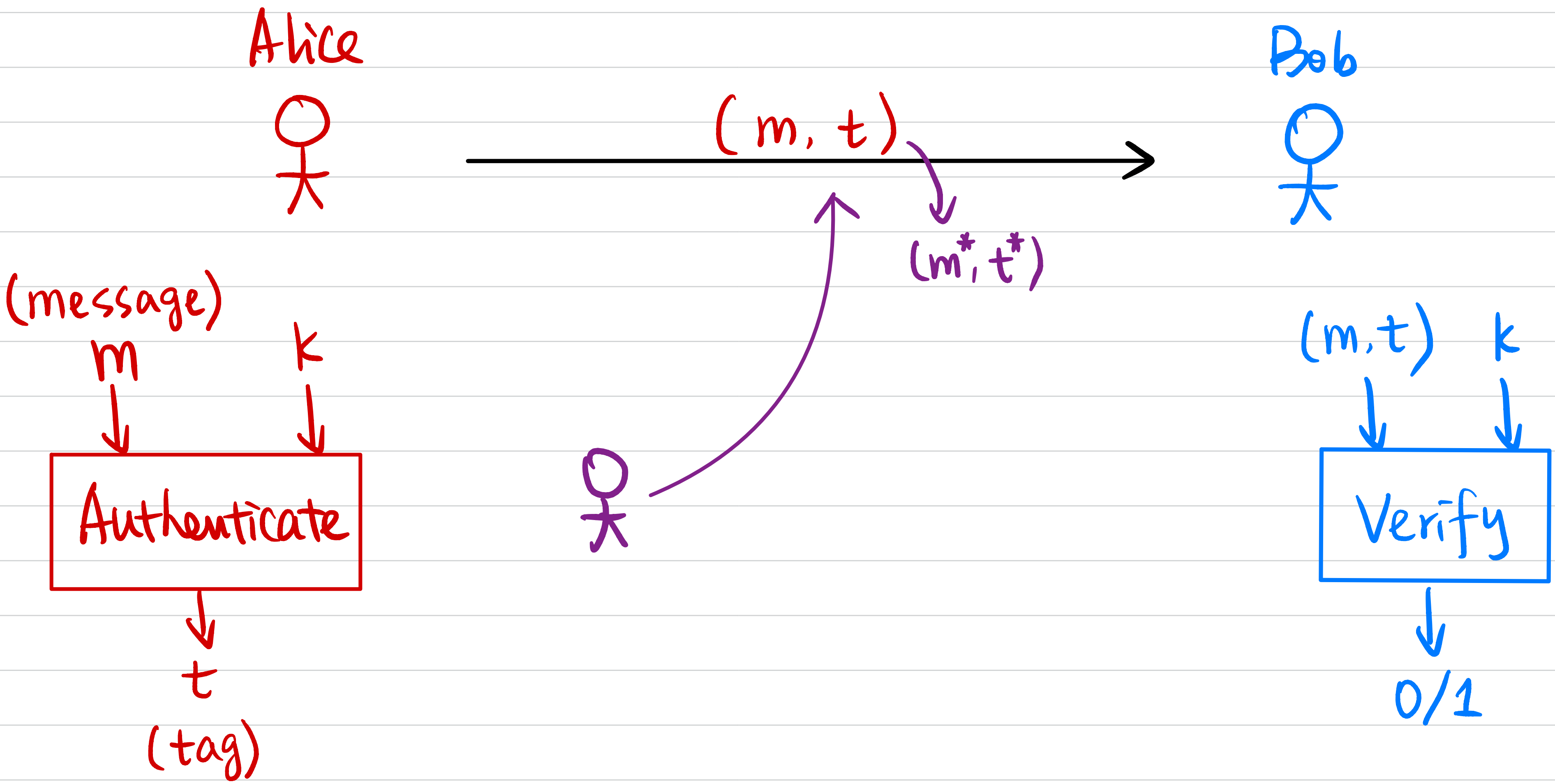
CSCI 1510

- 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):

