

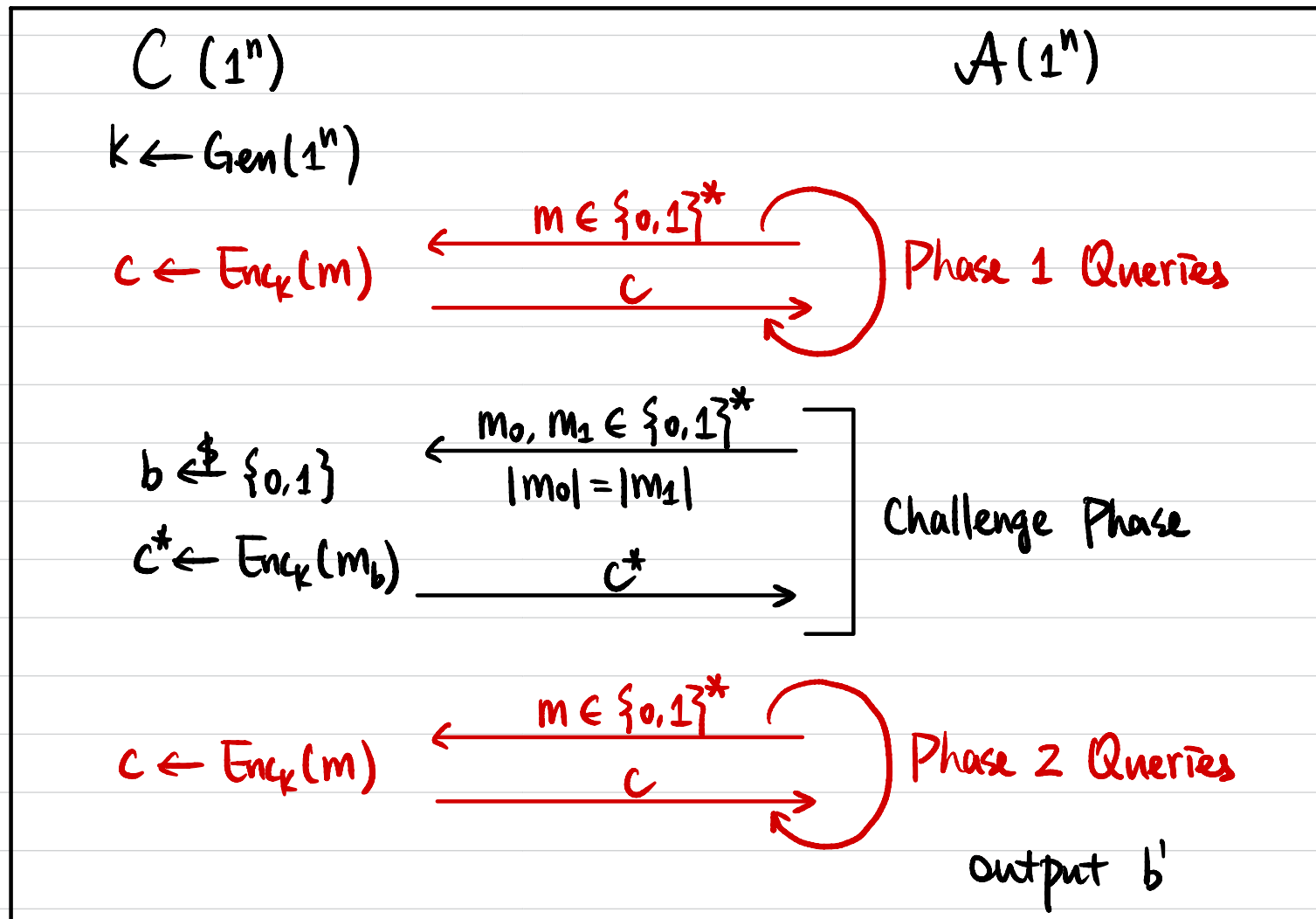
CSCI 1510

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

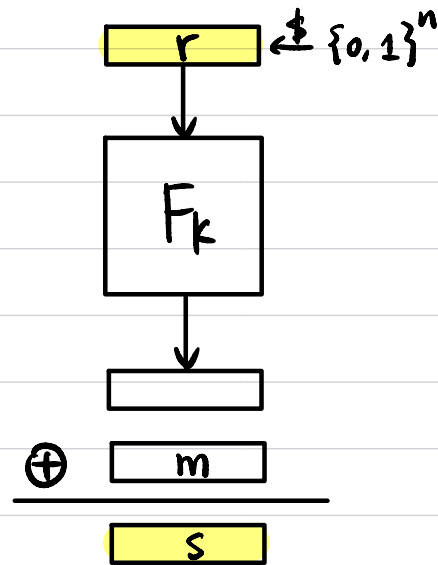


Constructing CPA-Secure Encryption

Pseudorandom Function (PRF)



CPA-Secure Encryption



$c = \langle r, s \rangle$

Pseudorandom Function (PRF)

