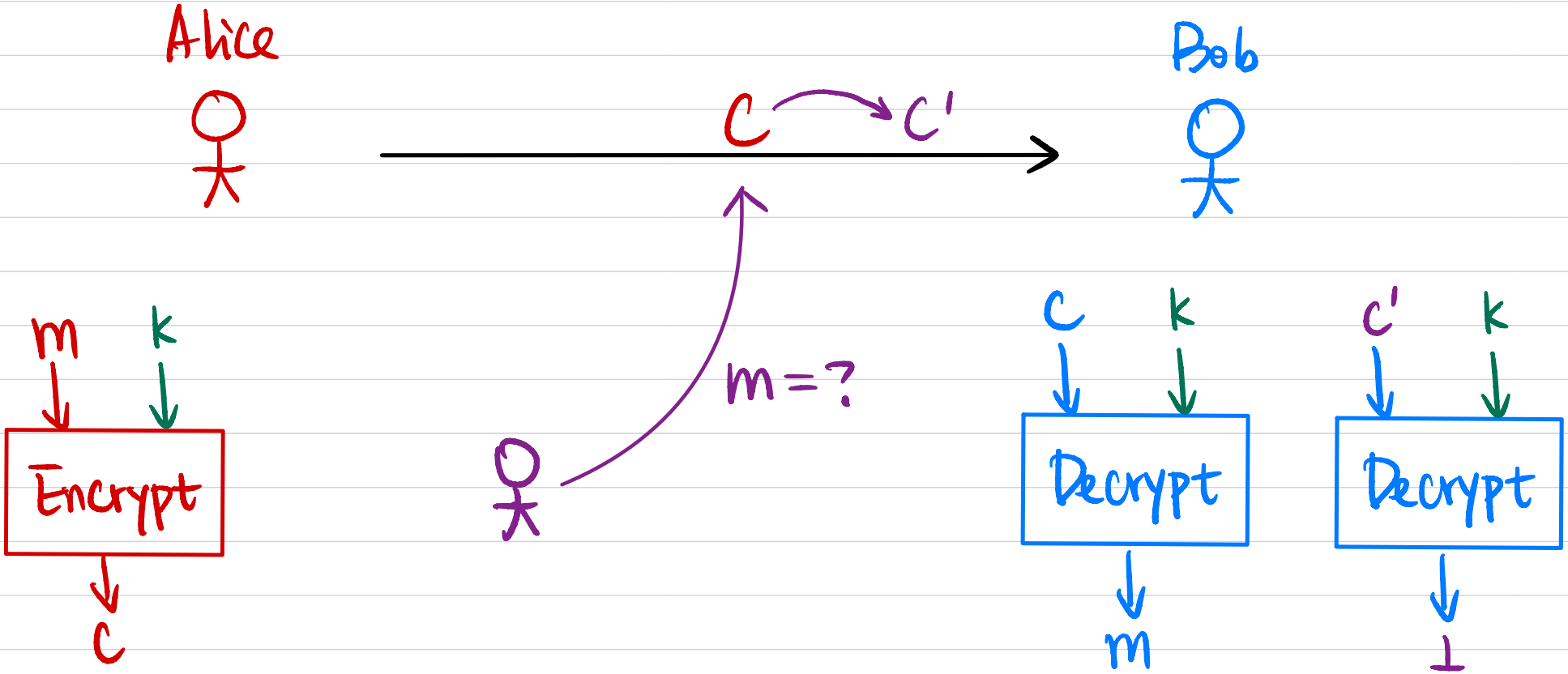
CSCI 1510

This Lecture:

- CCA-Security & Unforgeability
- Authenticated Encryption
- Generic Constructions

