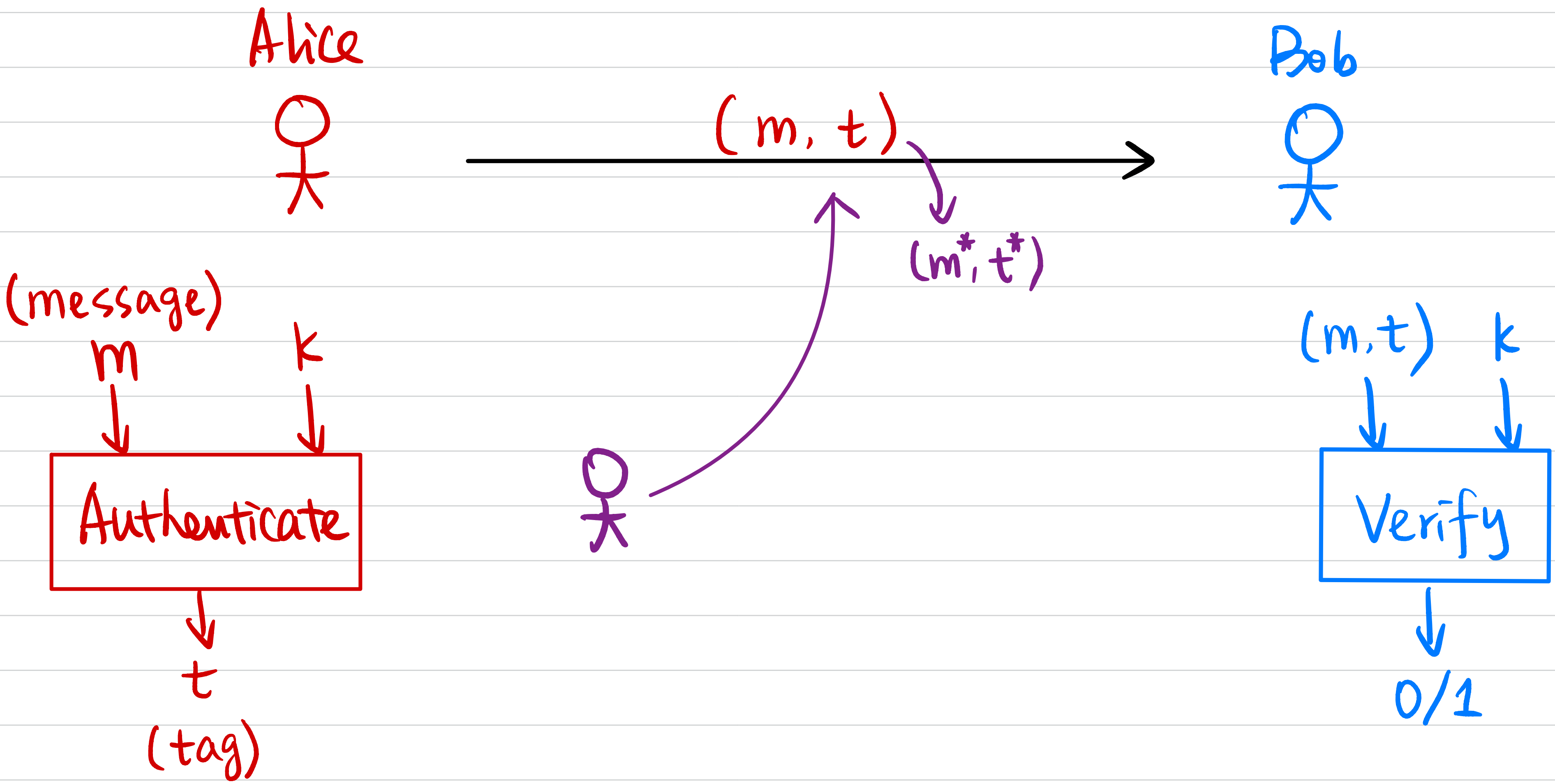
CSCI 1510

- Message Authentication Code (MAC)
- Fixed-Length MAC
- CBC-MAC

Message Integrity



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 $\mathrm{Gen}(1^n)$, $\forall m \in \{0,1\}^*$

