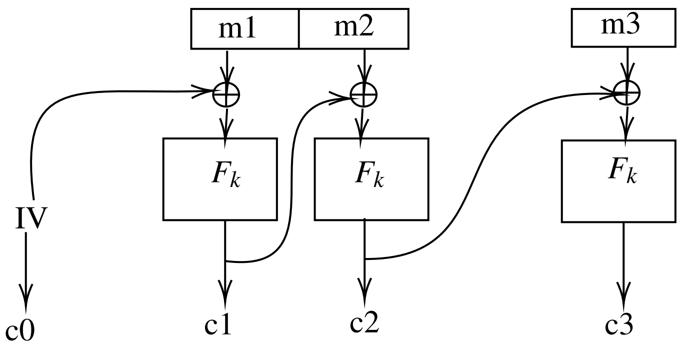
Assignment #: 2, SBU ID: 114963271

Thejesh Venkata Arumalla

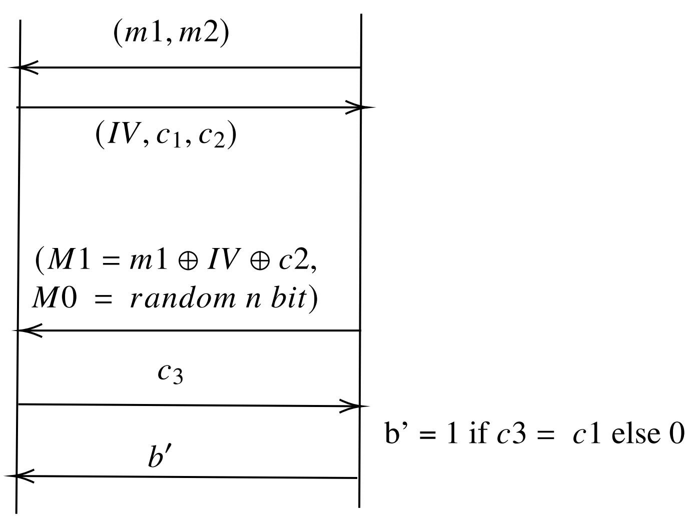
October 31, 2022

1. Problem1 - CBC-based encryption

   (a) Chained CBC mac is not secure. Consider the below scheme, we have chained the encryption.



- Initially we send $(m1, m2)$, we get the output (IV, c_1, c_2).
- Then we send
  - $M1 = m_1 \bigoplus IV \bigoplus c_2 \implies F_k(M1 \bigoplus c2) == F_k(m_1 \bigoplus IV)$
  - $M0 = \{0, 1\}^n$ is randomly chosen
- We receive c_3
- We return $b' = 1$ if $c3 == c1$

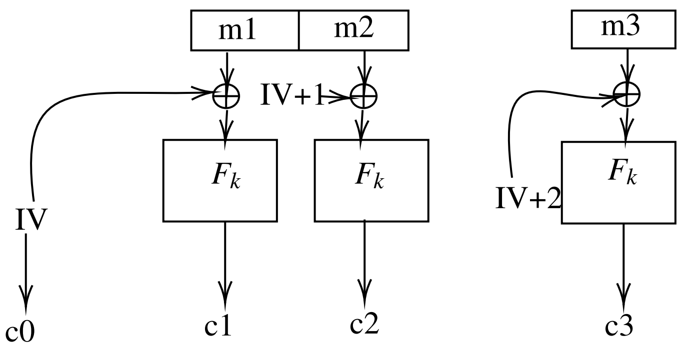


$$Pr\left[\frac{b' = 1}{b = 1}\right] = 1 \text{ as it is always true}$$

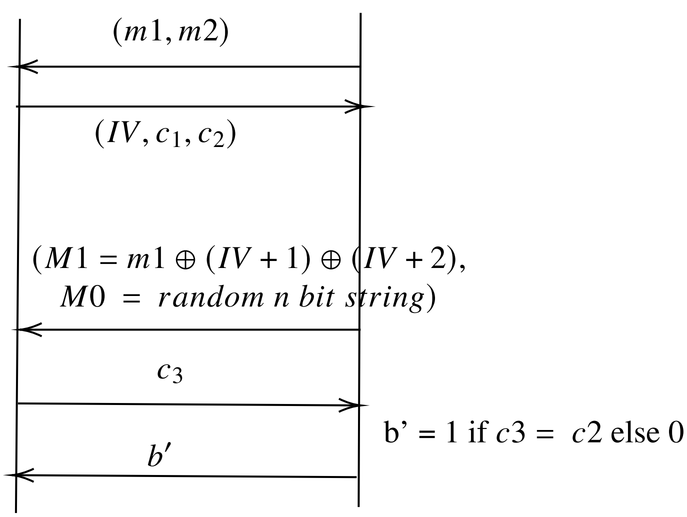
$$Pr\left[\frac{b' = 1}{b = 0}\right] = \frac{1}{2^n} \text{ as the random bits should exactly match with M1}$$

$$\therefore\ Pr\left[\frac{b' = 1}{b = 1}\right] - Pr\left[\frac{b' = 1}{b = 0}\right] = 1 - \frac{1}{2^n} \text{ which is not negligible}$$

