R_q + 2 \quad \dots \quad R_q + \ell
 \end{array}$$

$\rho(R + 1)$	$\rho(R + 2)$	$\rho(R + 3)$	\dots	$\rho(R + \ell)$
---------------	---------------	---------------	---------	------------------

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

1. $b \xleftarrow{\$} \{0,1\}$
2. $K \xleftarrow{\$} \text{CTR\$}.\text{KeyGen}$
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:

$$R_i + j = R_{i'} + j' \Rightarrow \rho(R_i + j) = \rho(R_{i'} + j') = \tilde{K}$$

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

by PRF-security

Security of CTR\$ – proof idea



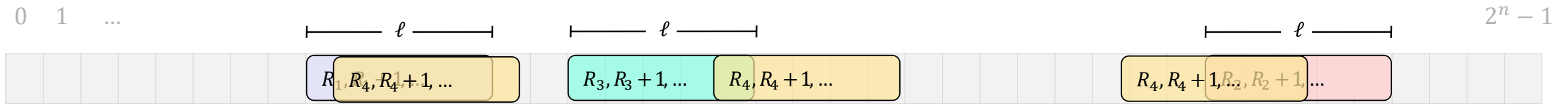
$$\begin{aligned}\Pr[\text{Coll}] &= \Pr[\text{Coll}_1 \vee \text{Coll}_2 \vee \dots \vee \text{Coll}_q] \\ &\leq \Pr[\text{Coll}_1] + \Pr[\text{Coll}_2] + \dots + \Pr[\text{Coll}_q] \\ &\leq 0 + \frac{2\ell}{2^n}\end{aligned}$$

Security of CTR\$ – proof idea



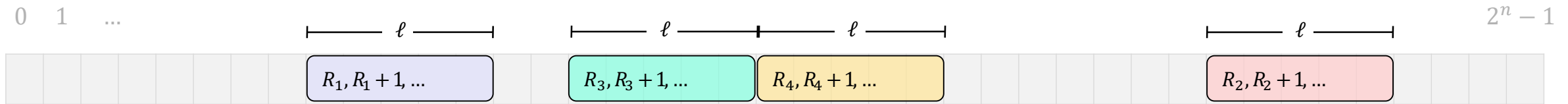
$$\begin{aligned}
 \Pr[\text{Coll}] &= \Pr[\text{Coll}_1 \vee \text{Coll}_2 \vee \dots \vee \text{Coll}_q] \\
 &\leq \Pr[\text{Coll}_1] + \Pr[\text{Coll}_2] + \dots + \Pr[\text{Coll}_q] \\
 &\leq 0 + \frac{2\ell}{2^n} + \frac{2 \cdot 2\ell}{2^n}
 \end{aligned}$$

