CSCI 1510

This Lecture:

- Fixed-Length MAC
- CBC-MAC

Message Authentication Code (MAC)

- **Syntax:**

  A **message authentication code (MAC)** scheme is defined by PPT algorithms (Gen, Mac, Vrfy):

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

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

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

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

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

- **Canonical Verification:**

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

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

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 $\forall$ PPT $\mathcal{A}$, $\exists$ negligible function $\varepsilon(\cdot)$ s.t.

$$\Pr[\text{MacForge}_{\mathcal{A},\Pi} = 1] \le \varepsilon(n).$$

$C(1^n)$		$\mathcal{A}(1^n)$
$k \leftarrow \text{Gen}(1^n)$		
	$\xleftarrow{\; m \in \{0,1\}^* \;}$	
$t \leftarrow \text{Mac}_k(m)$		
	$\xrightarrow{\; t \;}$	
		Output (m^*, t^*)

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

$\text{MacForge}_{\mathcal{A},\Pi} = 1$ ($\mathcal{A}$ 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 $\Pi = (\mathrm{Gen}, \mathrm{Mac}, \mathrm{Vrfy})$ is **strongly secure** if $\forall$ PPT $\mathcal{A}$, $\exists$ negligible function $\varepsilon(\cdot)$ s.t.

$$\Pr[\mathrm{MacForge}^{s}_{\mathcal{A},\Pi} = 1] \le \varepsilon(n).$$

$C(1^n)$		$\mathcal{A}(1^n)$
$k \leftarrow \mathrm{Gen}(1^n)$		
	$\xleftarrow{m \in \{0,1\}^*}$	
$t \leftarrow \mathrm{Mac}_k(m)$		
	$\xrightarrow{t}$	
		Output (m^*, t^*)

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

$\mathrm{MacForge}^{s}_{\mathcal{A},\Pi} = 1$ ($\mathcal{A}$ succeeds) if

① $(m^*, t^*) \notin Q$, and

② $\mathrm{Vrfy}_k(m^*, t^*) = 1$.

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

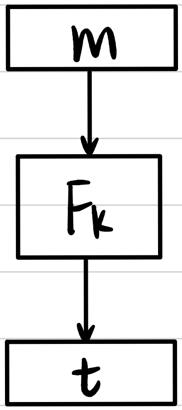
Fixed-Length MAC

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

Construct a MAC scheme:

- $Gen(1^n)$: sample $k \xleftarrow{\$} \{0,1\}^n$, output k.
- $Mac_k(m)$: $m \in \{0,1\}^n$

  output $t := F_k(m)$
- $Vrfy_k(m,t)$: $F_k(m) \stackrel{?}{=} t$



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

Proof $\forall$ PPT $\mathcal{A}$:

$\mathcal{H}_0$

$C(1^n)$	$\mathcal{A}(1^n)$
$k \leftarrow Gen(1^n)$
	$\xleftarrow{m \in \{0,1\}^n}$
$t := F_k(m)$
$\xrightarrow{t}$
	Output (m^*, t^*)

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

$\mathcal{A}$ succeeds if $m^* \notin Q$ and $F_k(m^*) = t^*$

$\mathcal{H}_1$

$C(1^n)$	$\mathcal{A}(1^n)$
$f \xleftarrow{\$} Func_n$
	$\xleftarrow{m \in \{0,1\}^*}$
$t := f(m)$
$\xrightarrow{t}$
	Output (m^*, t^*)

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

$\mathcal{A}$ succeeds if $m^* \notin Q$ and $f(m^*) = t^*$

Step 1: $\left| \Pr[\mathcal{A} \text{ succeeds in } \mathcal{H}_0] - \Pr[\mathcal{A} \text{ succeeds in } \mathcal{H}_1] \right| \leq negl(n)$.

Step 2: $\Pr[\mathcal{A} \text{ succeeds in } \mathcal{H}_1] \leq negl(n)$.

