

CSCI 1510

This Lecture:

- Fixed-Length MAC
- CBC-MAC
- Authenticated Encryption

Message Authentication Code (MAC)

- **Syntax:**

A **message authentication code (MAC)** scheme is defined by PPT algorithms $(\text{Gen}, \text{Mac}, \text{Vrfy})$:

$$k \leftarrow \text{Gen}(1^n)$$

$$t \leftarrow \text{Mac}_k(m) \quad m \in \{0,1\}^*$$

$$0/1 := \text{Vrfy}_k(m, t)$$

- **Correctness:** $\forall n, \forall k$ output by $\text{Gen}(1^n), \forall m \in \{0,1\}^*$

$$\text{Vrfy}_k(m, \text{Mac}_k(m)) = 1$$

- **Canonical Verification:**

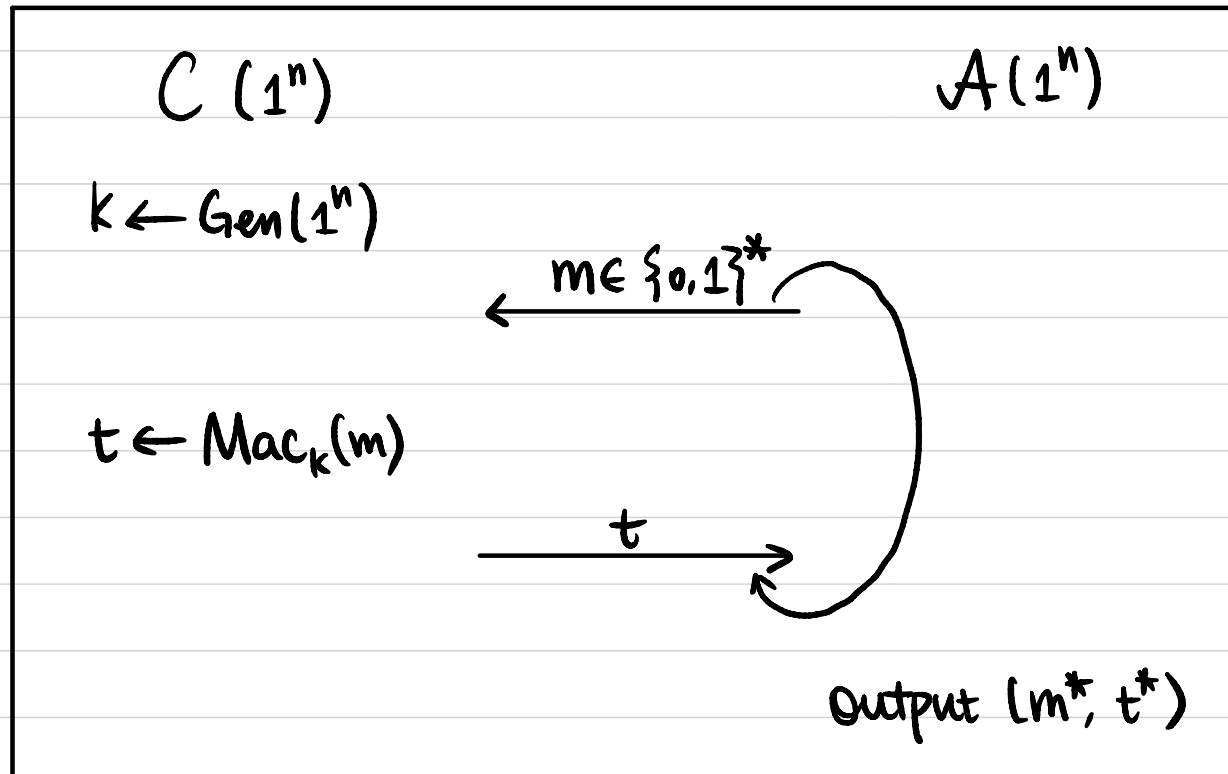
If $\text{Mac}_k(m)$ is deterministic, then $\text{Vrfy}_k(m, t)$ is straightforward.

$$\text{Mac}_k(m) \stackrel{?}{=} t$$

Message Authentication Code (MAC)

Def 1 A message authentication code (MAC) scheme $\pi = (\text{Gen}, \text{Mac}, \text{Vrfy})$ is **existentially unforgeable under adaptive chosen message attack**, or **EU-CMA-secure**, or **secure**, if $\forall \text{PPT } A, \exists \text{ negligible function } \epsilon(\cdot)$ s.t.

$$\Pr[\text{MacForge}_{A, \pi} = 1] \leq \epsilon(n).$$



$$Q := \{m \mid m \text{ queried by } A\}$$

$\text{MacForge}_{A, \pi} = 1$ (A succeeds) if

① $m^* \notin Q$, and

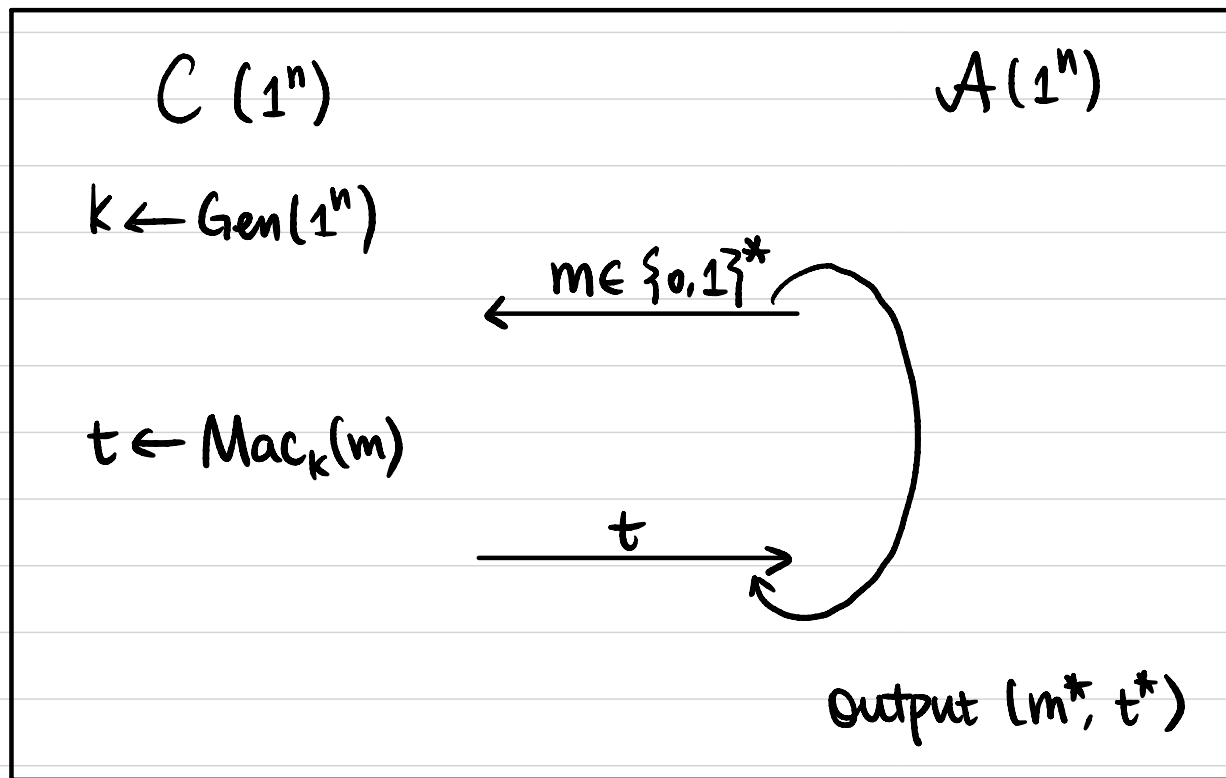
② $\text{Vrfy}_k(m^*, t^*) = 1$.

