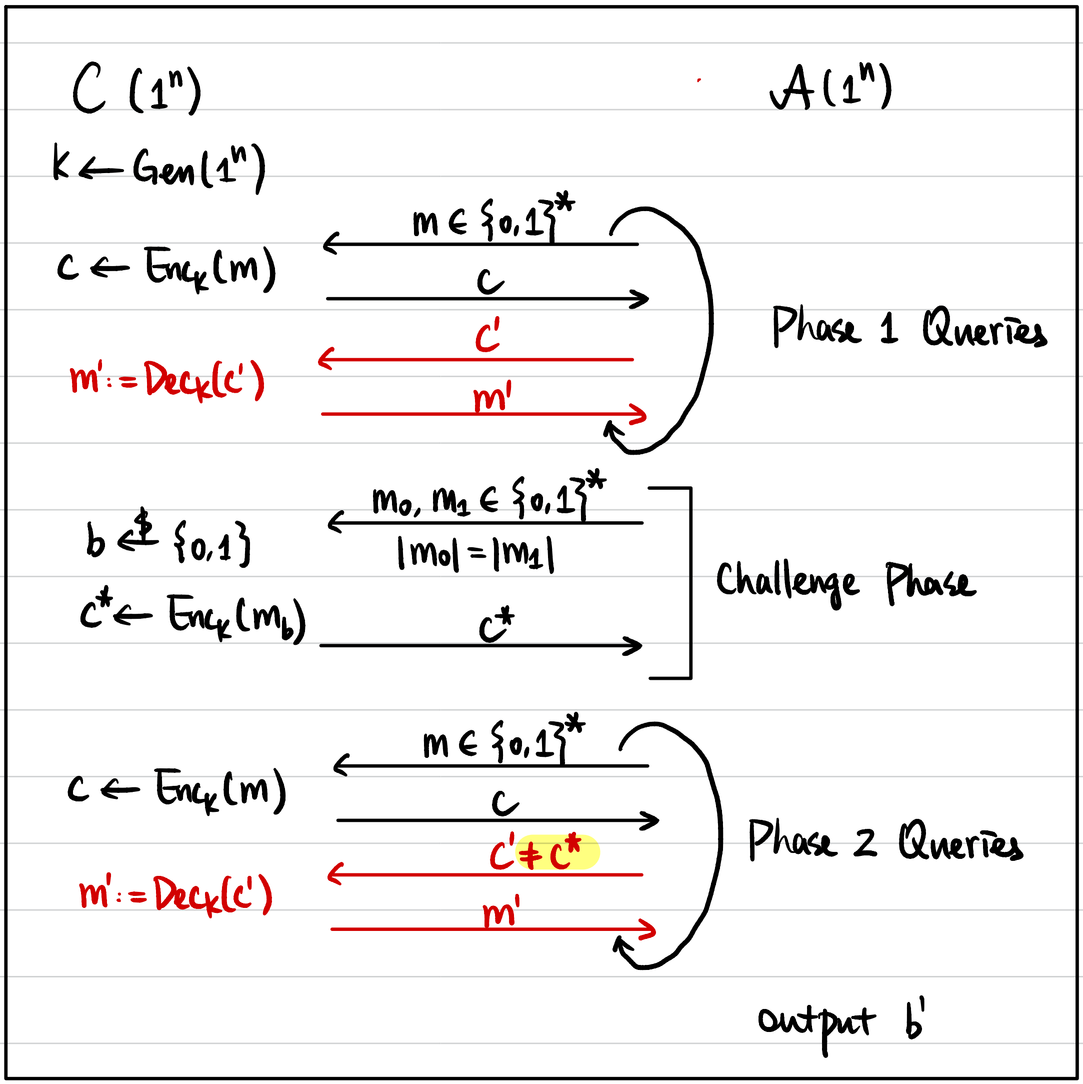
CSCI 1510

- Generic Constructions and Proofs of Authenticated Encryption

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



Unforgeability

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

$C(1^n)$		$\mathcal{A}(1^n)$
$k \leftarrow \mathrm{Gen}(1^n)$		
	$\xleftarrow{\; m \in \{0,1\}^* \;}$	
$c \leftarrow \mathrm{Enc}_k(m)$		
	$\xrightarrow{\; c \;}$	
		output c^*

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

$m^* := \mathrm{Dec}_k(c^*)$

$\mathrm{EncForge}_{\mathcal{A},\Pi} = 1$ ($\mathcal{A}$ 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.