$\downarrow$

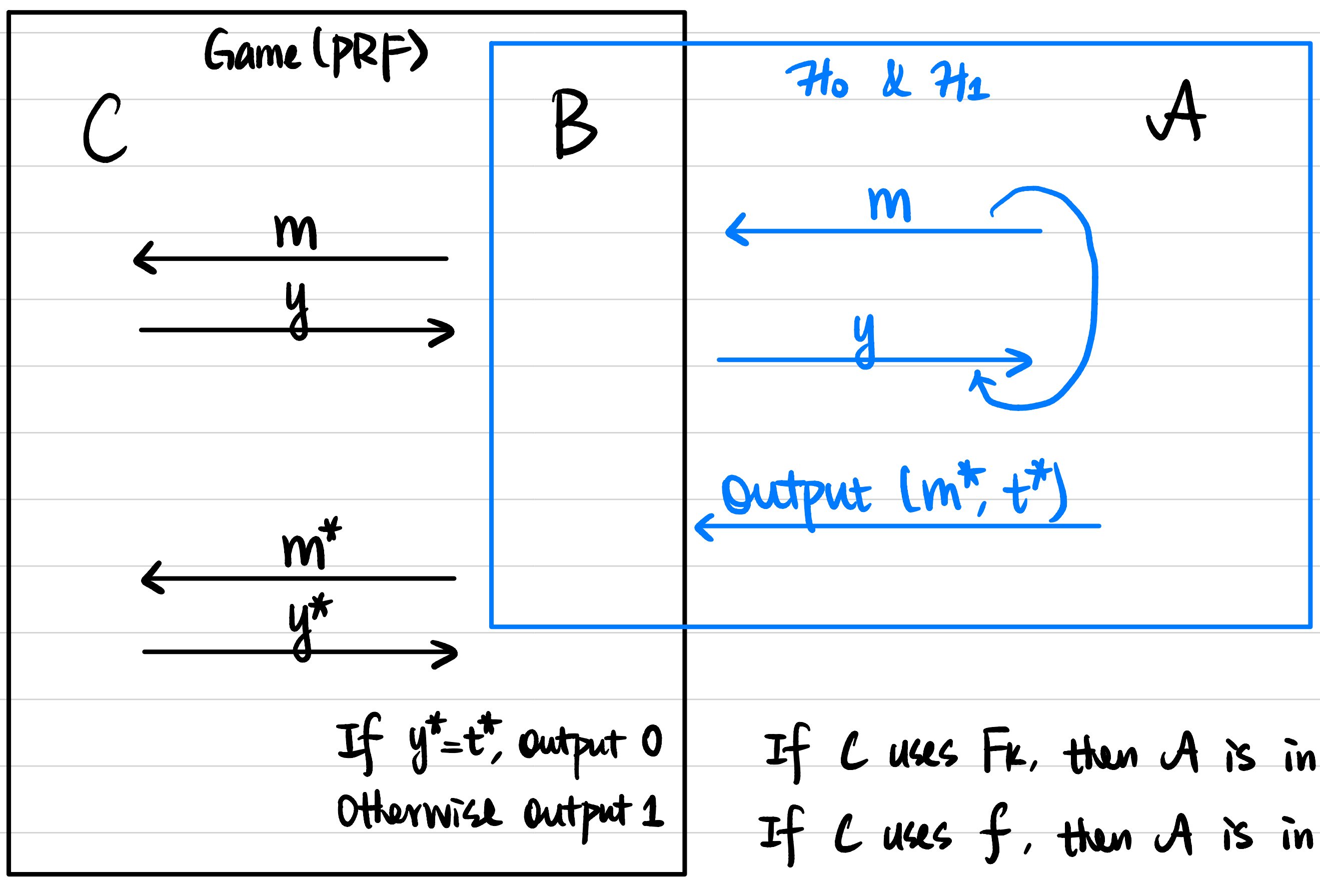
$1/2^n$

Step 1: $\forall$ PPT $\mathcal{A}$, $\left|\Pr[\mathcal{A} \text{ succeeds in } \mathcal{H}_0] - \Pr[\mathcal{A} \text{ succeeds in } \mathcal{H}_1]\right| \leq \text{negl}(n)$.

<u>Proof</u> Assume not, then $\exists$ PPT $\mathcal{A}$ such that

$$\left|\Pr[\mathcal{A} \text{ succeeds in } \mathcal{H}_0] - \Pr[\mathcal{A} \text{ succeeds in } \mathcal{H}_1]\right| \geq \text{non-negl}(n).$$

We construct PPT B to break the pseudorandomness of F.



If C uses F_k, then $\mathcal{A}$ is in $\mathcal{H}_0$

If C uses f, then $\mathcal{A}$ is in $\mathcal{H}_1$

$$\left|\Pr[B^{F_k(\cdot)} \text{ outputs } 0] - \Pr[B^{f(\cdot)} \text{ outputs } 0]\right|$$

$$= \left|\Pr[\mathcal{A} \text{ succeeds in } \mathcal{H}_0] - \Pr[\mathcal{A} \text{ succeeds in } \mathcal{H}_1]\right|$$