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

$C(1^n)$

$A(1^n)$

$b \xleftarrow{\$} \{0,1\}$

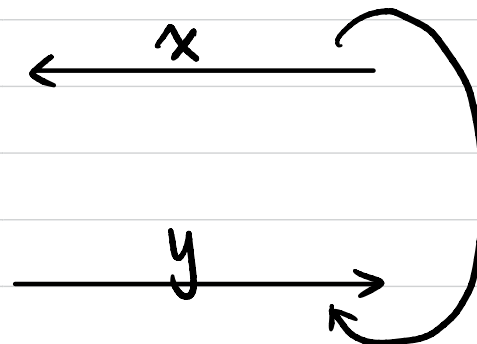
If $b=0$, then $k \xleftarrow{\$} \{0,1\}^n$

If $b=1$, then $f \xleftarrow{\$} \text{Func}_n$

$\{ F \mid F: \{0,1\}^n \rightarrow \{0,1\}^n \}$

If $b=0$, then $y := F_k(x)$

If $b=1$, then $y := f(x)$



output b'

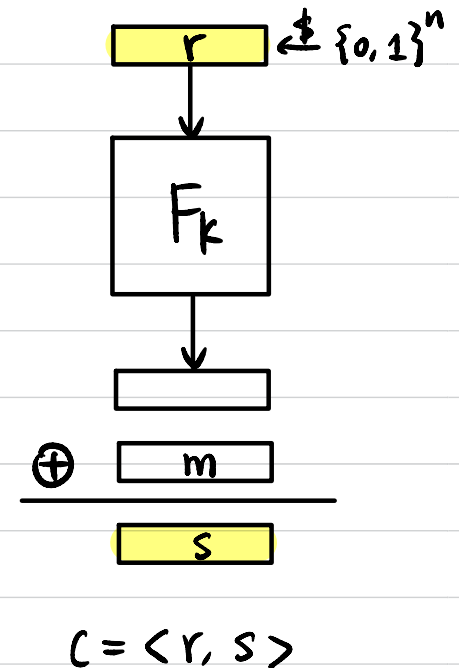
CPA-Secure Encryption Scheme

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

- $\text{Gen}(1^n)$: sample $k \leftarrow \{0,1\}^n$, output k .

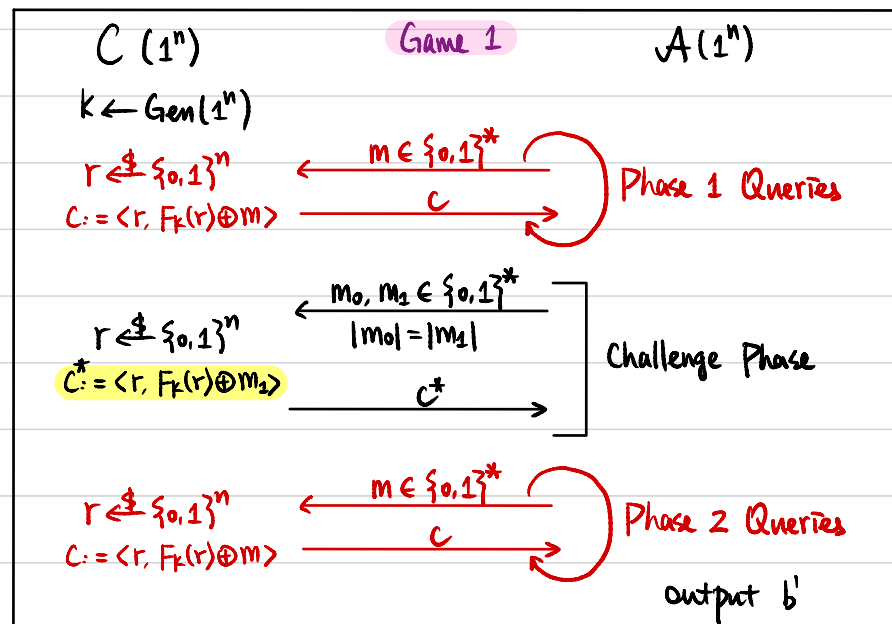
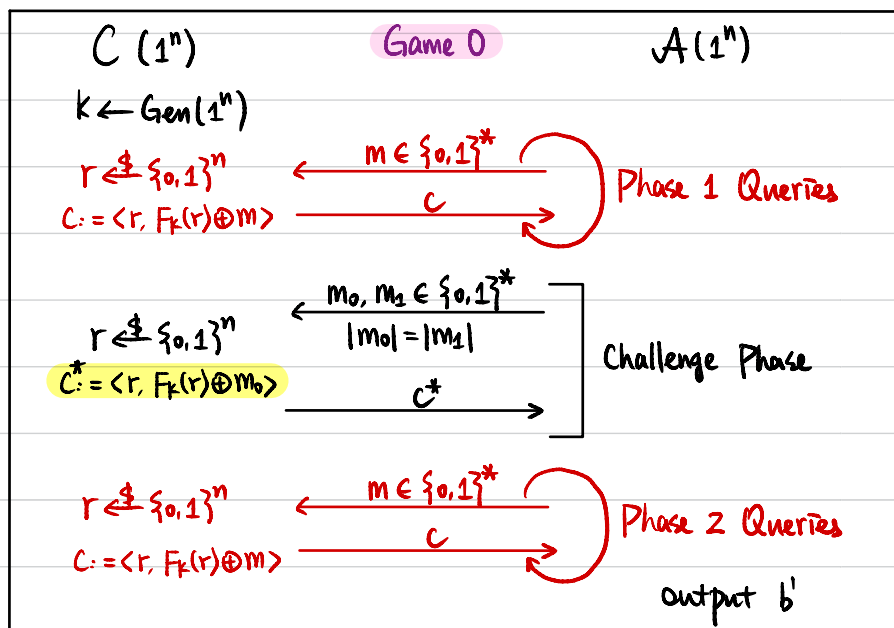
- $\text{Enc}_k(m)$: $m \in \{0,1\}^n$
 $r \leftarrow \{0,1\}^n$
output $c := \langle r, F_k(r) \oplus m \rangle$