Authenticated Encryption

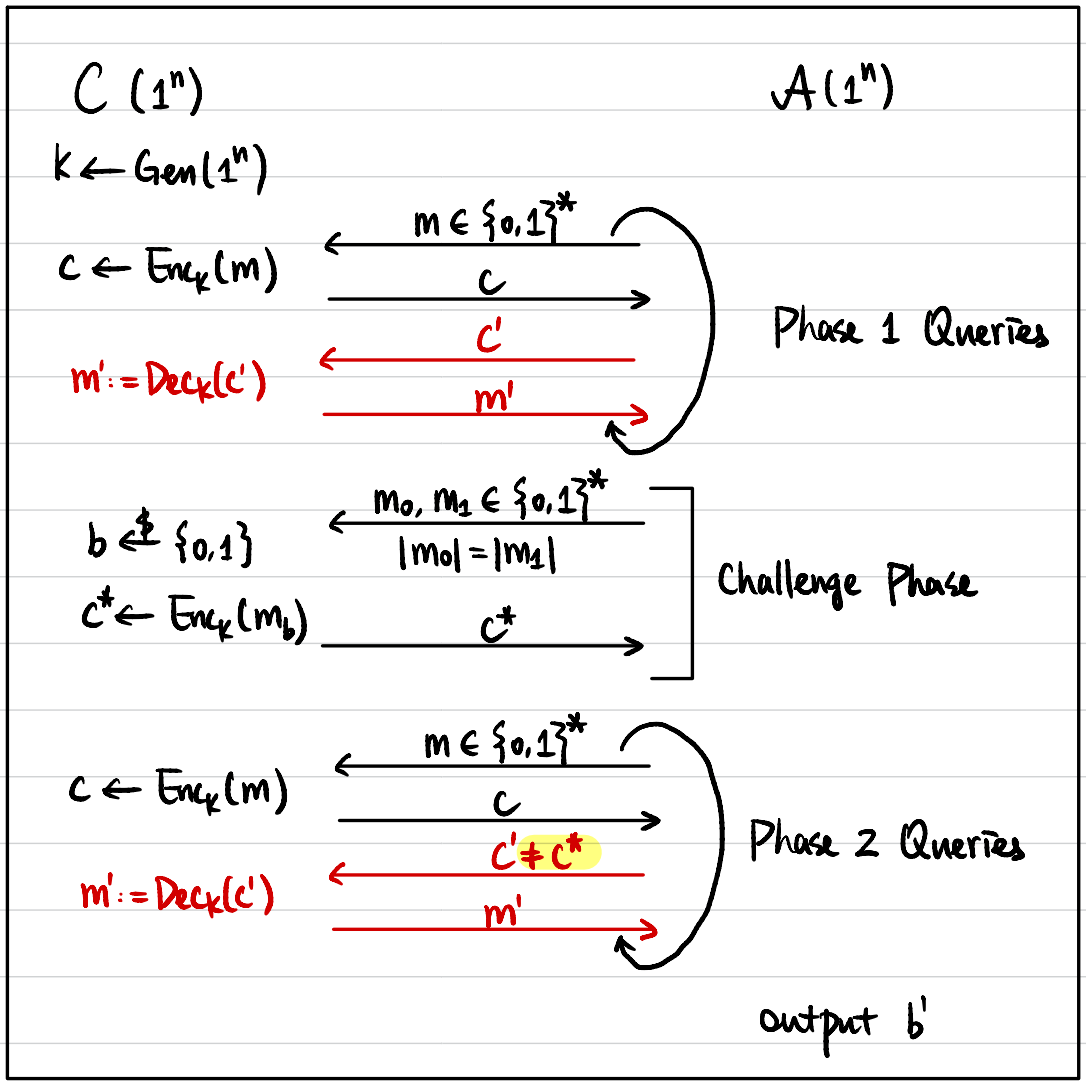


Security Guarantees:

- Message Secrecy: CCA Security
- Message Integrity: Unforgeability

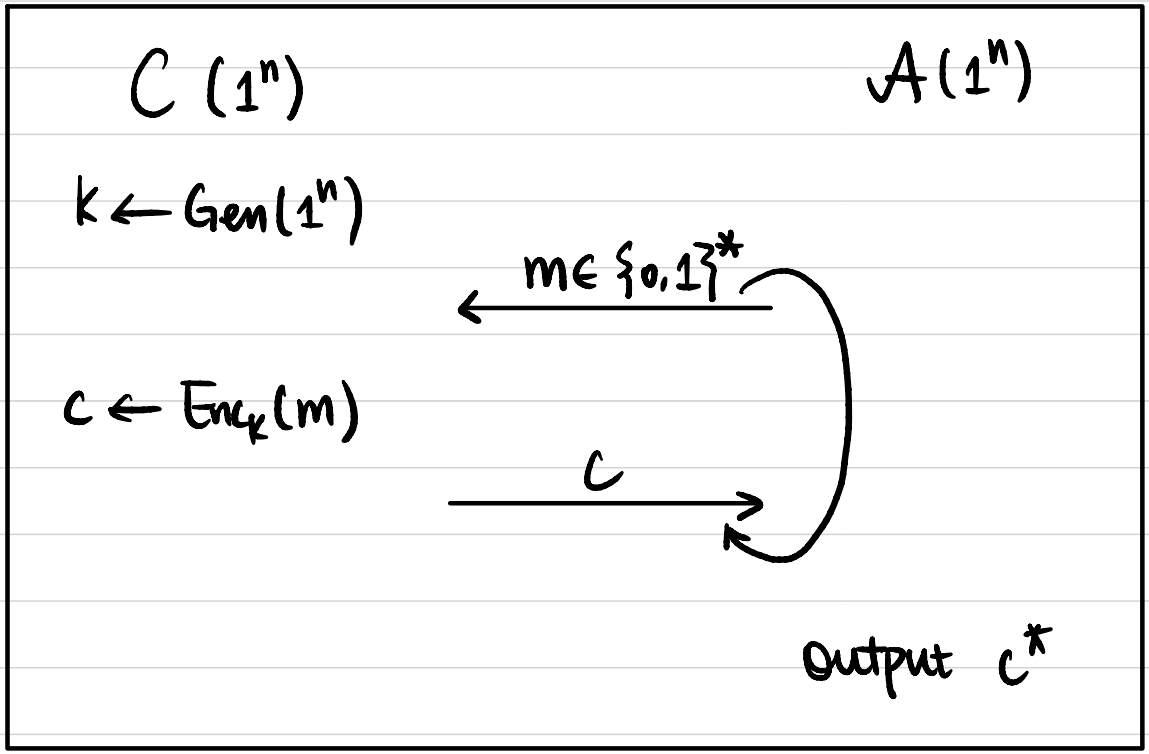
Chosen Ciphertext Attack (CCA) Security

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



Unforgeability

Def A symmetric-key encryption scheme $\Pi = (Gen, Enc, Dec)$ is **unforgeable** if $\forall$ PPT $\mathcal{A}$, $\exists$ negligible function $\varepsilon(\cdot)$ s.t. $\Pr[EncForge_{\mathcal{A},\Pi} = 1] \leq \varepsilon(n)$.



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

$m^* := Dec_k(c^*)$

$EncForge_{\mathcal{A},\Pi} = 1$ ($\mathcal{A}$ succeeds) if

① $m^* \notin Q$, and

② $m^* \neq \perp$

Def A symmetric-key encryption scheme is **authenticated encryption** if it is **CCA-secure** and **unforgeable**.

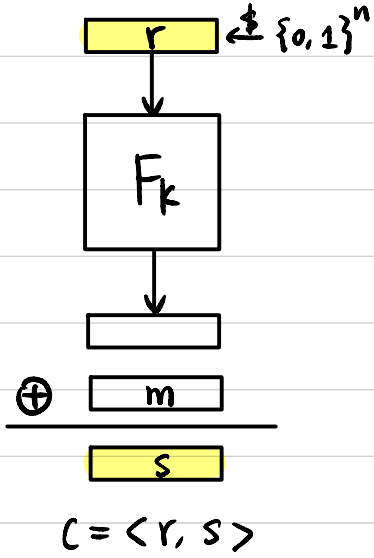
Exercises

Is the CPA-secure encryption from PRF CCA-secure? Unforgeable?