Message Authentication Code (MAC)

Def 2 A message authentication code (MAC) scheme $\pi = (\text{Gen}, \text{Mac}, \text{Vrfy})$ is

strongly secure if $\forall \text{PPT } A, \exists \text{negligible function } \epsilon(\cdot)$ s.t.

$$\Pr[\text{MacForge}_{A, \pi}^s = 1] \leq \epsilon(n).$$



$Q := \{(m, t) \mid m \text{ queried by } A, t \text{ is the response}\}$

$\text{MacForge}_{A, \pi}^s = 1$ (A succeeds) if

① $(m^*, t^*) \notin Q$, and

② $\text{Vrfy}_k(m^*, t^*) = 1$.

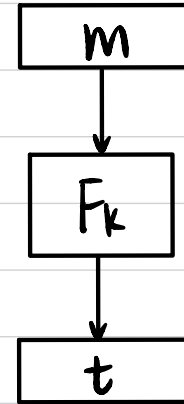
Thm If $\pi = (\text{Gen}, \text{Mac}, \text{Vrfy})$ is a secure MAC with canonical verification (Mac is a deterministic algorithm), then π is also strongly secure.

Fixed-Length MAC

Let $F: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a PRF.

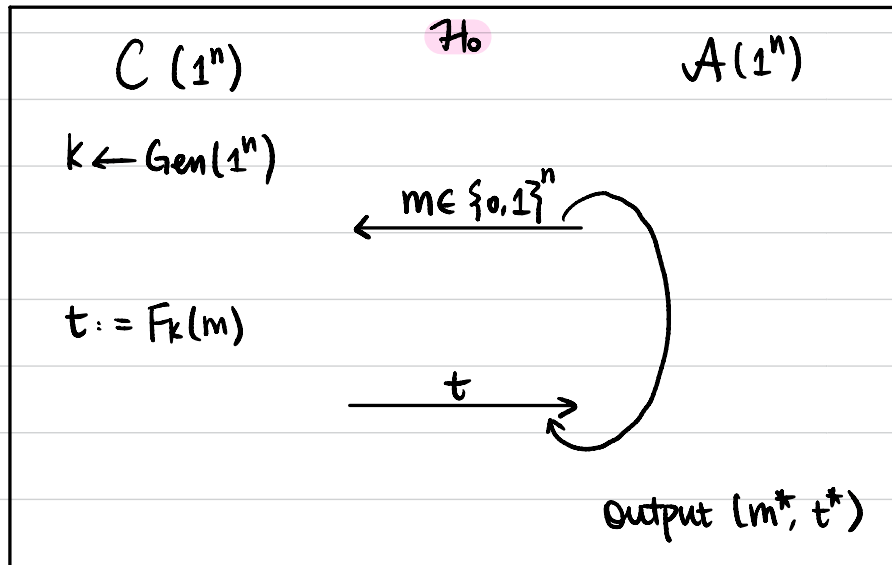
Construct a MAC Scheme:

- $\text{Gen}(1^n)$: Sample $k \leftarrow \{0,1\}^n$, output k .
- $\text{Mac}_k(m)$: $m \in \{0,1\}^n$
output $t := F_k(m)$
- $\text{Vrfy}_k(m,t)$: $F_k(m) \stackrel{?}{=} t$

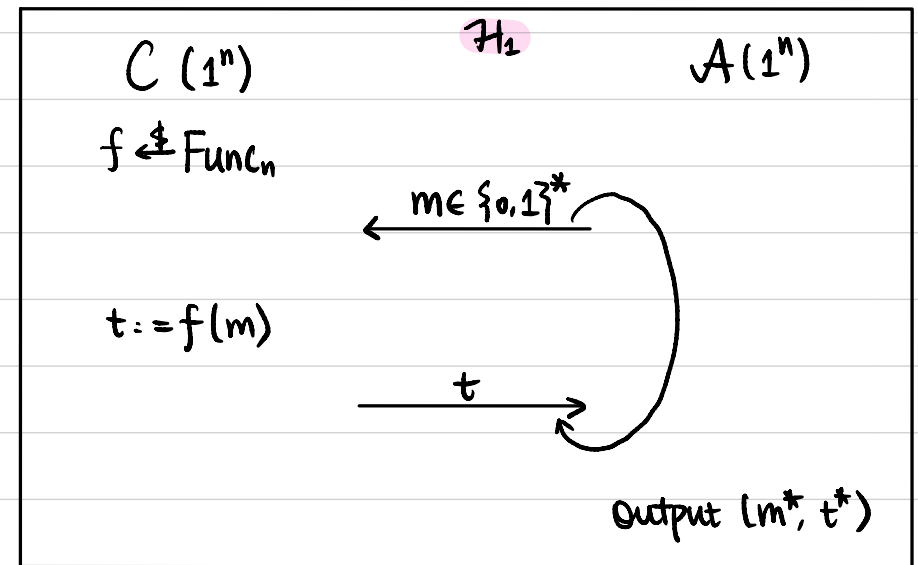


Thm If F is a PRF, then $\pi = (\text{Gen}, \text{Mac}, \text{Vrfy})$ is a secure MAC scheme for fixed-length messages of length n .