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

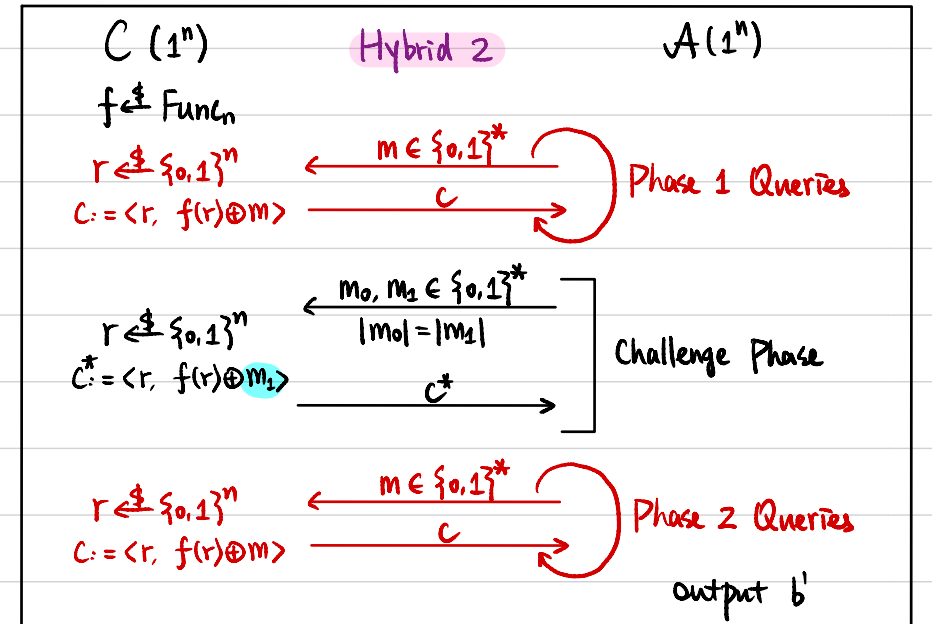
