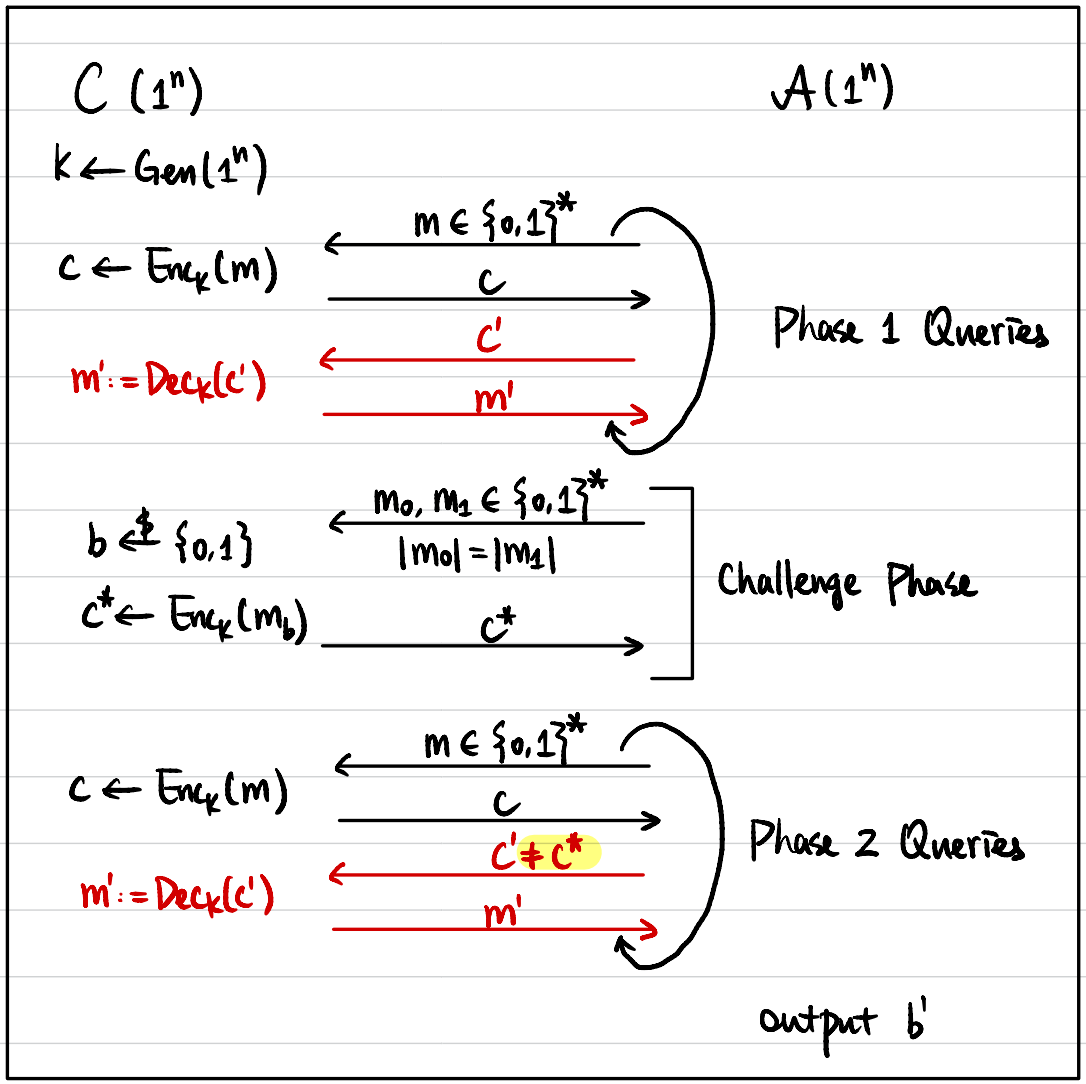
CSCI 1510

This Lecture:

- Generic Constructions of Authenticated Encryption (continued)
- Collision-Resistant Hash Function
- Birthday Attacks
- Merkle-Damgård Transform