Proof $\forall$ PPT A :



$Q := \{m \mid m \text{ queried by } A\}$
 A succeeds if $m^* \notin Q$ and $F_k(m^*) = t^*$



$Q := \{m \mid m \text{ queried by } A\}$
 A succeeds if $m^* \notin Q$ and $f(m^*) = t^*$

Step 1: $|\Pr[A \text{ succeeds in } H_0] - \Pr[A \text{ succeeds in } H_1]| \leq \text{negl}(n).$

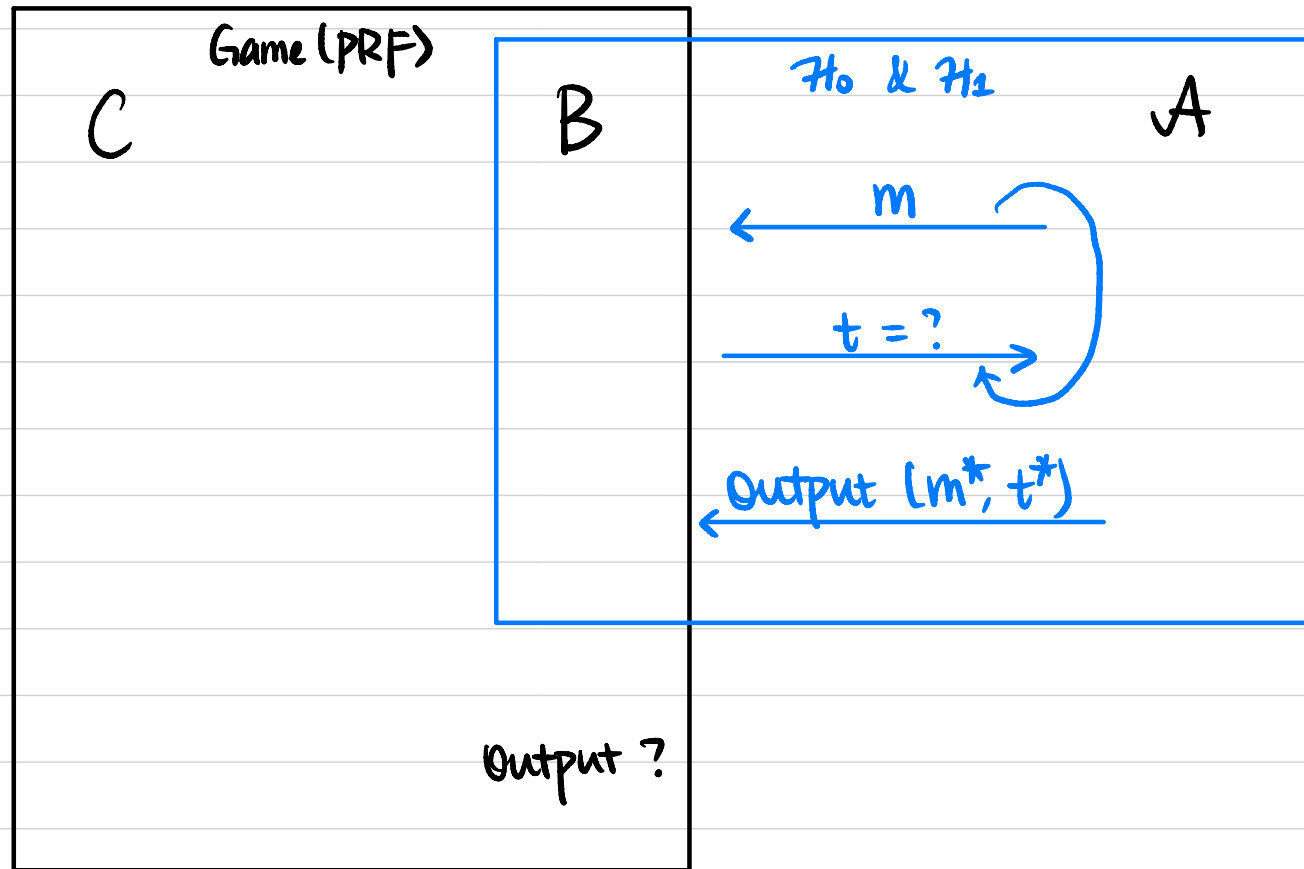
Step 2: $\Pr[A \text{ succeeds in } H_1] \leq \text{negl}(n).$

Step 1: $\forall \text{PPT } A, |\Pr[A \text{ succeeds in } H_0] - \Pr[A \text{ succeeds in } H_1]| \leq \text{negl}(n)$.

Proof Assume not, then $\exists \text{PPT } A$ such that

$$|\Pr[A \text{ succeeds in } H_0] - \Pr[A \text{ succeeds in } H_1]| \geq \text{non-negl}(n).$$

We construct PPT B to break the pseudorandomness of F .



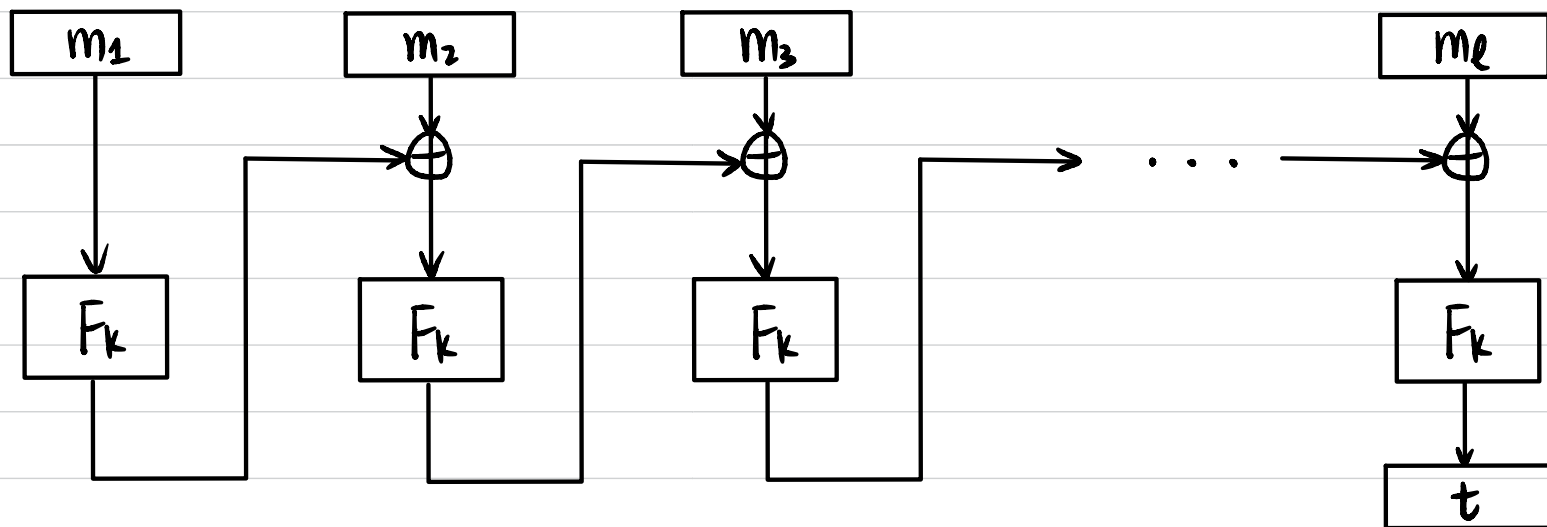
CBC-MAC (for fixed-length messages)