Intuitions

Can we have an encryption scheme that is unforgeable but not CCA-secure?

ct → ct' encrypting the same message

But hard to generate a new ct encrypting a new message

Can we have an encryption scheme that is CCA-secure but not unforgeable?

Easy to generate a new ct encrypting a new message

But hard to ct → ct' encrypting the same message

Generic Constructions

Let $\Pi^E = (\text{Gen}^E, \text{Enc}^E, \text{Dec}^E)$ be a CPA-secure encryption scheme.
Let $\Pi^M = (\text{Gen}^M, \text{Mac}^M, \text{Vrfy}^M)$ be a strongly secure MAC scheme.

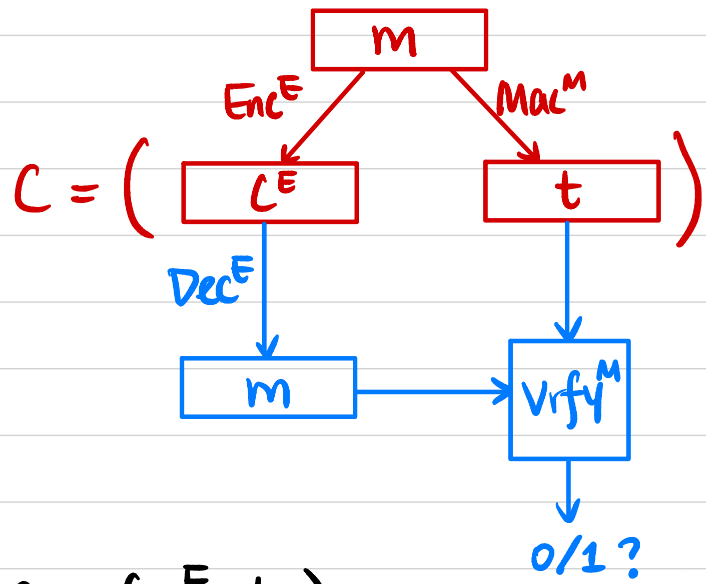
How to construct an authenticated encryption scheme?

① Encrypt-and-Authenticate

② Authenticate-then-Encrypt

③ Encrypt-then-Authenticate

Encrypt-and-Authenticate



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):

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

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

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

Dec$_k$(c): $c = (c^E, t_2)$

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

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

If $b = 1$, output m

Otherwise output $\perp$

Q1: Is it CPA-secure? No!

Q2: Is it CCA-secure? No!

Q3: Is it unforgeable? Yes!

Π is not necessarily CPA-secure.