(b) Incremental CBC mac is not secure



- Initially we send $(m1, m2)$, we get the output (IV, c_1, c_2).
- Then we send
  - $M1 = m_2 \bigoplus (IV + 1) \bigoplus (IV + 2) \implies F_k(M1 \bigoplus (IV + 2)) == F_k(m_2 \bigoplus (IV + 1))$
  - $M0 = \{0, 1\}^n$ is randomly chosen
- We receive c_3
- We return $b' = 1$ if $c_3 == c_2$



$$Pr\left[\frac{b' = 1}{b = 1}\right] \; = \; 1 \text{ as it is always true}$$

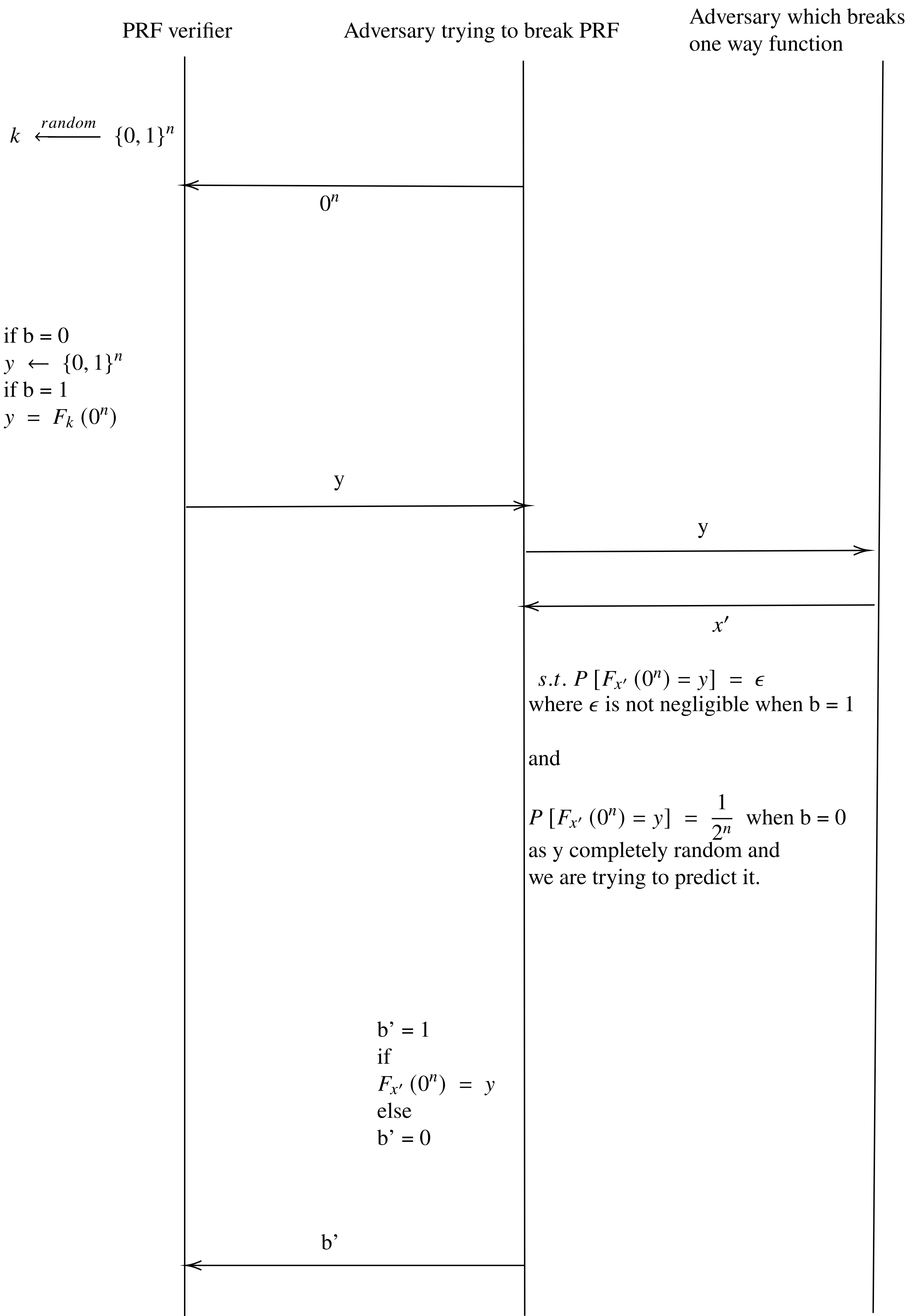
$$Pr\left[\frac{b' \; = \; 1}{b \; = \; 0}\right] \; = \frac{1}{2^n} \text{ as the random bits should exactly match with M1}$$

$$\therefore \; Pr\left[\frac{b' \; = \; 1}{b \; = \; 1}\right] \; - \; Pr\left[\frac{b' \; = \; 1}{b \; = \; 0}\right] \; = \; 1 \; - \; \frac{1}{2^n} \text{ which is not negligible}$$

2. Problem2 - One way function

   (a) Prove that $f(x) = F_x(0^n)$ is one way.