Let $F: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a PRF.

Construct a MAC Scheme for messages of length $\ell(n) \cdot n$:

- $\text{Gen}(1^n)$: Sample $k \leftarrow \{0,1\}^n$, output k .

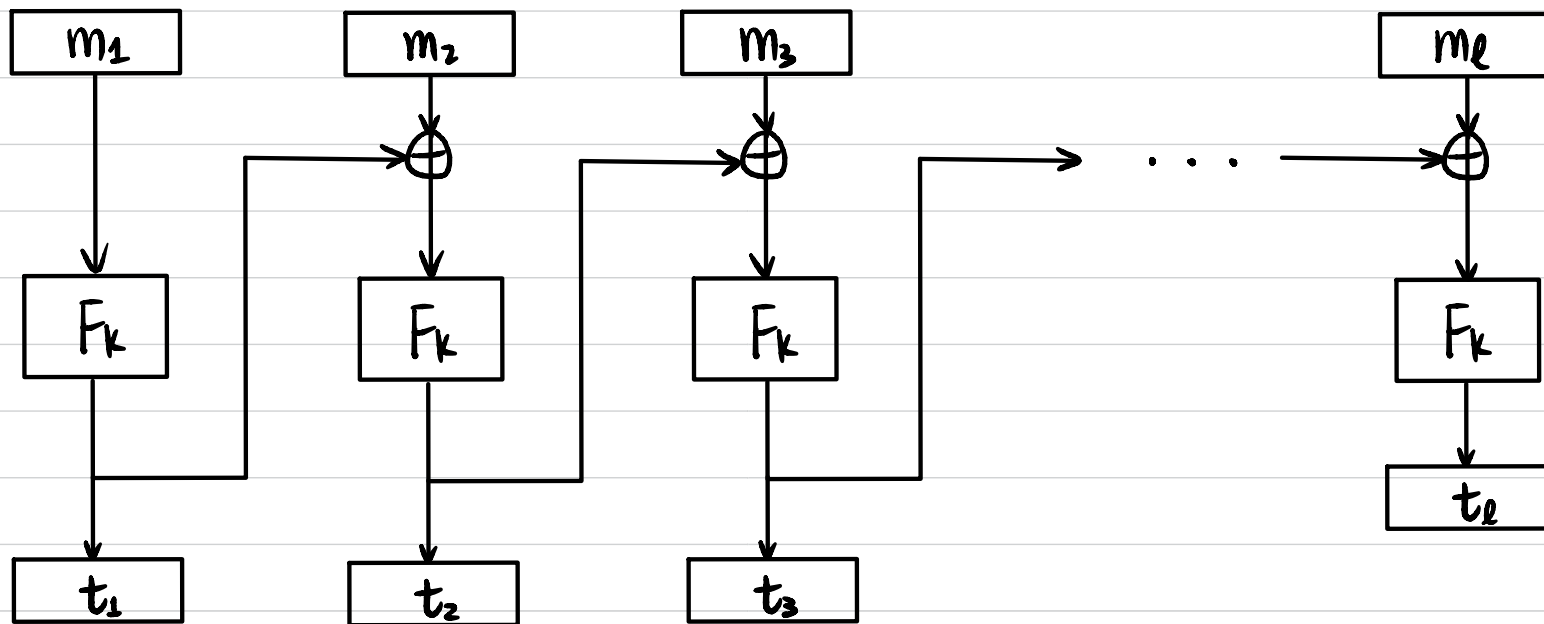
- $\text{Mac}_k(m)$: $m \in \{0,1\}^{\ell(n) \cdot n}$ $m = m_1 \parallel m_2 \parallel \dots \parallel m_\ell$ $m_i \in \{0,1\}^n$



- $\text{Vrfy}_k(m, t)$: $\text{Mac}_k(m) \stackrel{?}{=} t$

Thm If F is a PRF, then CBC-MAC is a secure MAC scheme for fixed-length messages of length $\ell(n) \cdot n$.