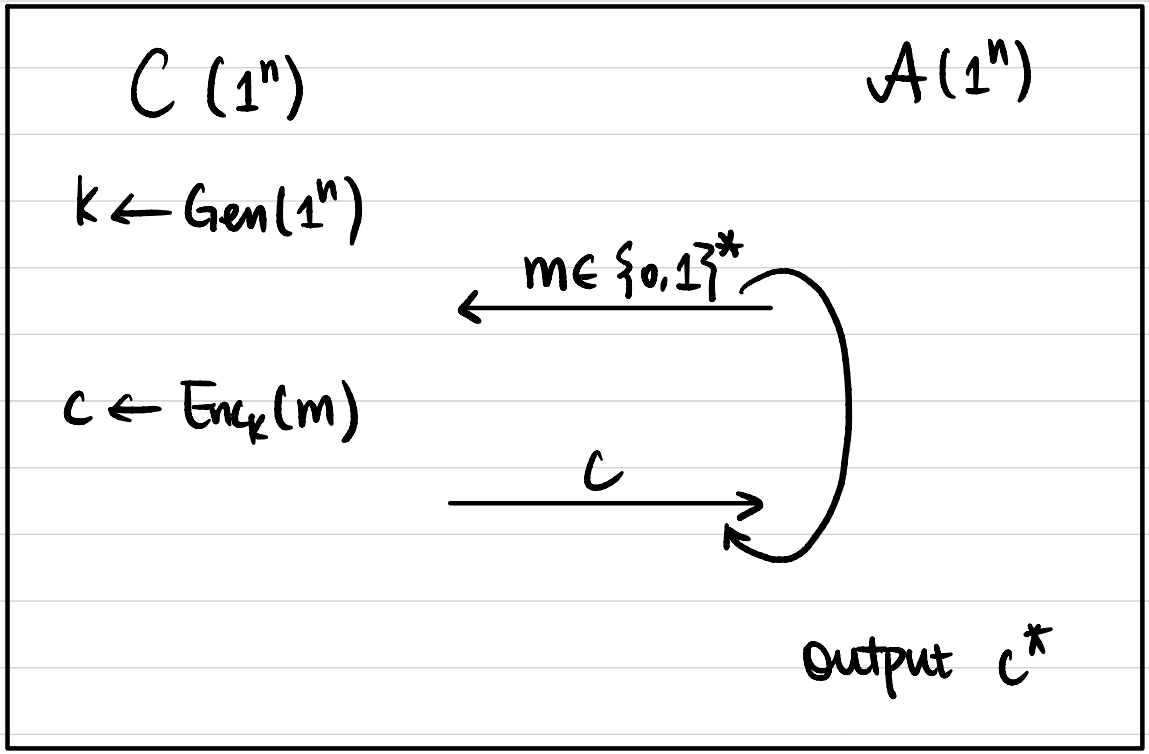
Chosen Ciphertext Attack (CCA) Security

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**.