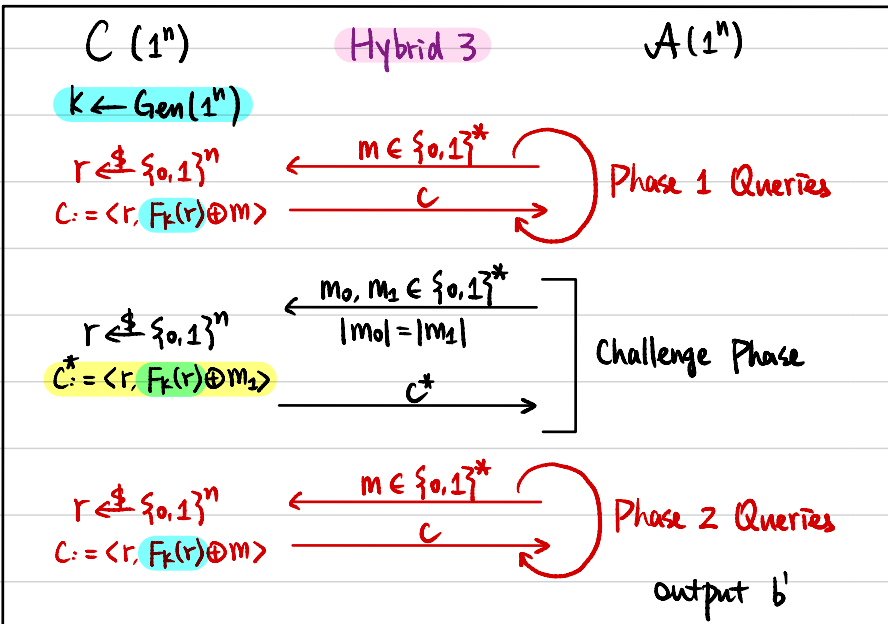
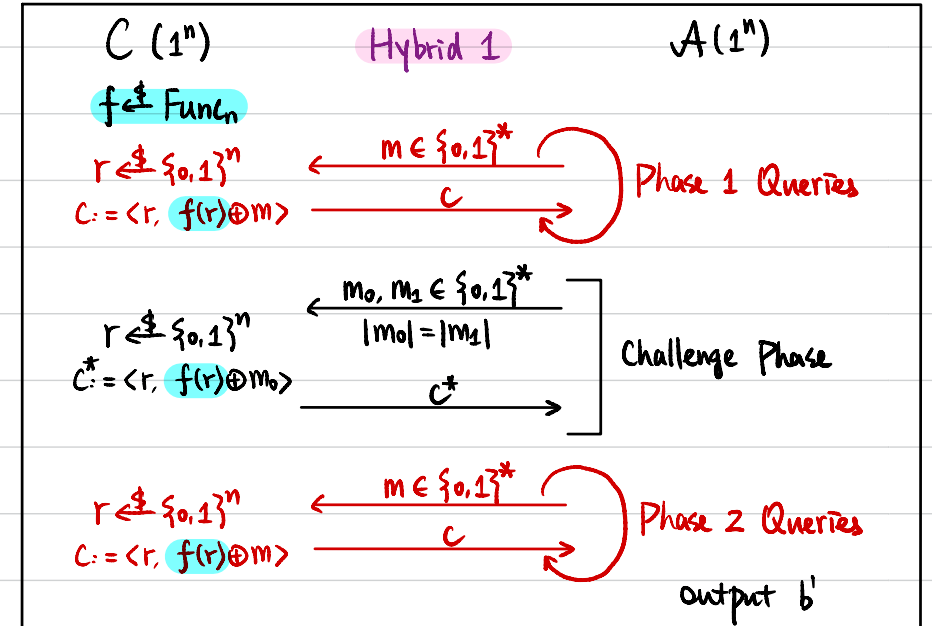
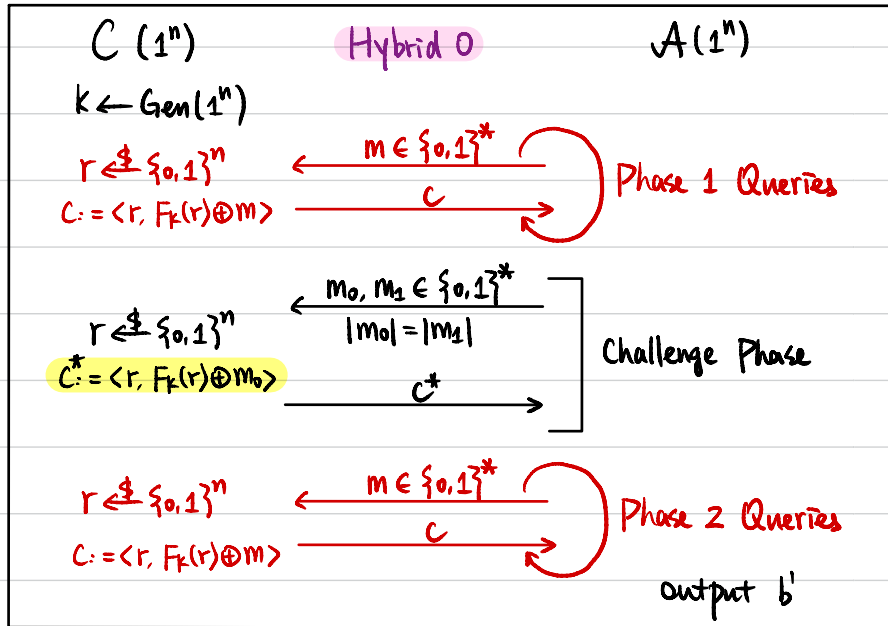