   We will prove by contradiction, we will assume there is an adversary which can break the one way function with a non-negligible $non - negl(n)$ probability, we will use it to break the PRF


PRF verifier
Adversary trying to break PRF
Adversary which breaks one way function
$k \xleftarrow{random} \{0,1\}^n$
0^n
if b = 0
$y \leftarrow \{0,1\}^n$
if b = 1
$y = F_k(0^n)$
y
y
x'
$s.t.\ P[F_{x'}(0^n) = y] = \epsilon$
where ϵ is not negligible when b = 1
and
$P[F_{x'}(0^n) = y] = \frac{1}{2^n}$ when b = 0
as y completely random and
we are trying to predict it.
b' = 1
if
$F_{x'}(0^n) = y$
else
b' = 0
b'

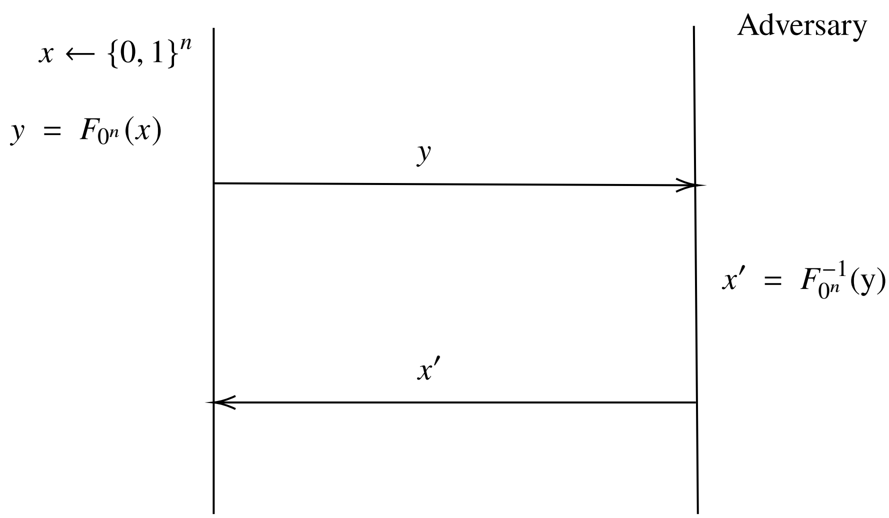
$$Pr\left[\frac{b' = 1}{b = 1}\right] = \epsilon \text{ which is non-negligible}$$

$$Pr\left[\frac{b' = 1}{b = 0}\right] <= \frac{1}{2^n} \text{ as we should guess a random y}$$

$$\therefore Pr\left[\frac{b' = 1}{b = 1}\right] - Pr\left[\frac{b' = 1}{b = 0}\right] \geqslant \epsilon - \frac{1}{2^n}\ \textit{which is not negligible}$$

Hence we proved that $F_k(x)$ is not a PRF as it is breaking for input 0^n.

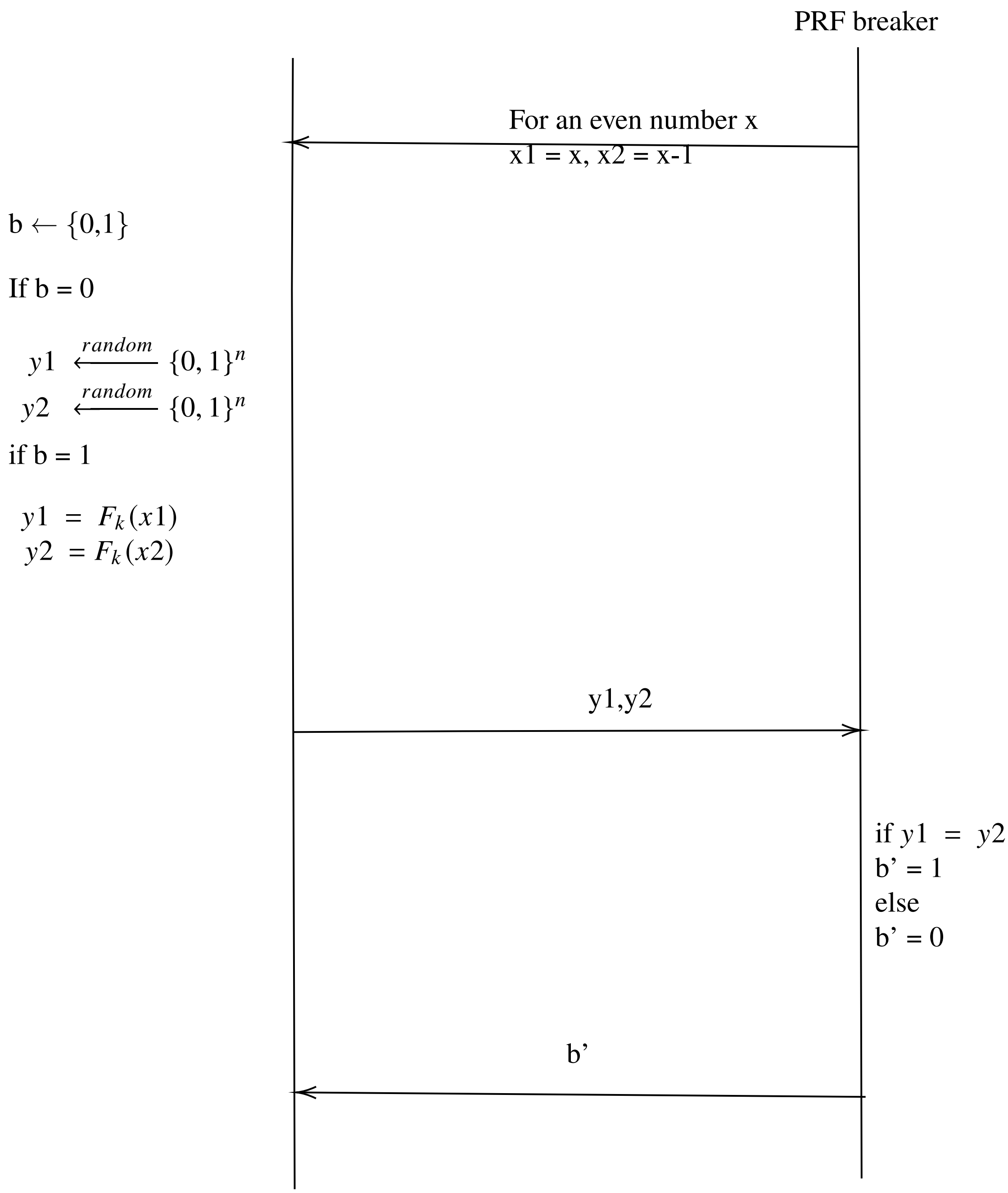
(b) Prove that $f(x) = F_{0^n}(x)$ is not one way.
We use the fact the inverse of PRP is easily computable within polynomial time