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

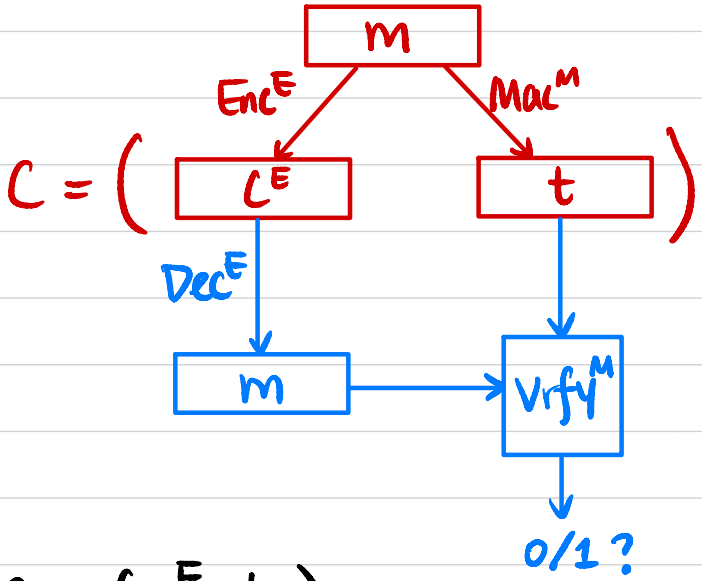
Encrypt-and-Authenticate

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

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

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

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

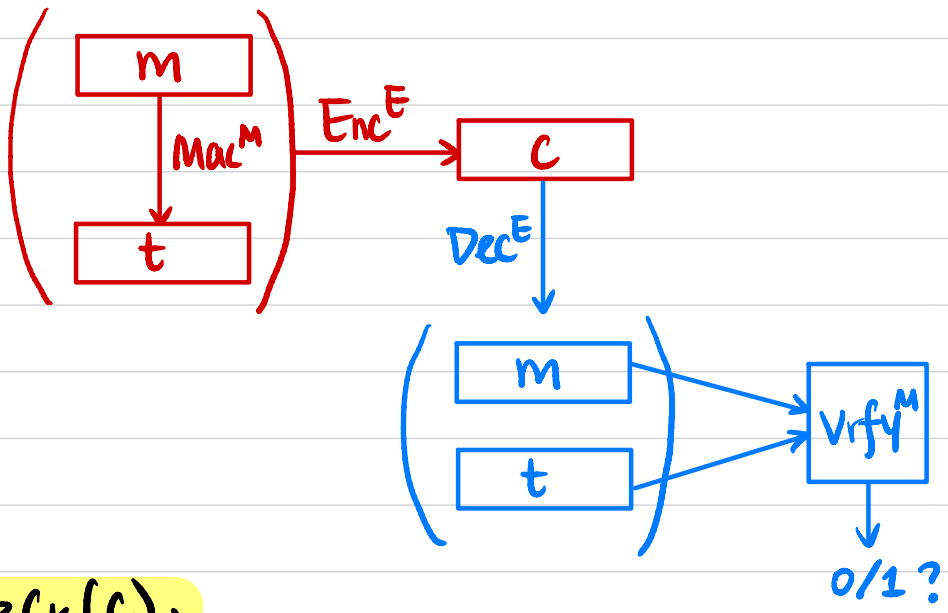
Otherwise output $\perp$

Q_1: Is it CPA-secure? No!

Q_2: Is it CCA-secure? No!

Q_3: Is it unforgeable? Yes!

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)

