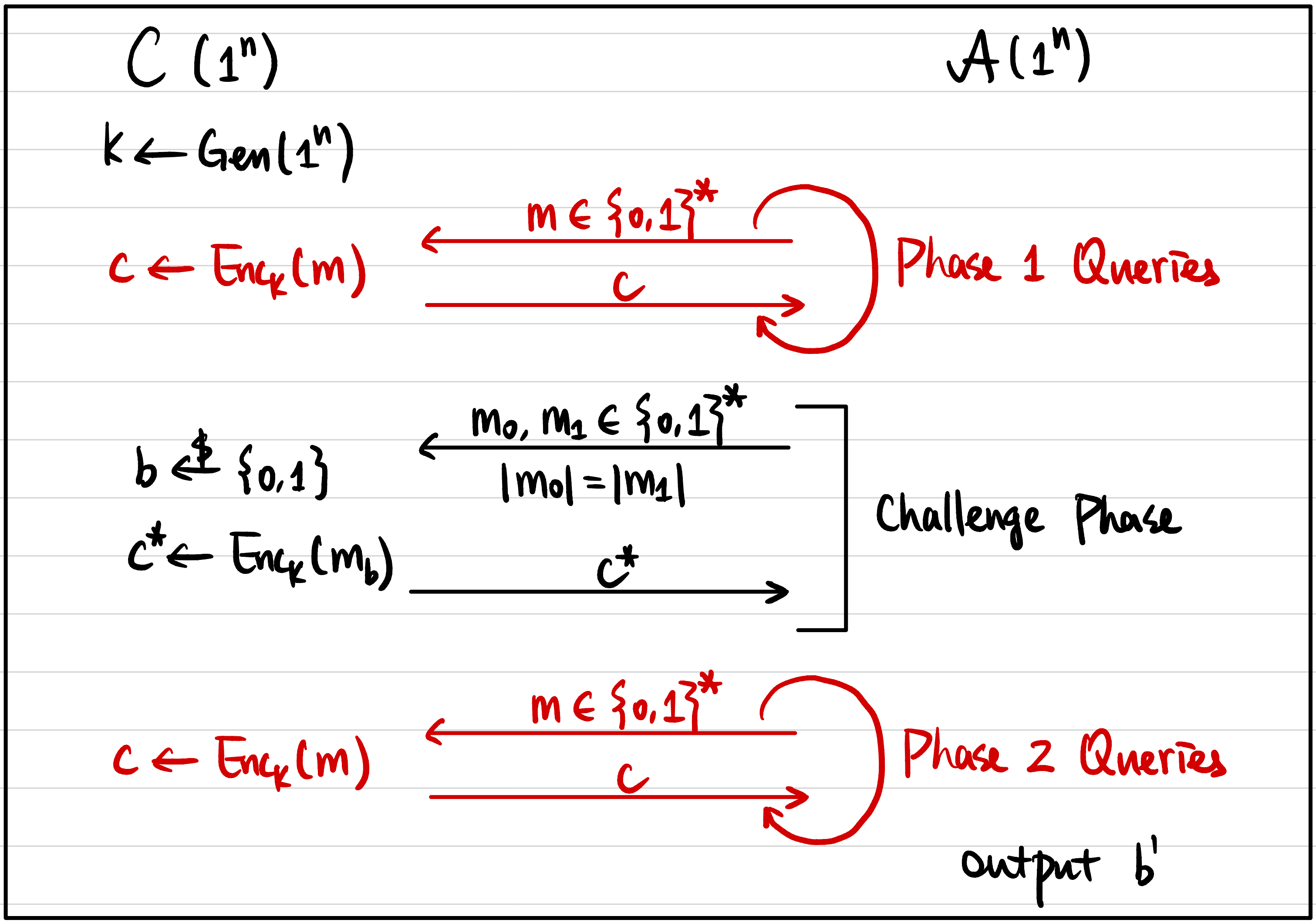
CSCI 1510

- Pseudorandom Function (continued)
- CPA-Secure Encryption from PRF
- Hybrid Argument
- Message Authentication Code (MAC)