$Pr\left[F_{0^n}(x') = y\right] = 1$ which is not negligible

3. Problem3 - More PRF's

(a) Prove that $F_k^{'}(x) = F_k(x)$ if x is even else it is $F_k(x+1)$ is not PRF.
No it is not a pseudo random function, we will send x and $x-1$ where x is even


PRF breaker
For an even number x
x1 = x, x2 = x-1
$b \leftarrow \{0,1\}$
If b = 0
$y1 \xleftarrow{random} \{0,1\}^n$
$y2 \xleftarrow{random} \{0,1\}^n$
if b = 1
$y1 = F_k(x1)$
$y2 = F_k(x2)$
y1,y2
if $y1 = y2$
b’ = 1
else
b’ = 0
b’

$$Pr\left[\frac{b' = 1}{b = 1}\right] = Pr\,[\,y1 = y2] = Pr\left[F_k^{'}(x) = F_k{}^{'}(x-1)\ where\ x\ is\ even\right]$$

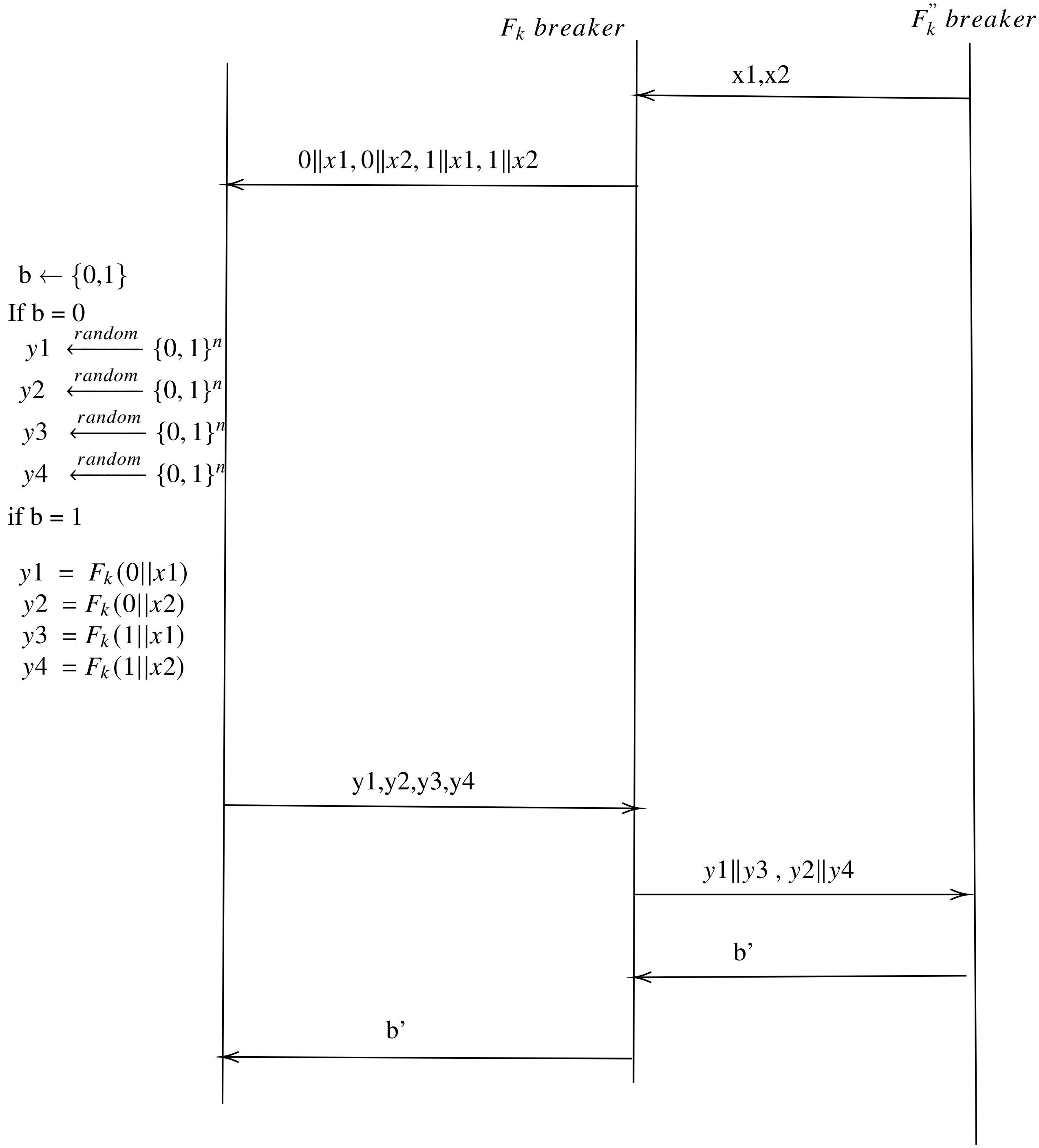
$$= Pr[F_k(x) = F_k(x)\,] = 1$$

$$Pr\left[\frac{b' = 1}{b = 0}\right] = \frac{1}{2^n}$$ as the first half should exactly match with second half

$$\therefore\ Pr\left[\frac{b' = 1}{b = 1}\right] - Pr\left[\frac{b' = 1}{b = 0}\right] = 1 - \frac{1}{2^n}$$ which is not negligible

(b) Prove that $F_k^{"}(x) = F_k(0||x)||F_k(1||x)$ is a PRF.

We will prove by contradiction, we will assume $F_k^{"}(x)$ is not a PRF and use it's adversary to break $F_k(x)$



F_k breaker
$F_k^{"}$ breaker
x1,x2
$0\|x1, 0\|x2, 1\|x1, 1\|x2$
b $\leftarrow$ {0,1}
If b = 0
$y1 \xleftarrow{random} \{0,1\}^n$
$y2 \xleftarrow{random} \{0,1\}^n$
$y3 \xleftarrow{random} \{0,1\}^n$
$y4 \xleftarrow{random} \{0,1\}^n$
if b = 1
$y1 = F_k(0||x1)$
$y2 = F_k(0||x2)$
$y3 = F_k(1||x1)$
$y4 = F_k(1||x2)$
y1,y2,y3,y4
$y1\|y3$, $y2\|y4$
b'
b'

$$\text{If b = 1 : } -$$

$$For\ F_k^{"}\ the\ situation\ is\ same\ as\ receiving\ pseudorandom\ output$$

$$Pr_{F_k\ adversary}\left[\frac{b' = 1}{b = 1}\right] = Pr_{F_k"\ \ adversary}\left[\frac{b' = 1}{b = 1}\right] \tag{1}$$

$$\text{If b = 0 : } -$$

$$For\ F_k^{"}\ the\ situtation\ is\ same\ as\ receiving\ two\ random\ messages\ as\ \mathbf{y1||y3\ is\ random\ and\ y2||y4\ is\ also\ random}.$$

$$Pr_{F_k\ adversary}\left[\frac{b' = 0}{b = 0}\right] = Pr_{F_k"\ \ adversary}\left[\frac{b' = 0}{b = 0}\right] \tag{2}$$

$$\implies Pr_{F_k\ adversary}\left[\frac{b' = 1}{b = 0}\right] = Pr_{F_k"\ \ adversary}\left[\frac{b' = 1}{b = 0}\right] \tag{3}$$

$$From\ (1)\ and\ (3)$$

$$\mathbf{Pr_{F_k\ adversary}\left[\frac{b' = 1}{b = 1}\right] - Pr_{F_k\ adversary}\left[\frac{b' = 0}{b = 1}\right]} \tag{4}$$

$$= \mathbf{Pr_{F"_k\ adversary}\left[\frac{b' = 1}{b = \ 1}\right] - Pr_{F"_k\ adversary}\left[\frac{b' = 1}{b = 0}\right]}$$