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

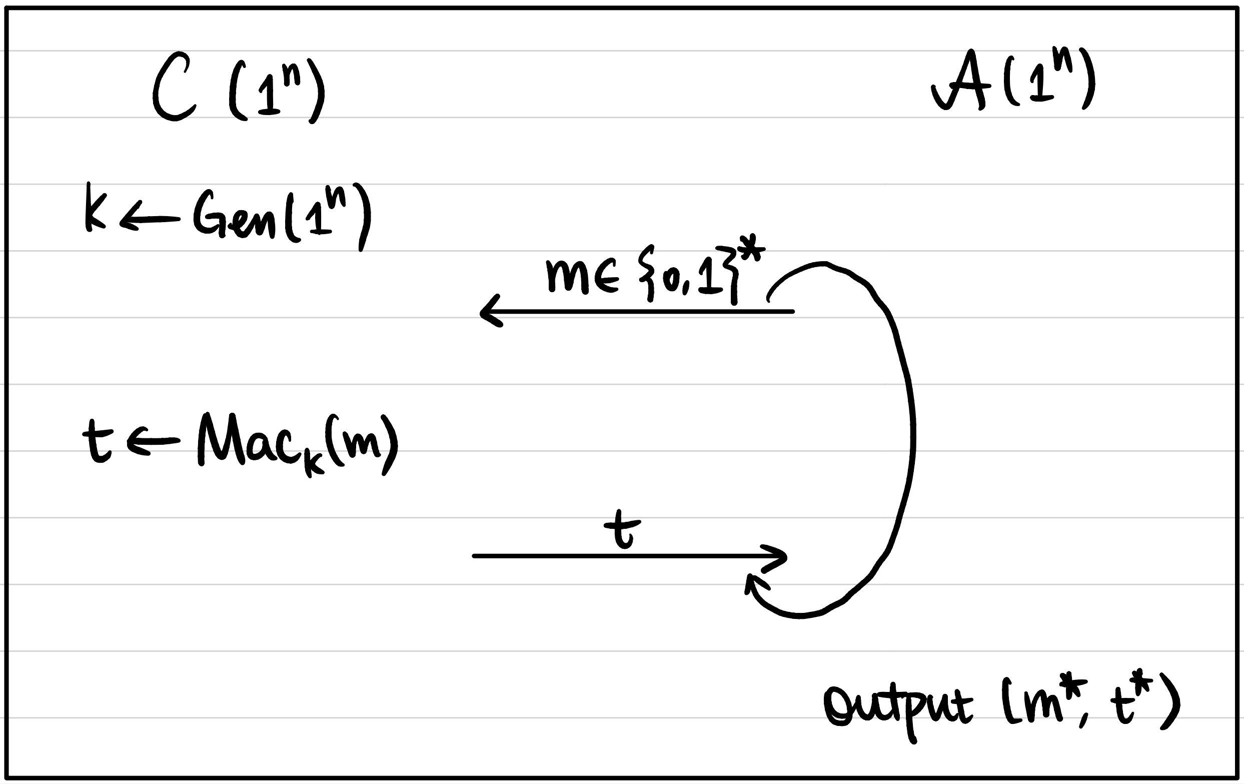
- **Canonical Verification:**

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

Message Authentication Code (MAC)