$\text{Enc}_k(m)$: $m \in \{0,1\}^n$

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

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



Not CCA-secure:

C ↔ $\mathcal{A}$

$\mathcal{A} \to C$: m_0, m_1

$C \to \mathcal{A}$: $c = \langle r, s \rangle$

$\mathcal{A} \to C$: $c' = \langle r, s' = s \oplus \tilde{m} \rangle$

$C \to \mathcal{A}$: m'

$m' = m_0 \oplus \tilde{m}$ OR $m_1 \oplus \tilde{m}$?

Not unforgeable: $\mathcal{A}$ can output an arbitrary 2n-bit string $\langle r, s \rangle$

Generic Constructions

Let $\Pi^E = (Gen^E, Enc^E, Dec^E)$ be a CPA-secure encryption scheme.

Let $\Pi^M = (Gen^M, Mac^M, Vrfy^M)$ be a strongly secure MAC scheme.

How to construct an authenticated encryption scheme?

① Encrypt-and-Authenticate

② Authenticate-then-Encrypt

③ Encrypt-then-Authenticate

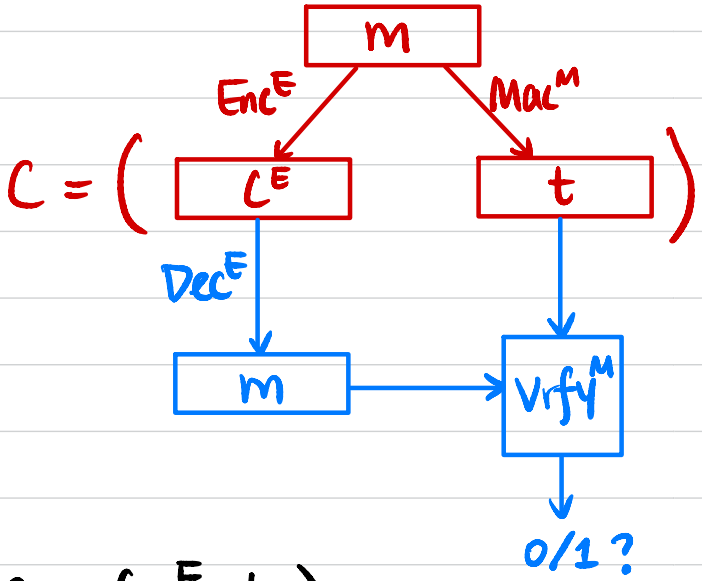
Encrypt-and-Authenticate

$\mathrm{Gen}(1^n)$:

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

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

Output $k = (k^E, k^M)$



$\mathrm{Enc}_k(m)$:

$C^E \leftarrow \mathrm{Enc}^E(k^E, m)$

$t \leftarrow \mathrm{Mac}^M(k^M, m)$

Output $C = (C^E, t)$

$\mathrm{Dec}_k(c)$: $C = (C^E, t_2)$

$m := \mathrm{Dec}^E(k^E, C^E)$

$b := \mathrm{Vrfy}^M(k^M, (m, t))$

If $b=1$, output m

Otherwise output $\perp$

Q_1: Is it CPA-secure? No!

Q_2: Is it CCA-secure? No!

Q_3: Is it unforgeable? Yes!

Π is not necessarily CPA-secure.

Step 1: Let $\tilde{\Pi} = (\tilde{Gen}^M, \tilde{Mac}^M, \tilde{Vrfy}^M)$ be a strongly secure MAC scheme.

Construct $\Pi^M = (Gen^M, Mac^M, Vrfy^M)$ as follows:

- $Gen^M(1^n)$: same as $\tilde{Gen}^M$.
- $Mac^M(k^M, m)$: $\tilde{t} \leftarrow \tilde{Mac}^M(k^M, m)$