  $$k \leftarrow Gen(1^n)$$

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

  $$0/1 := Vrfy_k(m,t)$$

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

  $$Vrfy_k(m, Mac_k(m)) = 1$$

- **Canonical Verification:**

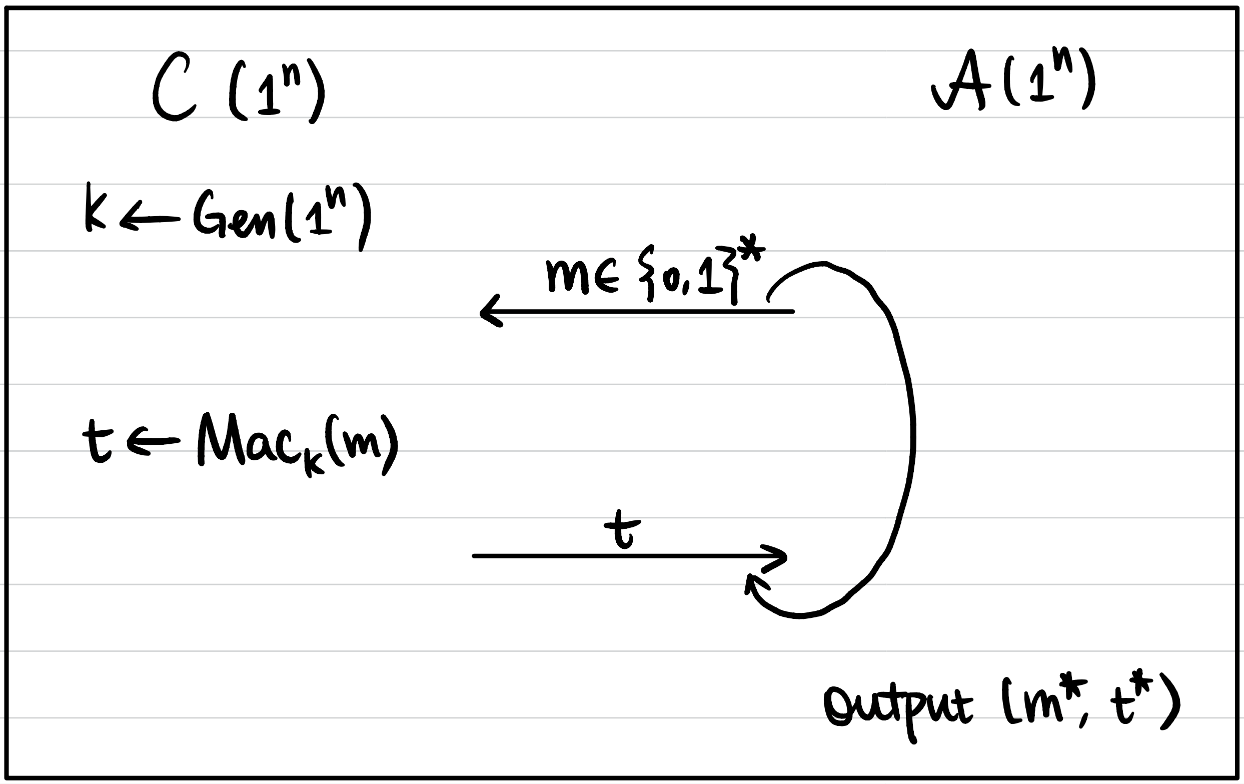
  If $Mac_k(m)$ is derterministic, then $Vrfy_k(m,t)$ is straightforward.

  $$Mac_k(m) \stackrel{?}{=} t$$

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 message 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.

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

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

$m^* \neq m$

Exercises

Let $F: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ 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?

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

$\xleftarrow{m = m_0 \| m_1}$

$\xrightarrow{t = t_0 \| t_1}$ $\Rightarrow$ $t_0 = F_k(0\|m_0)$, $t_1 = F_k(1\|m_1)$

$\xleftarrow{m = m_0' \| m_1'}$

$\xrightarrow{t = t_0' \| t_1'}$ $\Rightarrow$ $t_0' = F_k(0\|m_0')$, $t_1' = F_k(1\|m_1')$

Output $m^* = m_0 \| m_1'$

$t^* = t_0 \| t_1'$

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.