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

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



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

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

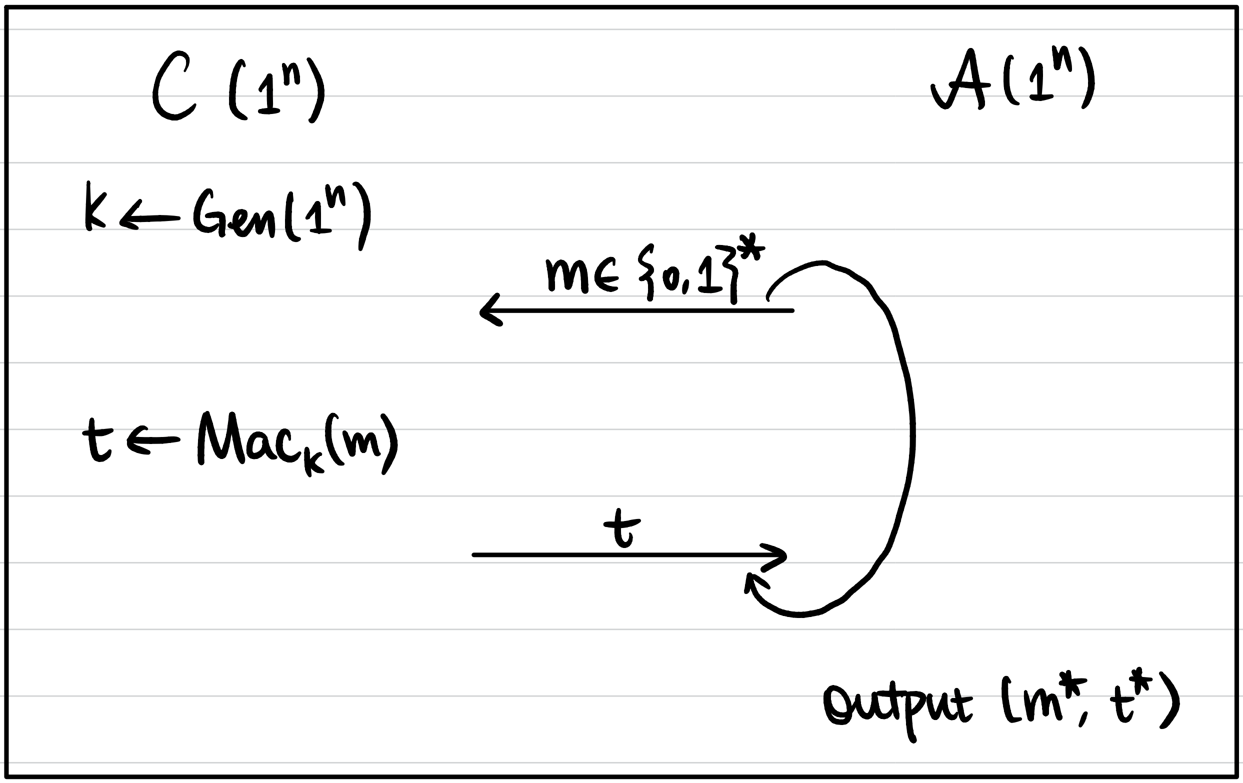
① $m^* \notin Q$, and

② $\mathsf{Vrfy}_k(m^*, t^*) = 1$.

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.

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



$Q := \{(m, t) \mid m$ 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.

Exercises

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

Construct a MAC scheme:

- $\mathrm{Gen}(1^n)$: sample $k \xleftarrow{\$} \{0,1\}^n$, output k.
- $\mathrm{Mac}_k(m)$: $m \in \{0,1\}^{2n-2}$

  $m = m_0 \| m_1$, $m_0, m_1 \in \{0,1\}^{n-1}$

  output $t := F_k(0\|m_0) \| F_k(1\|m_1)$
- $\mathrm{Vrfy}_k(m,t)$: $\mathrm{Mac}_k(m) \stackrel{?}{=} t$

Is this MAC scheme necessarily secure?

Exercises

Given a secure MAC scheme $\Pi = (\mathrm{Gen}, \mathrm{Mac}, \mathrm{Vrfy})$, construct another MAC scheme $\tilde{\Pi} = (\widetilde{\mathrm{Gen}}, \widetilde{\mathrm{Mac}}, \widetilde{\mathrm{Vrfy}})$ that is secure but not 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: $\left| \Pr[\mathcal{A} \text{ succeeds in } \mathcal{H}_0] - \Pr[\mathcal{A} \text{ succeeds in } \mathcal{H}_1] \right| \le negl(n)$.