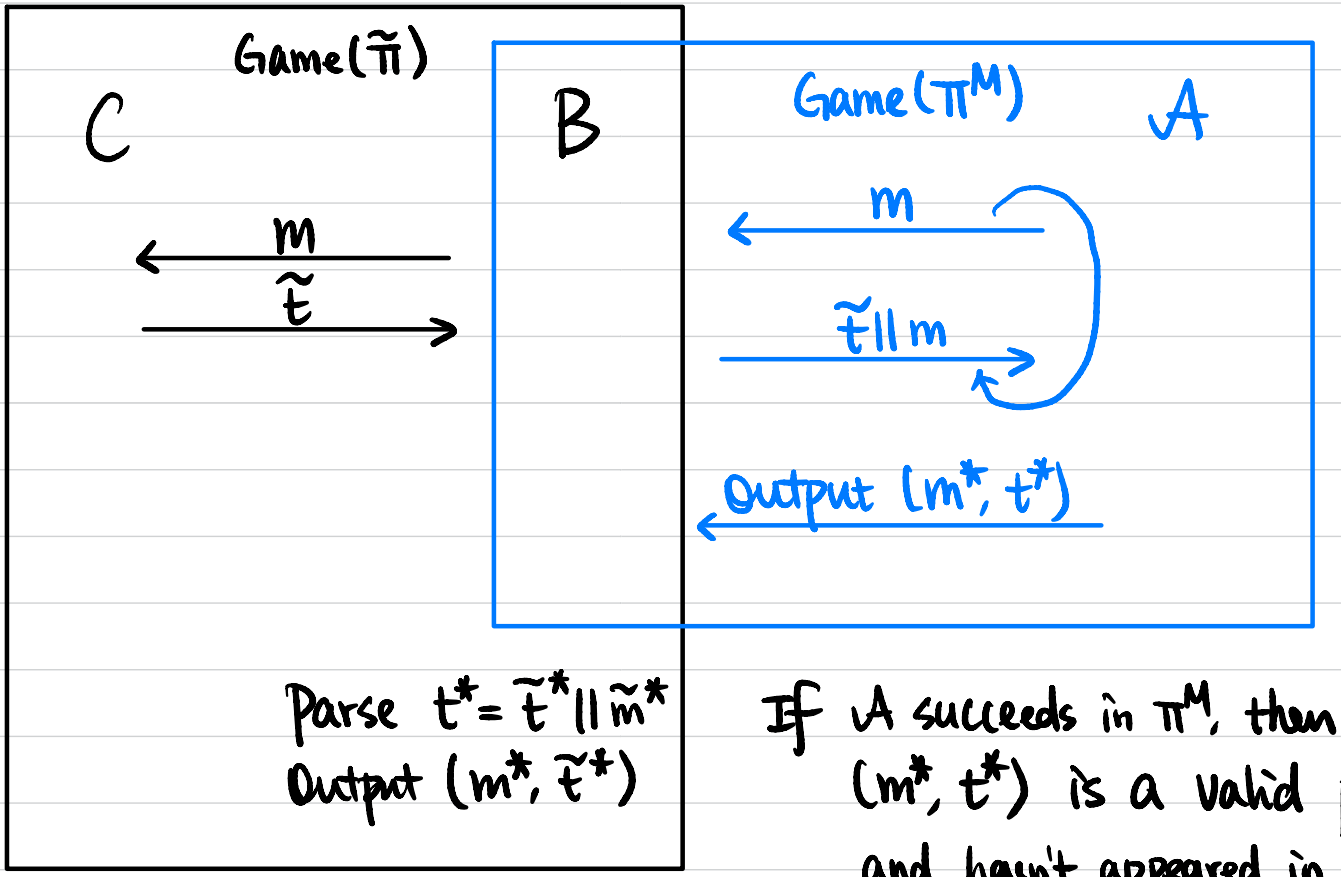
  Output $t = \tilde{t} \| m$
- $Vrfy^M(k^M, (m,t))$: Parse $t = \tilde{t} \| \tilde{m}$

  Output 1 iff $\tilde{Vrfy}^M(k^M, (\tilde{t}, m)) = 1 \wedge m = \tilde{m}$.

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

Proof Assume not, then $\exists$ PPT $\mathcal{A}$ that breaks Π^M

We construct PPT B to break $\tilde{\Pi}$

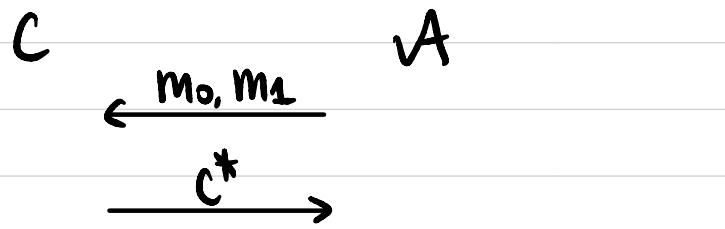


If $\mathcal{A}$ succeeds in Π^M, then (m^*, t^*) is a valid pair for Π^M and hasn't appeared in the queries.

So $(m^*, \tilde{t}^*)$ is a valid pair for $\tilde{\Pi}$ and hasn't appeared in the queries.

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

Step 3: Π instantiated with Π^M is not CPA-secure.



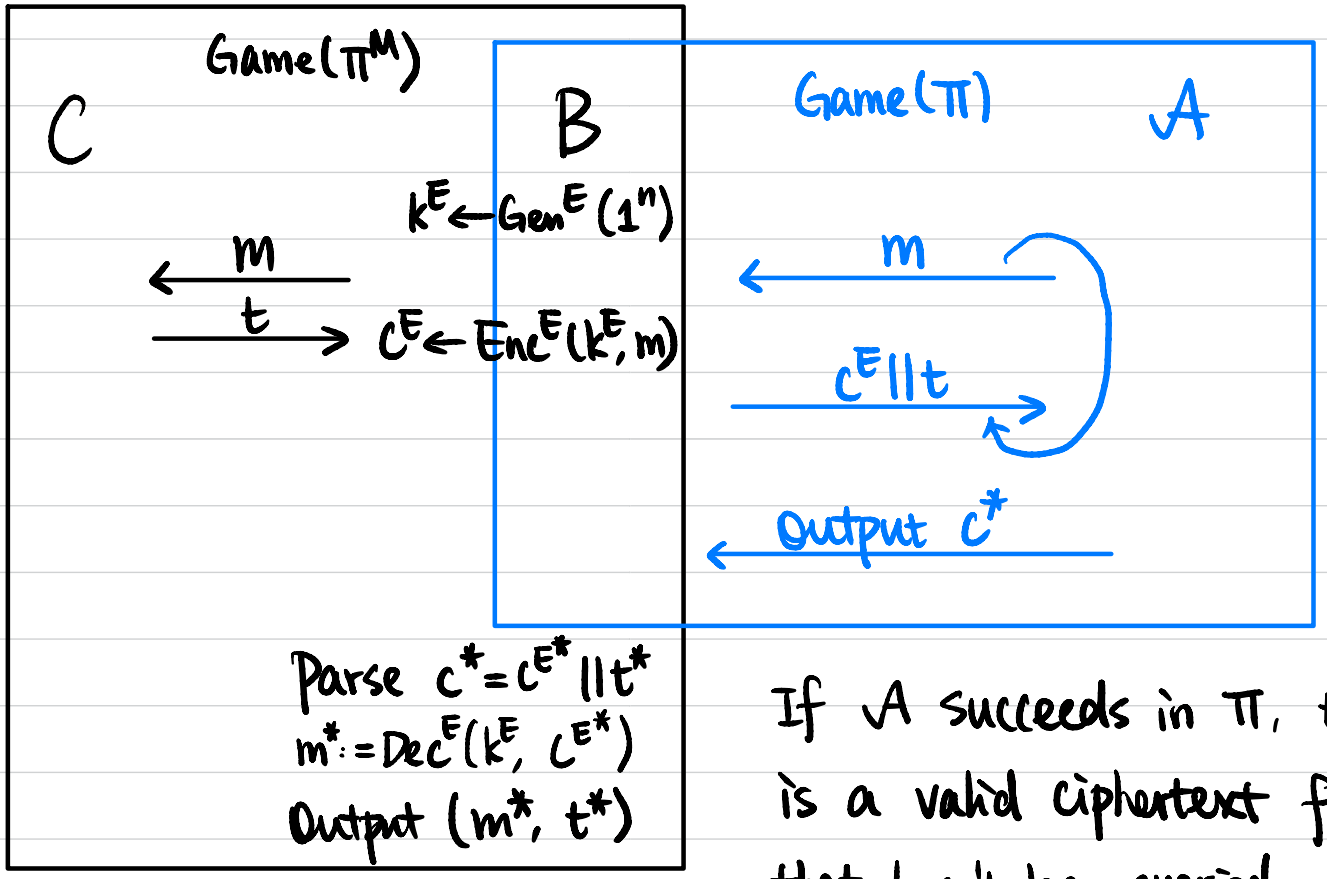
$c^* = \langle c^{E^*}, t^* = \tilde{t}^* \| m^* \rangle$