Exercises

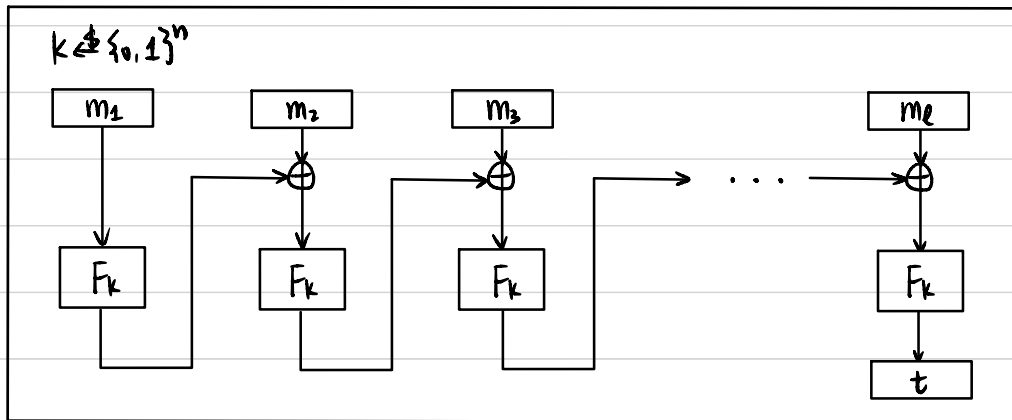


$$t = t_1 \parallel t_2 \parallel \dots \parallel t_\ell$$

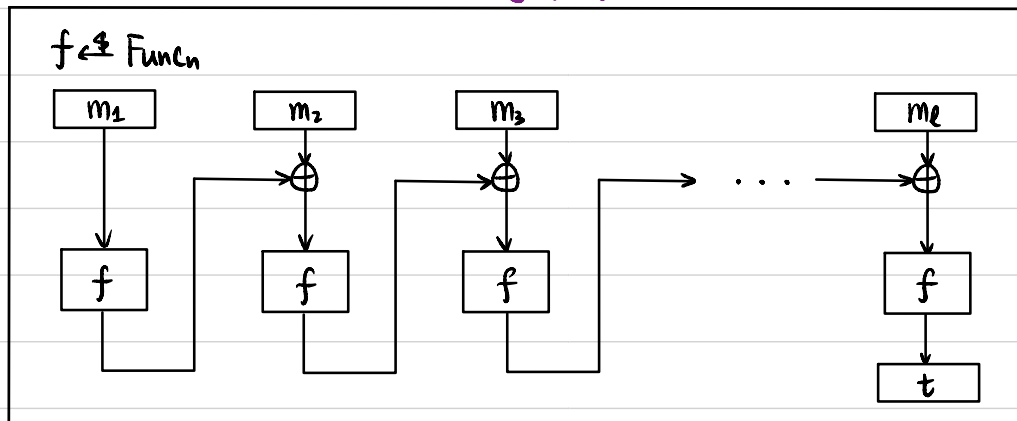
Show this is not a secure MAC for fixed-length messages of length $\ell(n) \cdot n$.

Thm If F is a PRF, then CBC-MAC is a secure MAC scheme for fixed-length messages of length $\ell(n) \cdot n$.

Proof Sketch $\text{Mac}: \{0,1\}^n \times \{0,1\}^{\ell(n) \cdot n} \rightarrow \{0,1\}^n$
 Suffices to show Mac is a PRF.