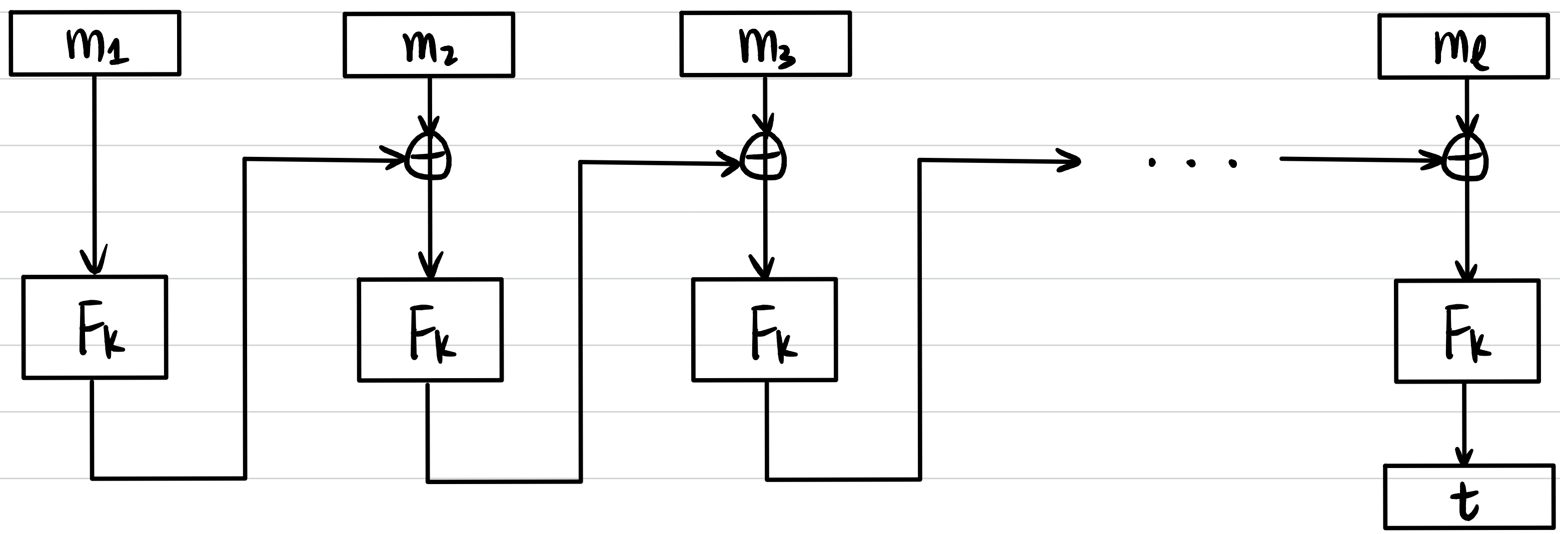
$$\geq \text{non-negl}(n).$$

CBC-MAC (for fixed-length messages)

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

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

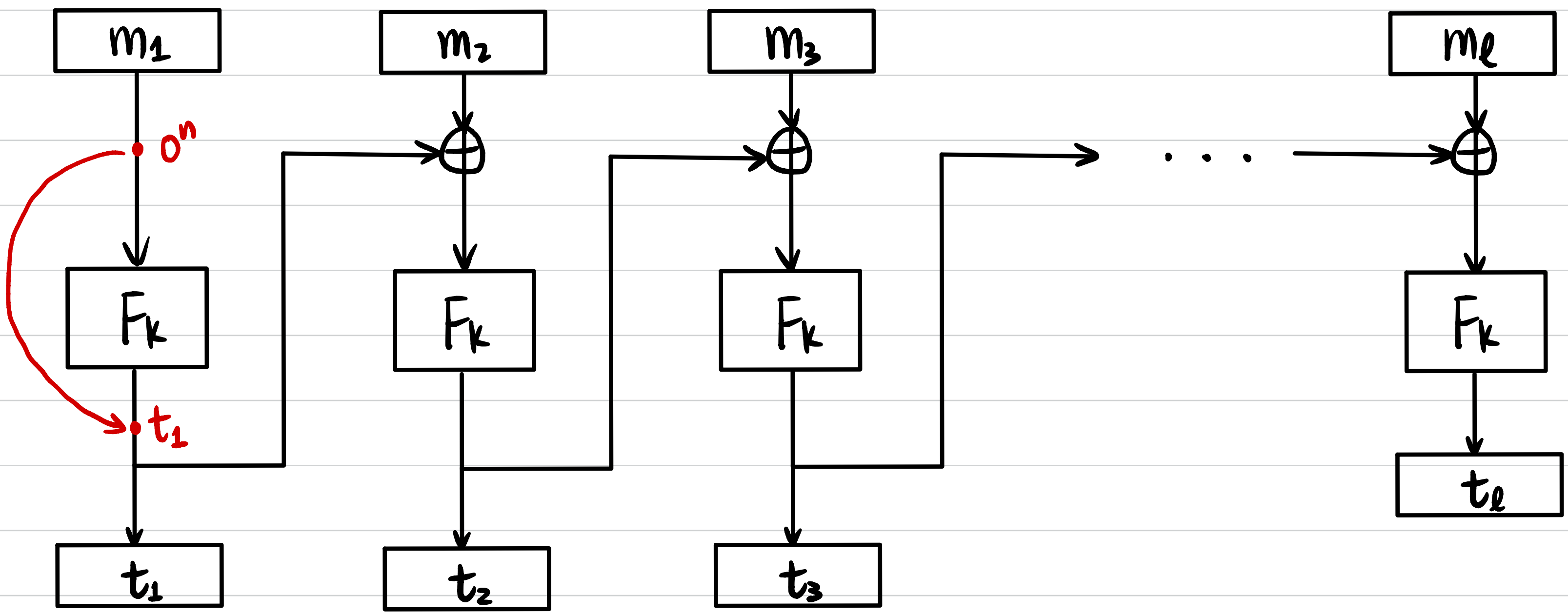
- $\text{Gen}(1^n)$: sample $k \xleftarrow{\$} \{0,1\}^n$, output k.
- $\text{Mac}_k(m)$: $m \in \{0,1\}^{\ell(n)\cdot n}$ $\quad m = m_1 \| m_2 \| \cdots \| m_\ell \quad m_i \in \{0,1\}^n$