Step 1: Construct $\tilde{\Pi}$ from Π

- $\widetilde{\mathrm{Gen}}(1^n)$: $k \leftarrow \mathrm{Gen}(1^n)$, output k
- $\widetilde{\mathrm{Mac}}_k(m)$: $t \leftarrow \mathrm{Mac}_k(m)$, $b \xleftarrow{\$} \{0,1\}$, output $\tilde{t} = t \| b$.
- $\widetilde{\mathrm{Vrfy}}_k(m, \tilde{t})$: Parse $\tilde{t} = t \| b$. Output $\mathrm{Vrfy}_k(m, t)$

Step 2: If Π is secure, then $\tilde{\Pi}$ is also secure.

Step 3: $\tilde{\Pi}$ is not strongly secure.

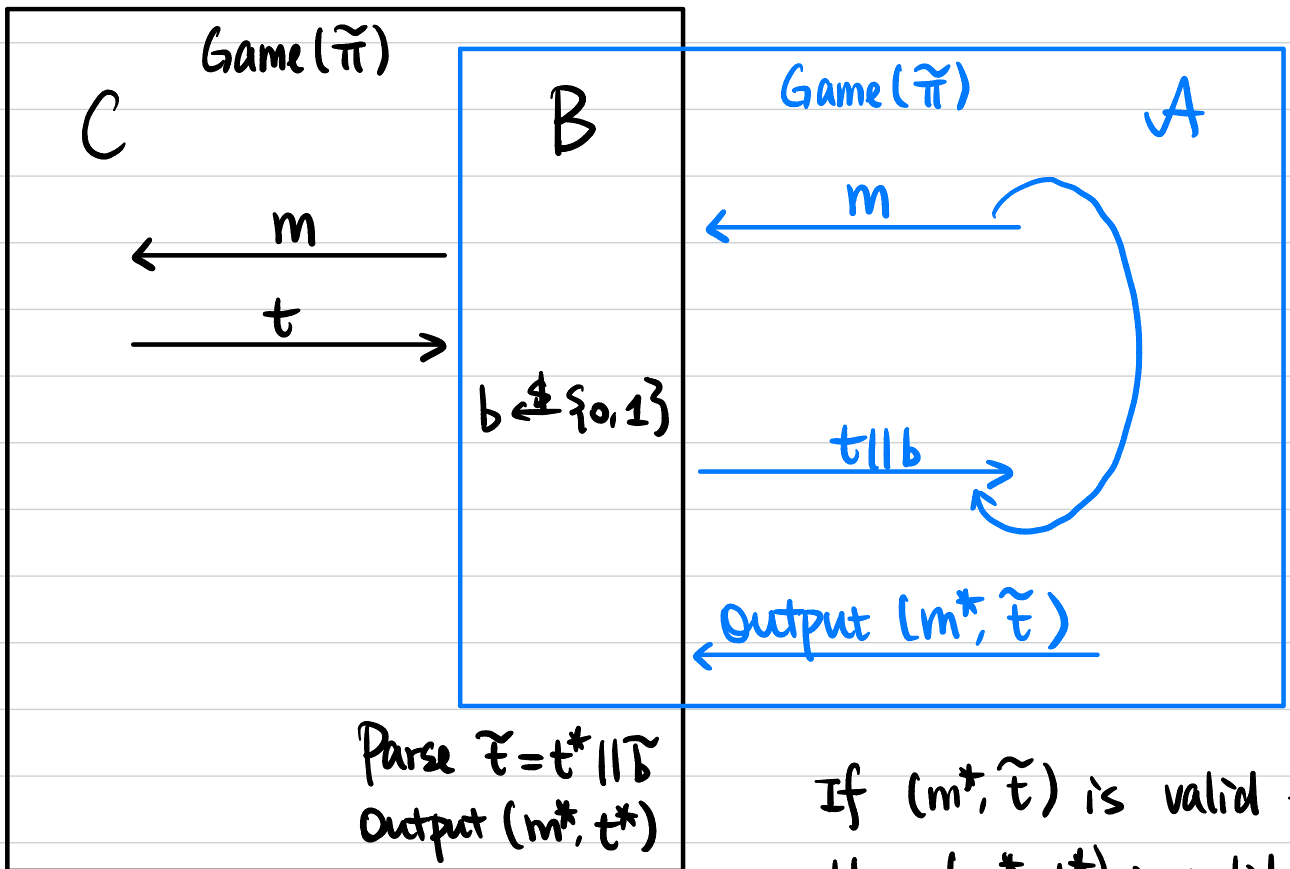
$$\begin{array}{ccc} \mathcal{C} & & \mathcal{A} \\ & \xleftarrow{\quad m \quad} & \\ & \xrightarrow{\tilde{t} = t \| b} & \end{array}$$