Chosen Plaintext Attack (CPA) Security

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



Pseudorandom Function (PRF)

Def Let $F: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a deterministic, poly-time, keyed function. F is a pseudorandom function (PRF) if $\forall$PPT $\mathcal{A}$, $\exists$ negligible function $\varepsilon(\cdot)$ s.t. $\Pr[b = b'] \le \frac{1}{2} + \varepsilon(n)$

$C(1^n)$		$\mathcal{A}(1^n)$
$b \xleftarrow{\$} \{0,1\}$		
If $b=0$, then $k \xleftarrow{\$} \{0,1\}^n$	$\{F \mid F: \{0,1\}^n \to \{0,1\}^n\}$	
If $b=1$, then $f \xleftarrow{\$} \mathrm{Func}_n$		
	$\xleftarrow{\quad x \quad}$	
If $b=0$, then $y := F_k(x)$		
If $b=1$, then $y := f(x)$	$\xrightarrow{\quad y \quad}$	
		output b'

Exercises

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

Define $F': \{0,1\}^n \times \{0,1\}^{n-1} \to \{0,1\}^{2n}$ as follows.

Is F' necessarily a PRF?

a) $F'_k(x) = F_k(0\|x) \,\|\, F_k(0\|x)$ $\qquad F_k(0\,\boxed{\;x\;}) \,\|\, F_k(0\,\boxed{\;x\;})$

b) $F'_k(x) = F_k(0\|x) \,\|\, F_k(1\|x)$ $\qquad F_k(0\,\boxed{\;x\;}) \,\|\, F_k(1\,\boxed{\;x\;})$

c) $F'_k(x) = F_k(0\|x) \,\|\, F_k(x\|0)$ $\qquad F_k(0\,\boxed{\;x\;}) \,\|\, F_k(\boxed{\;x\;}\,0)$

d) $F'_k(x) = F_k(0\|x) \,\|\, F_k(x\|1)$ $\qquad F_k(0\,\boxed{\;x\;}) \,\|\, F_k(\boxed{\;x\;}\,1)$