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

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

Exercises



$t = t_1 \| t_2 \| \cdots \| t_\ell$

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

C A

$m = 0^n \| \cdots \| 0^n \| 1^n$

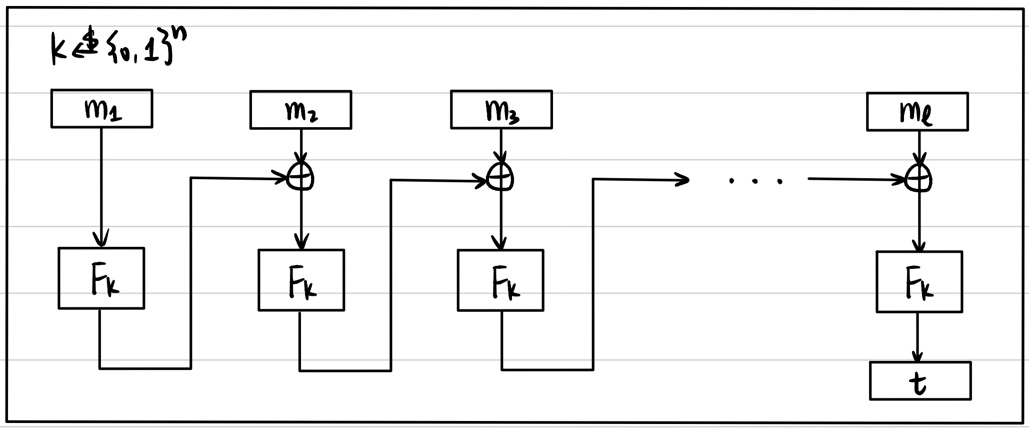
$t = t_1 \| \cdots \| t_\ell$

Output $m^* = 0^n \| \cdots \| 0^n \| t_{\ell-1}$
$t^* = t_1 \| \cdots \| t_{\ell-1} \| t_1$

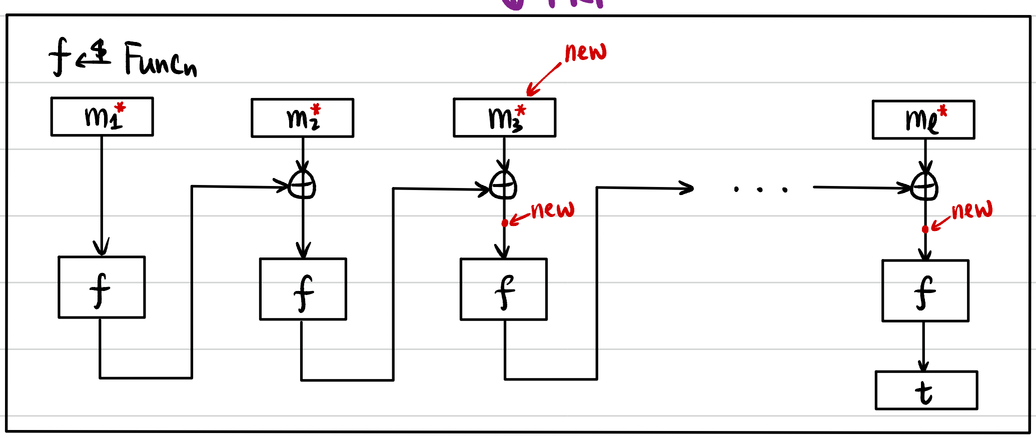
Thm If F is a PRF, then CBC-MAC is a secure MAC scheme for fixed-length messages of length $\ell(n)\cdot n$.

Proof Sketch Mac: $\{0,1\}^n \times \{0,1\}^{\ell(n)\cdot n} \to \{0,1\}^n$

Suffices to show Mac is a PRF.



