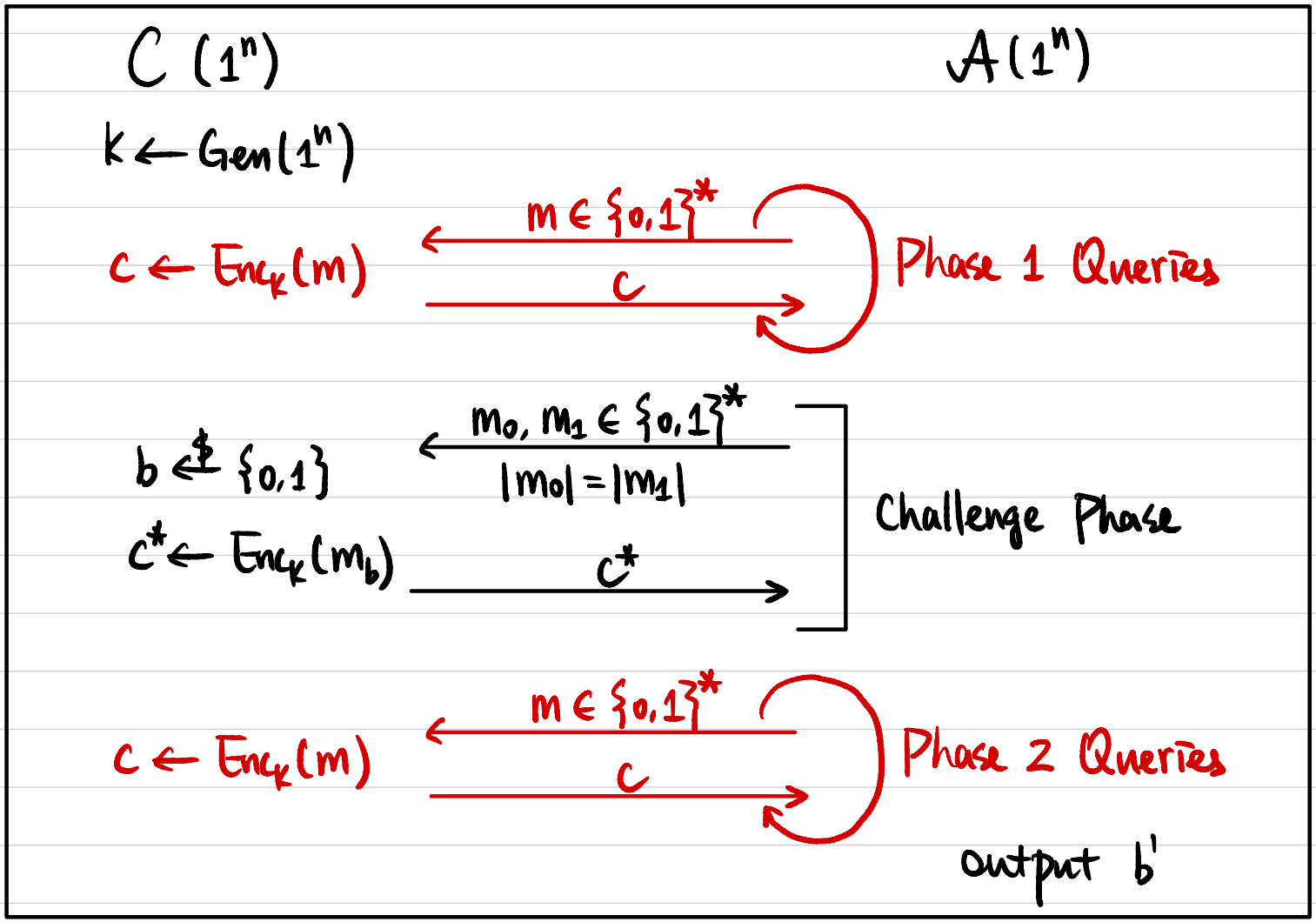
CSCI 1510

This Lecture:

- CPA-Secure Encryption from PRF (Continued)
- Hybrid Argument
- Message Authentication Code (MAC)

Chosen Plaintext Attack (CPA) Security

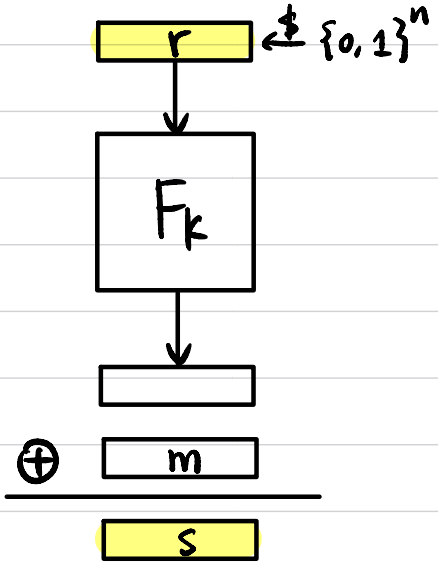
Def A symmetric-key encryption scheme (Gen, Enc, Dec) is **secure against chosen plaintext attacks**, or **CPA-secure**, if $\forall$ PPT $\mathcal{A}$, $\exists$ negligible function $\varepsilon(\cdot)$ s.t. $\Pr[b = b'] \leq \frac{1}{2} + \varepsilon(n)$