Theorem If F is a PRF, then $\pi = (\text{Gen}, \text{Enc}, \text{Dec})$ is CPA-Secure.

Proof $\forall$ PPT A ,



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



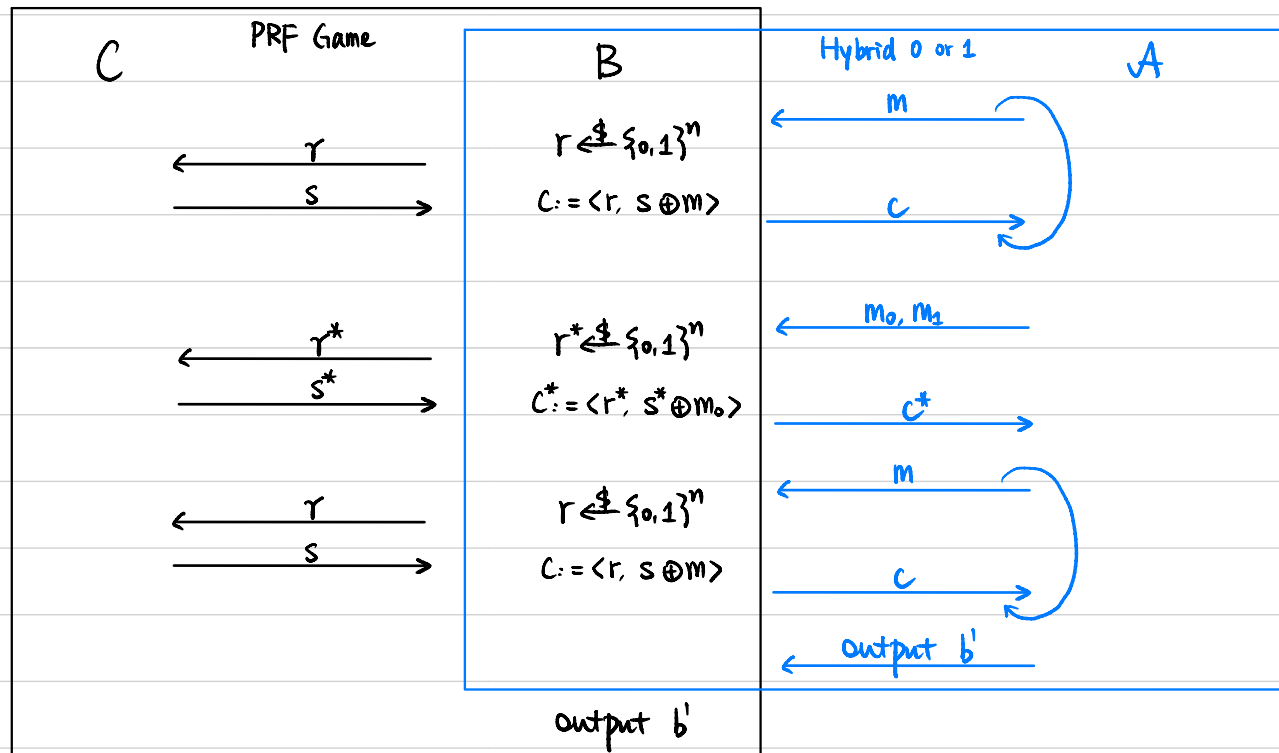
$$\begin{aligned}
& \left| \Pr[A \text{ outputs } 1 \text{ in Game } 0] - \Pr[A \text{ outputs } 1 \text{ in Game } 1] \right| \\
&= \left| \Pr[A \text{ outputs } 1 \text{ in Hybrid } 0] - \Pr[A \text{ outputs } 1 \text{ in Hybrid } 1] + \right. \\
&\quad \Pr[A \text{ outputs } 1 \text{ in Hybrid } 1] - \Pr[A \text{ outputs } 1 \text{ in Hybrid } 2] + \\
&\quad \left. \Pr[A \text{ outputs } 1 \text{ in Hybrid } 2] - \Pr[A \text{ outputs } 1 \text{ in Hybrid } 3] \right| \\
&\leq \left| \Pr[A \text{ outputs } 1 \text{ in Hybrid } 0] - \Pr[A \text{ outputs } 1 \text{ in Hybrid } 1] \right| \leq \epsilon_1(n) + \\
&\quad \left| \Pr[A \text{ outputs } 1 \text{ in Hybrid } 1] - \Pr[A \text{ outputs } 1 \text{ in Hybrid } 2] \right| \leq \epsilon_2(n) + \\
&\quad \left| \Pr[A \text{ outputs } 1 \text{ in Hybrid } 2] - \Pr[A \text{ outputs } 1 \text{ in Hybrid } 3] \right| \leq \epsilon_3(n)
\end{aligned}$$

Lemma 1 $\forall$ PPT A , $\exists$ negligible function $\epsilon_1(\cdot)$ st.

$$|\Pr[A \text{ outputs } 1 \text{ in Hybrid } 0] - \Pr[A \text{ outputs } 1 \text{ in Hybrid } 1]| \leq \epsilon_1(n)$$

Proof Assume not, then $\exists$ PPT A that distinguishes Hybrid 0 & Hybrid 1.

We construct PPT B to break the pseudorandomness of F .



If C uses F_k , then A is in Hybrid 0

If C uses a random function, then A is in Hybrid 1

$$|\Pr[B \text{ outputs } 1 \text{ on } F_k] - \Pr[B \text{ outputs } 1 \text{ on a random function}]|$$

$$= |\Pr[A \text{ outputs } 1 \text{ in Hybrid } 0] - \Pr[A \text{ outputs } 1 \text{ in Hybrid } 1]| \geq \text{non-negl}(n)$$

Lemma 2 $\forall$ PPT A , $\exists$ negligible function $\epsilon_2(\cdot)$ st.

$$\left| \Pr[A \text{ outputs 1 in Hybrid 1}] - \Pr[A \text{ outputs 1 in Hybrid 2}] \right| \leq \epsilon_2(n)$$

Proof Let r_i be the r value sampled for the i -th query in Phase 1 & 2.

Let r^* be the r value sampled for the Challenge Phase.

$$\forall i, \Pr[r_i = r^*] = 2^{-n}$$

$$\Pr[\exists i \text{ st. } r_i = r^*] \leq 2^{-n} \cdot Q \quad Q := \text{total \# queries in Phase 1 \& 2.}$$

$$A \text{ is PPT} \Rightarrow Q \leq p(n) \quad \leftarrow \text{polynomial}$$

$$\begin{aligned} & \left| \Pr[A \text{ outputs 1 in Hybrid 1}] - \Pr[A \text{ outputs 1 in Hybrid 2}] \right| \\ & \leq \Pr[\exists i \text{ st. } r_i = r^*] \leq 2^{-n} \cdot p(n) \rightarrow \text{negligible} \end{aligned}$$

Lemma 3 $\forall$ PPT A , $\exists$ negligible function $\epsilon_3(\cdot)$ st.

$$\left| \Pr[A \text{ outputs 1 in Hybrid 2}] - \Pr[A \text{ outputs 1 in Hybrid 3}] \right| \leq \epsilon_3(n)$$