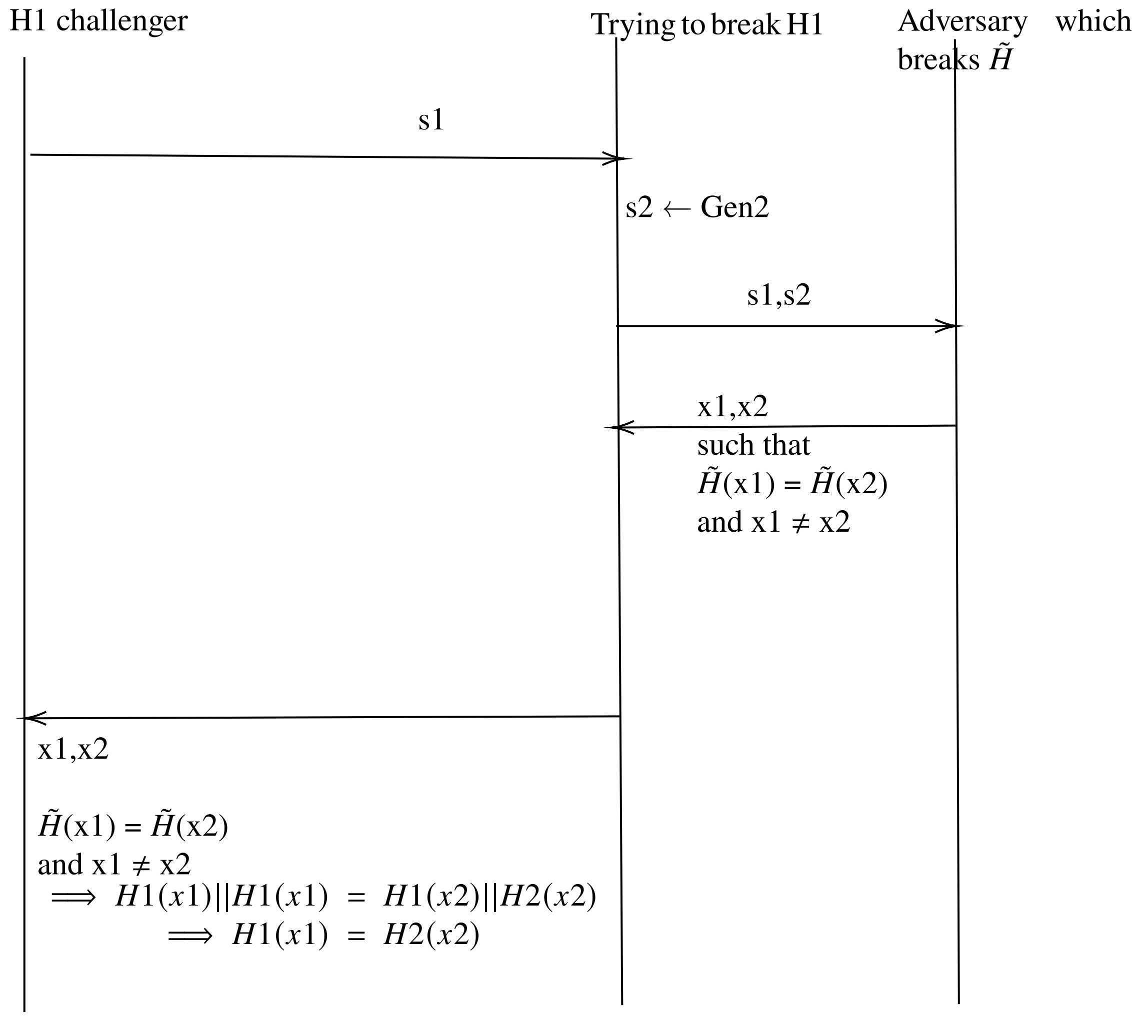
$$= \mathbf{non-negligible(n)}\ --As\ we\ know\ F"_k\ (x)\ is\ not\ a\ PRF \tag{5}$$

$$\implies We\ broke\ the\ PRF\ property\ for\ F_k$$

4. Problem4 - Secure Hashing - $\tilde{H}(x) = H_1(x)||H_2(x)$ - Prove or disprove

   (a) If $H1$ and $H2$ are both collision resistant then $\tilde{H}$ is collision resistant, we will prove it.

   - We will prove that if $\tilde{H}$ is not collision resistant then the statement "$H1$ and $H2$ are both collision resistant", is not true.
   - To prove that $H1$ and $H2$ are both collision resistant is not true, we will prove that $H1$ is not collision resistant.

