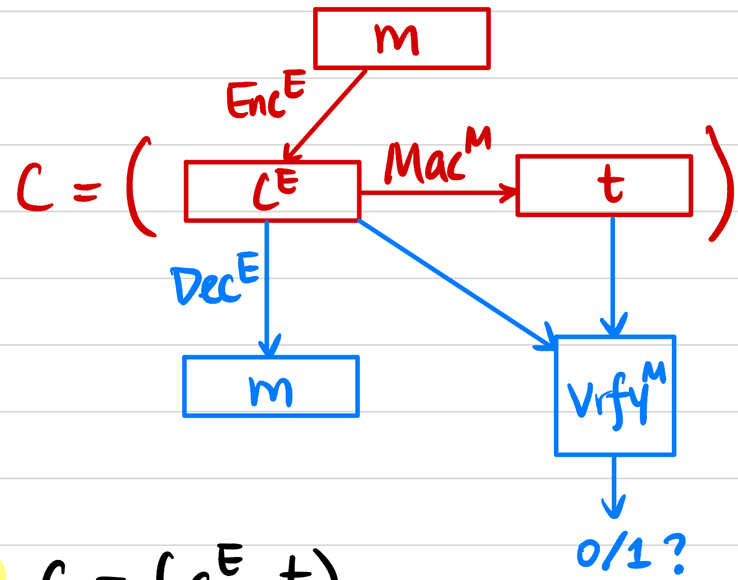
CSCI 1510

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

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)

$C(1^n)$ $\quad\mathcal{H}_0\quad$ $\mathcal{A}(1^n)$

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

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

$\xleftarrow{\quad m \quad}$

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

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

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

$\xleftarrow{\quad c \quad}$

$c=(c^E, t)$

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

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'