Message Integrity

Alice



(message)

m

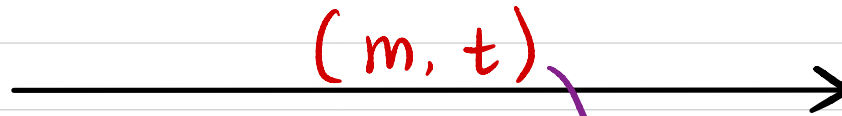
k

Authenticate



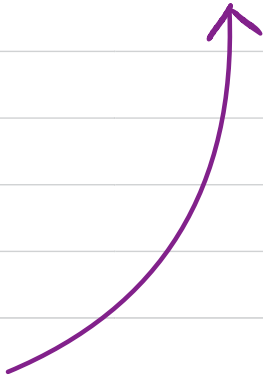
t

(tag)



(m, t)

(m^*, t^*)



Bob



(m, t)

k

Verify



0/1

Message Integrity vs. Secrecy

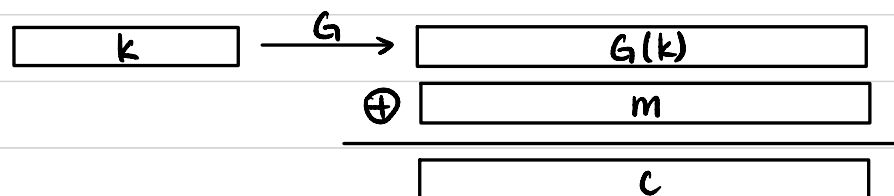
Does encryption solve the problem? $t \leftarrow \text{Enc}_k(m)$

• OTP? $t = k \oplus m$

$$(m, t) \Rightarrow k \Rightarrow (m^*, t^*)$$

• Pseudo OTP? $t = G(k) \oplus m$

$$(m, t) \Rightarrow G(k) \Rightarrow (m^*, t^*)$$

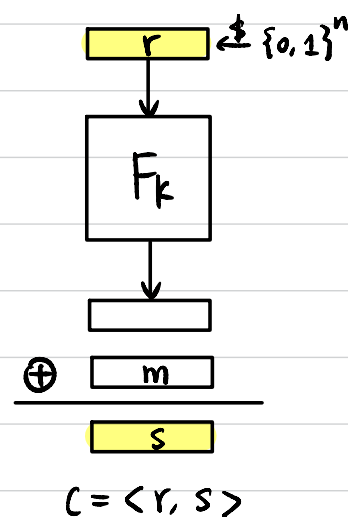


• CPA-secure encryption from PRF?

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

$$(m, t = \langle r, s \rangle) \Rightarrow F_k(r) \Rightarrow (m^*, t^*)$$

||
 $\langle r, F_k(r) \oplus m^* \rangle$



Message Authentication Code (MAC)

- **Syntax:**

A **message authentication code (MAC)** scheme is defined by PPT algorithms $(\text{Gen}, \text{Mac}, \text{Vrfy})$:

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

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

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

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

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

- **Canonical Verification:**

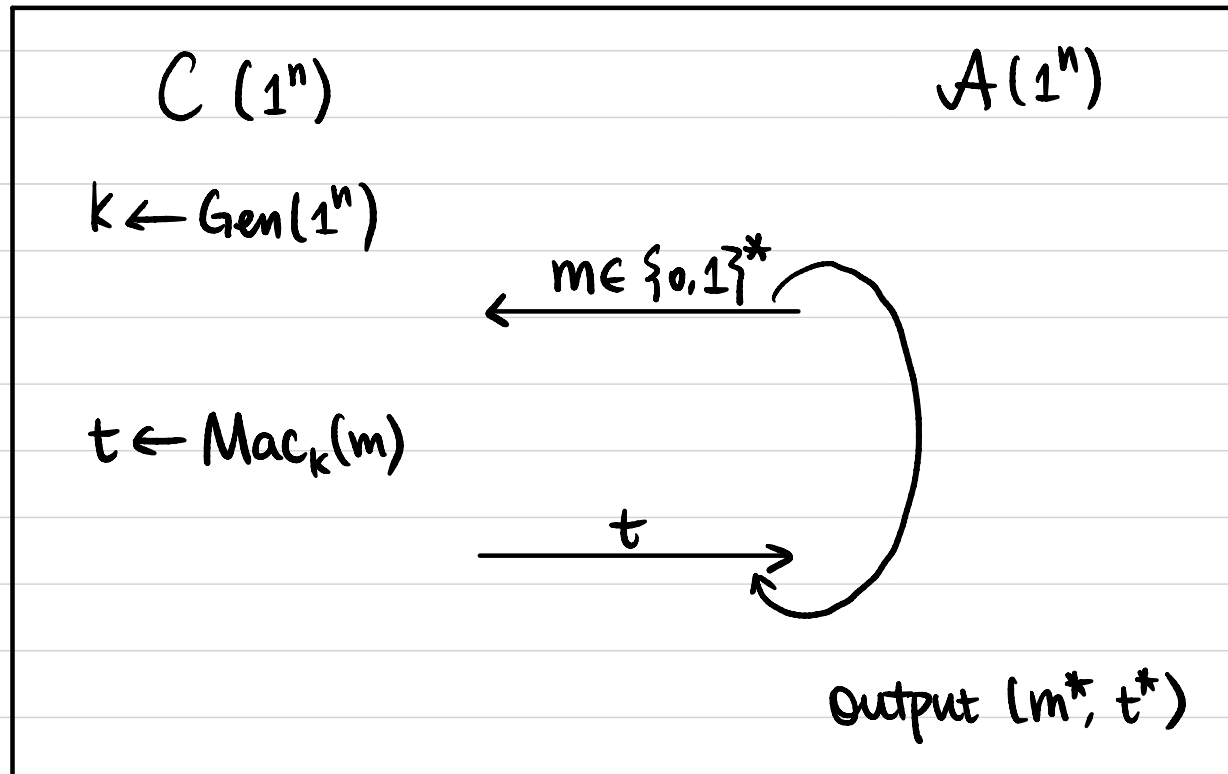
If $\text{Mac}_k(m)$ is deterministic, then $\text{Vrfy}_k(m, t)$ is straightforward.