Constructing CPA-Secure Encryption

Pseudorandom Function (PRF)

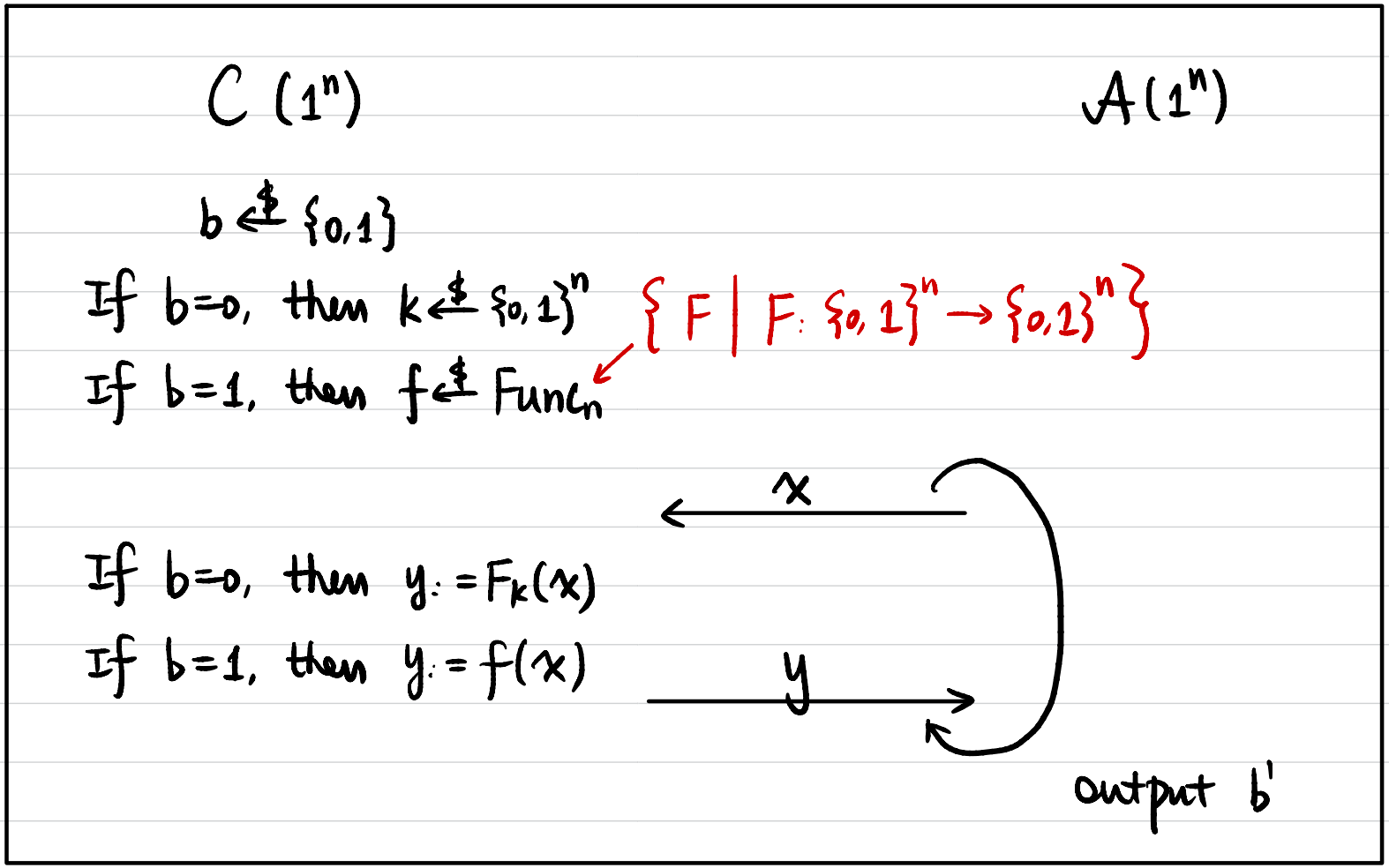
CPA-Secure Encryption



$C = \langle r, s \rangle$

Pseudorandom Function (PRF)

Def 1 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 A, $\exists$ negligible function $\varepsilon(\cdot)$ s.t. $\Pr[b = b'] \leq \frac{1}{2} + \varepsilon(n)$