$C(1^n)$ $\quad\mathcal{H}_1\quad$ $\mathcal{A}(1^n)$

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

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

$\xleftarrow{\quad m \quad}$

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

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

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

$\xleftarrow{\quad c \quad}$

$c=(c^E, t)$

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

Otherwise reply $\perp$

$\xrightarrow{\quad m \quad}$

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

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

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

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

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

$\xleftarrow{\quad m \quad}$

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

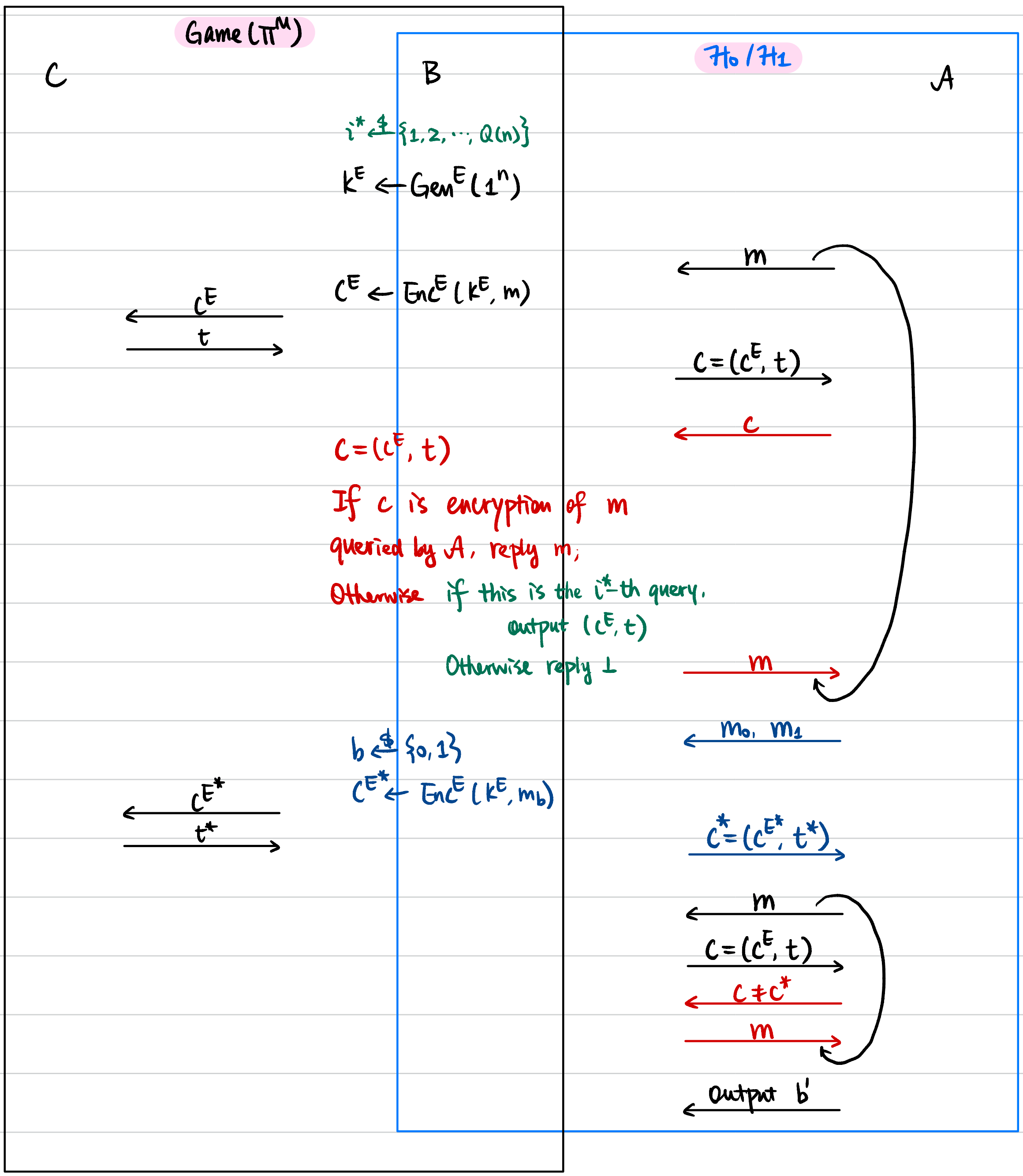
$\xleftarrow{\quad c \neq c^* \quad}$

$\xrightarrow{\quad m \quad}$

Output b'

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

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



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.

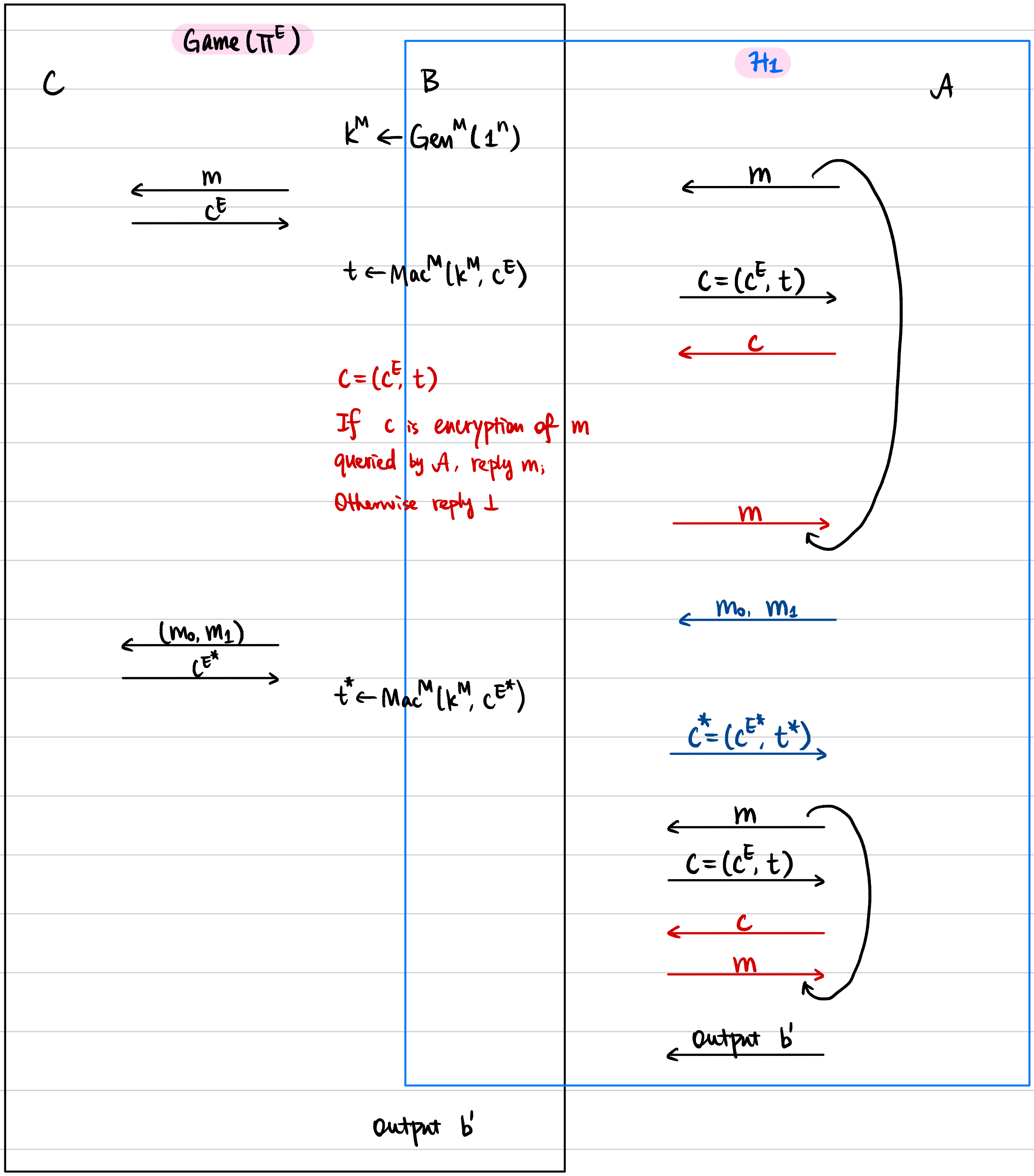
$Q(n) := \max \#$ of queries by $\mathcal{A}$.