a) C $\qquad$ A

$C \xleftarrow{\;x\;} A$

$C \xrightarrow{\;y_1 \| y_2\;} A$

$y_1 \stackrel{?}{=} y_2$

c) C $\qquad$ A

$C \xleftarrow{\;x = 0\cdots0\;} A$

$C \xrightarrow{\;y_1 \| y_2\;} A$

$y_1 \stackrel{?}{=} y_2$

d) C $\qquad$ A

$C \xleftarrow{\;x_1 = 0\cdots0\;} A$

$C \xrightarrow{\;y_1 \| y_2\;} A$

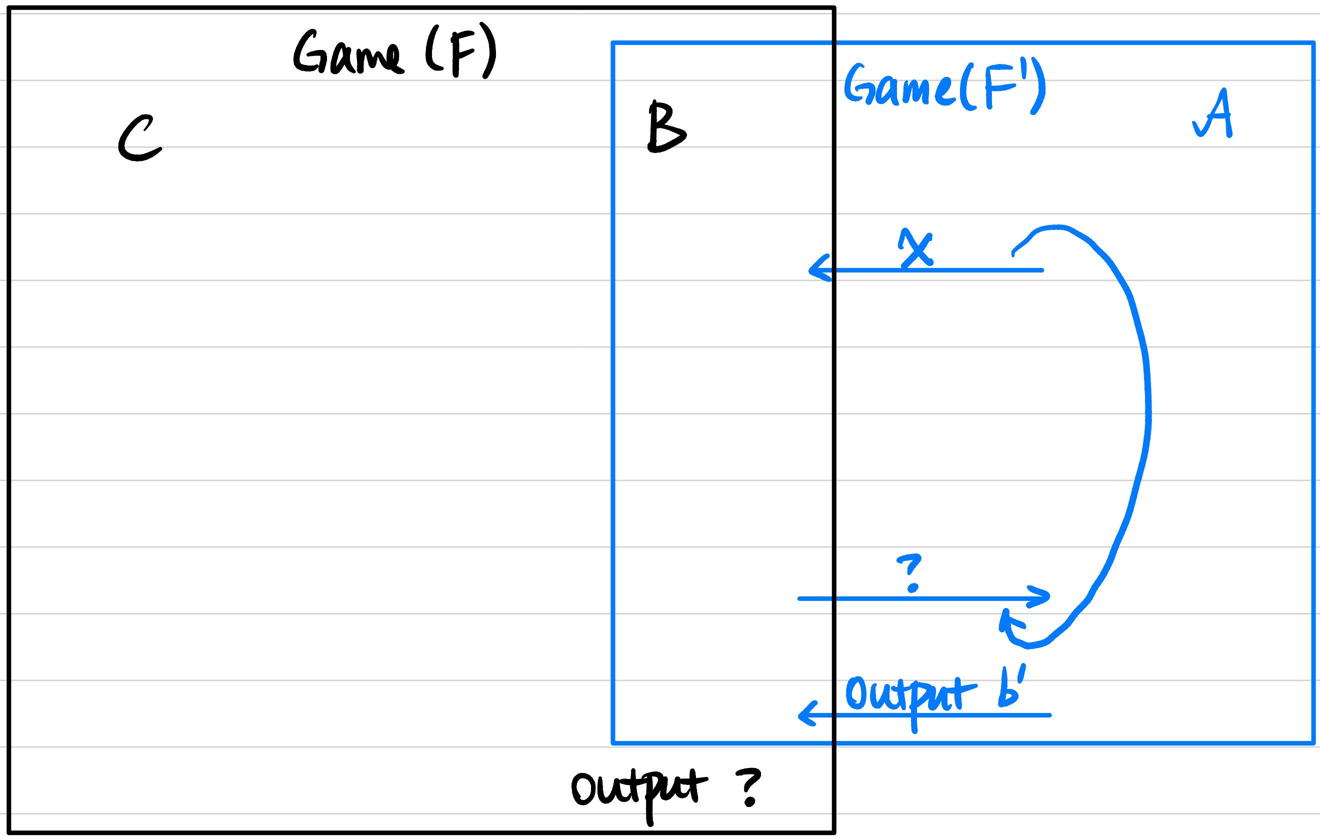
$C \xleftarrow{\;x_2 = 0\cdots1\;} A$

$C \xrightarrow{\;y_3 \| y_4\;} A$

$y_2 \stackrel{?}{=} y_3$

b) $F'_k(x) = F_k(0||x) \,||\, F_k(1||x)$ is a PRF

Proof Assume not, then $\exists$ PPT $\mathcal{A}$ that breaks the pseudorandomness of F'.
We construct PPT B to break the pseudorandomness of F.



PRF $\Leftrightarrow$ PRG

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

Construct $G: \{0,1\}^n \to \{0,1\}^{2n}$

"$\Leftarrow$": Let $G: \{0,1\}^n \to \{0,1\}^{2n}$ be a PRG,

Construct $F: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$

Constructing CPA-Secure Encryption

Pseudorandom Function (PRF)

$$\Downarrow$$

CPA-Secure Encryption

CPA-Secure Encryption Scheme

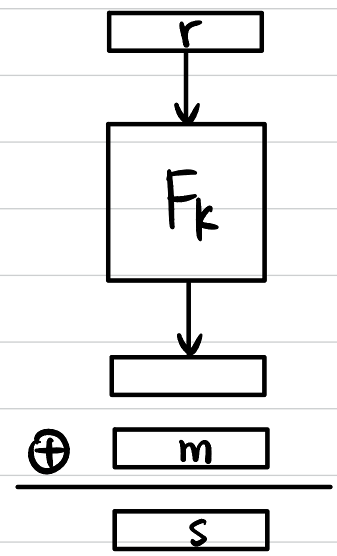
Let $F: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a PRF,

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

  $r \xleftarrow{\$} \{0,1\}^n$

  output $c := \langle r, F_k(r) \oplus m \rangle$
- $Dec_k(c)$: $c = \langle r, s \rangle$