$m^* = m_0$ or m_1 ?

Thm If Π^M is strongly secure, then $\Pi = (Gen, Enc, Dec)$ is unforgeable.

Proof Assume not, then $\exists$ PPT $\mathcal{A}$ that breaks the unforgeability of Π.

We construct PPT B to break the strong security of Π^M.

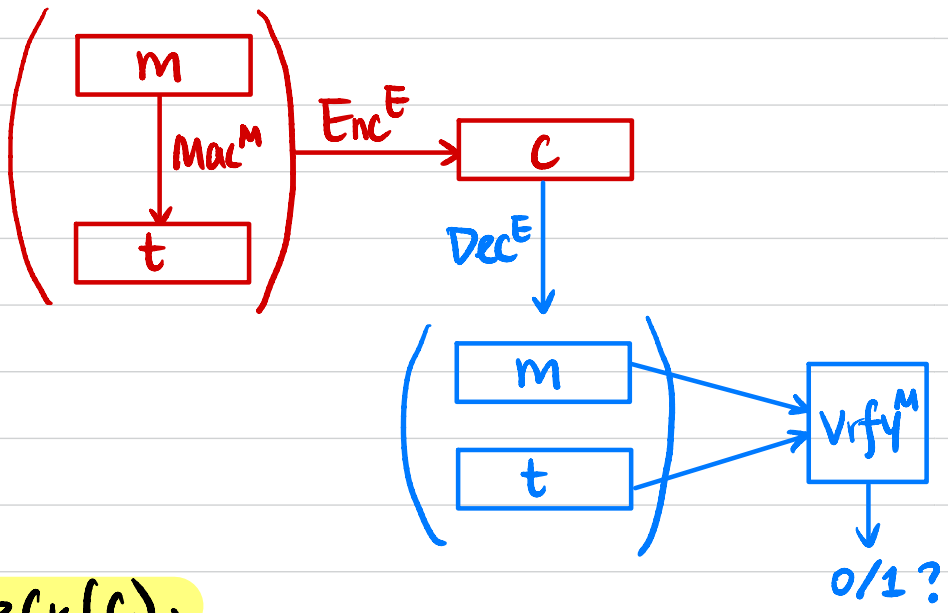


If $\mathcal{A}$ succeeds in Π, then $c^* = c^{E^*} || t^*$ is a valid ciphertext for a message m^* that hasn't been queried.

So (m^*, t^*) is a valid pair for Π^M and hasn't appeared in the queries.

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

Authenticate-then-Encrypt



$Gen(1^n)$:

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

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

Output $k=(k^E, k^M)$

$Enc_k(m)$:

$t \leftarrow Mac^M(k^M, m)$

$c \leftarrow Enc^E(k^E, m||t)$

output c

$Dec_k(c)$:

$m||t := Dec^E(k^E, c)$

$b := Vrfy^M(k^M, (m,t))$

If $b=1$, output m

Otherwise output $\perp$

Q_1: Is it CPA-secure? (exercise)

Q_2: Is it CCA-secure? No!

Q_3: Is it unforgeable? (exercise)

Π is not necessarily CCA-secure.

Step 1: Let $\tilde{\Pi} = (\tilde{Gen}^E, \tilde{Enc}^E, \tilde{Dec}^E)$ be a CPA-secure encryption scheme.
Construct $\Pi^E = (Gen^E, Enc^E, Dec^E)$ as follows:

- $Gen^E(1^n)$: same as $\tilde{Gen}^E$.
- $Enc^E(k^E, m)$: $\tilde{c}^E \leftarrow \tilde{Enc}^E(k^E, m)$