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

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

$$\Pr[\text{MacForge}_{A, \pi} = 1] \leq \epsilon(n).$$



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

$\text{MacForge}_{A, \pi} = 1$ (A succeeds) if

① $m^* \notin Q$, and

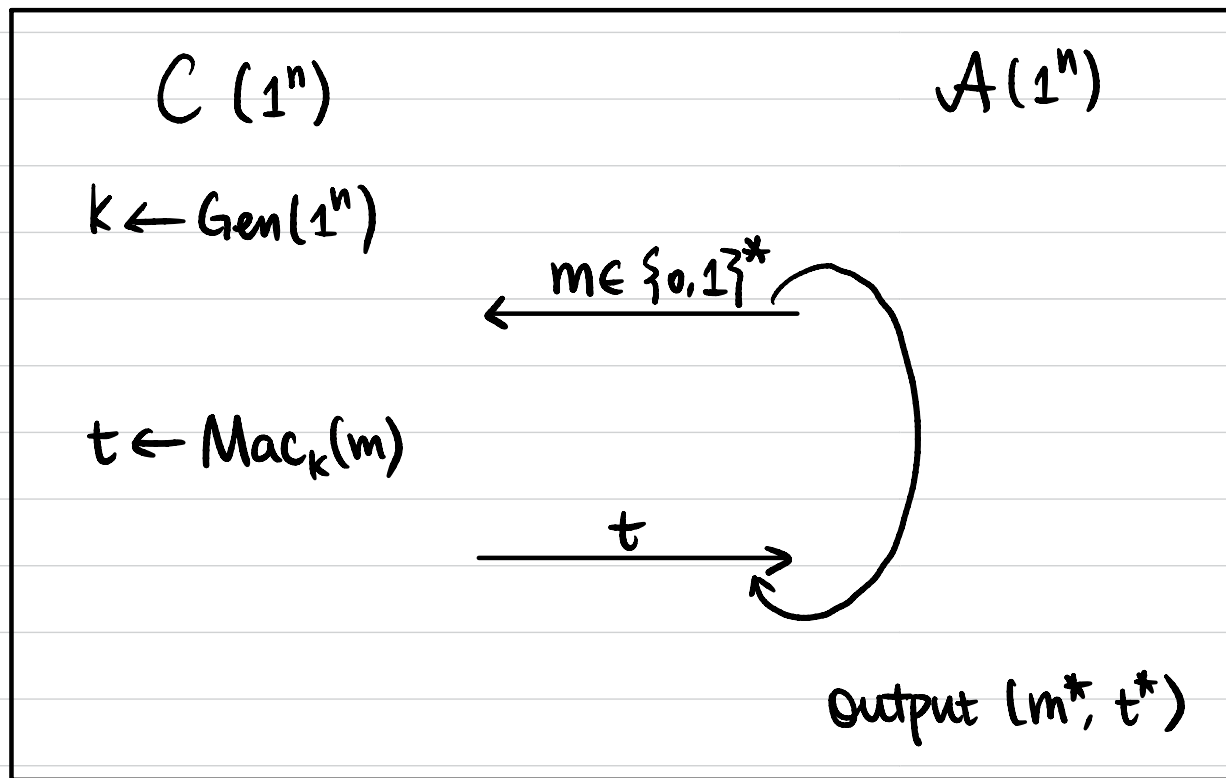
② $\text{Vrfy}_k(m^*, t^*) = 1$.

Message Authentication Code (MAC)

Def 2 A message authentication code (MAC) scheme $\pi = (\text{Gen}, \text{Mac}, \text{Vrfy})$ is

strongly secure if $\forall \text{PPT } A, \exists \text{negligible function } \epsilon(\cdot)$ s.t.

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



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

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

① $(m^*, t^*) \notin Q$, and

② $\text{Vrfy}_k(m^*, t^*) = 1$.

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

Exercises

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

Construct a MAC scheme:

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

Is this MAC scheme necessarily secure?