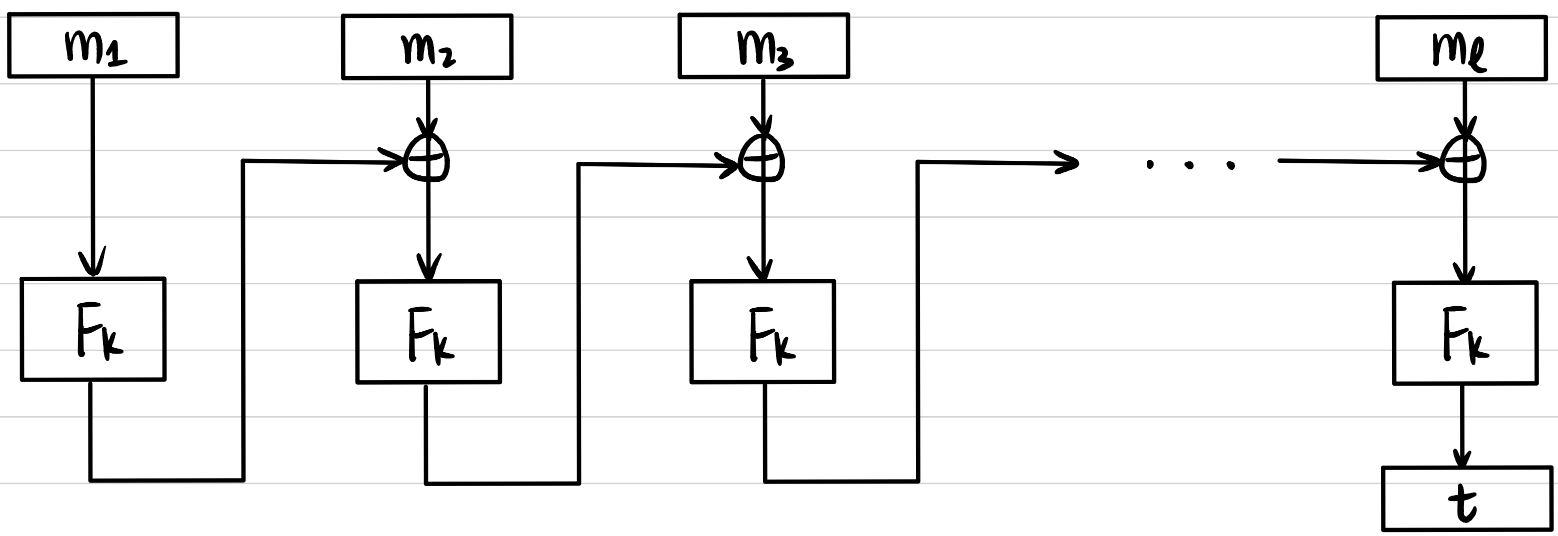
Step 2: $\Pr[\mathcal{A} \text{ succeeds in } \mathcal{H}_1] \le negl(n)$.

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 $\ell(n) \cdot n$:

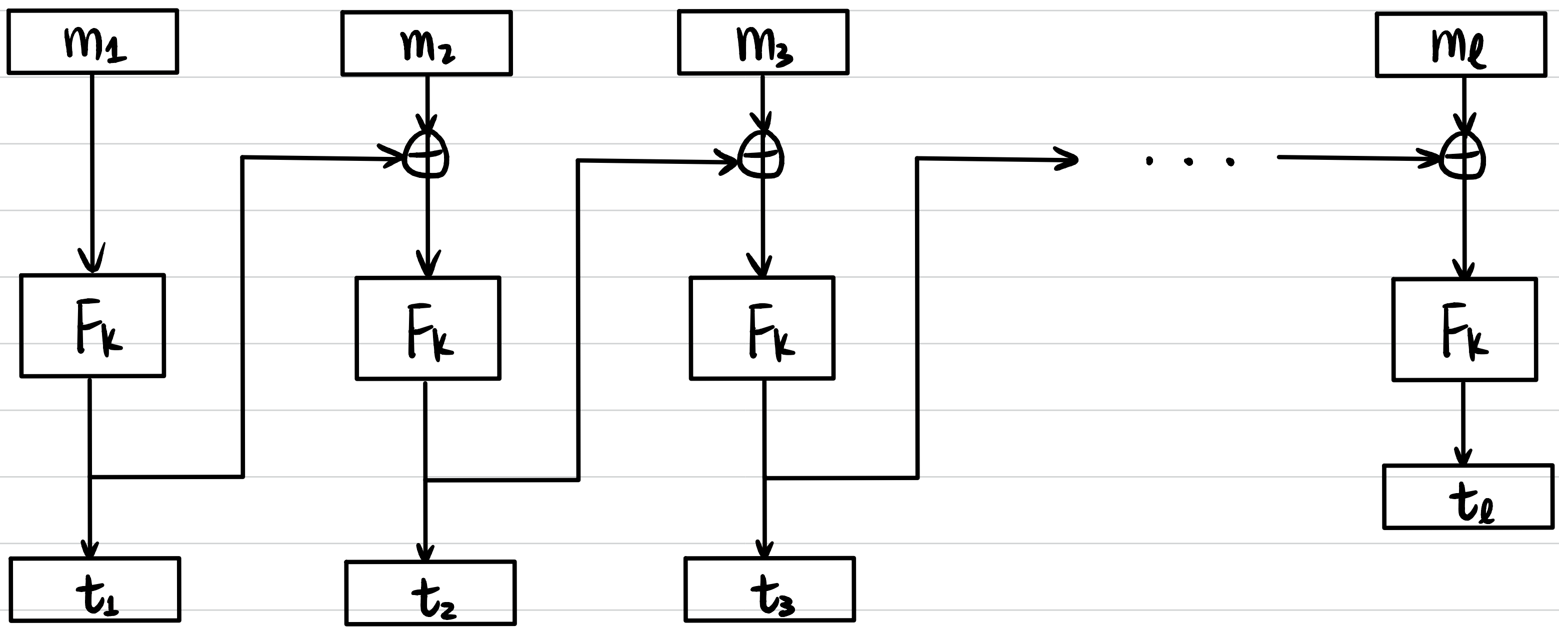
- $Gen(1^n)$: sample $k \xleftarrow{\$} \{0,1\}^n$, output k.
- $Mac_k(m)$: $m \in \{0,1\}^{\ell(n)\cdot n}$ $\quad m = m_1 \| m_2 \| \cdots \| m_\ell \quad m_i \in \{0,1\}^n$