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

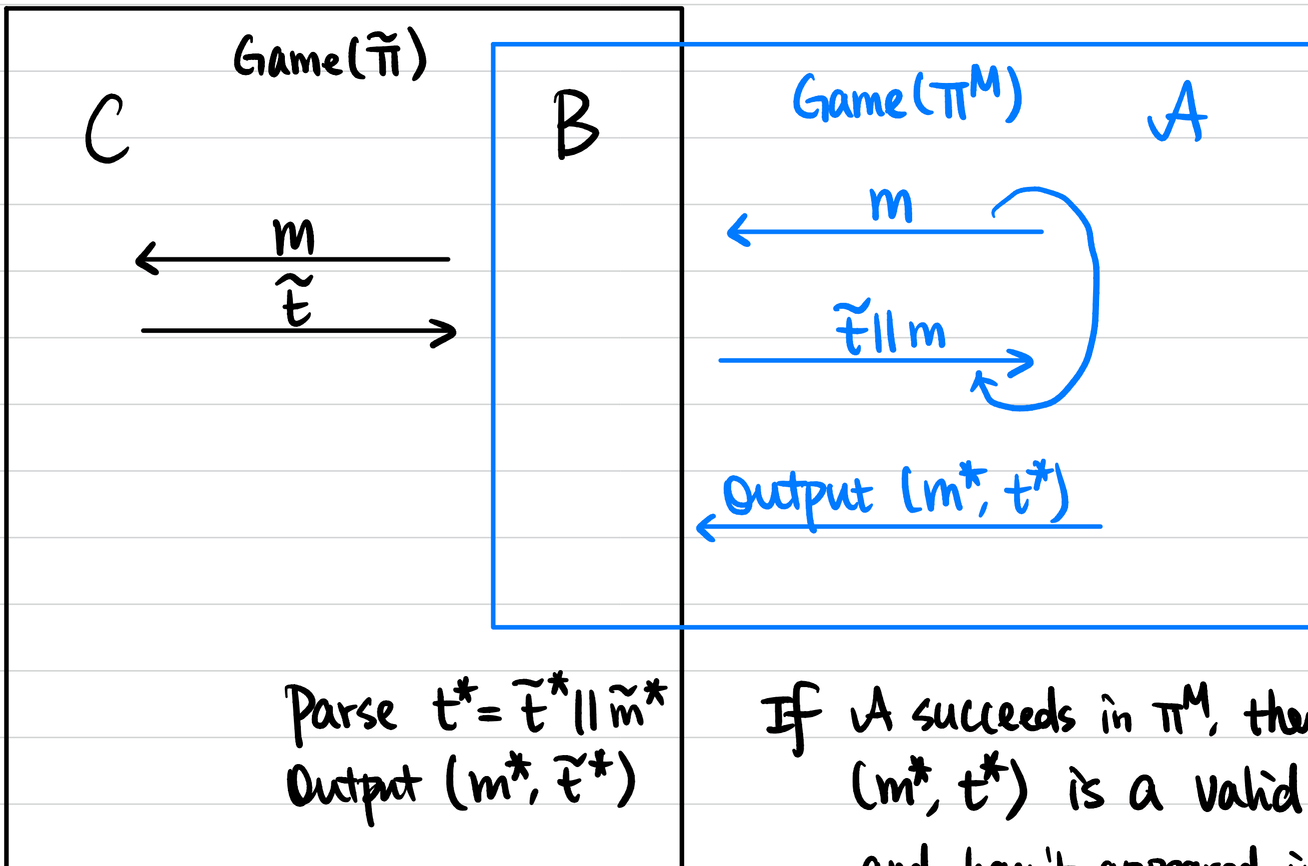
Construct $\Pi^M = (Gen^M, Mac^M, Vrfy^M)$ as follows:

- $Gen^M(1^n)$: same as $\widetilde{Gen}^M$.
- $Mac^M(k^M, m)$: $\tilde{t} \leftarrow \widetilde{Mac}^M(k^M, m)$
  Output $t = \tilde{t} \| m$
- $Vrfy^M(k^M, (m,t))$: Parse $t = \tilde{t} \| \tilde{m}$
  Output 1 iff $\widetilde{Vrfy}^M(k^M, (\tilde{t}, m)) = 1 \wedge m = \tilde{m}$.

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

<u>Proof</u> 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.