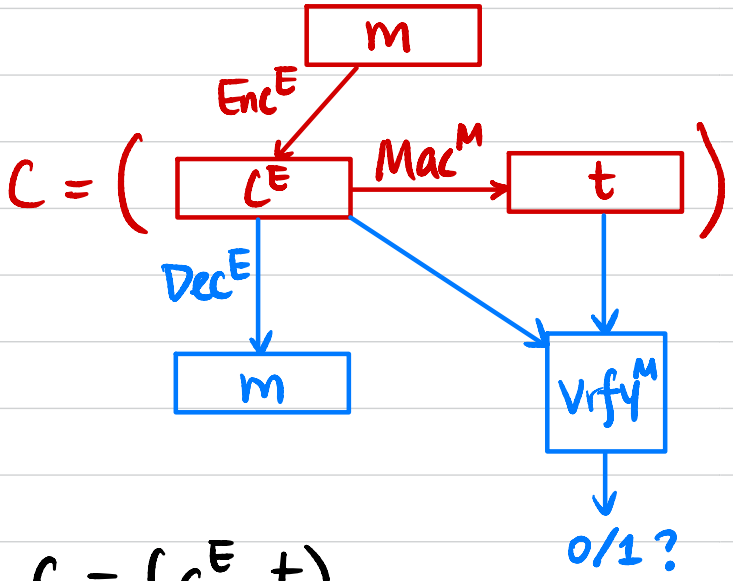
Encrypt-then-Authenticate

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

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

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