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

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

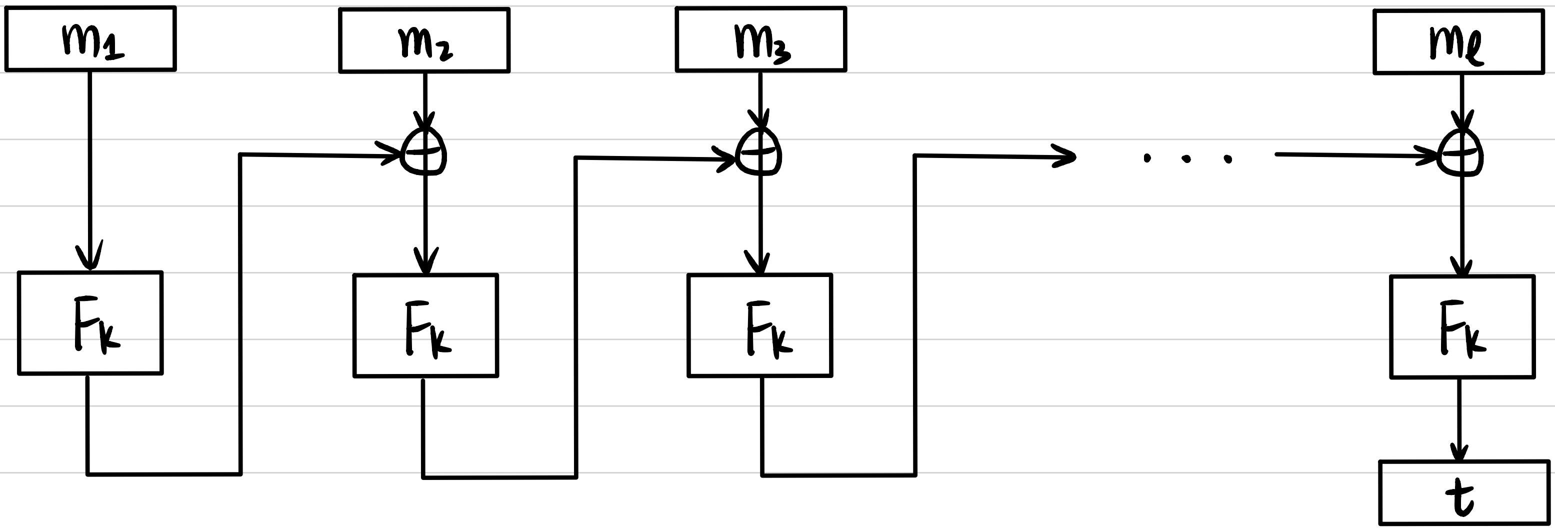
Exercises



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

