CS171 HW4

Q1.1 ~~Suppose $g(n)$ isn't negligible, i.e. there exists some $P(n)$ such that for infinitely many~~
~~n, $g(n) = 2^{-f(n)} \geq \frac{1}{P(n)}$~~
~~Taking $\log_2$ both sides: $-f(n) \geq -\log_2(P(n))$~~
~~Substituting $f(n) = w\log n$: $w\log n \leq \log_2(P(n))$~~

$f(n) = \omega(\log n)$ means $f(n) > c\log n$ for any c

$g(n) = 2^{-f(n)} = \frac{1}{2^{f(n)}}$ where $\frac{1}{2^{f(n)}} < \frac{1}{2^{c\log n}}$

$\therefore g(n) < \frac{1}{n^c} < \frac{1}{P(n)}$

$P(n) < n^c$ (for any Polynomial $P(n)$ there exists c that $P(n) < n^c$ holds)

Q1.2 $f(n) = O(\log n)$ means $f(n) \leq c\log n$

$g(n) = 2^{-f(n)} = \frac{1}{2^{f(n)}}$ where $\frac{1}{2^{f(n)}} \geq \frac{1}{2^{c\log n}}$

$\therefore g(n) > \frac{1}{n^c}$

$n^c > g(n)$ ($g(n)$ is PPT in n, non-negligible.

Q1.3 a) negligible

b) negligible

c) Non-negligible

Q2. If A cannot break 0,1, it cannot break 0,2 too.

$\because$ Given $\Pr[G_{A,\Pi}(n) = 1] \leq \frac{1}{2} + negl(n)$

Since in 0,2, the adversary doesn't know b: $\begin{cases} \Pr[H_{A,\Pi}(n,0)=1] \\ \Pr[H_{A,\Pi}(n,1)=1] \end{cases} = \Pr[G_{A,\Pi}(n)=1] \leq \frac{1}{2} + negl(n)$

So, $|\Pr[H_{A,\Pi}(n,0)=1] - \Pr[H_{A,\Pi}(n,1)=1]| \leq negl(n)$

If A cannot break 0,2, it cannot break 0,1 too.

$\because$ Given $|\Pr[H_{A,\Pi}(n,0)=1] - \Pr[H_{A,\Pi}(n,1)=1]| \leq negl(n)$

$$\begin{aligned} \Pr[G_{A,\Pi}(n)=1] &= \tfrac{1}{2}\Pr[H_{A,\Pi}(n,0)=0] + \tfrac{1}{2}\Pr[H_{A,\Pi}(n,1)=1] \\ &\leq \tfrac{1}{2}(\Pr[H_{A,\Pi}(n,0)=0] + (\Pr[H_{A,\Pi}(n,0)=1] \pm negl(n))) \\ &\leq \tfrac{1}{2}(1 \pm negl(n)) \\ &\leq \tfrac{1}{2} \pm negl(n) \end{aligned}$$

No.

Date

Q3. XOR

0	0	0
0	1	1
1	0	1
1	1	0

We know: $L_0, R_0 = L_1, L_3, R_3$

$\forall k, x$ 1st bit of $f_k(x) = $ 1st bit of x

We know:

After a): $L_1 = R_0$; 1st bit of R_1

After b): 1st bit of L_2 ; 1st bit of R_2

After c): 1st bit of L_3 ; 1st bit of R_3

Let $L_{i,1}$ & $R_{i,1}$ denote 1st bit of L_i & R_i

$$\begin{aligned} \therefore R_{3,1} &= L_{2,1} \oplus R_{2,1} \\ &= R_{1,1} \oplus (L_{1,1} \oplus R_{1,1}) \\ &= L_{1,1} \\ &= R_{0,1} \end{aligned}$$

$\therefore$ A can query F with m_0 & m_1 where m_0 starts with 0 & m_1 starts with 1 & $|m_0| = |m_1|$

If 1st bit of R_3 $\begin{cases} \text{equals } 0, \text{ output } 0 \\ \text{equals } 1, \text{ output } 1 \end{cases}$

This way, A break security of F.