$\updownarrow$ PRF

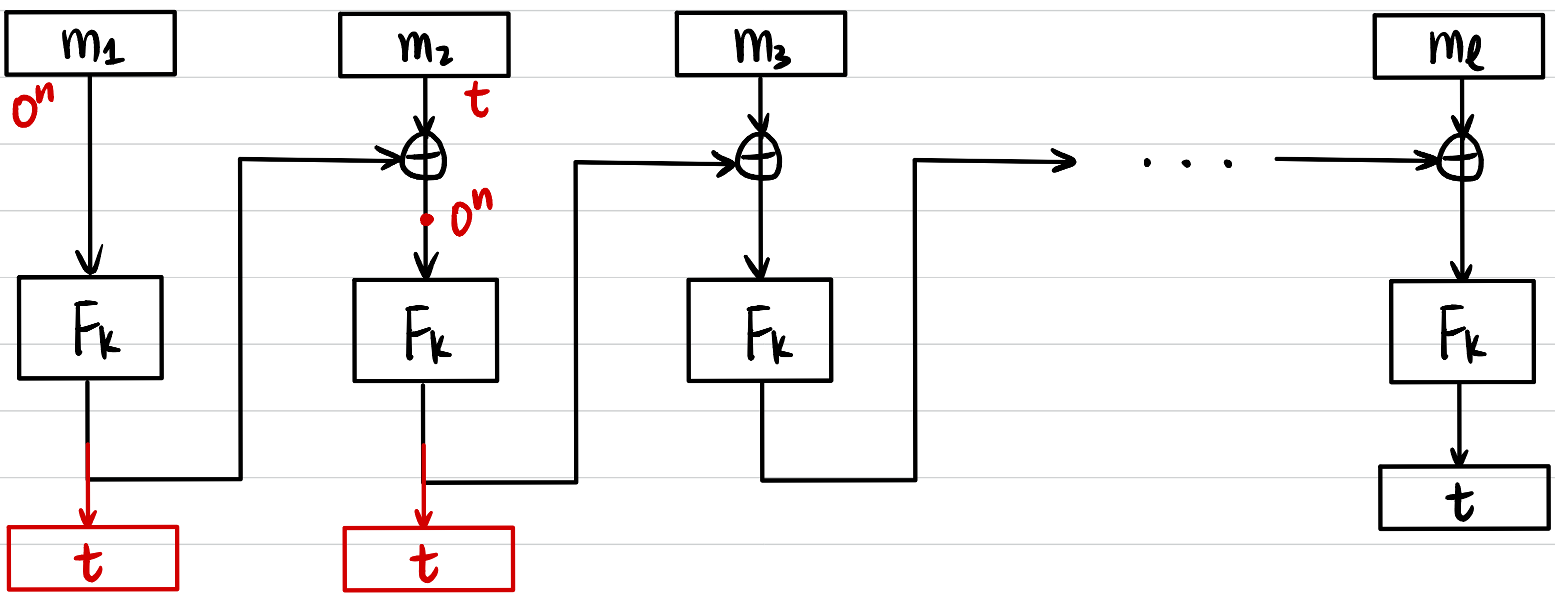


$\updownarrow$ statistical

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

$t := g(m_1 \| \cdots \| m_\ell)$

Exercises



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

