

QUIZ 1

Problem 1: Are the following negligible or not?

1) $\mu_1(n) := \frac{1}{n \log n}$

Solution: Yes, it is negligible.

To prove take arbitrary constant $c > 0$ & observe that $\frac{1}{n \log n} < \frac{1}{n^c} \Rightarrow n^c < n \log n$ which happens when $\log n > c$
 $\Rightarrow$

This shows that $\forall$ constants $c > 0$, $\exists n_c$ such that $\forall n > n_c$, $\mu_1(n) < \frac{1}{n^c} \Rightarrow \mu_1$ is negligible.

2) $\mu_2(n) := \nu_1(n)/\nu_2(n)$, for any negligible functions ν_1, ν_2 .

Solution: No, μ_2 is not negligible $\forall$ choices of negligible functions ν_1 & ν_2 .

Example (there are many examples):

Take $\nu_1 = \nu_2$ to be the same negligible function. Then $\mu_2(n) := 1$, the constant function. This is clearly not negligible.

3) $\mu_3(n) := n^{\log n} \cdot \nu(n)$, for any negligible function ν .

Solution No, μ_3 is not negligible $\forall$ choices of negligible ν .

Example:

Take $\nu(n) := \frac{1}{n \log n}$, which was shown to be negligible in a). Then $\mu_3(n) := 1$, which is not negligible.

Problem 2: Let $F := \{f_k: \{0,1\}^n \rightarrow \{0,1\}^n\}_{k \in \{0,1\}^n}$ be a PRF.
 Define $F' := \{f'_k: \{0,1\}^n \rightarrow \{0,1\}^n\}_{k \in \{0,1\}^n}$ as:

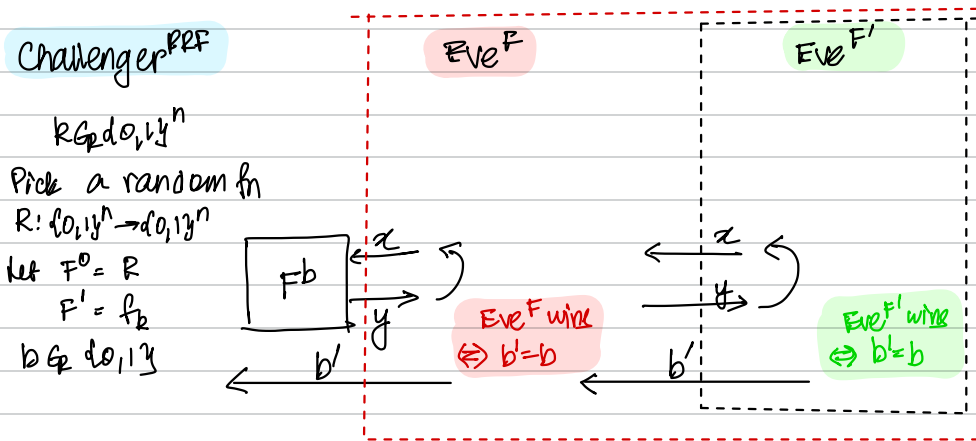
$$f'_k(x) := \begin{cases} 0^n, & \text{if } k = 0^n \\ f_k(x), & \text{otherwise} \end{cases}$$

Prove that if F is a PRF, then F' is a PRF.

Solution (sketch) $\rightarrow$ (you can prove using any of the two defs)

Suppose F' is not a PRF $\Rightarrow \exists$ $\text{Eve}^{F'}$ that breaks the security of the PRF F' .

We will build Eve^F that breaks F as follows:



Analysis:

Note that $\text{Eve}^{F'}$ gets the correct responses according to f'_k except for when $k = 0^n \rightarrow$ which happens w.p. $\frac{1}{2^n}$.

$$\Pr[\text{Eve}^F \text{ wins}] = \Pr[\text{Eve}^{F'} \text{ wins} \mid k \neq 0^n] \cdot \Pr[k \neq 0^n] + \Pr[\text{Eve}^{F'} \text{ wins} \mid k = 0^n] \cdot \Pr[k = 0^n]$$

$\downarrow$

Now, complete this analysis to argue

$$\Pr[\text{Eve}^F \text{ wins}] \geq \frac{1}{2} + \text{non-neg}(n)$$

Problem 3: Show that G_1 and G_2 are not PRGs & that F is not a PRF.

a) $G_1(s) := G(s) || G(\bar{s})$, for any PRG G

b) $G_2(s) := f_1(s) || f_2(s) || \dots || f_n(s)$, for any PRF $\{f_k\}_{k \in \{0,1\}^n}$

c) For $n \times n$ Boolean matrix A & n -bit boolean vector b , $F_{A,b}: \{0,1\}^n \rightarrow \{0,1\}^n$ defined by $F_{A,b}(a) := Aa + b$. (all operations modulo 2).