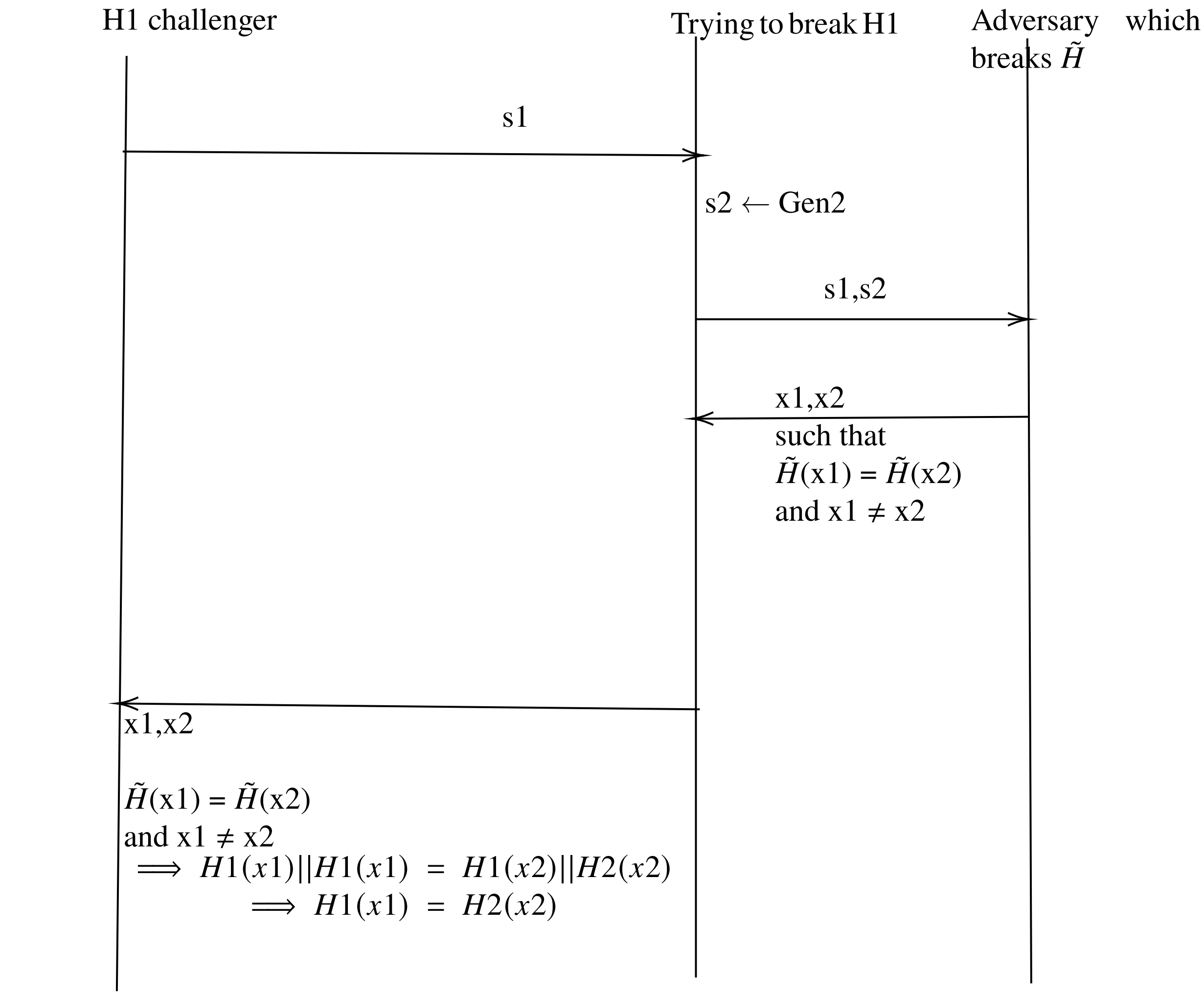


So we returned x1,x2 where $H1(x1) = H2(x2)$ and $x1 \neq x2$.

(b) If at-least one of $H1$ or $H2$ is collision resistant then H is collision resistant. We will prove that this is **true**.

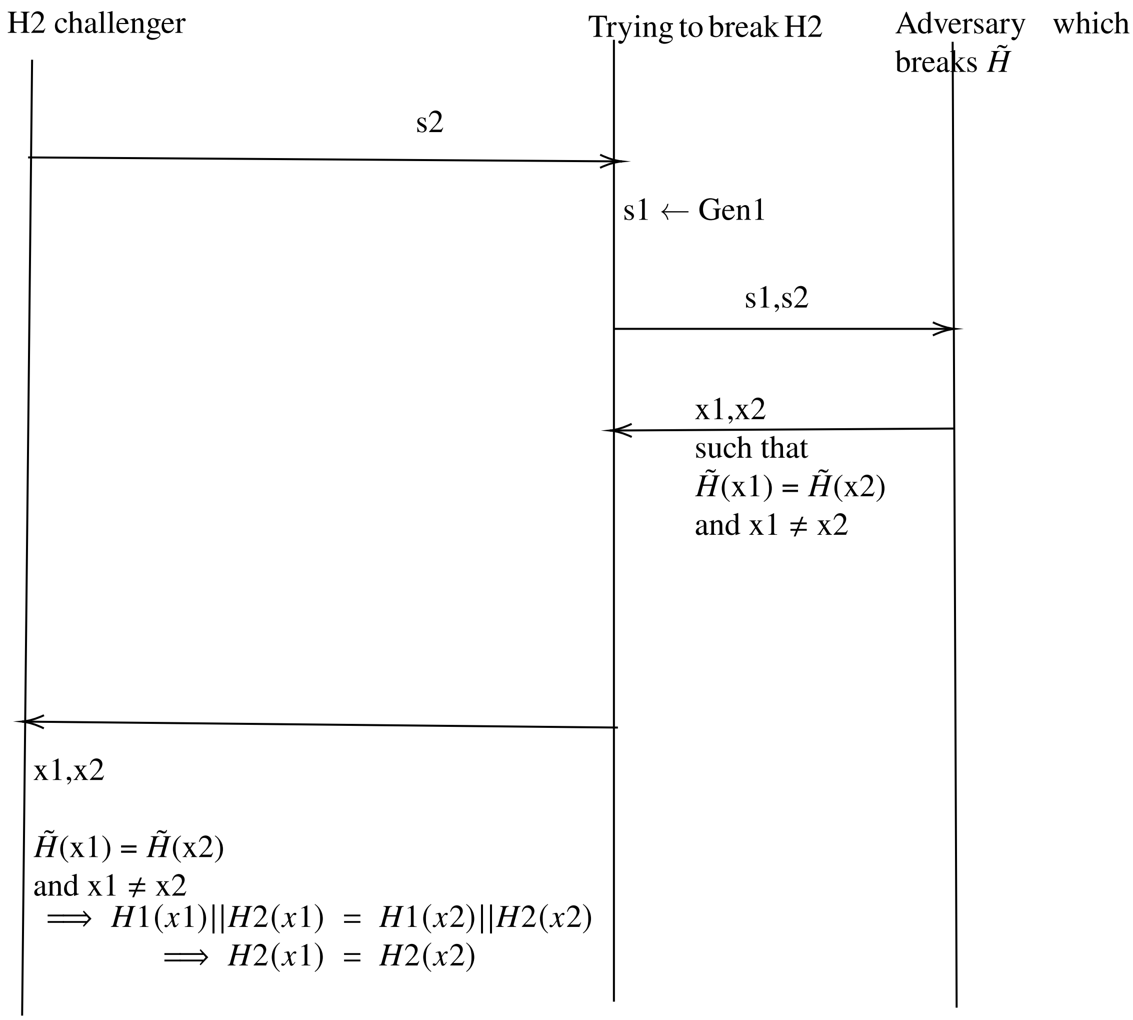
- There are 3 cases
  - Both H1 and H2 are collision resistant. This case is same as previous problem, we will not be proving again.
  - H1 is collision resistant but H2 is not collision resistant. We will prove that this is true by assuming H is not collision resistant and showing H1 is not collision resistant.Diagram **i** below.
  - H2 is collision resistant but H1 is collision resistant. We will prove that this is true by assuming H is not collisiob resistant and showing H2 is not collision resistant.Diagram **ii** below.

i.