$\mathcal{C}$ $\qquad\qquad$ $\mathcal{A}$

$\xleftarrow{m = 0^n}$

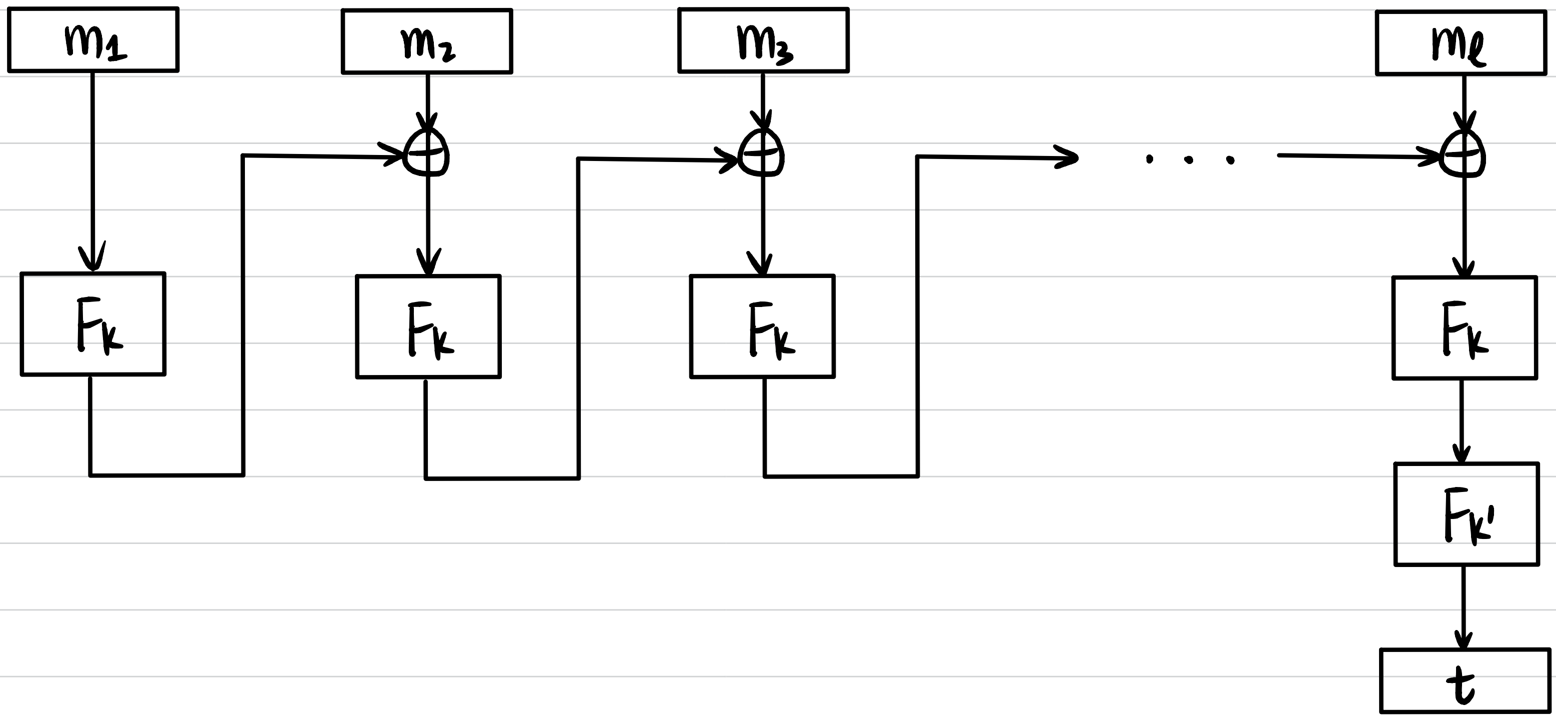
$\xrightarrow{t}$

Output $m^* = 0^n \| t$

$t^* = t$

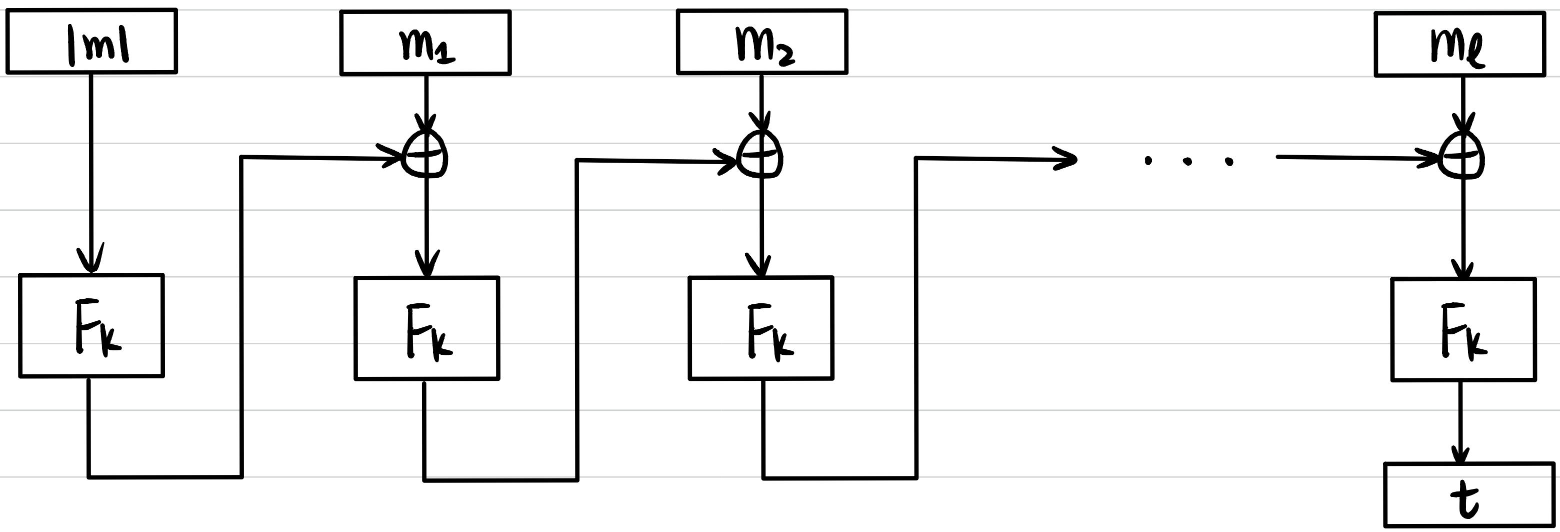
MAC for messages of arbitrary length (multiple of n)