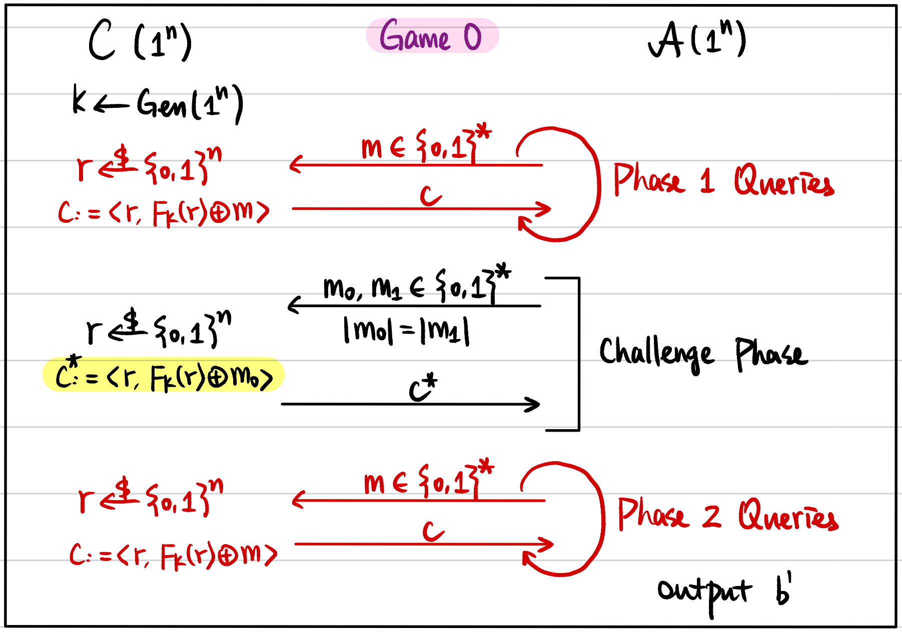
  output $m := F_k(r) \oplus s$

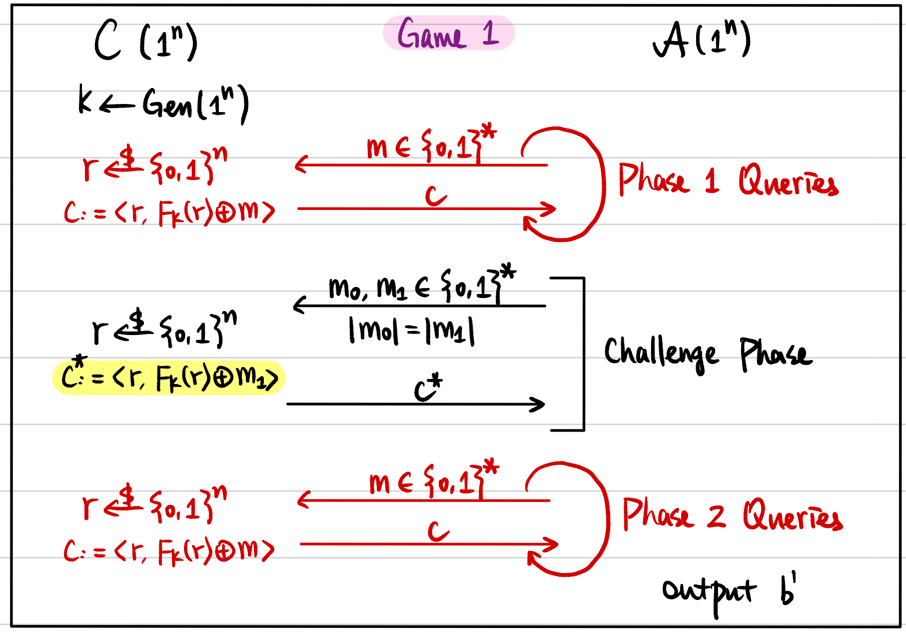


Theorem If F is a PRF, then $\Pi = (Gen, Enc, Dec)$ is CPA-Secure.