CPA-Secure Encryption Scheme

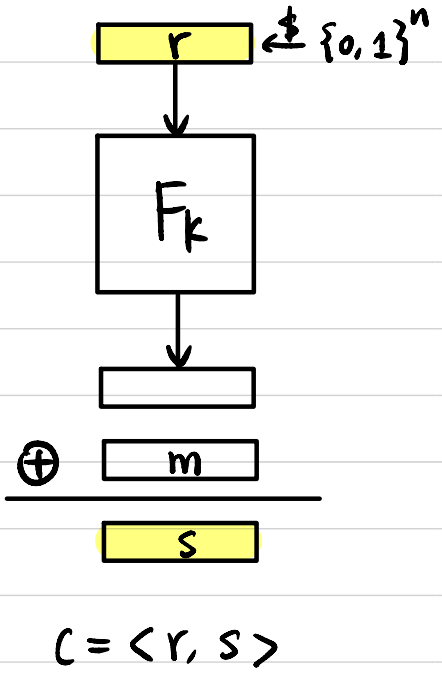
Let $F: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a PRF,

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

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

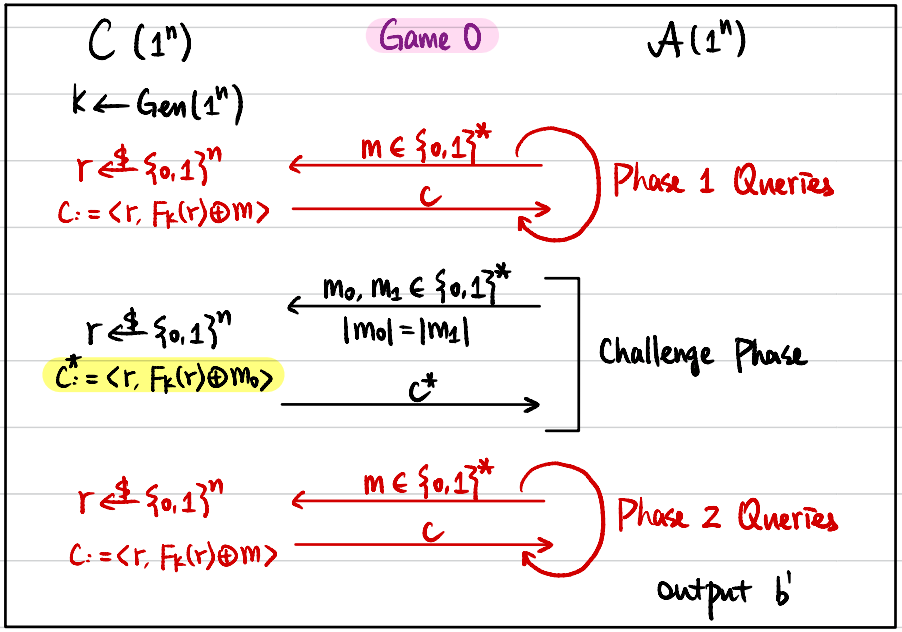
  output $c := \langle r, F_k(r) \oplus m \rangle$
- $\text{Dec}_k(c)$: $c = \langle r, s \rangle$