Security of CTR\$ – proof idea



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

Security of CTR\$ – proof idea



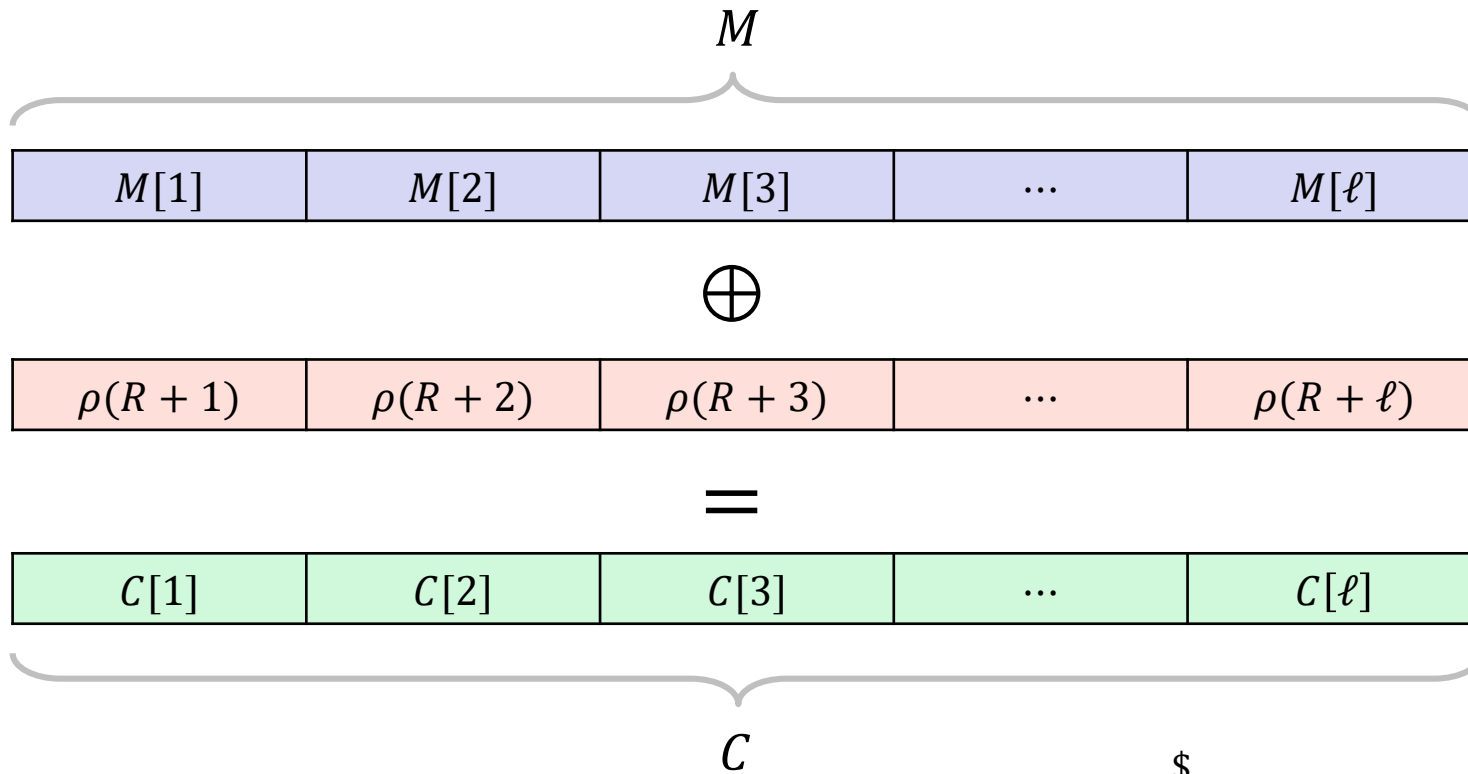
$$\begin{aligned}
 \Pr[\text{Coll}] &= \Pr[\text{Coll}_1 \vee \text{Coll}_2 \vee \dots \vee \text{Coll}_q] \\
 &\leq \Pr[\text{Coll}_1] + \Pr[\text{Coll}_2] + \dots + \Pr[\text{Coll}_q] \\
 &\leq 0 + \frac{2\ell}{2^n} + \frac{2 \cdot 2\ell}{2^n} + \frac{3 \cdot 2\ell}{2^n} + \dots + \frac{(q-1) \cdot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

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

Security of CTR\$ – proof idea

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

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



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

Exp_{CTR\$}^{ind-cpa}(A)

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

$\mathcal{E}(M)$

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

Nonce-based encryption

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

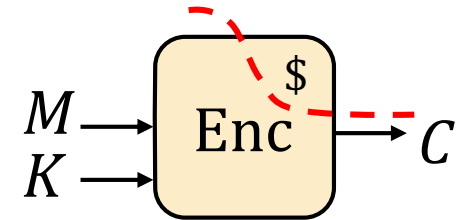
$$\text{Enc}(K, M) = \text{Enc}_K(M)$$

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

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

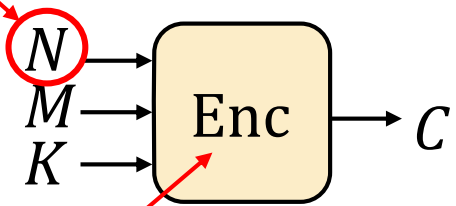
How to create the nonce?

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



Randomized

"number used once" = Nonce



Nonce-based

Deterministic

CTR\$ vs. (nonce-based) CTR

Probabilistic

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

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

VS.