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

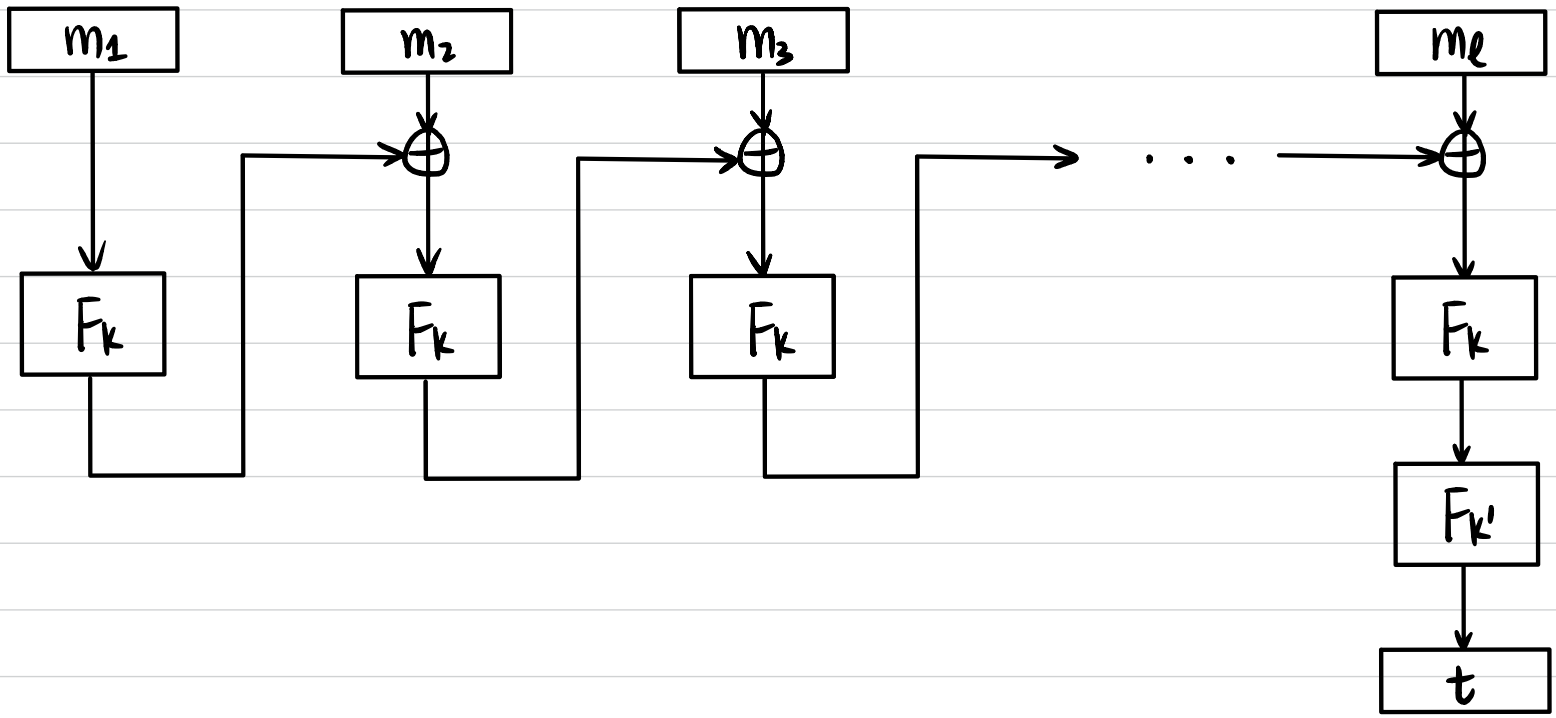
Exercises



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

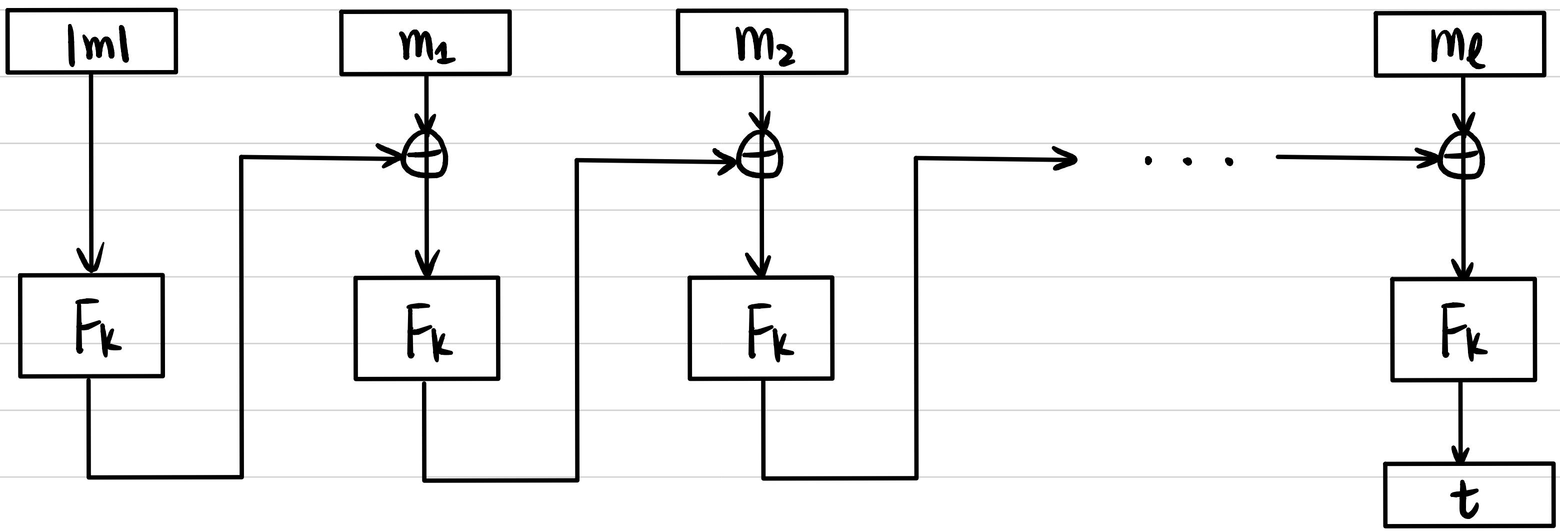
MAC for messages of arbitrary length (multiple of n)