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

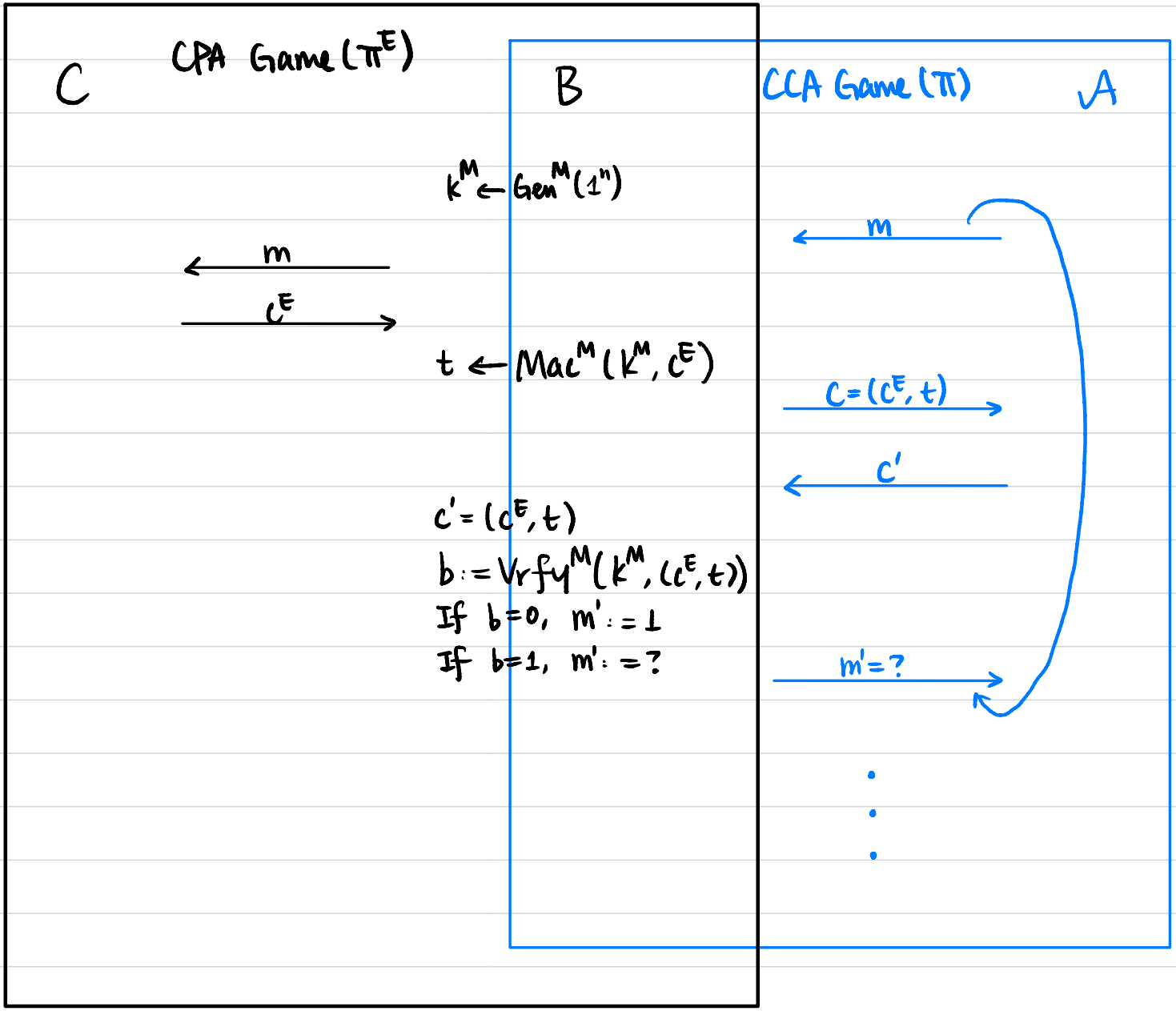
Otherwise output $\perp$

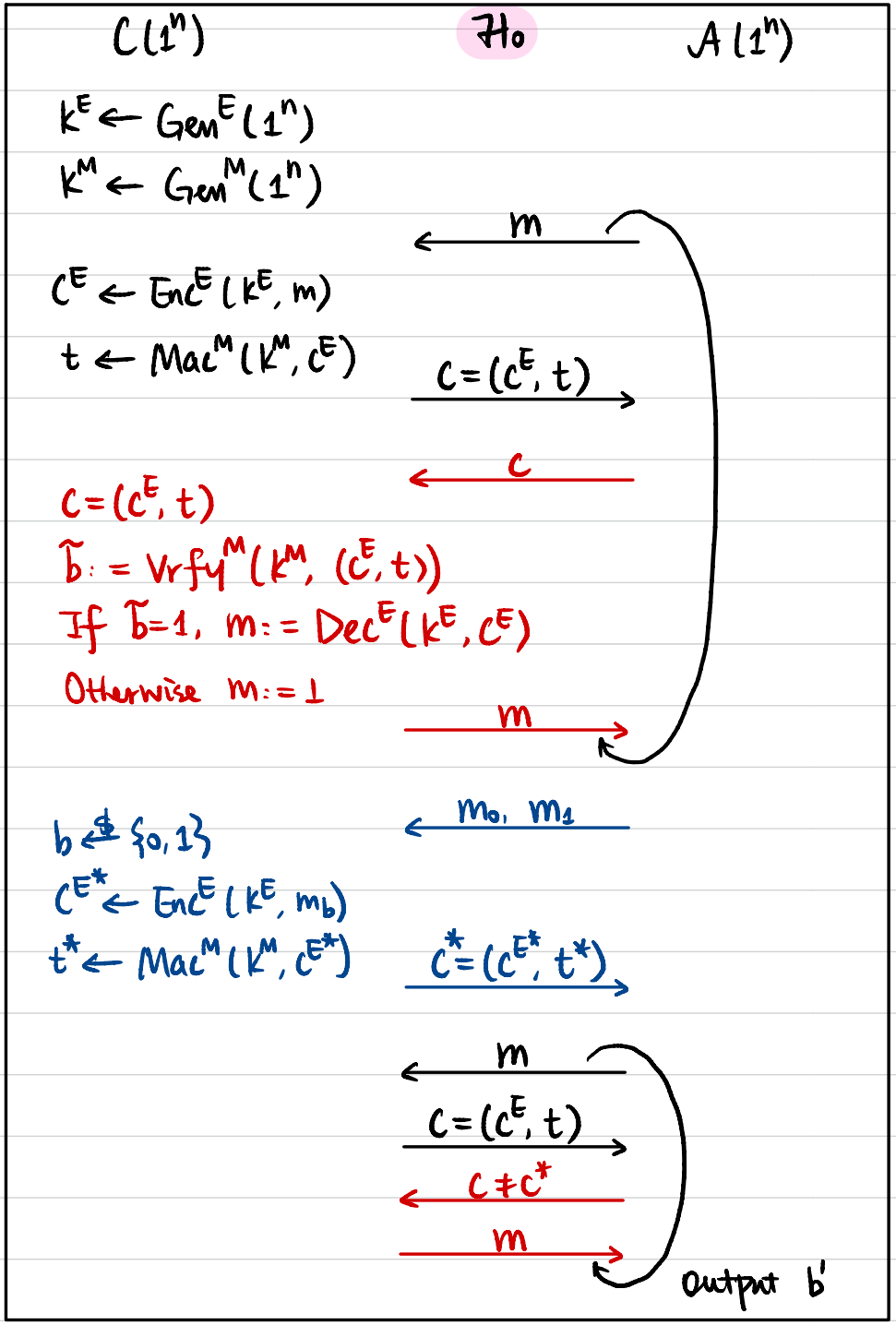
Q_1: Is it CPA-secure? (exercise)