Output $m^* = m$

$t^* = t \| \bar{b}$

Step 2: If Π is secure, then $\tilde{\Pi}$ is also secure.

Proof Assume not, then $\exists$ PPT $\mathcal{A}$ that breaks the security of $\tilde{\Pi}$.
We construct PPT B to break the security of Π.



If $(m^*, \tilde{t})$ is valid for $\tilde{\Pi}$,
then (m^*, t^*) is valid for Π.

$\Pr[B \text{ succeeds in } \Pi] = \Pr[\mathcal{A} \text{ succeeds in } \tilde{\Pi}] \geq \text{non-negl}(n)$.

Fixed-Length MAC

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

Construct a MAC scheme:

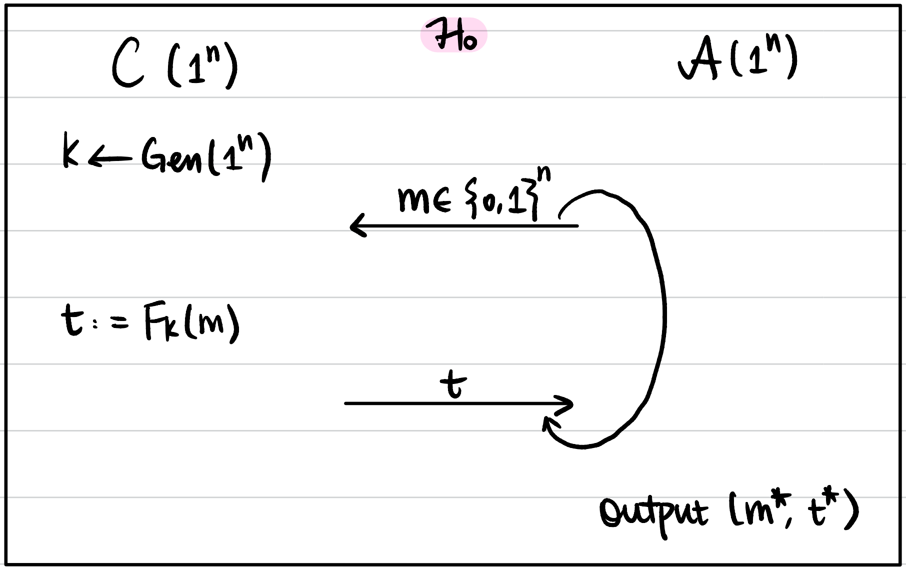
- $\mathrm{Gen}(1^n)$: sample $k \xleftarrow{\$} \{0,1\}^n$, output k.
- $\mathrm{Mac}_k(m)$: $m \in \{0,1\}^n$