Approach 1: MAC of CBC-MAC

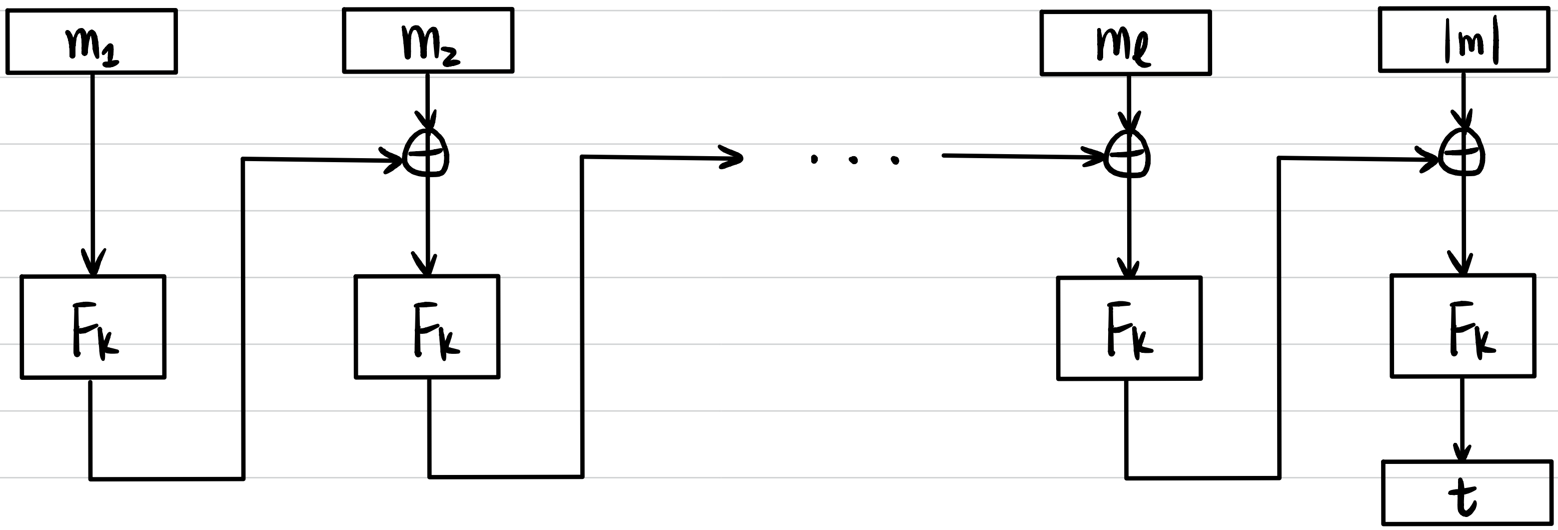


MAC for messages of arbitrary length (multiple of n)

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



Exercises



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