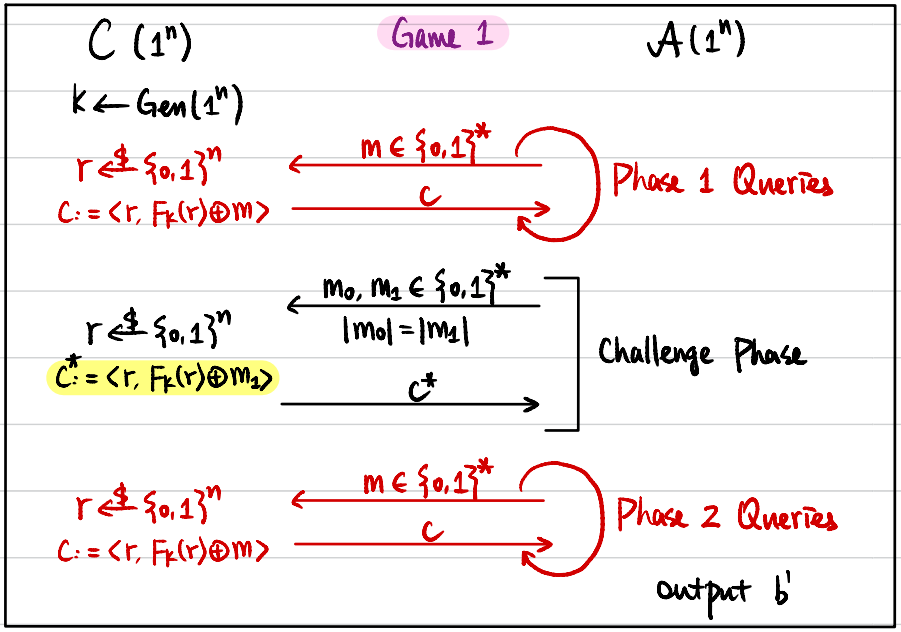
  output $m := F_k(r) \oplus s$



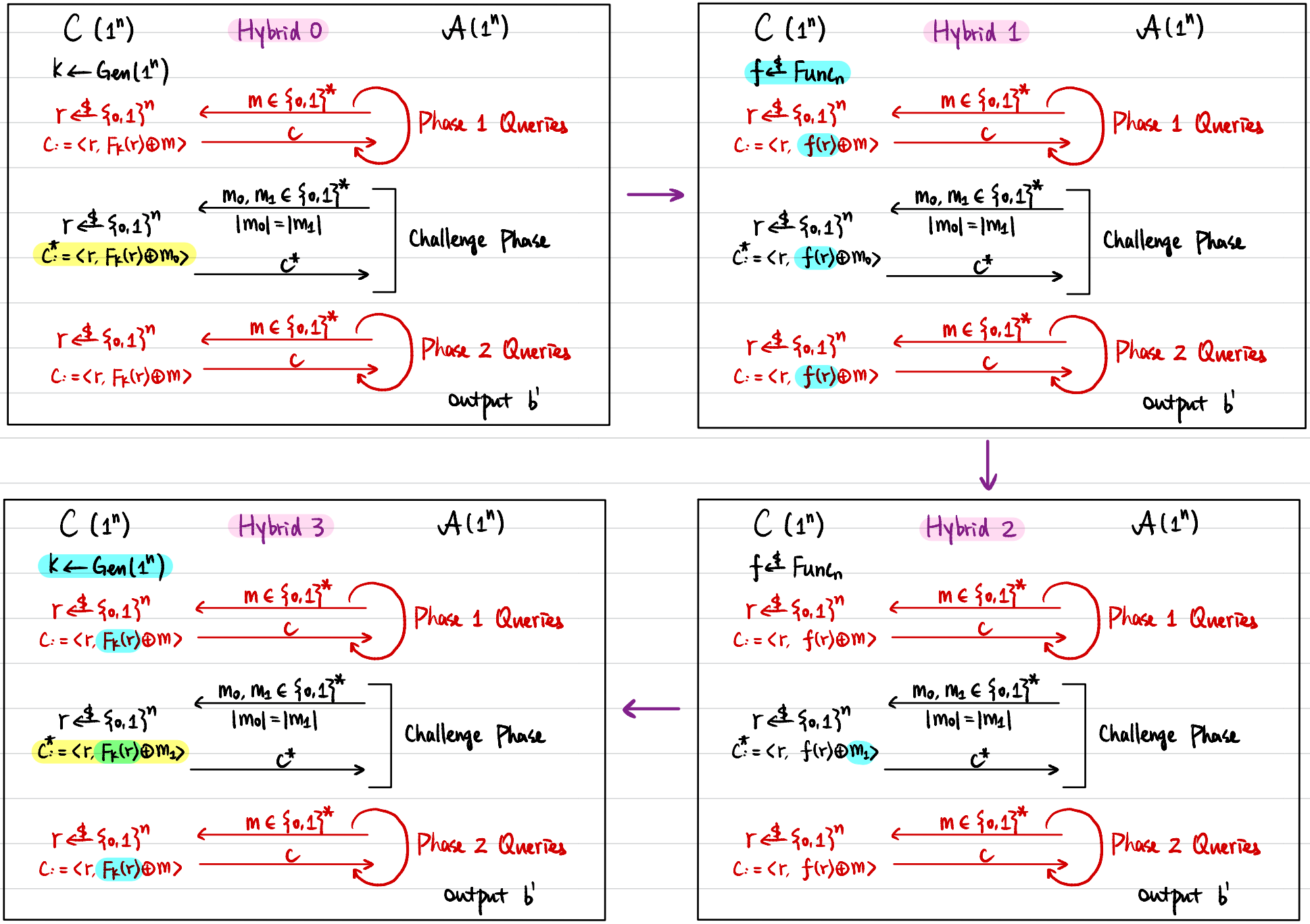
Theorem If F is a PRF, then $\Pi = (Gen, Enc, Dec)$ is CPA-secure.