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

$$m \to \boxed{F_k} \to t$$

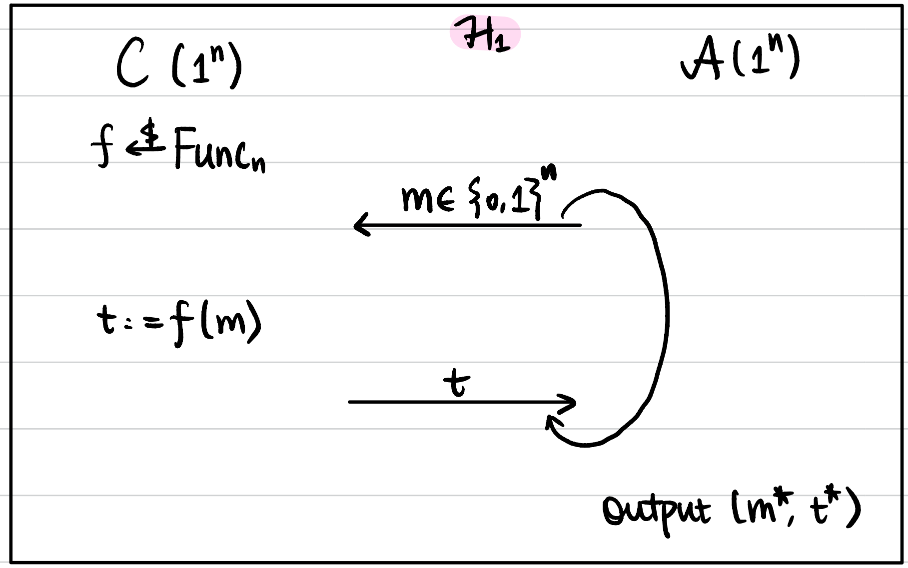
<u>Thm</u> If F is a PRF, then $\Pi = (\mathrm{Gen}, \mathrm{Mac}, \mathrm{Vrfy})$ is a secure MAC scheme for fixed-length messages of length n.

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



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

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



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

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

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

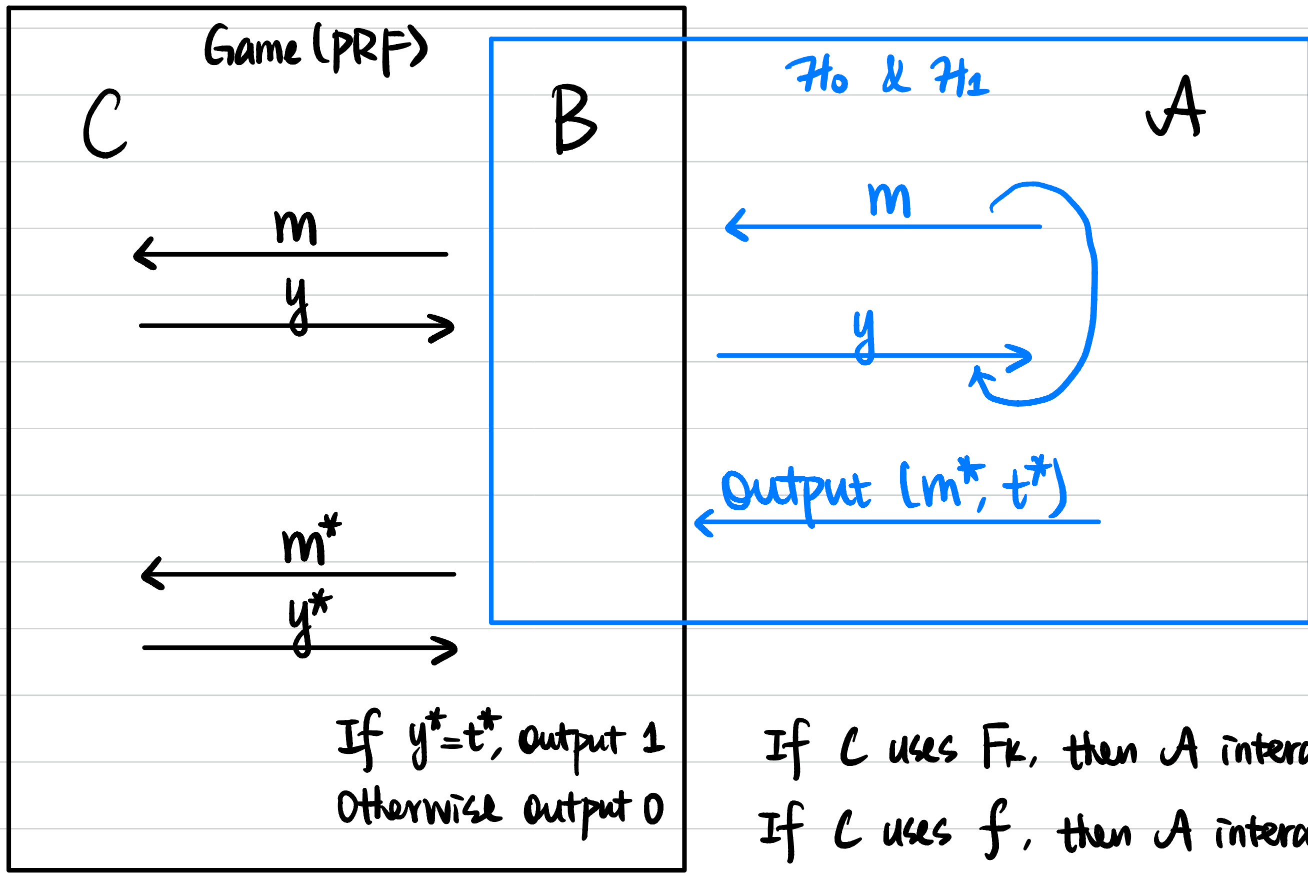
Step 2: $\underbrace{\Pr[\mathcal{A} \text{ succeeds in } \mathcal{H}_1]}_{= 2^{-n}} \le \text{negl}(n)$.