↕ PRF

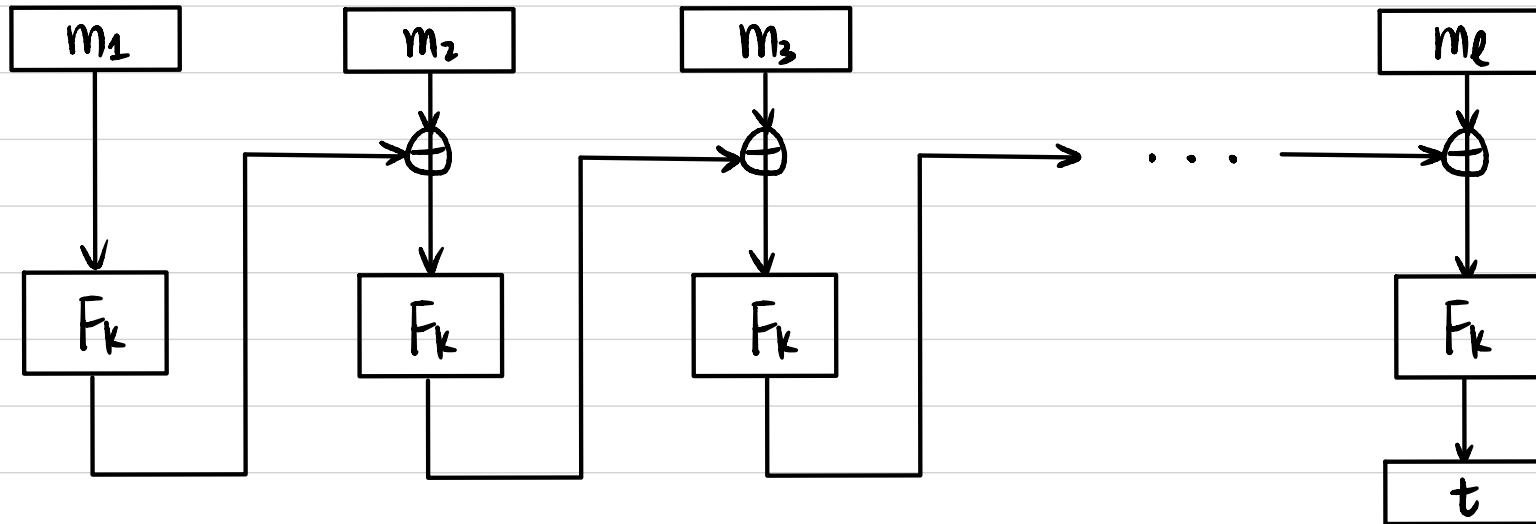


↕ statistical

$$g \leftarrow \{ h \mid h: \{0,1\}^{\ell(n) \cdot n} \rightarrow \{0,1\}^n \}$$

$$t := g(m_1 \parallel \dots \parallel m_\ell)$$

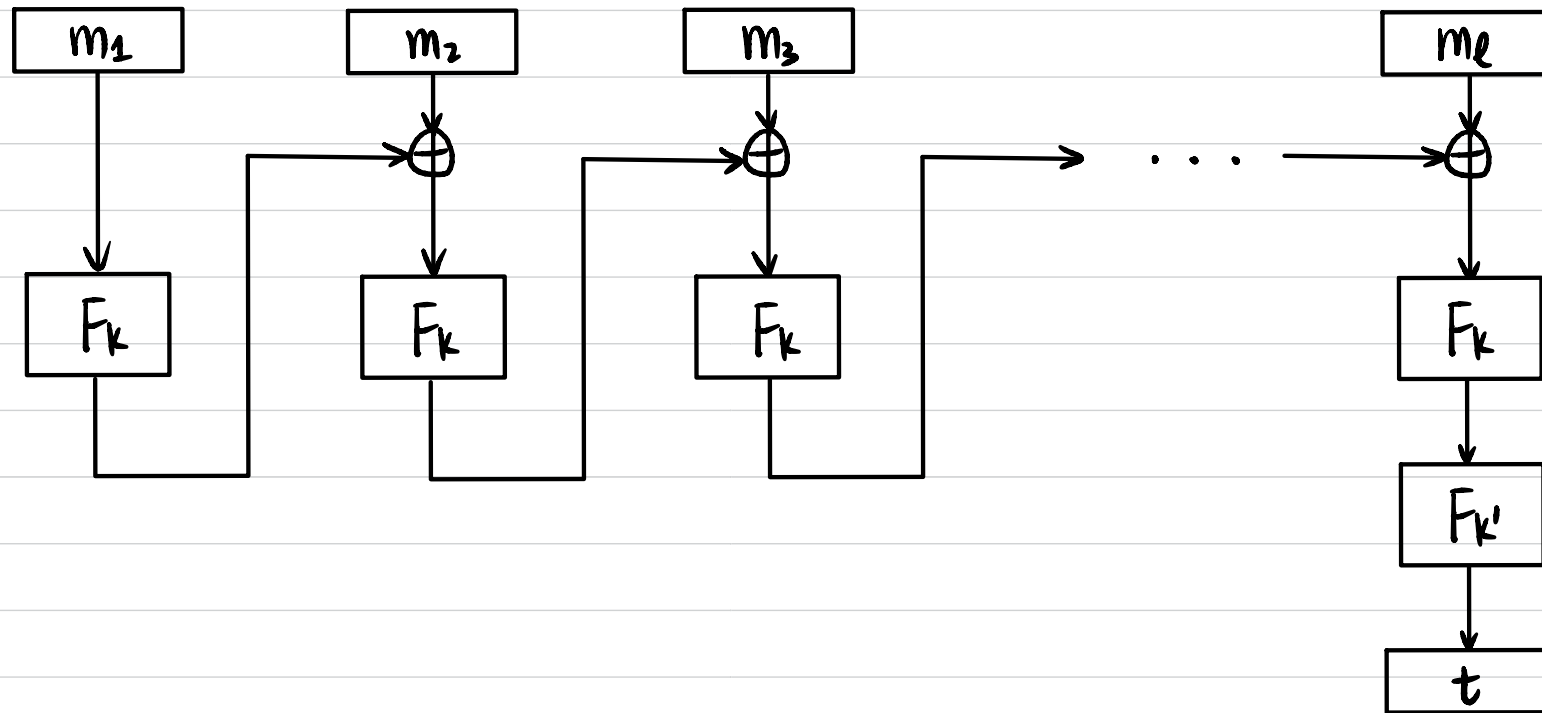
Exercises



Is CBC-MAC a secure MAC for messages of arbitrary length (multiple of n)?

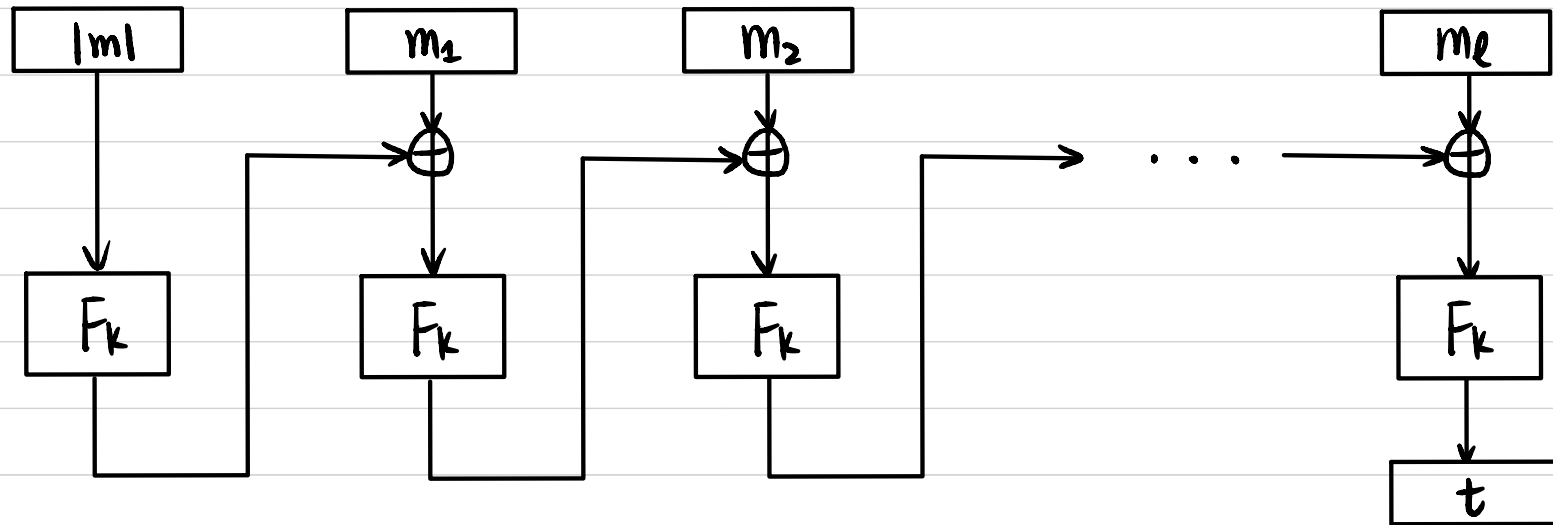
MAC for messages of arbitrary length (multiple of n)