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





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

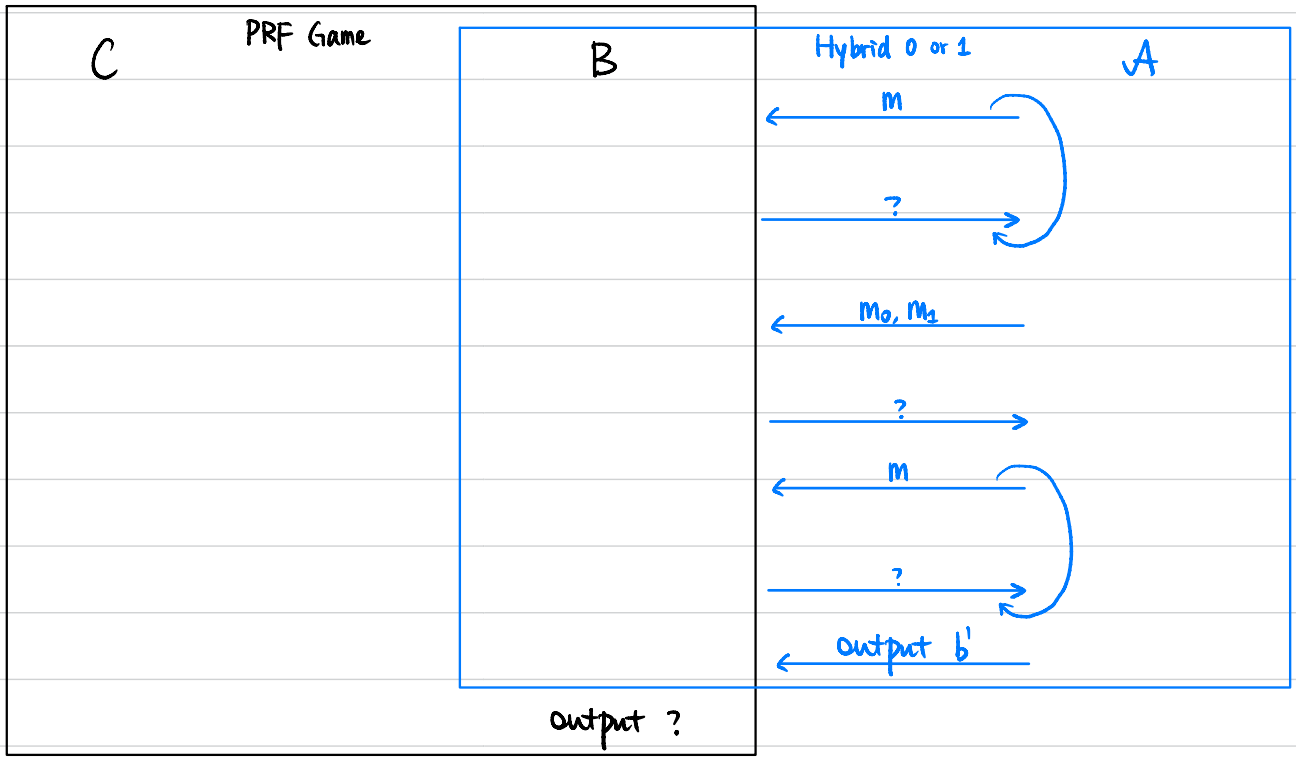

C (1^n)
Hybrid 0
A (1^n)
k ← Gen(1^n)
r ←$ {0,1}^n
C := ⟨r, F_k(r) ⊕ m⟩
m ∈ {0,1}^*
c
Phase 1 Queries
r ←$ {0,1}^n
C* := ⟨r, F_k(r) ⊕ m_0⟩
m_0, m_1 ∈ {0,1}^*
|m_0| = |m_1|
c*
Challenge Phase
r ←$ {0,1}^n
C := ⟨r, F_k(r) ⊕ m⟩
m ∈ {0,1}^*
c
Phase 2 Queries
output b'
C (1^n)
Hybrid 1
A (1^n)
f ←$ Func_n
r ←$ {0,1}^n
C := ⟨r, f(r) ⊕ m⟩
m ∈ {0,1}^*
c
Phase 1 Queries
r ←$ {0,1}^n
C* := ⟨r, f(r) ⊕ m_0⟩
m_0, m_1 ∈ {0,1}^*
|m_0| = |m_1|
c*
Challenge Phase
r ←$ {0,1}^n
C := ⟨r, f(r) ⊕ m⟩
m ∈ {0,1}^*
c
Phase 2 Queries
output b'
C (1^n)
Hybrid 2
A (1^n)
f ←$ Func_n
r ←$ {0,1}^n
C := ⟨r, f(r) ⊕ m⟩
m ∈ {0,1}^*
c
Phase 1 Queries
r ←$ {0,1}^n
C* := ⟨r, f(r) ⊕ m_1⟩
m_0, m_1 ∈ {0,1}^*
|m_0| = |m_1|
c*
Challenge Phase
r ←$ {0,1}^n
C := ⟨r, f(r) ⊕ m⟩
m ∈ {0,1}^*
c
Phase 2 Queries
output b'
C (1^n)
Hybrid 3
A (1^n)
k ← Gen(1^n)
r ←$ {0,1}^n
C := ⟨r, F_k(r) ⊕ m⟩
m ∈ {0,1}^*
c
Phase 1 Queries
r ←$ {0,1}^n
C* := ⟨r, F_k(r) ⊕ m_1⟩
m_0, m_1 ∈ {0,1}^*
|m_0| = |m_1|
c*
Challenge Phase
r ←$ {0,1}^n
C := ⟨r, F_k(r) ⊕ m⟩
m ∈ {0,1}^*
c
Phase 2 Queries
output b'