Nonce-based

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

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

Nonce-based CTR – IND-CPA security

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

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

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

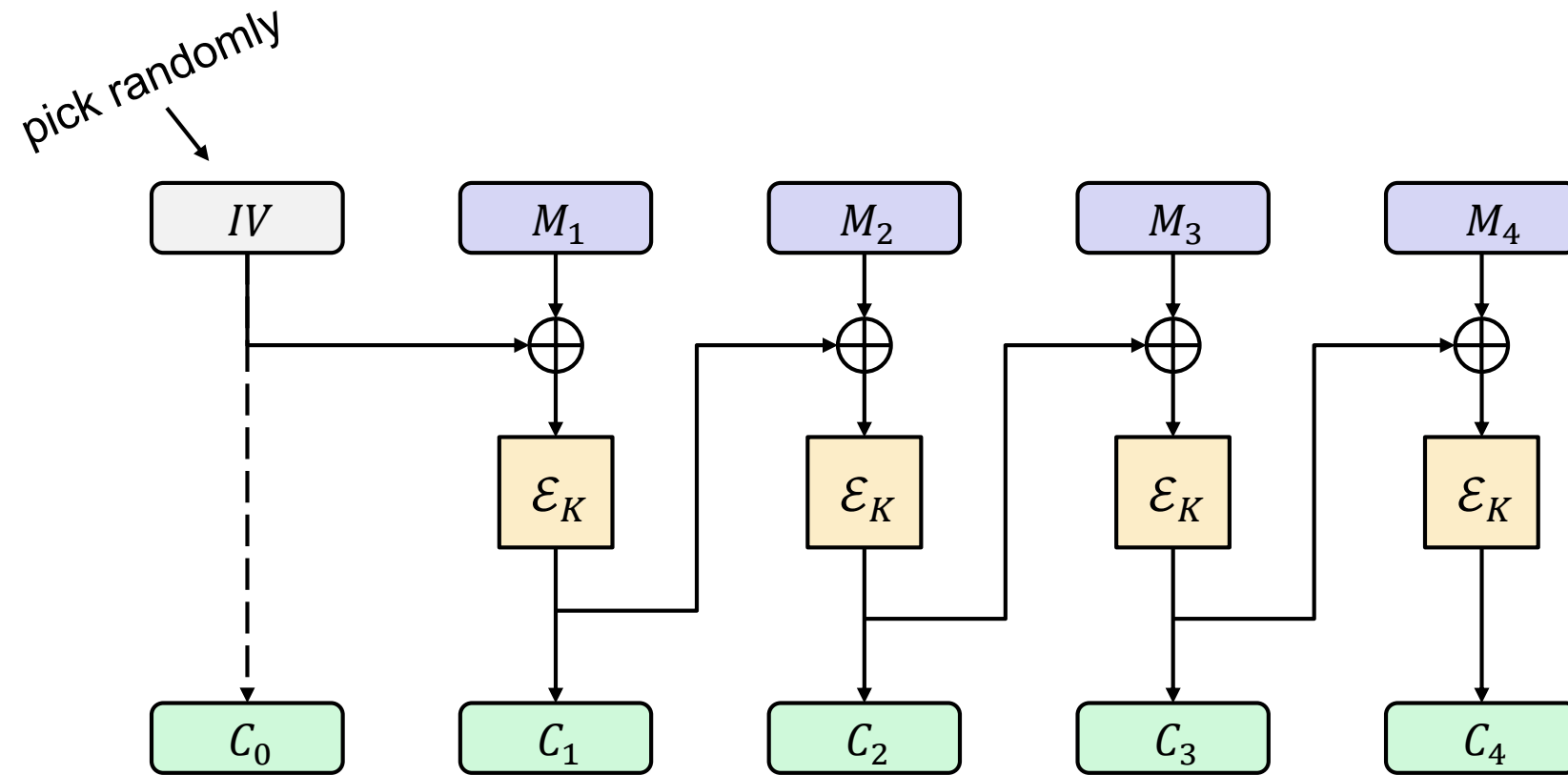
vs.