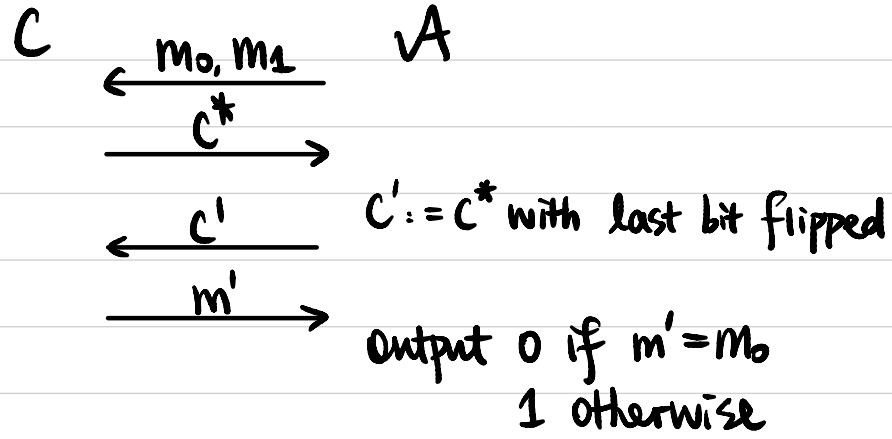
  $b \xleftarrow{\$} \{0,1\}$

  Output $c^E = \tilde{c}^E \| b$ ← or always attach 0
- $Dec^E(k^E, c^E)$: Parse $c^E = \tilde{c}^E \| b$

  Output $\tilde{Dec}^E(k^E, \tilde{c}^E)$

Step 2: If $\tilde{\Pi}$ is CPA-secure, then Π^E is also CPA-secure. (exercise)

Step 3: Π instantiated with Π^M is not CCA-secure



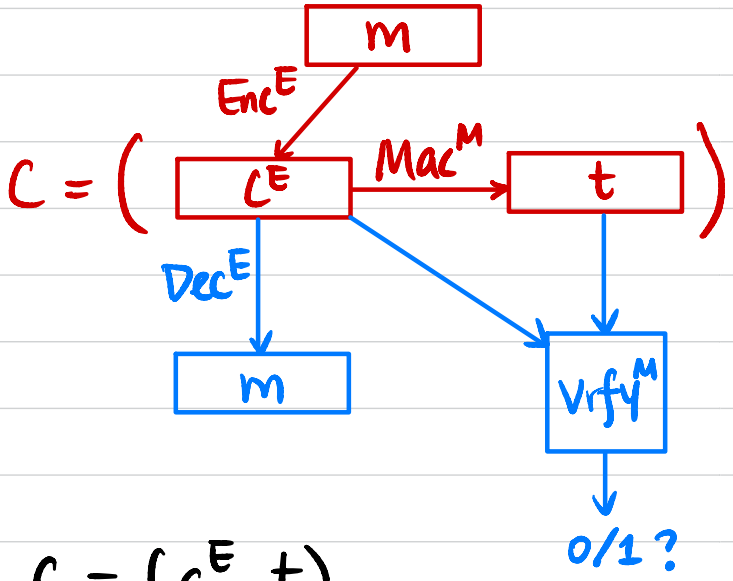
Encrypt-then-Authenticate

$\mathrm{Gen}(1^n)$:

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

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

Output $k = (k^E, k^M)$



$\mathrm{Enc}_k(m)$:

$c^E \leftarrow \mathrm{Enc}^E(k^E, m)$

$t \leftarrow \mathrm{Mac}^M(k^M, c^E)$

Output $c = (c^E, t)$

$\mathrm{Dec}_k(c)$: $c = (c^E, t)$

$m := \mathrm{Dec}^E(k^E, c^E)$

$b := \mathrm{Vrfy}^M(k^M, (c^E, t))$

If $b=1$, output m

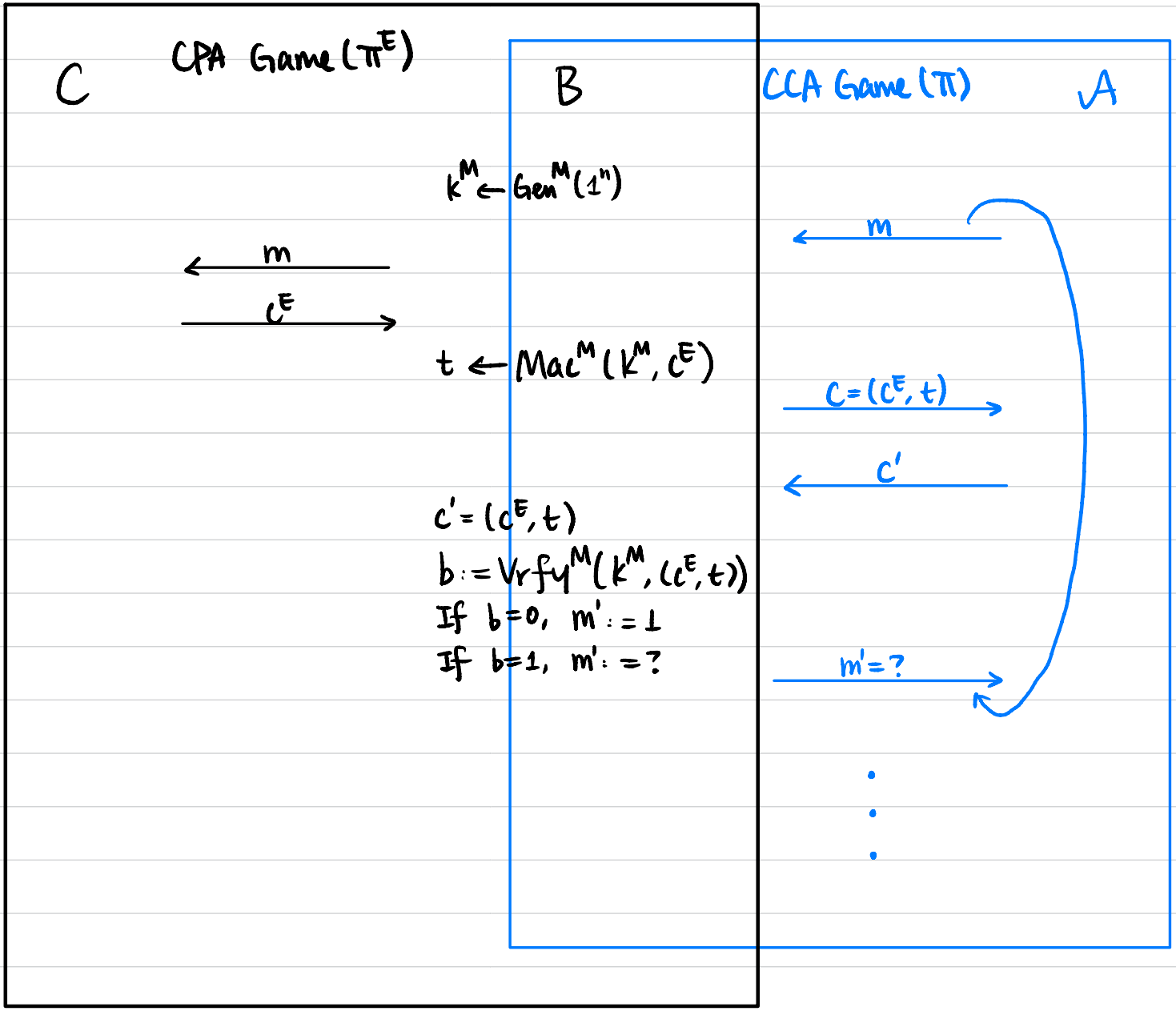
Otherwise output $\perp$

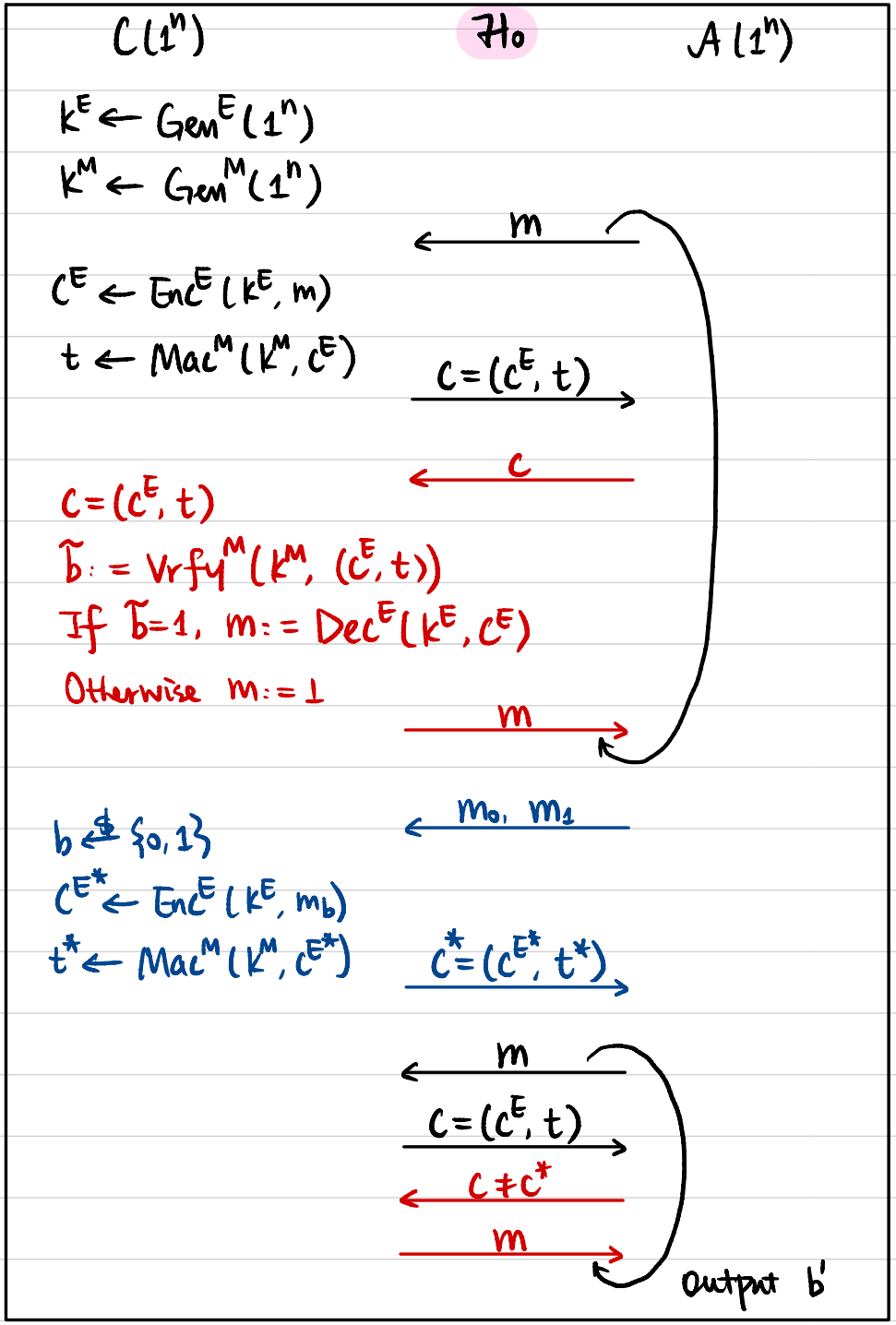
Q_1: Is it CPA-secure? (exercise)