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

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

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

We construct PPT B to break the pseudorandomness of F.



If C uses F_k, then $\mathcal{A}$ interacts with $\mathcal{H}_0$

If C uses f, then $\mathcal{A}$ interacts with $\mathcal{H}_1$

$$\left|\Pr[B^{F_k(\cdot)} \text{ outputs } 1] - \Pr[B^{f(\cdot)} \text{ outputs } 1]\right|$$

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

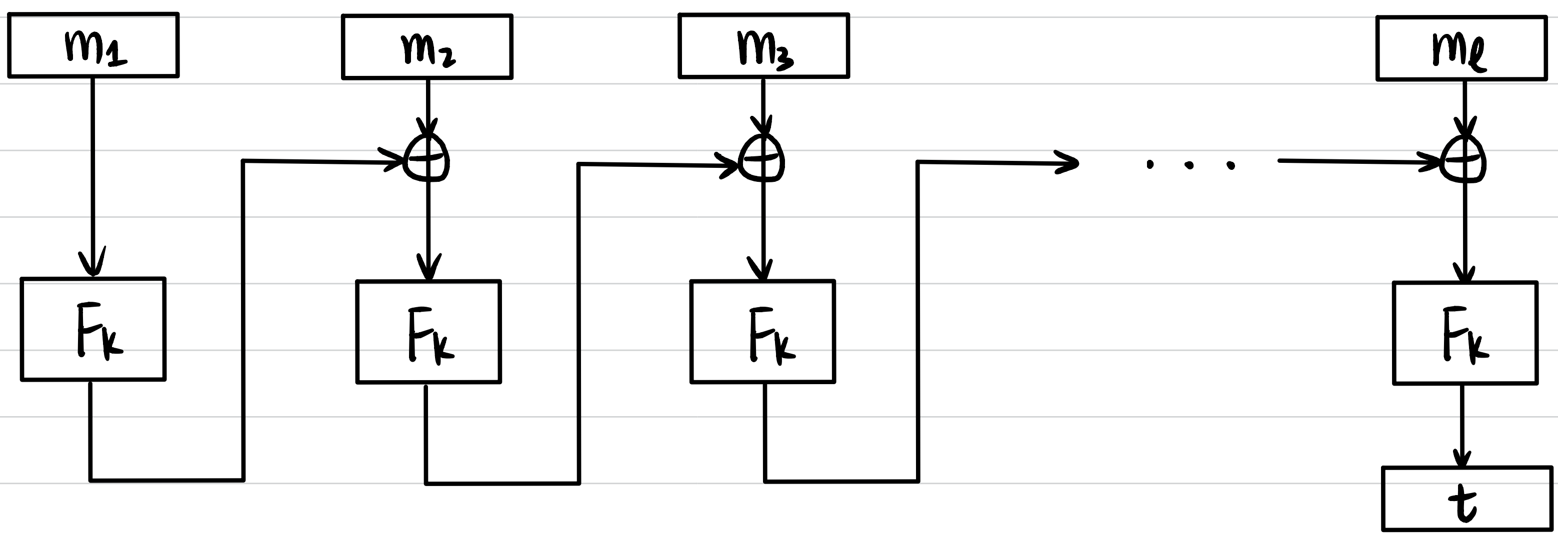
$$\ge \text{non-negl}(n).$$

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 $\ell(n) \cdot n$:

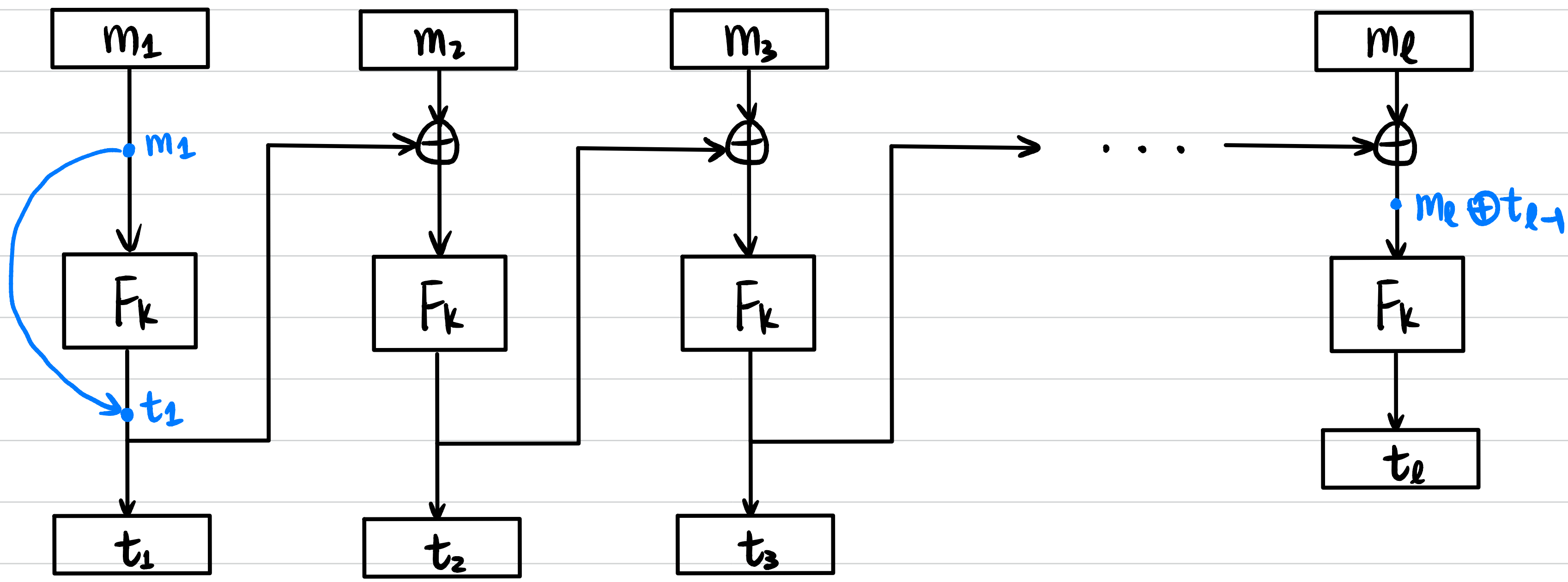
- $Gen(1^n)$: sample $k \xleftarrow{\$} \{0,1\}^n$, output k.
- $Mac_k(m)$: $m \in \{0,1\}^{\ell(n) \cdot n}$ $\quad m = m_1 \| m_2 \| \cdots \| m_\ell \quad m_i \in \{0,1\}^n$



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

Thm 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 $\ell(n) \cdot n$.