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

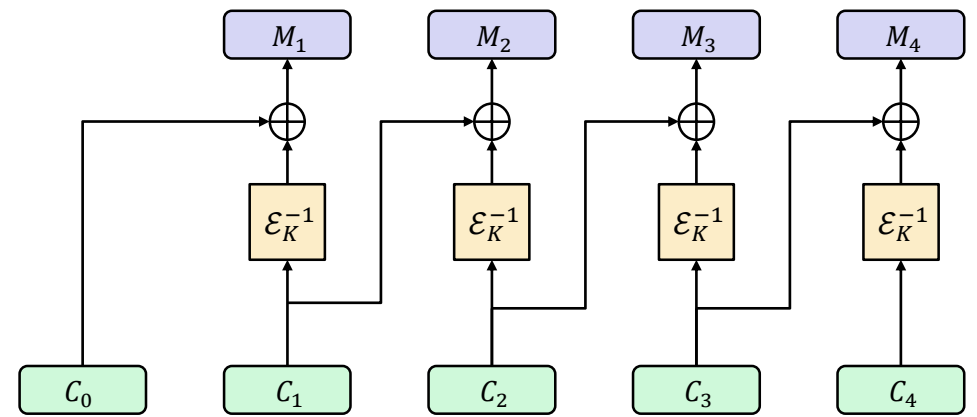
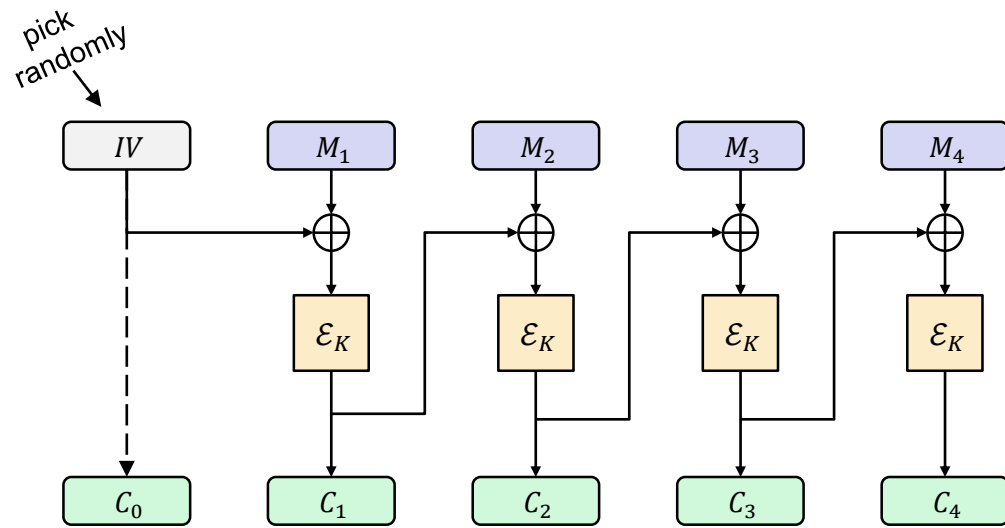
$$\text{Adv}_{\text{CTR}[F]}^{\text{ind-cpa}}(A) \leq \text{Adv}_F^{\text{prf}}(B)$$