$$
\begin{aligned}
&\left|\Pr[\mathcal{A}\text{ outputs 1 in Game 0}] - \Pr[\mathcal{A}\text{ outputs 1 in Game 1}]\right| \\
= &\left|\Pr[\mathcal{A}\text{ outputs 1 in Hybrid 0}] - \Pr[\mathcal{A}\text{ outputs 1 in Hybrid 1}] + \right. \\
&\quad \Pr[\mathcal{A}\text{ outputs 1 in Hybrid 1}] - \Pr[\mathcal{A}\text{ outputs 1 in Hybrid 2}] + \\
&\quad \left.\Pr[\mathcal{A}\text{ outputs 1 in Hybrid 2}] - \Pr[\mathcal{A}\text{ outputs 1 in Hybrid 3}]\right| \\
\leq &\left|\Pr[\mathcal{A}\text{ outputs 1 in Hybrid 0}] - \Pr[\mathcal{A}\text{ outputs 1 in Hybrid 1}]\right| + \\
&\left|\Pr[\mathcal{A}\text{ outputs 1 in Hybrid 1}] - \Pr[\mathcal{A}\text{ outputs 1 in Hybrid 2}]\right| + \\
&\left|\Pr[\mathcal{A}\text{ outputs 1 in Hybrid 2}] - \Pr[\mathcal{A}\text{ outputs 1 in Hybrid 3}]\right|
\end{aligned}
$$

Lemma 1 $\forall$ PPT A, $\exists$ negligible function $\varepsilon_1(\cdot)$ s.t.

$$\left| \Pr[A \text{ outputs 1 in Hybrid 0}] - \Pr[A \text{ outputs 1 in Hybrid 1}] \right| \leq \varepsilon_1(n)$$

Proof Assume not, then $\exists$ PPT A that distinguishes Hybrid 0 & Hybrid 1.
We construct PPT B to break the pseudorandomness of F.



Lemma 2 $\forall$ PPT $\mathcal{A}$. $\exists$ negligible function $\varepsilon_2(\cdot)$ s.t.

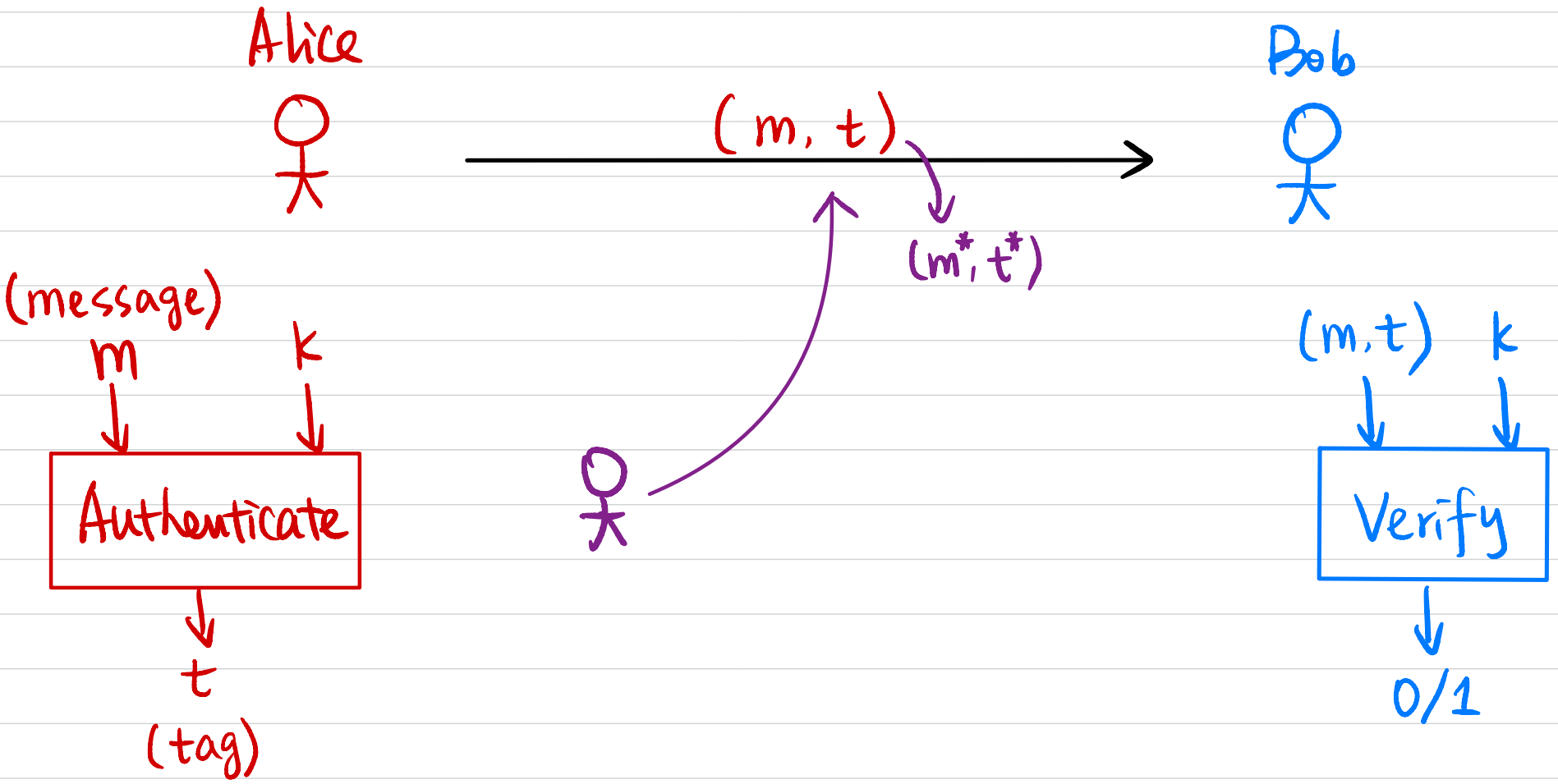
$$\left| \Pr[\mathcal{A} \text{ outputs } 1 \text{ in Hybrid } 1] - \Pr[\mathcal{A} \text{ outputs } 1 \text{ in Hybrid } 2] \right| \leq \varepsilon_2(n)$$