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

$\geq \varepsilon(n) \cdot \dfrac{1}{Q(n)} \rightarrow$ non-negligible

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

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



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

$\Pr[B \text{ outputs } b=b' \text{ in CPA-game}(\pi^E)]$

$= \Pr[\mathcal{A} \text{ outputs } b=b' \text{ in } \mathcal{H}_1]$

$\ge non\text{-}negl(n) + \frac{1}{2}$

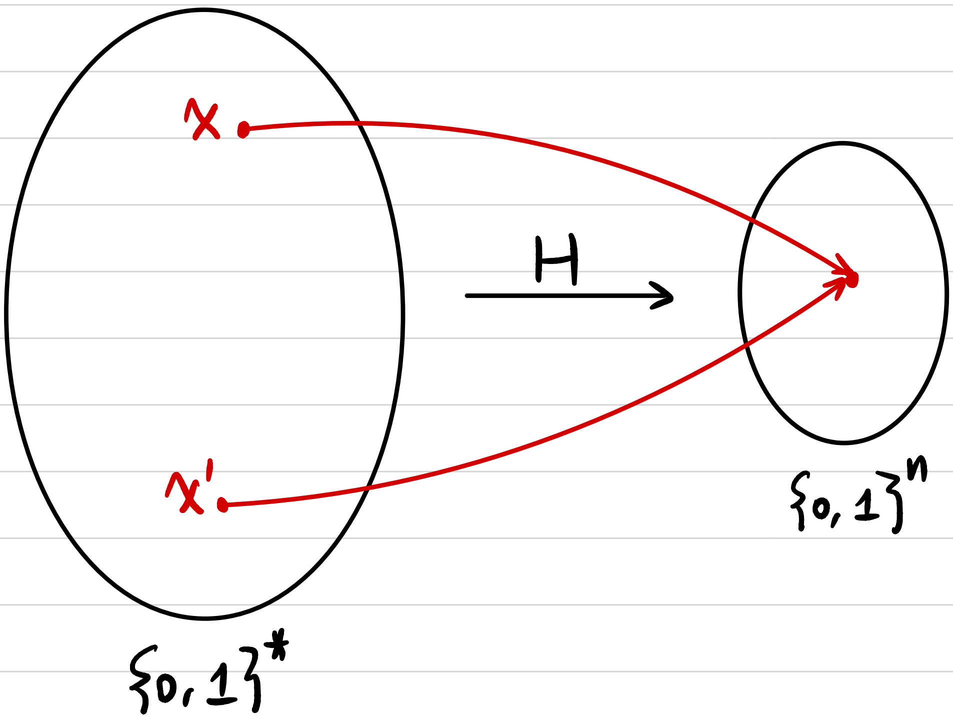
Cryptographic Hash Function

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

$\forall$ PPT $\mathcal{A}$, $\Pr[\mathcal{A}$ finds a collision$] \leq negl(n)$?