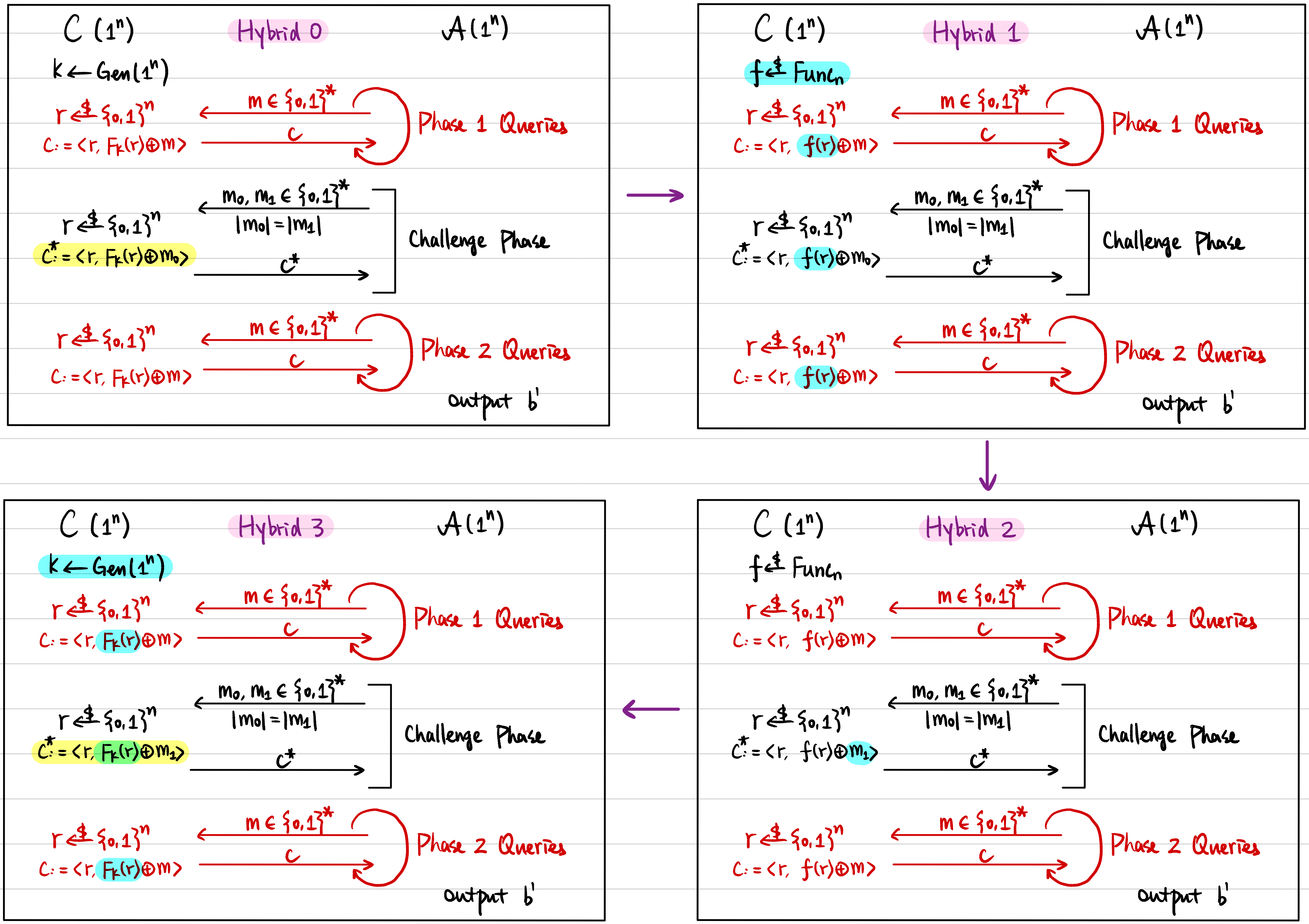
Theorem If F is a PRF, then $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ is CPA-Secure.