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

$$\mathcal{C} \xleftarrow{\quad m_0,\, m_1 \quad} \mathcal{A}$$

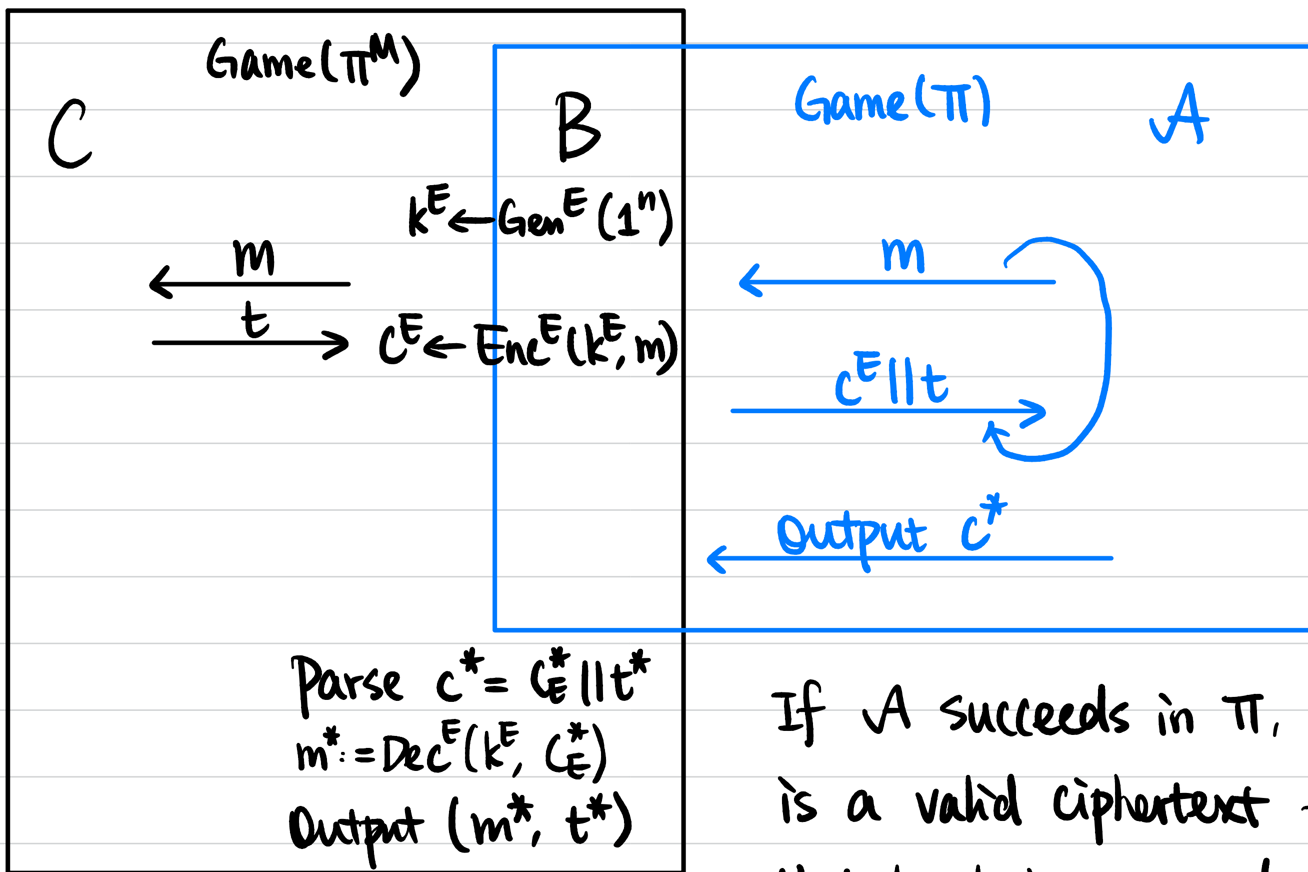
$$\mathcal{C} \xrightarrow{\quad c^* \quad} \mathcal{A}$$