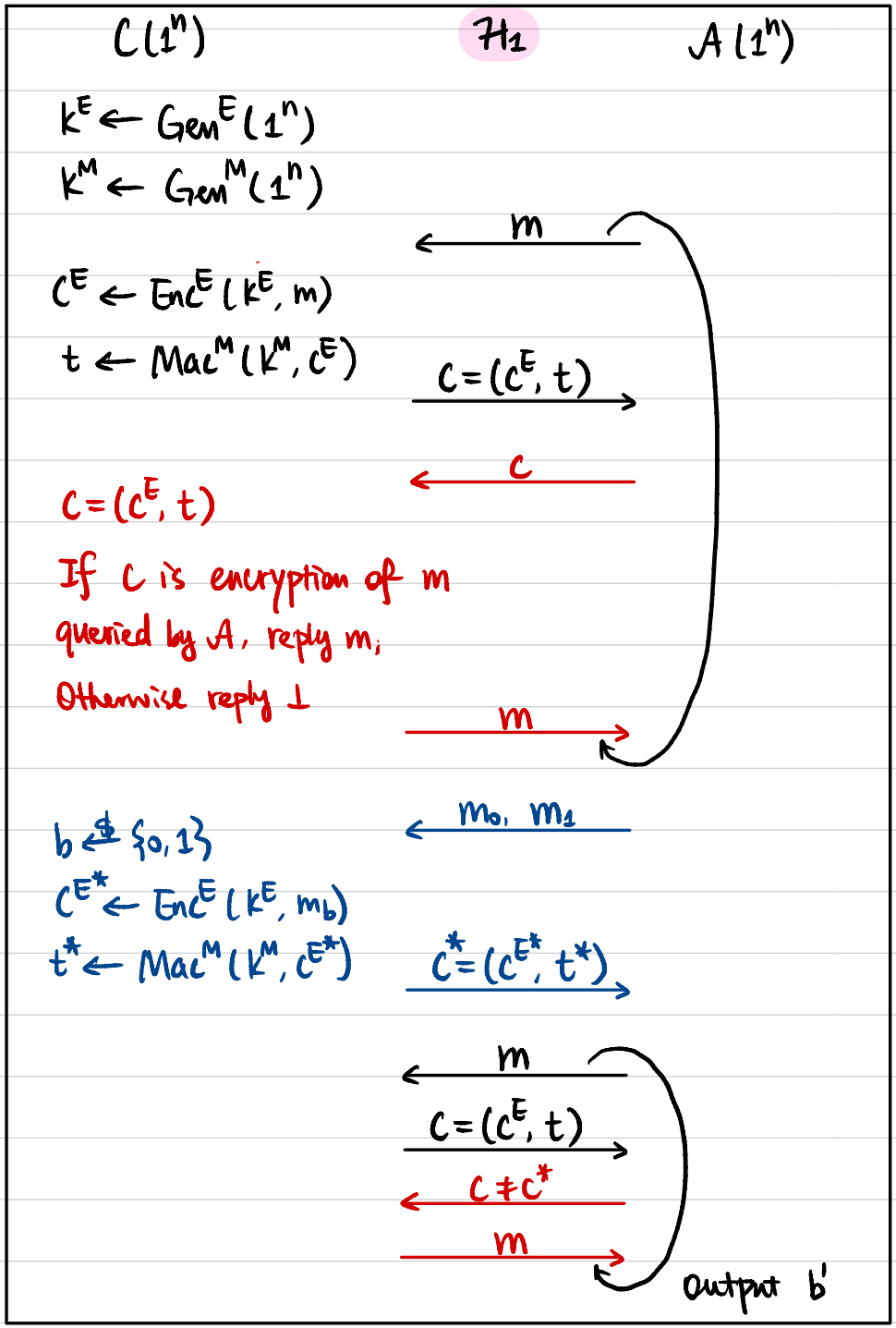
Q_2: Is it CCA-secure?

Q_3: Is it unforgeable? (exercise)

First Attempt: Assume $\exists$ PPT $\mathcal{A}$ that breaks the CCA-security of Π
We construct PPT B to break the CPA-security of Π^E.




$C(1^n)$
H_0
$A(1^n)$
$k^E \leftarrow Gen^E(1^n)$
$k^M \leftarrow Gen^M(1^n)$
m
$c^E \leftarrow Enc^E(k^E, m)$
$t \leftarrow Mac^M(k^M, c^E)$
$c = (c^E, t)$
c
$c = (c^E, t)$
$\tilde{b} := Vrfy^M(k^M, (c^E, t))$
If $\tilde{b}=1$, $m := Dec^E(k^E, c^E)$
Otherwise $m := \perp$
m
m_0, m_1
$b \xleftarrow{\$} \{0,1\}$
$c^{E*} \leftarrow Enc^E(k^E, m_b)$
$t^* \leftarrow Mac^M(k^M, c^{E*})$
$c^* = (c^{E*}, t^*)$
m
$c = (c^E, t)$
$c \neq c^*$
m
output b'


$C(1^n)$
H_1
$A(1^n)$
$k^E \leftarrow Gen^E(1^n)$
$k^M \leftarrow Gen^M(1^n)$
m
$c^E \leftarrow Enc^E(k^E, m)$
$t \leftarrow Mac^M(k^M, c^E)$
$c = (c^E, t)$
c
$c = (c^E, t)$
If c is encryption of m
queried by A, reply m;
Otherwise reply $\perp$
m
m_0, m_1
$b \xleftarrow{\$} \{0,1\}$
$c^{E*} \leftarrow Enc^E(k^E, m_b)$
$t^* \leftarrow Mac^M(k^M, c^{E*})$
$c^* = (c^{E*}, t^*)$
m
$c = (c^E, t)$
$c \neq c^*$
m
output b'

Lemma 1 $\forall$ PPT $\mathcal{A}$. $|\Pr[\mathcal{A} \text{ outputs } 1 \text{ in } H_0] - \Pr[\mathcal{A} \text{ outputs } 1 \text{ in } H_1]| \leq \text{negl}(n)$.

Proof Assume not. then $\exists$ PPT $\mathcal{A}$ that distinguishes H_0 & H_1 with non-negligible probability $\varepsilon(n)$.

We construct a PPT B to break the strong security of π^M.

Lemma 2 $\forall$ PPT A. $|\Pr[b=b' \text{ in } \mathcal{H}_1]| \leq \text{negl}(n)$.

Proof Assume not. then $\exists$ PPT A s.t. $|\Pr[b=b' \text{ in } \mathcal{H}_1]| \geq \text{non-negl}(n)$.

We construct a PPT B to break the CPA-security of π^E.