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





$$\left| \Pr[\mathcal{A} \text{ outputs } 1 \text{ in Game } 0] - \Pr[\mathcal{A} \text{ outputs } 1 \text{ in Game } 1] \right| \le \mathrm{negl}(n) \; ?$$


Hybrid 0
$\mathcal{C}(1^n)$
$\mathcal{A}(1^n)$
$k \leftarrow Gen(1^n)$
$r \xleftarrow{\$} \{0,1\}^n$
$c := \langle r, F_k(r) \oplus m \rangle$
$m \in \{0,1\}^*$
c
Phase 1 Queries
$r \xleftarrow{\$} \{0,1\}^n$
$c^* := \langle r, F_k(r) \oplus m_0 \rangle$
$m_0, m_1 \in \{0,1\}^*$
$|m_0| = |m_1|$
c^*
Challenge Phase
$r \xleftarrow{\$} \{0,1\}^n$
$c := \langle r, F_k(r) \oplus m \rangle$
$m \in \{0,1\}^*$
c
Phase 2 Queries
output b'
Hybrid 1
$\mathcal{C}(1^n)$
$\mathcal{A}(1^n)$
$f \xleftarrow{\$} Func_n$
$r \xleftarrow{\$} \{0,1\}^n$
$c := \langle r, f(r) \oplus m \rangle$
$m \in \{0,1\}^*$
c
Phase 1 Queries
$r \xleftarrow{\$} \{0,1\}^n$
$c^* := \langle r, f(r) \oplus m_0 \rangle$
$m_0, m_1 \in \{0,1\}^*$
$|m_0| = |m_1|$
c^*
Challenge Phase
$r \xleftarrow{\$} \{0,1\}^n$
$c := \langle r, f(r) \oplus m \rangle$
$m \in \{0,1\}^*$
c
Phase 2 Queries
output b'
Hybrid 3
$\mathcal{C}(1^n)$
$\mathcal{A}(1^n)$
$k \leftarrow Gen(1^n)$
$r \xleftarrow{\$} \{0,1\}^n$
$c := \langle r, F_k(r) \oplus m \rangle$
$m \in \{0,1\}^*$
c
Phase 1 Queries
$r \xleftarrow{\$} \{0,1\}^n$
$c^* := \langle r, F_k(r) \oplus m_1 \rangle$
$m_0, m_1 \in \{0,1\}^*$
$|m_0| = |m_1|$
c^*
Challenge Phase
$r \xleftarrow{\$} \{0,1\}^n$
$c := \langle r, F_k(r) \oplus m \rangle$
$m \in \{0,1\}^*$
c
Phase 2 Queries
output b'
Hybrid 2
$\mathcal{C}(1^n)$
$\mathcal{A}(1^n)$
$f \xleftarrow{\$} Func_n$
$r \xleftarrow{\$} \{0,1\}^n$
$c := \langle r, f(r) \oplus m \rangle$
$m \in \{0,1\}^*$
c
Phase 1 Queries
$r \xleftarrow{\$} \{0,1\}^n$
$c^* := \langle r, f(r) \oplus m_1 \rangle$
$m_0, m_1 \in \{0,1\}^*$
$|m_0| = |m_1|$
c^*
Challenge Phase
$r \xleftarrow{\$} \{0,1\}^n$
$c := \langle r, f(r) \oplus m \rangle$
$m \in \{0,1\}^*$
c
Phase 2 Queries
output b'

$$\left| \Pr[\mathcal{A} \text{ outputs } 1 \text{ in Game } 0] - \Pr[\mathcal{A} \text{ outputs } 1 \text{ in Game } 1] \right|$$

$$= \left| \Pr[\mathcal{A} \text{ outputs } 1 \text{ in Hybrid } 0] - \Pr[\mathcal{A} \text{ outputs } 1 \text{ in Hybrid } 1] + \right.$$

$$\Pr[\mathcal{A} \text{ outputs } 1 \text{ in Hybrid } 1] - \Pr[\mathcal{A} \text{ outputs } 1 \text{ in Hybrid } 2] +$$