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

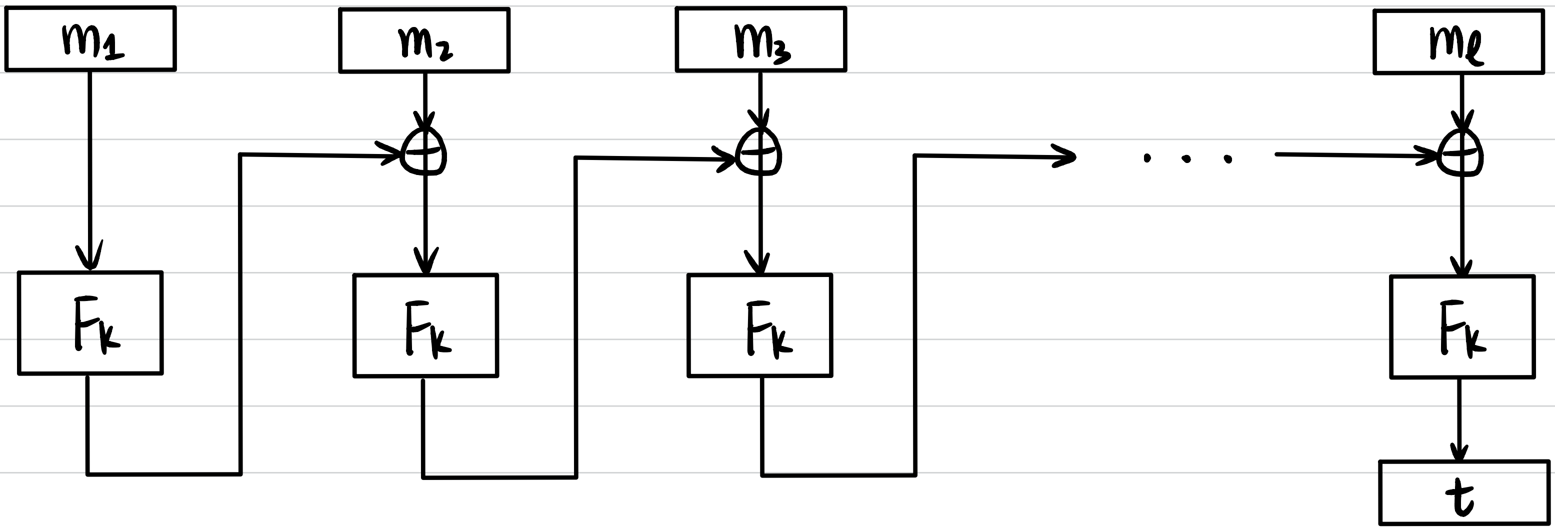
$\xleftarrow{m = m_1 \| \cdots \| m_\ell}$

$\xrightarrow{t = t_1 \| \cdots \| t_\ell}$

Output $m^* = m_1 \| \cdots \| m_{\ell-1} \| m_1 \oplus t_{\ell-1}$

$t^* = t_1 \| \cdots \| t_{\ell-1} \| t_1$

Exercises



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

C $\quad\quad\quad$ $\mathcal{A}$

$\xleftarrow{m_1 \in \{0,1\}^n}$

$\xrightarrow{t_1}$

$\xleftarrow{m_2 \in \{0,1\}^n}$

$\xrightarrow{t_2}$

Output $m^* = m_1 \| t_1 \oplus m_2$

$t^* = t_2$