C

✓

$$\begin{array}{c} \leftarrow m_0^* \parallel 0^{n-1} \\ \hline t_0^* \parallel t_1^* \end{array}$$

$$\begin{array}{c} \leftarrow 0^{n-1} \parallel m_1^* \\ \hline t_0 \parallel t_1^* \end{array}$$

$$\begin{array}{l} \text{Output } m^* = \overset{0^{n-1}}{\#} m_0^* \parallel \overset{0^{n-1}}{\#} m_1^* \\ t^* = t_0^* \parallel t_1^* \end{array}$$

Exercises

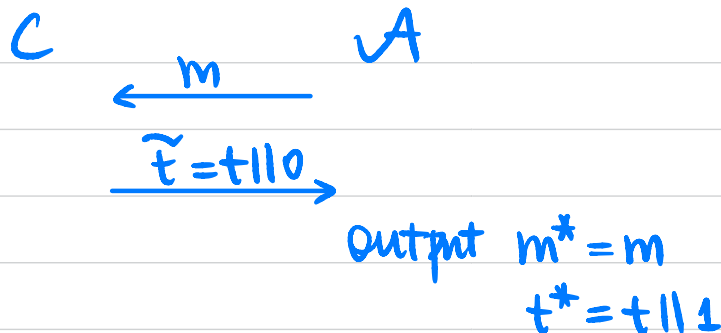
Given a secure MAC scheme $\pi = (\text{Gen}, \text{Mac}, \text{Vrfy})$, construct another MAC scheme $\tilde{\pi} = (\tilde{\text{Gen}}, \tilde{\text{Mac}}, \tilde{\text{Vrfy}})$ that is secure but not strongly secure.

Step 1: Construct $\tilde{\pi}$ from π

- $\tilde{\text{Gen}} = \text{Gen}$
- $\tilde{\text{Mac}}_k(m)$: $t \leftarrow \text{Mac}_k(m)$
output $\tilde{t} = t \parallel 0$
- $\tilde{\text{Vrfy}}_k(m, \tilde{t})$: Parse $\tilde{t} = t \parallel b$
Output $\text{Vrfy}_k(m, t)$

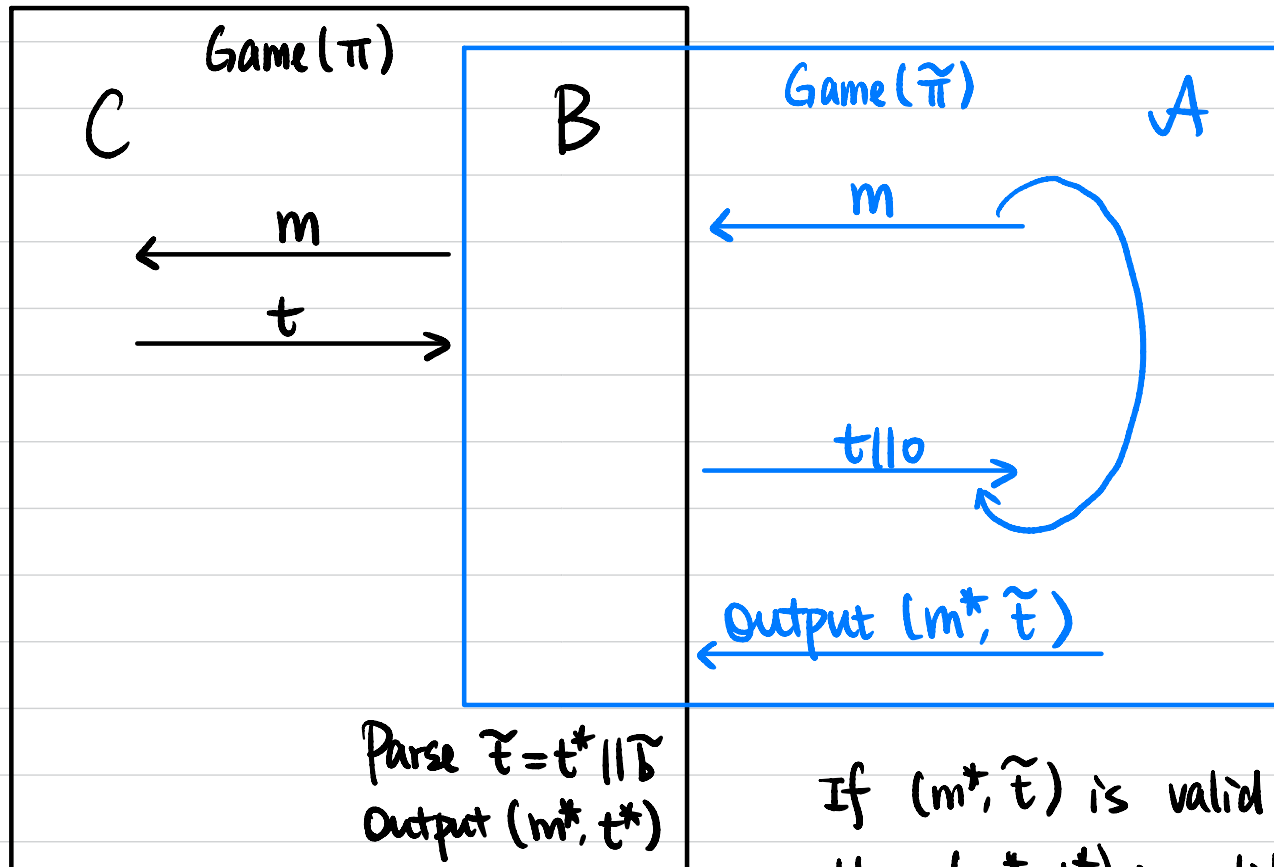
Step 2: If π is secure, then $\tilde{\pi}$ is also secure.

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



Step 2: If π is secure, then $\tilde{\pi}$ is also secure.

Proof Assume not, then $\exists$ PPT 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 .

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