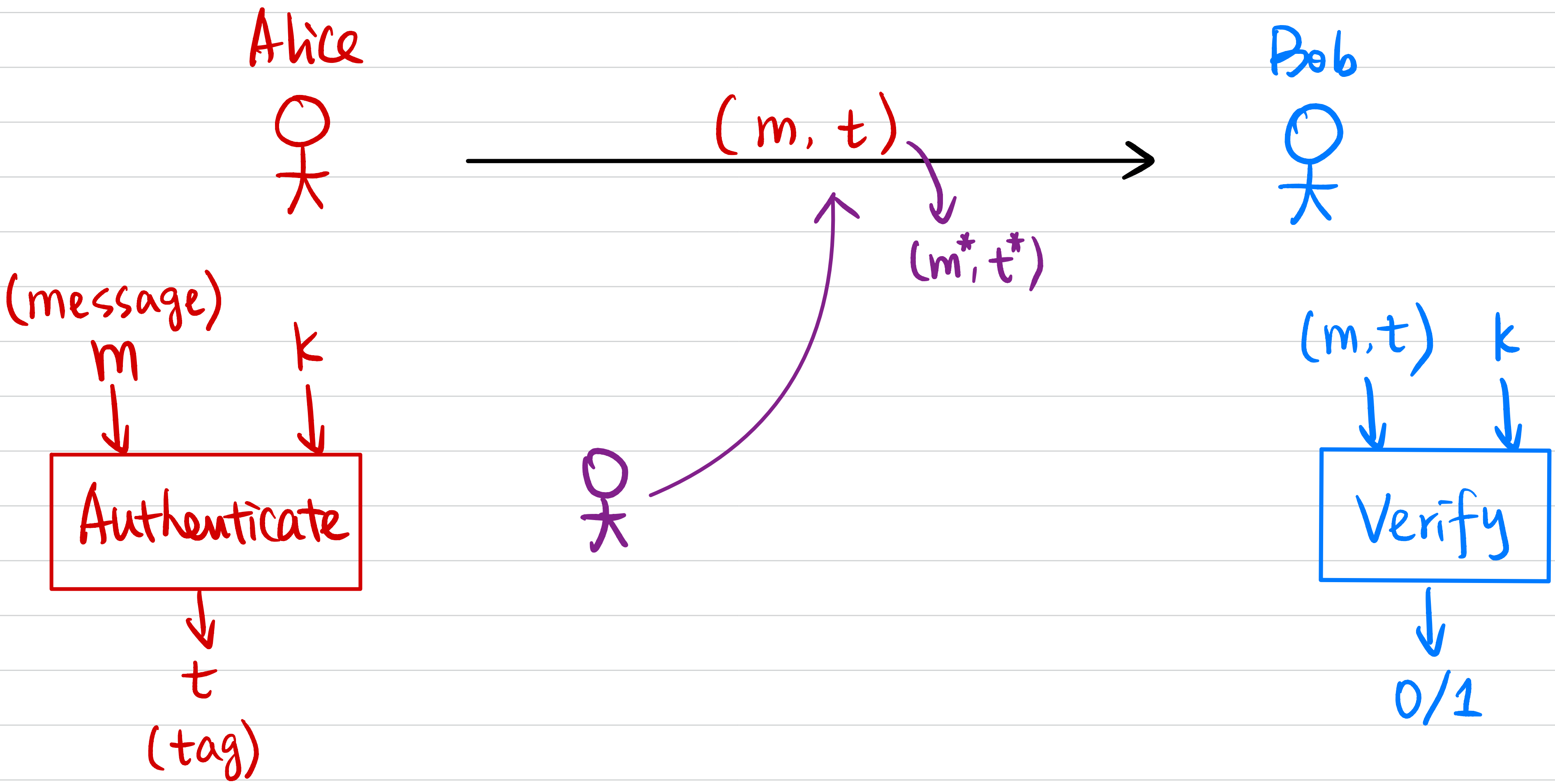
$$\left. \Pr[\mathcal{A} \text{ outputs } 1 \text{ in Hybrid } 2] - \Pr[\mathcal{A} \text{ outputs } 1 \text{ in Hybrid } 3] \right|$$

$$\leq \left| \Pr[\mathcal{A} \text{ outputs } 1 \text{ in Hybrid } 0] - \Pr[\mathcal{A} \text{ outputs } 1 \text{ in Hybrid } 1] \right| +$$

$$\left| \Pr[\mathcal{A} \text{ outputs } 1 \text{ in Hybrid } 1] - \Pr[\mathcal{A} \text{ outputs } 1 \text{ in Hybrid } 2] \right| +$$

$$\left| \Pr[\mathcal{A} \text{ outputs } 1 \text{ in Hybrid } 2] - \Pr[\mathcal{A} \text{ outputs } 1 \text{ in Hybrid } 3] \right|$$

Message Integrity



Message Integrity vs. Secrecy

Does encryption solve the problem?