Approach 1: MAC of CBC-MAC

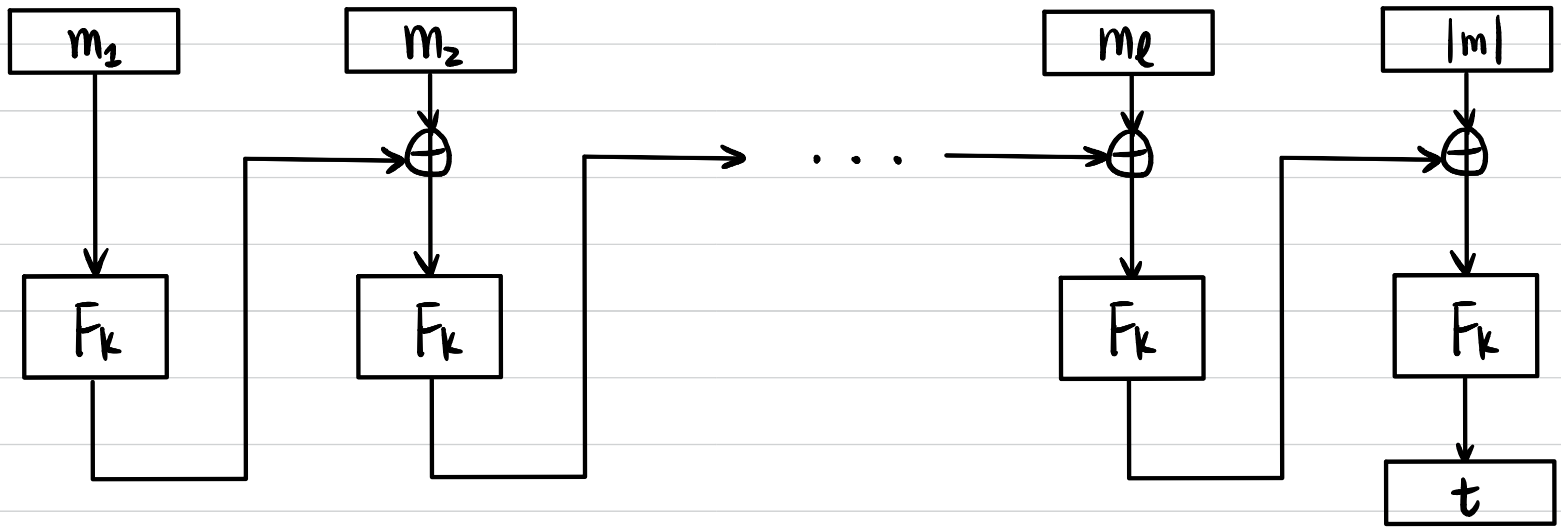


MAC for messages of arbitrary length (multiple of n)