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

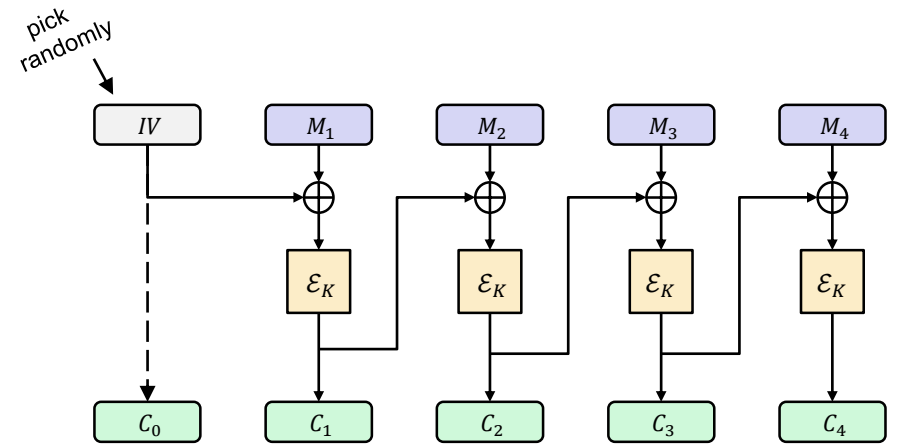


CBC\$ – Cipher Block Chaining mode

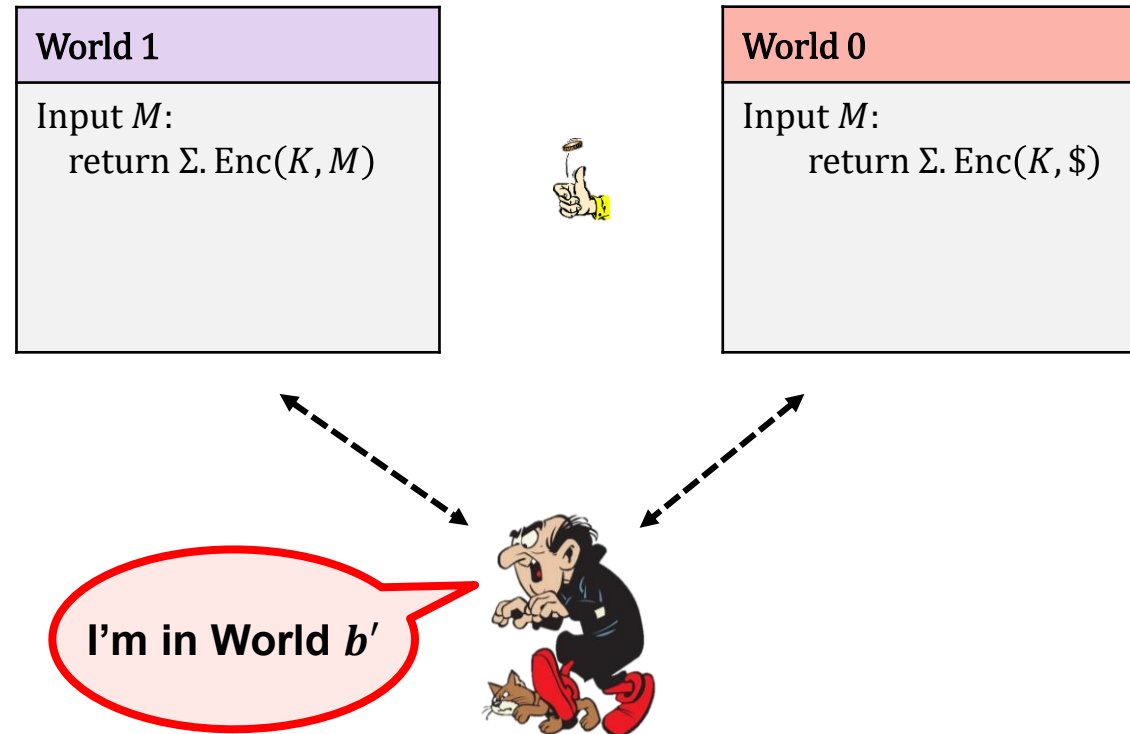


CBC

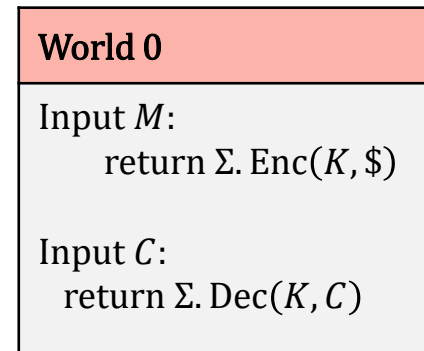
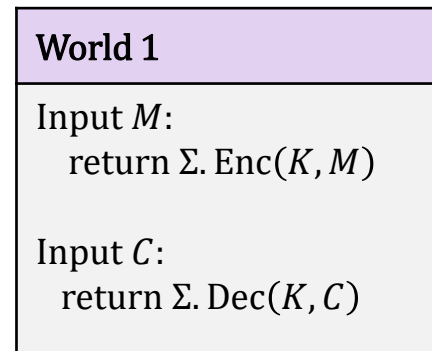
- **Theorem:** IND-CPA secure for *random* IV (assuming \mathcal{E} is a good block cipher)
- Not IND-CPA secure for nonce-based IV
 - (exercise: show this)
- Not parallelizable; cannot precompute values
- Inverse of block cipher \mathcal{E} needed for decryption
- Padding needed for messages not a multiple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