- OTP?

- Pseudo OTP?

- CPA-secure encryption from PRF?

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

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

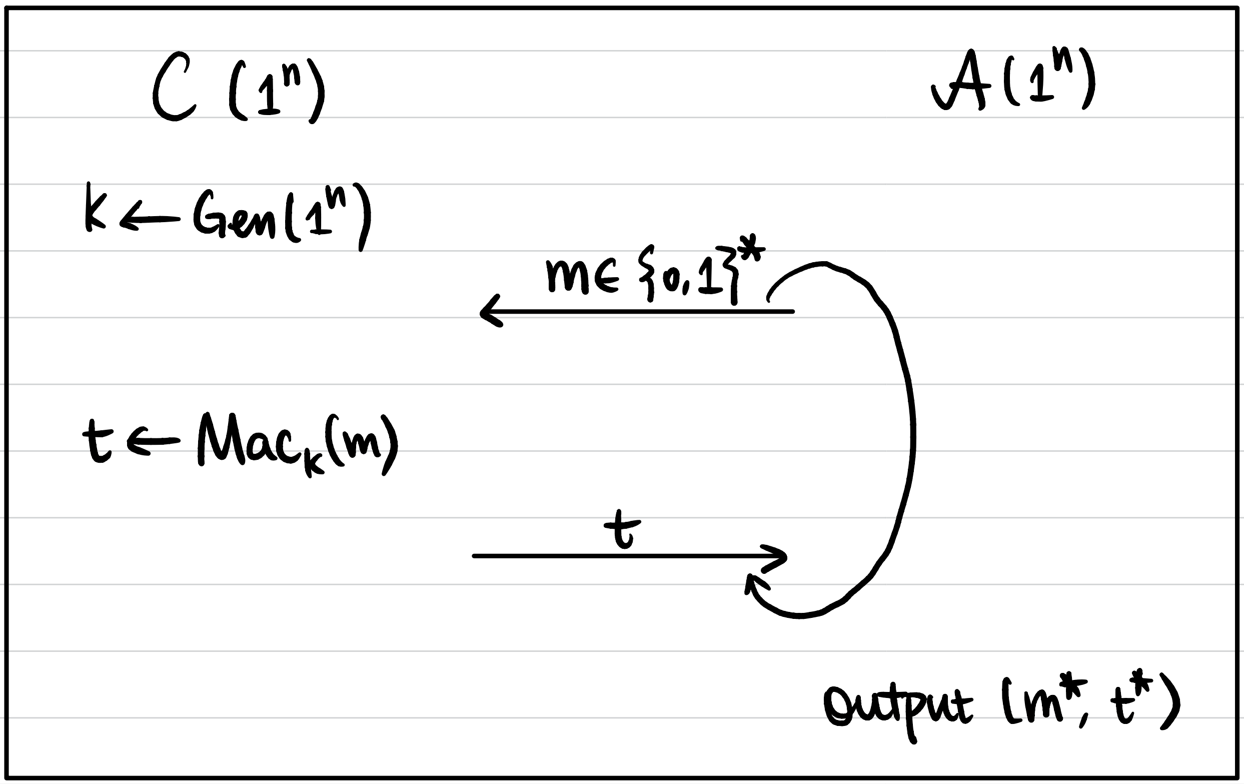
- **Canonical Verification:**

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

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.

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



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

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

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

$C(1^n)$ | $\mathcal{A}(1^n)$

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

$\xleftarrow{m \in \{0,1\}^*}$

$t \leftarrow \text{Mac}_k(m)$

$\xrightarrow{t}$

Output (m^*, t^*)

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

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

① $(m^*, t^*) \notin Q$, and

② $\text{Vrfy}_k(m^*, t^*) = 1$.

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.