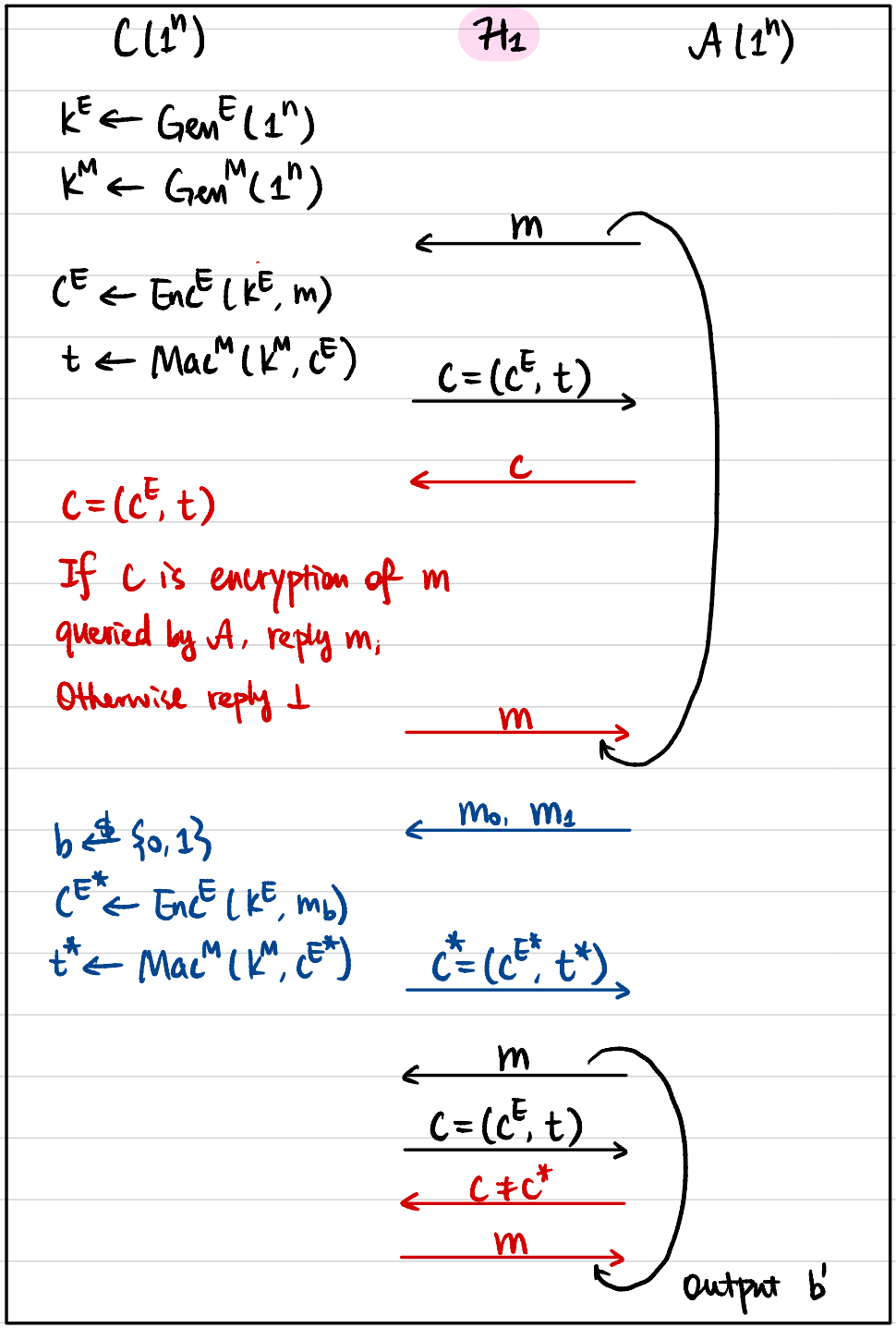
Q_2: Is it CCA-secure?

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.