Proof

Lemma 3 $\forall$ PPT $\mathcal{A}$. $\exists$ negligible function $\varepsilon_3(\cdot)$ s.t.

$$\left| \Pr[\mathcal{A} \text{ outputs } 1 \text{ in Hybrid } 2] - \Pr[\mathcal{A} \text{ outputs } 1 \text{ in Hybrid } 3] \right| \leq \varepsilon_3(n)$$

Message Integrity



Message Integrity vs. Secrecy

Does encryption solve the problem? $t \leftarrow Enc_k(m)$

- OTP? $t = k \oplus m$

- Pseudo OTP? $t = G(k) \oplus m$

- CPA-secure encryption from PRF?

  $t = \langle r, F_k(r) \oplus m \rangle$

Message Authentication Code (MAC)

- **Syntax:**

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

  $k \leftarrow Gen(1^n)$

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

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

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

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

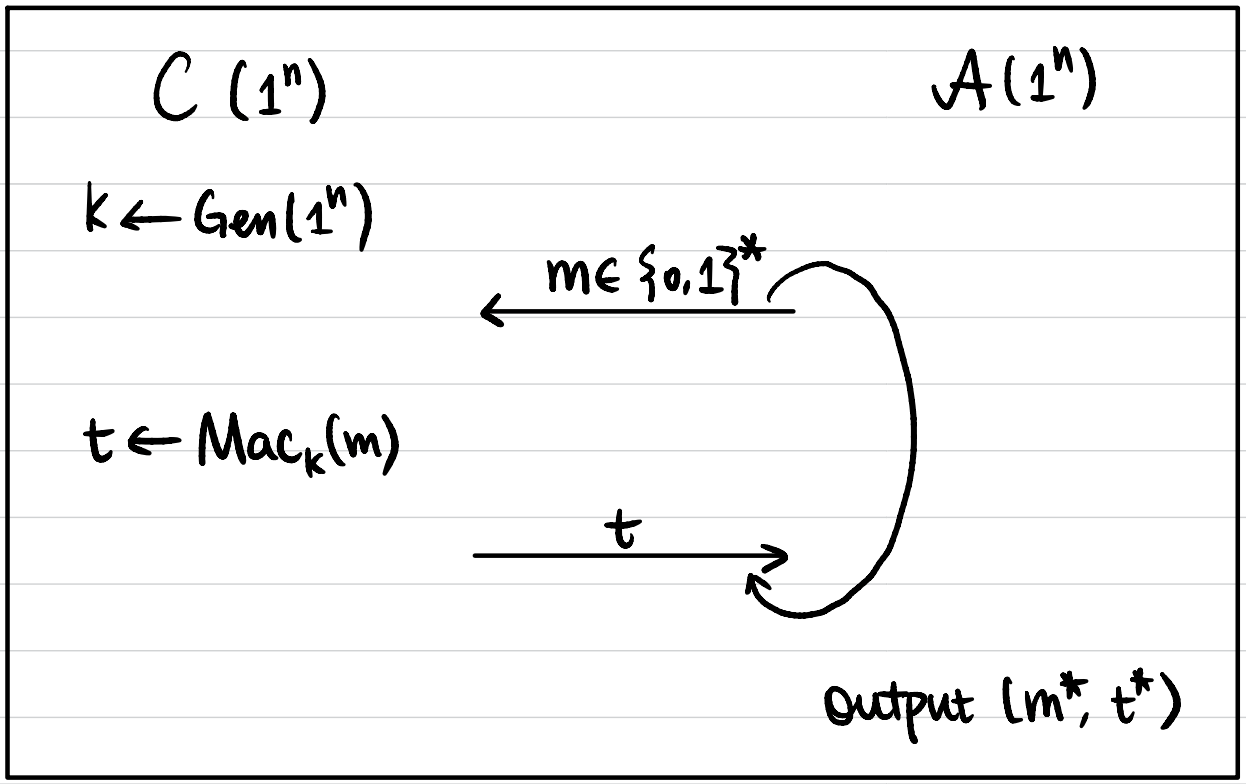
- **Canonical Verification:**

  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 $\pi = (Gen, Mac, Vrfy)$ 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.