Approach 1: MAC of CBC-MAC

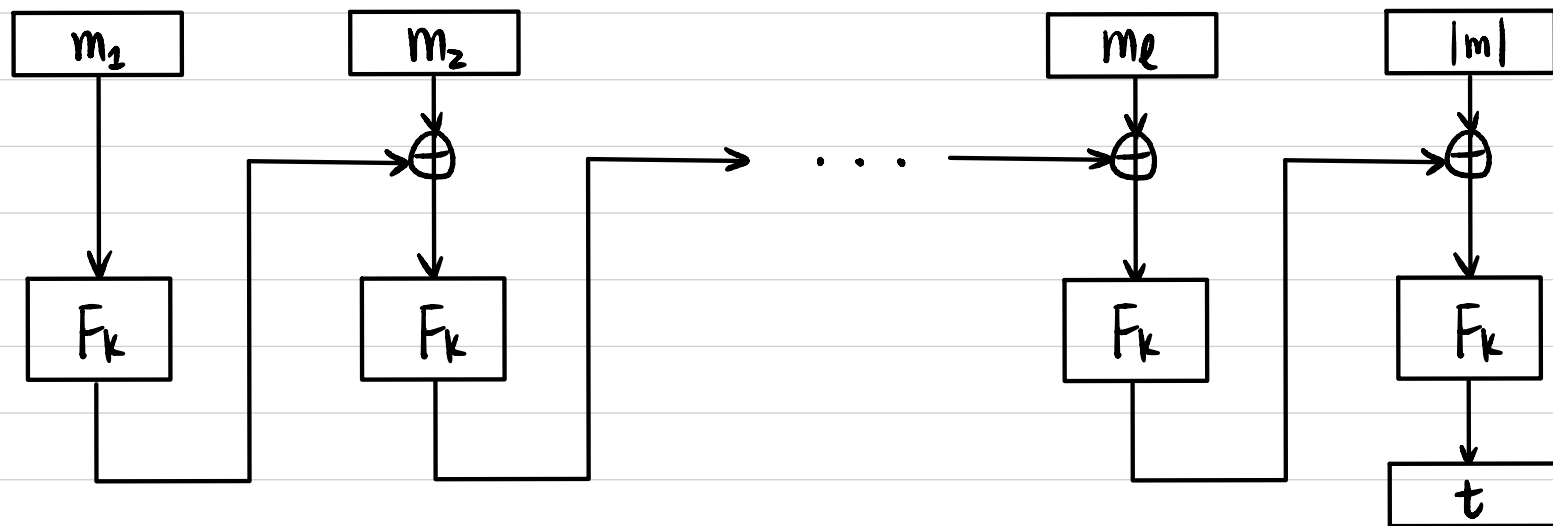


MAC for messages of arbitrary length (multiple of n)

Approach 2: CBC-MAC on $|m| \parallel m$

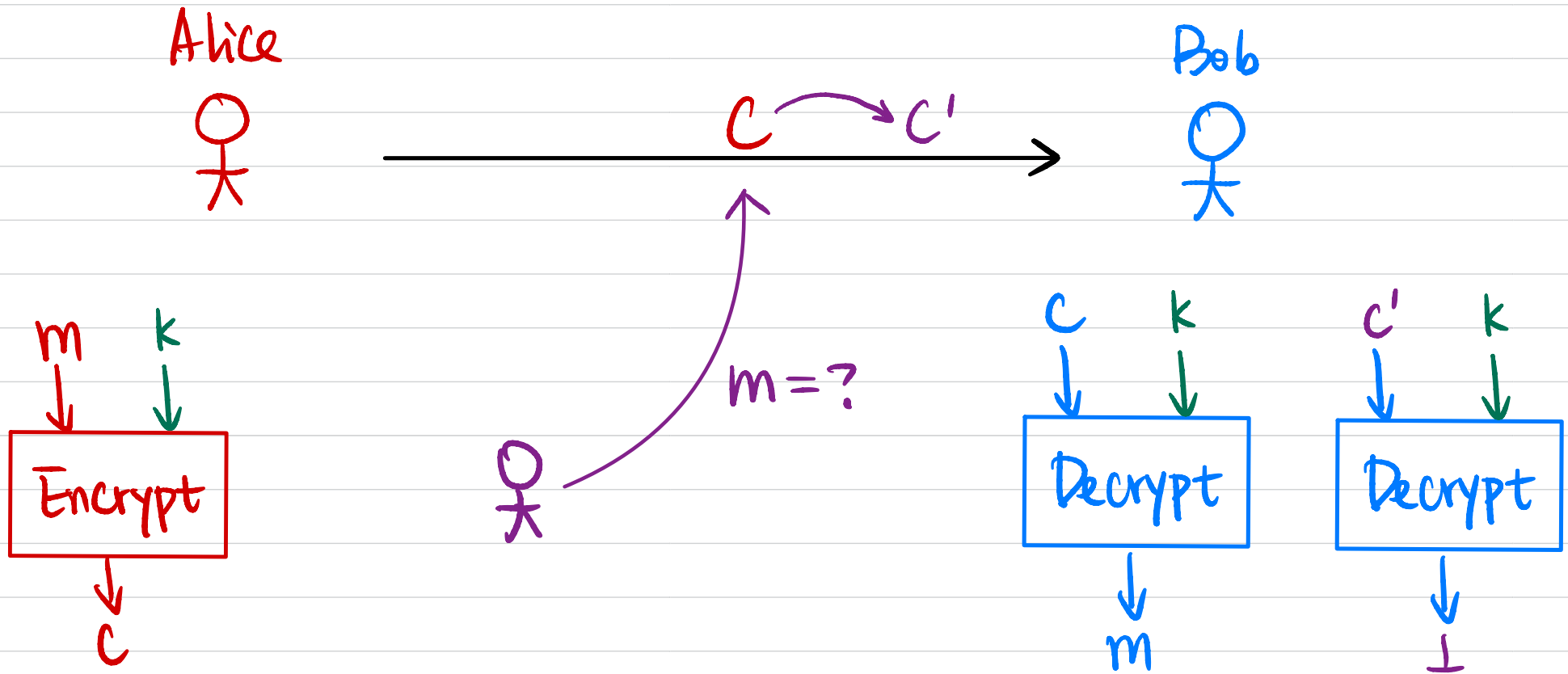


Exercises



Show this is not a secure MAC for messages of arbitrary length (multiple of n).