$\exists$ PPT $\mathcal{A}^*(x, x')$:

output x, x'



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)

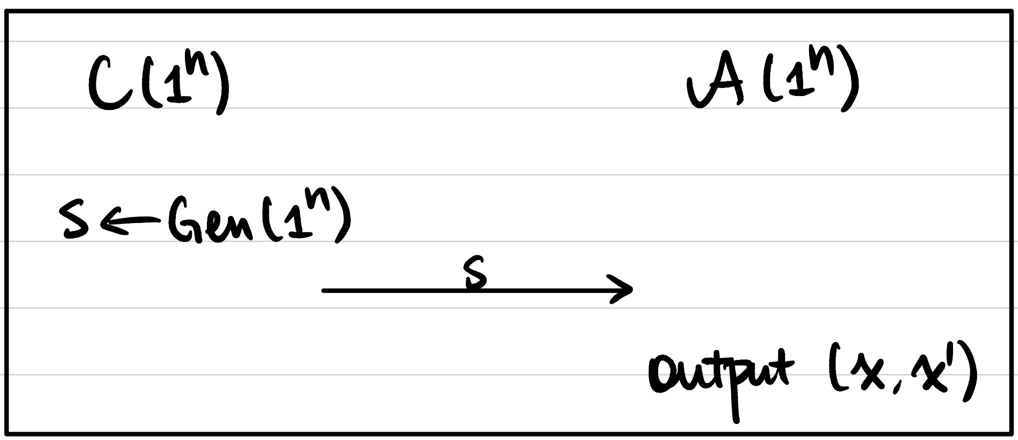
Collision-Resistant Hash Function (CRHF)

- **Syntax:**

  A hash function is defined by a pair of PPT algorithms (Gen, H):
  - $\mathrm{Gen}(1^n)$: 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?

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

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 $q = 2^\ell + 1 \Rightarrow$ prob. $= 1$

If $q = 2 \Rightarrow$ prob. $= 1/2^\ell$

If $q = k \Rightarrow$ Prob. $= 1 - \Pr[\text{no collision}]$

$$= 1 - \frac{2^\ell - 1}{2^\ell} \cdot \frac{2^\ell - 2}{2^\ell} \cdots \frac{2^\ell - k + 1}{2^\ell}$$

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. $\simeq 50\%$

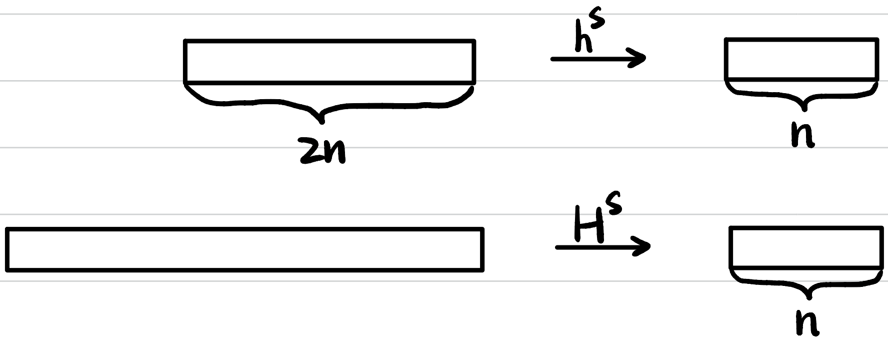
If security parameter $n = 128$, $\ell = ?$

$T(A) \ll 2^{128}$ $\quad q \ll \sqrt{2^{\ell}}$ $\quad \ell \sim 256$

Domain Extension: Merkle–Damgård Transform

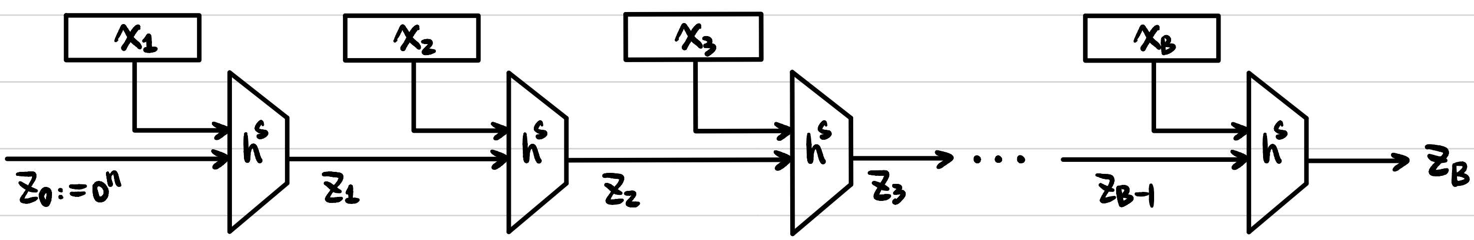
Given a CRHF (Gen, h) from $\{0,1\}^{2n}$ to $\{0,1\}^n$,

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



① Assume $|x|$ is a multiple of n

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



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

Is this a CRHF for arbitrary-length messages (multiple of n)? No!

Step 1: Assume $(\widetilde{Gen}, \tilde{h})$ is a CRHF from $\{0,1\}^{2n}$ to $\{0,1\}^{n-1}$.