$$Pr[MacForge_{\mathcal{A},\pi} = 1] \leq \varepsilon(n).$$



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

$MacForge_{\mathcal{A},\pi} = 1$ ($\mathcal{A}$ succeeds) if

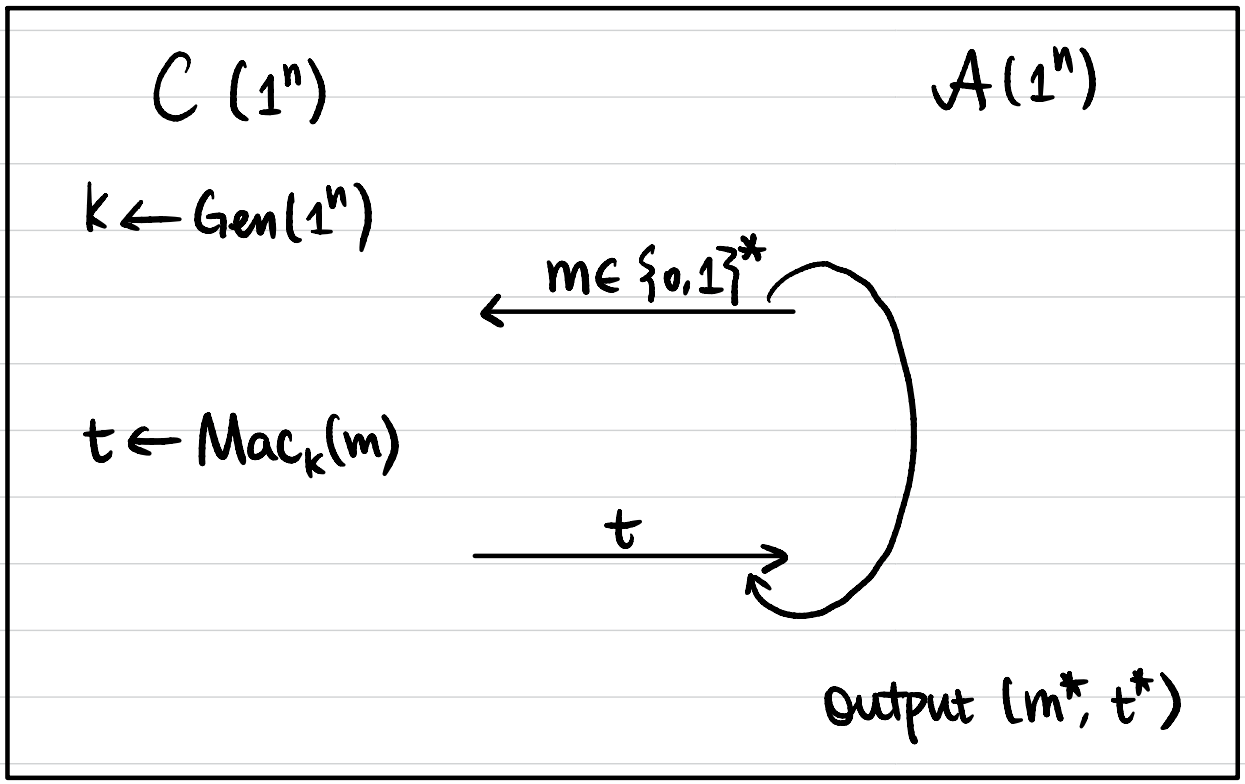
① $m^* \notin Q$, and

② $Vrfy_k(m^*, t^*) = 1$.

Message Authentication Code (MAC)

Def 2 A message authentication code (MAC) scheme $\Pi = (Gen, Mac, Vrfy)$ is **strongly secure** if $\forall$ PPT $\mathcal{A}$, $\exists$ negligible function $\varepsilon(\cdot)$ s.t.

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



$Q := \{(m, t) \mid m$ 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 $\text{Vrfy}_k(m^*, t^*) = 1$.

Thm If $\Pi = (Gen, Mac, Vrfy)$ 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:

- $\text{Gen}(1^n)$: sample $k \xleftarrow{\$} \{0,1\}^n$, output k.
- $\text{Mac}_k(m)$: $m \in \{0,1\}^{2n-2}$
  $m = m_0 \| m_1$, $m_0, m_1 \in \{0,1\}^{n-1}$
  output $t := F_k(0 \| m_0) \| F_k(1 \| m_1)$
- $\text{Vrfy}_k(m,t)$: $\text{Mac}_k(m) \stackrel{?}{=} t$

Is this MAC scheme necessarily secure?

Exercises

Given a secure MAC scheme $\Pi = (Gen, Mac, Vrfy)$, construct another MAC scheme $\tilde{\Pi} = (\tilde{Gen}, \tilde{Mac}, \tilde{Vrfy})$ that is secure but not strongly secure.

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

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

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