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

$$m^* = m_0 \text{ or } m_1 \ ?$$

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

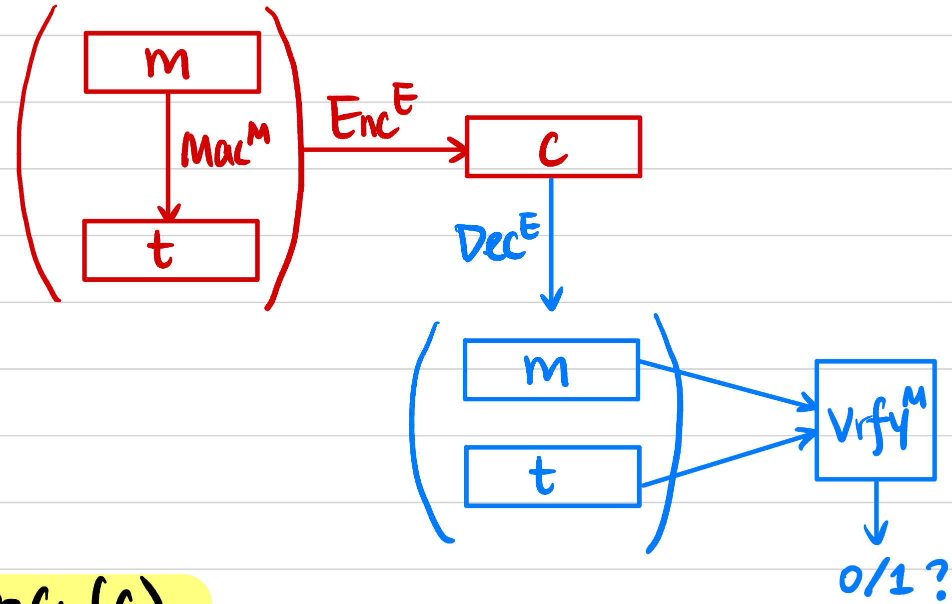


If $\mathcal{A}$ succeeds in Π, then $c^* = c_E^* \| t^*$ is a valid ciphertext for a message m^* that hasn't been queried.

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 $\perp$

Q1: Is it CPA-secure? (Yes, exercise)

Q2: Is it CCA-secure? No!

Q3: Is it unforgeable? (Yes, exercise)

Π is not necessarily CCA-secure.

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

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

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

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

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

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

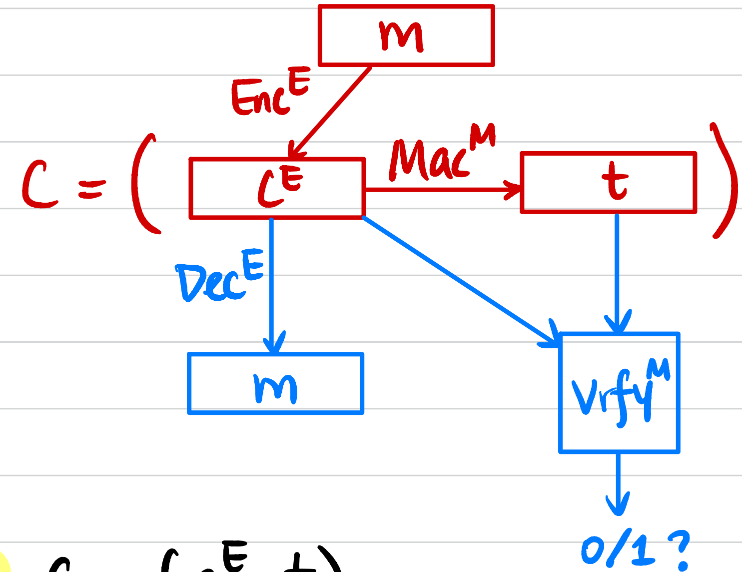
$\xleftarrow{\quad m_0, m_1 \quad}$

$\xrightarrow{\quad c^* \quad}$

$\xleftarrow{\quad c' \quad}$ $\qquad$ $c' := c^*$ with last bit flipped

$\xrightarrow{\quad m' \quad}$ $\qquad$ output 0 if $m' = m_0$
1 otherwise

Encrypt-then-Authenticate



$Gen(1^n)$:

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

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

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

$Enc_k(m)$:

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

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

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

$Dec_k(c)$: $c = (c^E, t)$

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

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

If $b = 1$, output m

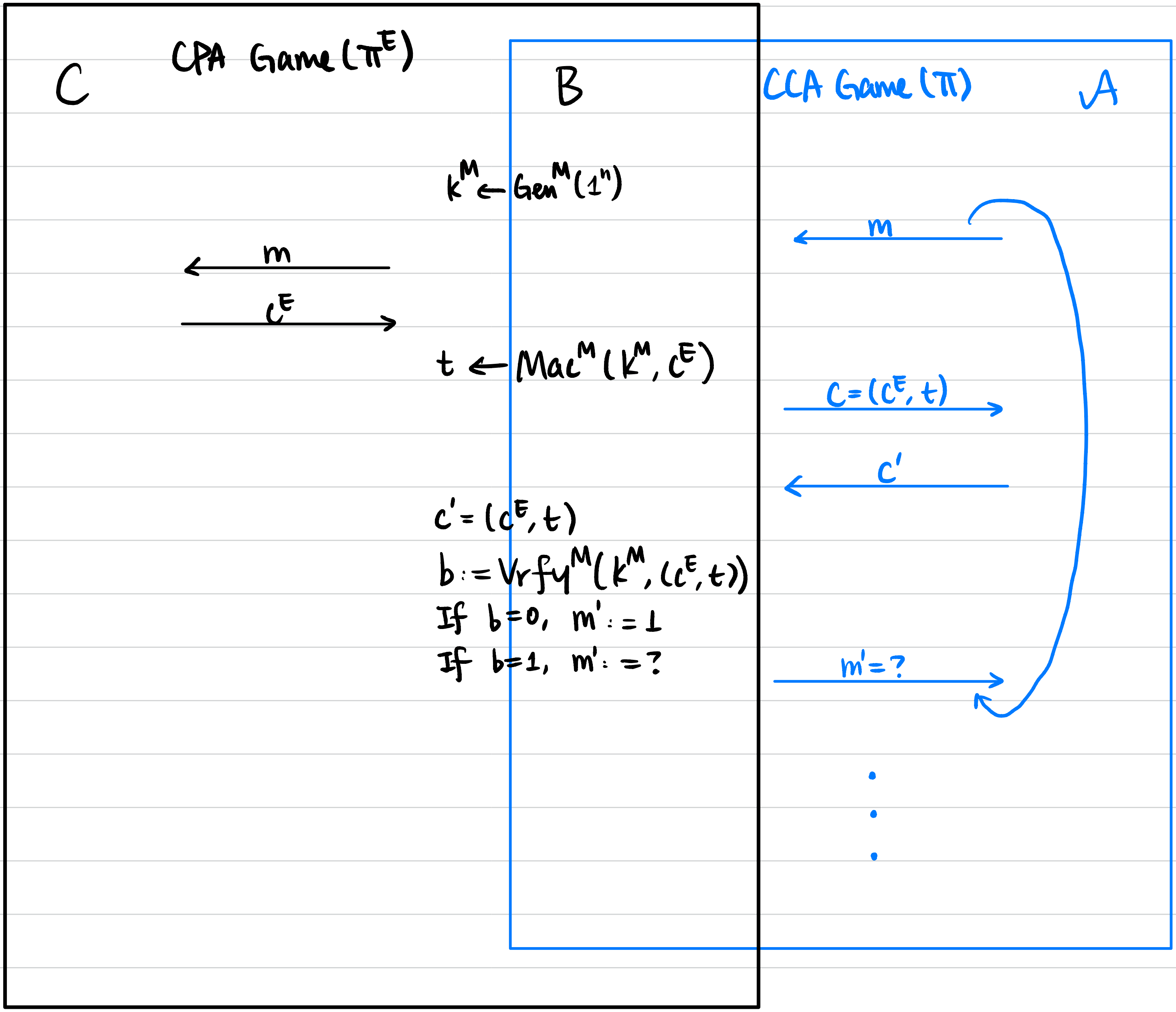
Otherwise output $\perp$

Q1: Is it CPA-secure ?