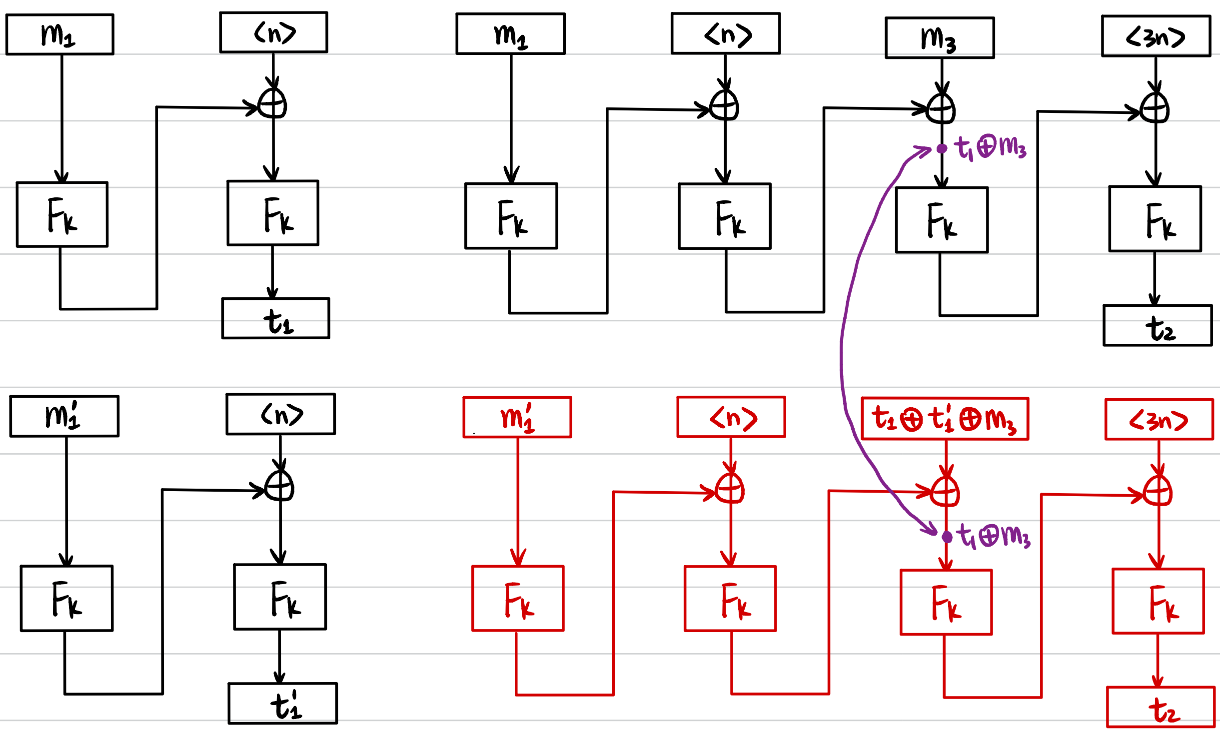
Approach 2: CBC-MAC on $|m| \| m$



Exercises



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



$\mathcal{C}$ $\qquad\qquad$ $\mathcal{A}$

$\xleftarrow{\quad m_1 \quad}$

$\xrightarrow{\quad t_1 \quad}$

$\xleftarrow{\quad m_1' \quad}$

$\xrightarrow{\quad t_1' \quad}$

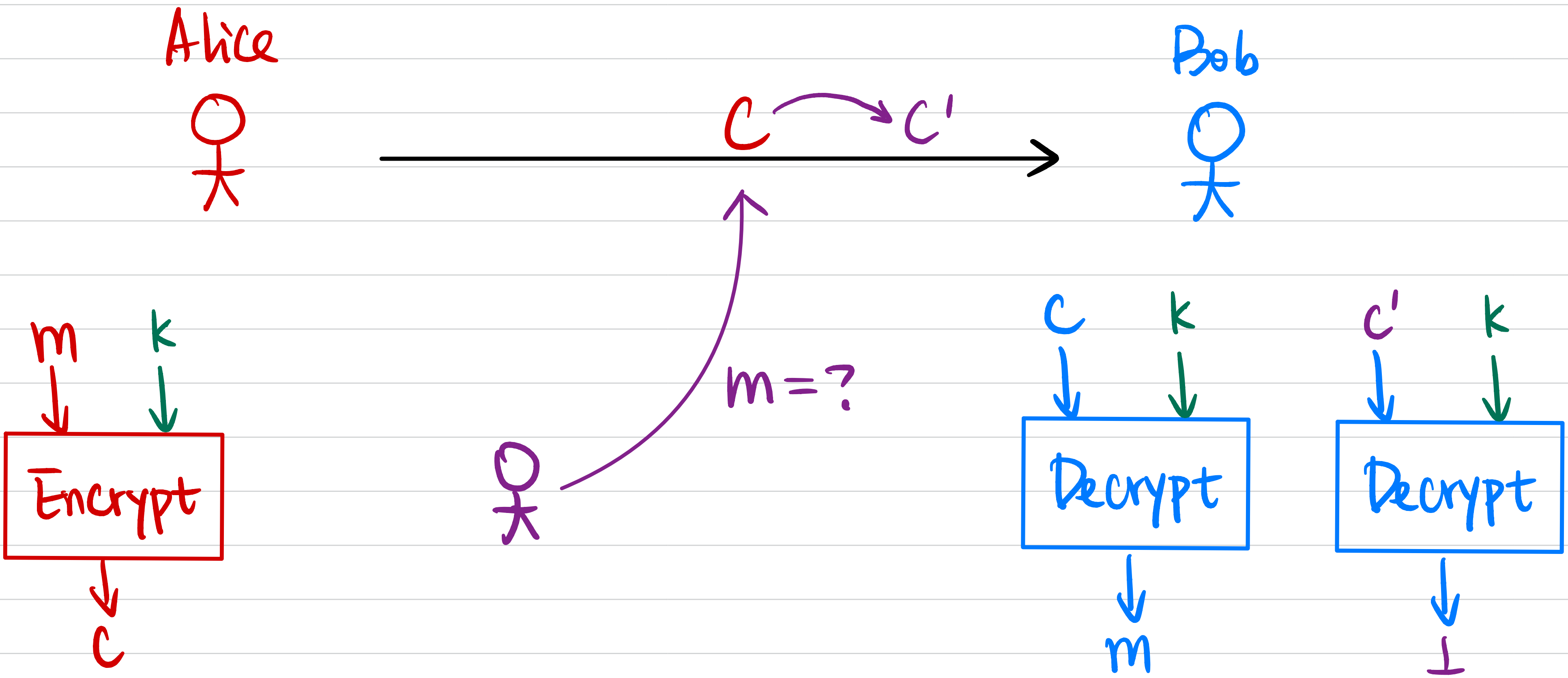
$\xleftarrow{\quad m_1 \| \langle n \rangle \| m_3 \quad}$

$\xrightarrow{\quad t_2 \quad}$

Output $m^* = m_1' \| \langle n \rangle \| t_1 \oplus t_1' \oplus m_3$

$t^* = t_2$

Authenticated Encryption



Security Guarantees:

- Message Secrecy: CCA Security
- Message Integrity: Unforgeability