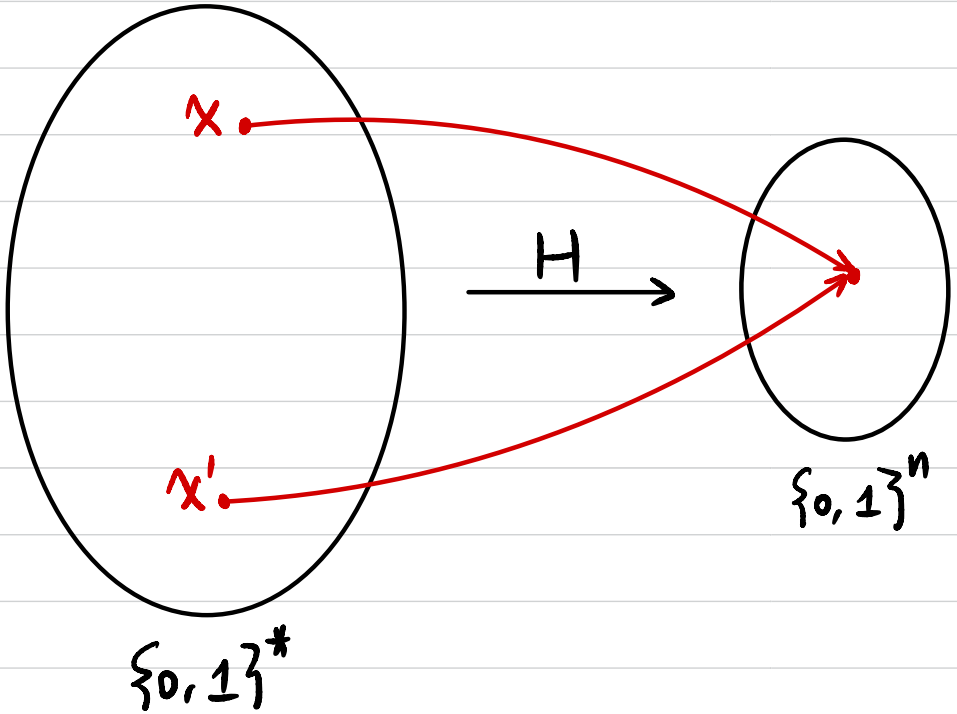
Intuitions

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

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

Cryptographic Hash Function

$H: \{0,1\}^* \longrightarrow \{0,1\}^n$



Collision-Resistant Hash Function (CRHF):

It's computationally hard to find $x, x' \in \{0,1\}^*$ s.t.

$x \neq x'$, $H(x) = H(x')$ (collision)

Collision-Resistant Hash Function (CRHF)

- **Syntax:**

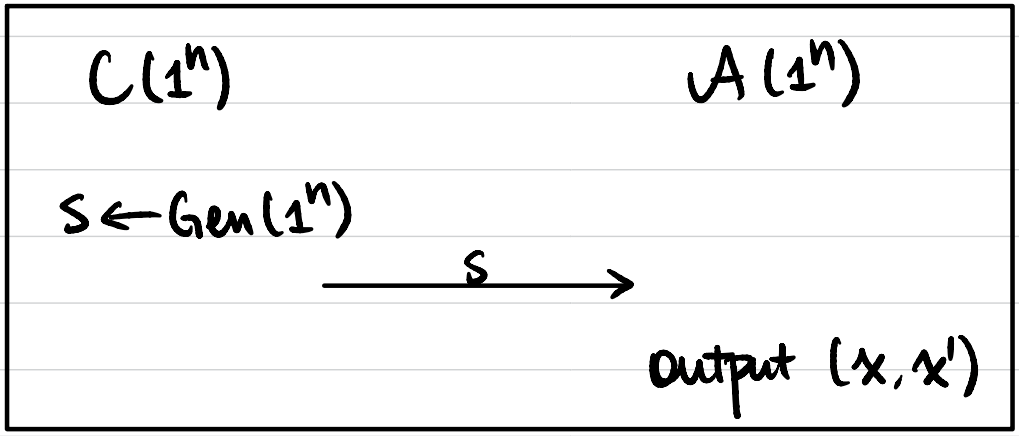
  A hash function is defined by a pair of PPT algorithms (Gen, H):

  - $Gen(1^n)$: output s
  - $H^s(x)$: $x \in \{0,1\}^*$, output $h \in \{0,1\}^{\ell(n)}$

- **Security**

  A hash function (Gen, H) is **collision-resistant** if

  $\forall$ PPT $\mathcal{A}$, $\exists$ negligible function $\varepsilon(\cdot)$ s.t. $\Pr[x \neq x' \wedge H^s(x) = H^s(x')] \leq \varepsilon(n)$.