So we returned x1,x2 where $H1(x1) = H2(x2)$ and $x1 \neq x2$, which shows H1 is not collision resistant.

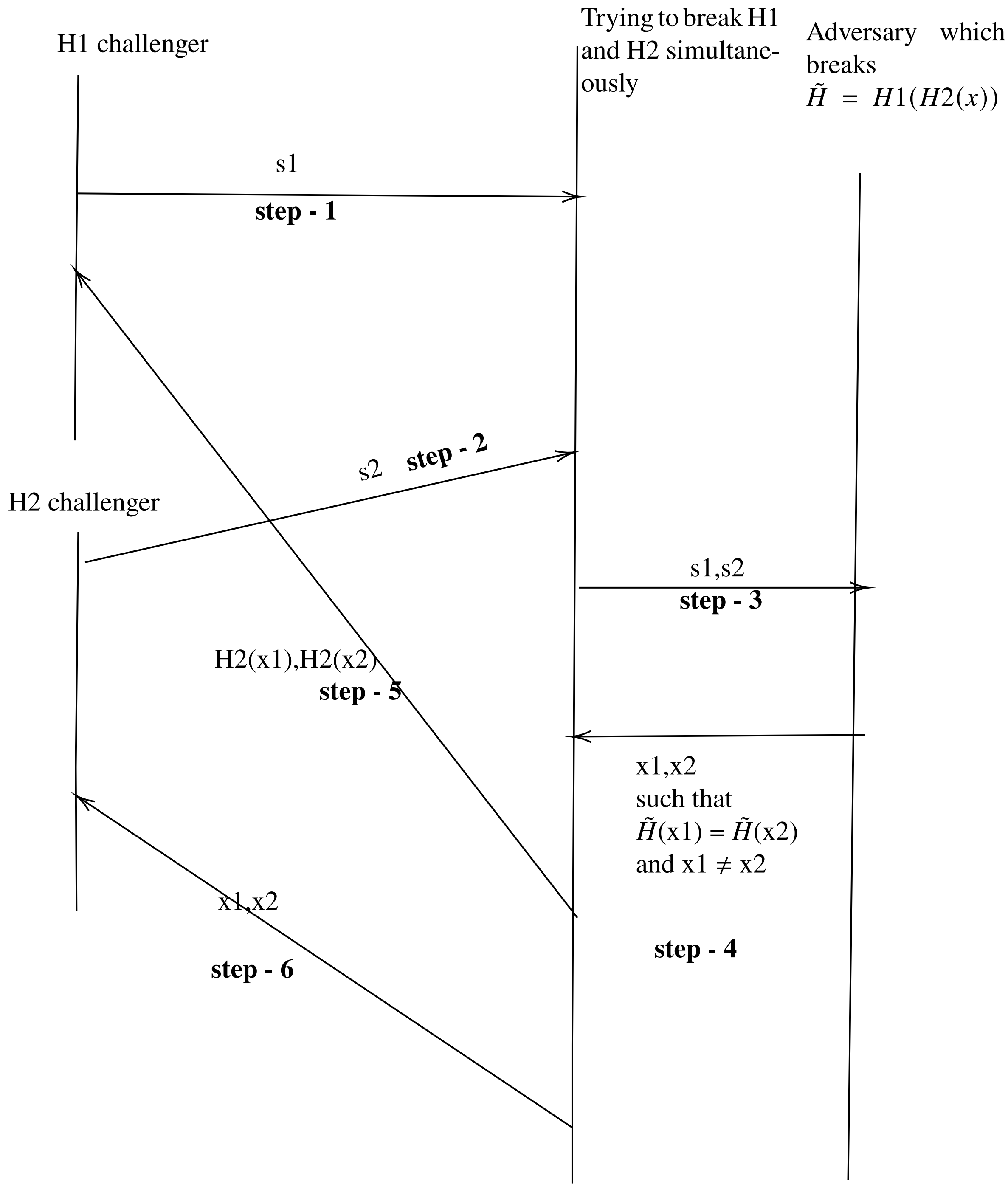
ii.



So we returned x1,x2 where $H1(x1) = H2(x2)$ and $x1 \neq x2$, which shows H2 is not collision resistant.

(c) $H(x) = H_1(H_2(x))$, then if both $H1$ and $H2$ are collision resistant then H is collision resistant. This is **True**

- We will prove this by showing that if H is not collision resistant then **atleast** one of H1 or H2 is not collision resistant.



- We know that $H1(H2(x1)) == H1(H2(x2))$
- There are two possibilities from the above diagram
  - H2(x1) == H2(x2), in this case H2 will be broken as $x1 \neq x2$ but their hashes using H2 are equal.
  - H2(x1) ≠ H2(x2), in this case H1 will be broken as $H2(x1) \neq H2(x2)$ but their hashes using H1 are equal.
- From the above we are sure that atleast one of H1 or H2 can be broken with a non-negligible probability.