We construct (Gen, h) from $\{0,1\}^{2n}$ to $\{0,1\}^{n}$ as follows:

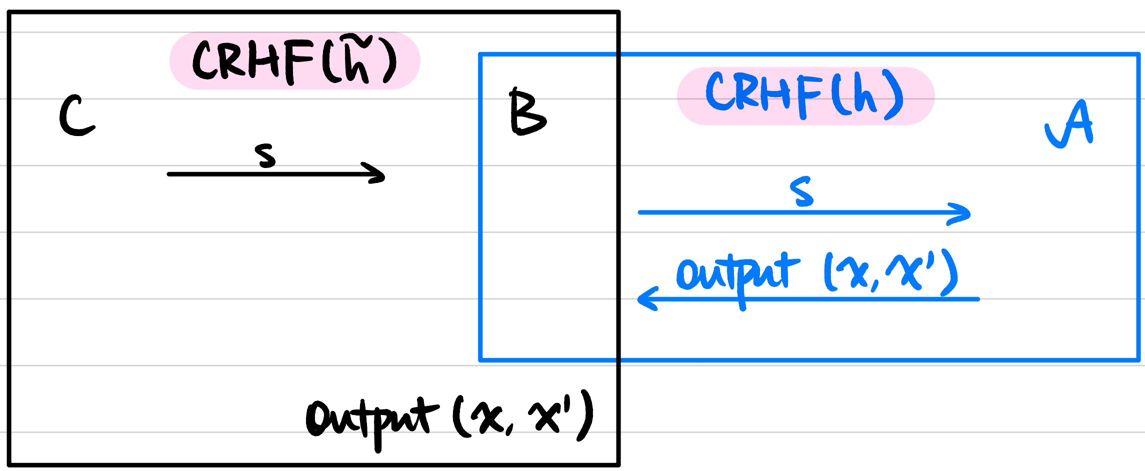
- $Gen(1^n)$: same as $\widetilde{Gen}(1^n)$.
- $h^s(x)$: $x \in \{0,1\}^{2n}$.

  If $x = 0^{2n}$, then output 0^n

  Otherwise output $1 \,\|\, \tilde{h}^s(x)$

Step 2: If $(\widetilde{Gen}, \tilde{h})$ is a CRHF, then so is (Gen, h).

Proof Assume not, then $\exists$ PPT $\mathcal{A}$ that breaks the collision resistence of (Gen, h).
We construct a PPT B to break the collision resistence of $(\widetilde{Gen}, \tilde{h})$.



If $h^s(x) = h^s(x') \wedge x \neq x'$,
the output must start with 1.
$\tilde{h}^s(x) = \tilde{h}^s(x')$

$\Rightarrow$ (x, x') is a collision for $\tilde{h}^s$.

Step 3: (Gen, H) instantiated with (Gen, h) is not a CRHF for arbitrary-length messages.

$C \xrightarrow{s} \mathcal{A}$

output $x = 0^{2n}$, $x' = 0^n$

Domain Extension: Merkle–Damgård Transform

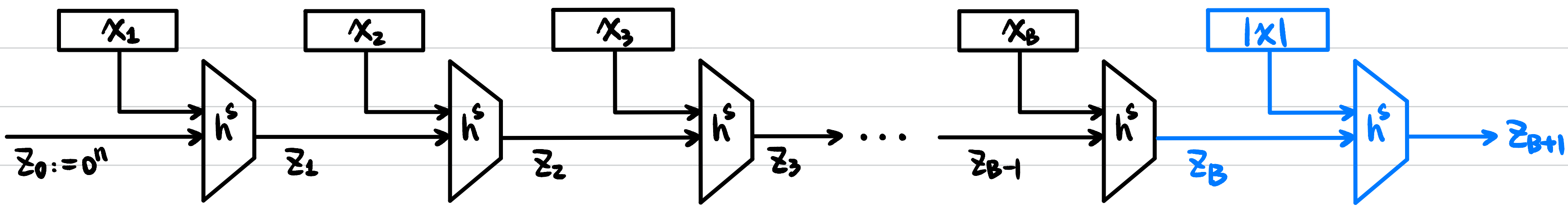
Given a CRHF (Gen, h) from $\{0,1\}^{2n}$ to $\{0,1\}^n$,

Construct (Gen, H):

- Gen(1^n): remains unchanged.
- $H^s(x)$: $x \in \{0,1\}^*$

① Pad x with $100\cdots0$ to a multiple of $n \to \tilde{x}$

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



bit representation of $|x|$

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

<u>Thm</u> If (Gen, h) is CRHF, then so is (Gen, H).