Q2: Is it CCA-secure ? Yes !

Q3: Is it unforgeable ? (Yes, exercise)

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



$\mathcal{H}_0$

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

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

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

$\xleftarrow{\quad m \quad}$

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

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

$\xrightarrow{\quad c=(c^E, t) \quad}$

$\xleftarrow{\quad c \quad}$

$c=(c^E, t)$

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

If $\tilde{b}=1$, $m := Dec^E(k^E, c^E)$

Otherwise $m := \perp$

$\xrightarrow{\quad m \quad}$

$\xleftarrow{\quad m_0, m_1 \quad}$

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

$c^{E*} \leftarrow Enc^E(k^E, m_b)$

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

$\xrightarrow{\quad c^* = (c^{E*}, t^*) \quad}$

$\xleftarrow{\quad m \quad}$

$\xrightarrow{\quad c=(c^E, t) \quad}$

$\xleftarrow{\quad c \neq c^* \quad}$

$\xrightarrow{\quad m \quad}$

Output b'

$\mathcal{H}_1$

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

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

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

$\xleftarrow{\quad m \quad}$

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

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

$\xrightarrow{\quad c=(c^E, t) \quad}$

$\xleftarrow{\quad c \quad}$

$c=(c^E, t)$

If c is encryption of m queried by $\mathcal{A}$, reply m;

Otherwise reply $\perp$

$\xrightarrow{\quad m \quad}$

$\xleftarrow{\quad m_0, m_1 \quad}$

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

$c^{E*} \leftarrow Enc^E(k^E, m_b)$

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

$\xrightarrow{\quad c^* = (c^{E*}, t^*) \quad}$

$\xleftarrow{\quad m \quad}$

$\xrightarrow{\quad c=(c^E, t) \quad}$

$\xleftarrow{\quad c \neq c^* \quad}$

$\xrightarrow{\quad m \quad}$

Output b'

Lemma 1 $\forall$ PPT $\mathcal{A}$, $|\Pr[\mathcal{A} \text{ outputs } 1 \text{ in } \mathcal{H}_0] - \Pr[\mathcal{A} \text{ outputs } 1 \text{ in } \mathcal{H}_1]| \le \mathrm{negl}(n)$.

Proof Assume not, then $\exists$ PPT $\mathcal{A}$ that distinguishes $\mathcal{H}_0$ & $\mathcal{H}_1$ with non-negligible probability $\varepsilon(n)$.

Game (Π^M)

$\mathcal{H}_0 / \mathcal{H}_1$

C B $\mathcal{A}$

$i^* \xleftarrow{\$} \{1, 2, \cdots, Q(n)\}$

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

$\mathcal{A} \to B$: m

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

$B \to C$: c^E

$C \to B$: t

$B \to \mathcal{A}$: $c = (c^E, t)$

$\mathcal{A} \to B$: c

$c = (c^E, t)$

If c is encryption of m queried by $\mathcal{A}$, reply m;

Otherwise if this is the i^*-th query, output (c^E, t)

Otherwise reply $\perp$

$B \to \mathcal{A}$: m

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

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

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

$B \to C$: c^{E*}

$C \to B$: t^*

$B \to \mathcal{A}$: $c^* = (c^{E*}, t^*)$

$\mathcal{A} \to B$: m

$B \to \mathcal{A}$: $c = (c^E, t)$

$\mathcal{A} \to B$: $c \neq c^*$

$B \to \mathcal{A}$: m

$\mathcal{A} \to B$: Output b'

It must be the case that $\mathcal{A}$ queries for decryption of a new, valid ciphertext with probability at least $\varepsilon(n)$.

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

$Q(n) := \max \#$ of queries by $\mathcal{A}$.

$\Pr[B \text{ outputs a valid new pair } (c^E, t)]$

$\ge \varepsilon(n) \cdot \frac{1}{Q(n)}$ → non-negligible