Authenticated Encryption

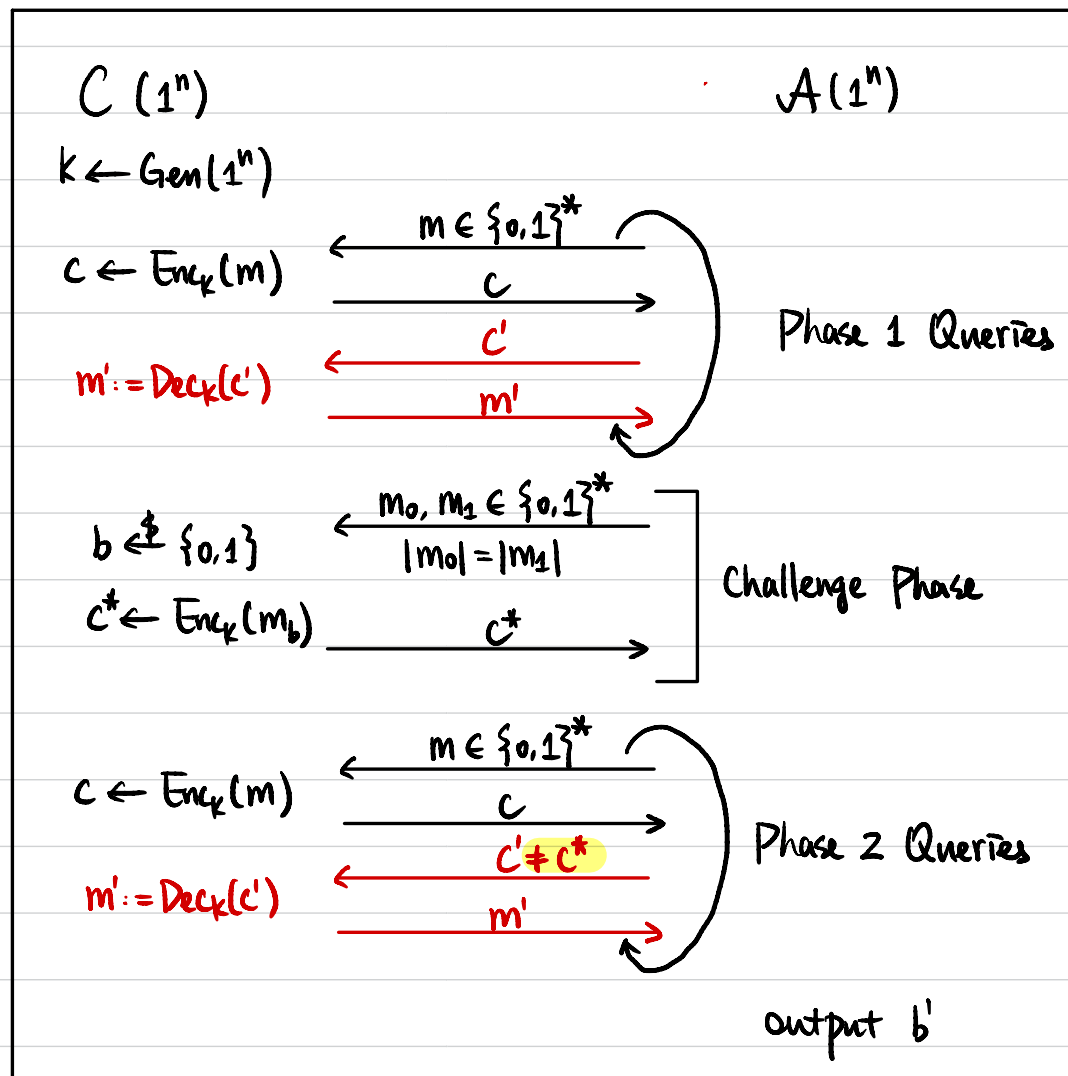


Security Guarantees:

- Message Secrecy: CCA Security
- Message Integrity: Unforgeability

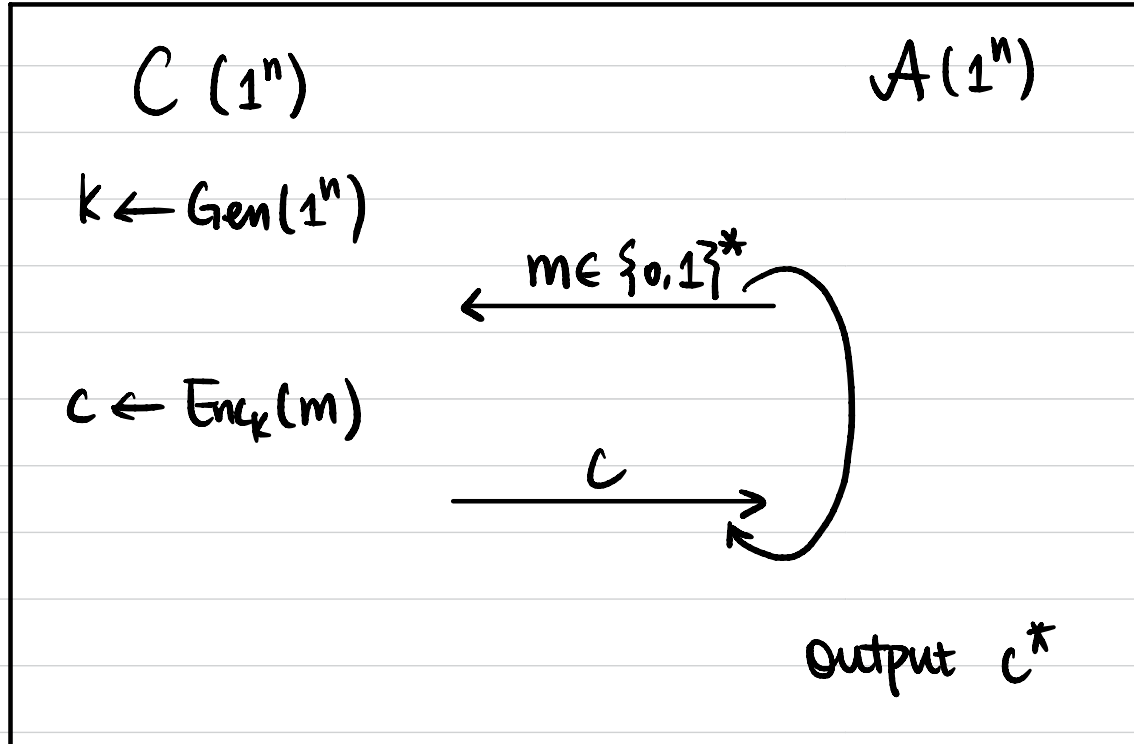
Chosen Ciphertext Attack (CCA) Security

Def A symmetric-key encryption scheme $(\text{Gen}, \text{Enc}, \text{Dec})$ is **secure against chosen ciphertext attacks**, or **CCA-secure**, if $\forall \text{PPT } A$,
 $\exists$ negligible function $\varepsilon(\cdot)$ s.t. $\Pr[b = b'] \leq \frac{1}{2} + \varepsilon(n)$



Unforgeability

Def A symmetric-key encryption scheme $\pi = (\text{Gen}, \text{Enc}, \text{Dec})$ is **Unforgeable** if $\forall \text{PPT } A, \exists \text{ negligible function } \epsilon(\cdot)$ s.t. $\Pr[\text{EncForge}_{A, \pi} = 1] \leq \epsilon(n)$.



$$Q := \{m \mid m \text{ queried by } A\}$$
$$m^* := \text{Dec}_k(c^*)$$

$\text{EncForge}_{A, \pi} = 1$ (A succeeds) if

- ① $m^* \notin Q$, and
- ② $m^* \neq \perp$

Def A symmetric-key encryption scheme is **authenticated encryption** if it is **CCA-secure** and **unforgeable**.

Exercises

Is the CPA-secure encryption from PRF CCA-secure? Unforgeable?

$\text{Enc}_k(m): m \in \{0,1\}^n$
 $r \xleftarrow{\$} \{0,1\}^n$
output $c := \langle r, F_k(r) \oplus m \rangle$