- **Why does it have to be a keyed function (theoretically)?**

How to find a collision ?

$$H^s : \{0,1\}^* \longrightarrow \{0,1\}^l$$

Try $H^s(x_1), H^s(x_2), \cdots, H^s(x_q)$

If $H(x_i)$ outputs a random value,
what's the probability of finding a collision ?

If $q = 2^l + 1 \Rightarrow$ prob. $= 1$

If $q = 2 \Rightarrow$ prob. $= ?$

If $q = k \Rightarrow$ prob. $= ?$

Birthday Problem / Paradox

There are q students in a class.

Assume each student's birthday is a random $y_i \xleftarrow{\$} [365]$

What's the probability of a collision?

$q = 366 \Rightarrow$ prob. $= 1$

$q = 23 \Rightarrow$ prob. $\simeq 50\%$

$q = 70 \Rightarrow$ prob. $\simeq 99.9\%$

$y_i \xleftarrow{\$} [N]$

$q = N+1 \Rightarrow$ prob. $= 1$

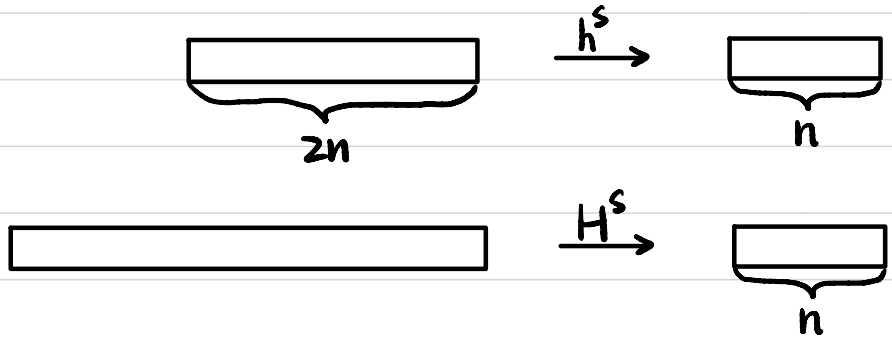
$q = \sqrt{N} \Rightarrow$ prob. $\simeq 50\%$

If security parameter $n = 128$, $l = ?$

Domain Extension: Merkle-Damgård Transform

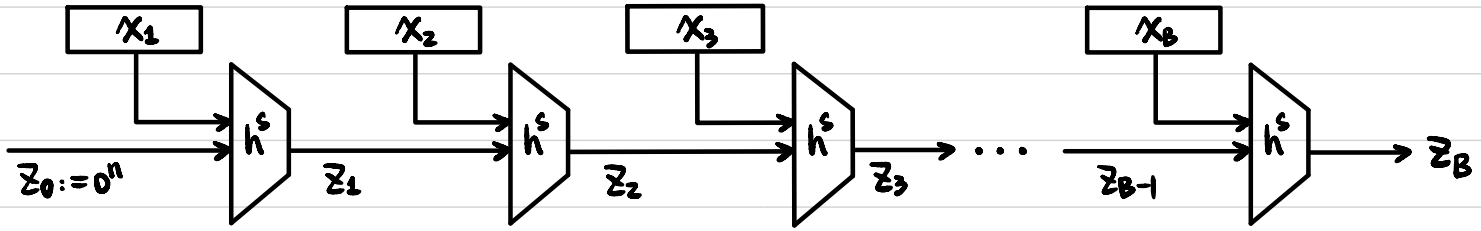
Given a CRHF (Gen, h) from $\{0,1\}^{2n}$ to $\{0,1\}^n$.

Construct a CRHF (Gen, H) from $\{0,1\}^*$ to $\{0,1\}^n$.



① Assume $|x|$ is a multiple of n

② Parse $x = x_1 \| x_2 \| \cdots \| x_B$, $x_i \in \{0,1\}^n$ $\forall i \in [B]$



$z_0 := 0^n$ $\quad z_i := h^s(z_{i-1} \| x_i)$ $\forall i \in [B]$ $\quad H^s(x) := z_B$.

Is this a CRHF for arbitrary-length messages (multiple of n)?