Solution

a) Let $H: \{0,1\}^{n+1} \rightarrow \{0,1\}^n$ be a PRG. Define $G: \{0,1\}^n \rightarrow \{0,1\}^{n+1}$

$$G(s) = H(\underbrace{s_1 s_2 \dots s_n}_{\text{first } n \text{ bits of } s}) || \underbrace{s_n}_{\text{last bit of } s}$$

Argue that if H is a PRG then G is a PRG.

Intuitively, $\because s$ is picked at random from $\{0,1\}^n$, s_n is a random bit & $\because H$ is a PRG, $H(s_1 \dots s_n)$ is pseudorandom. $\therefore G(s)$ is pseudorandom. (reduction is simple if you want to formally prove)

Now,

$$G_1(s) = G(s) || G(\bar{s}) = H(s_1 \dots s_n) || s_n || H(\bar{s}_1 \dots \bar{s}_n) || \bar{s}_n$$

Now, clearly $G_1(s)$ is next-bit predictable as given s_n , you know the last bit is $\bar{s}_n$.

b) The hint for this question was in the instructions (you can use constructions in other questions)

Use the PRF F' from problem 2 with a slight modification.

$$f'_k(x) := \begin{cases} 0^n, & \text{if } k=1 \\ f_k(x), & \text{otherwise} \end{cases} \quad (\text{where } F \text{ is a PRF})$$

Then, as proved in problem 2, $\{f'_k\}_{k \in \{0,1\}^n}$ is a PRF.

even an expansion of this level was enough to get you 1 mark.

$$\text{But now, } G_2(s) = f'_1(s) \parallel f'_2(s) \parallel \dots \parallel f'_n(s) \\ = 0^n \parallel f_2(s) \parallel \dots \parallel f_n(s)$$

Clearly G_2 is next-bit predictable!

c) $F_{A,b}(x) = Ax + b$

Observe that: $F_{A,b}(x_1 + x_2) = A(x_1 + x_2) + b \\ = Ax_1 + Ax_2 + b$

& $F_{A,b}(0^n) = A \cdot 0^n + b = b$

$\Rightarrow F_{A,b}(x_1 + x_2) = F_{A,b}(x_1) + F_{A,b}(x_2) + F_{A,b}(0^n)$

Exact attack: query the oracle on $x_1, x_2, 0^n + x_1 + x_2$ for some $x_1, x_2 \in \{0,1\}^n$, and get responses $y_{x_1}, y_{x_2}, y_{0^n}$ & $y_{x_1+x_2}$

If $y_{x_1+x_2} = y_{x_1} + y_{x_2} + y_{0^n}$ the guess PRF

Else it is a random oracle.

What is the winning probability?
(non-negligible, but find this probability)

Problem 4: For each of the following symmetric key encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$, is Π secure against: ciphertext only attack (COA) & chosen plaintext attack (CPA)?

a) $f_k: \{0,1\}^n \rightarrow \{0,1\}^n$ random be a PRF.

Define Π for $M = \{0,1\}^n$ as:

$\text{Gen}(1^n)$: Output $k \in \{0,1\}^n$

$\text{Enc}(k, m)$: • Generate $r \in \{0,1\}^n$
• Output $C = (r, f_k(r) \oplus m, f_k(m))$.

$\text{Dec}(k, c = (r, s, t))$: • compute $m = f_k(r) \oplus s$.
• If $f_k(m) = t$, output m
Else, output $\perp$.

Solution: It is COA-secure, but not CPA-secure.

CPA: • Eve can send m_0, m_1 ($m_0 \neq m_1$) as challenge messages.
& get back $C_b = (r, f_k(r) \oplus m_b, t_b = f_k(m_b))$

• Now, Eve queries $\text{Enc}_k(\cdot)$ oracle on m_0 & m_1 , again & get $C_0 = (r_0, s_0, t_0)$ & $C_1 = (r_1, s_1, t_1)$, resp.

If $t_b = t_0$, Eve outputs $b' = 0$

If $t_b = t_1$, Eve outputs $b' = 1$

What is the winning probability?

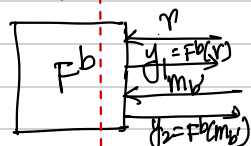
COA: To prove it is COA secure is a simple reduction.
Assume $\exists$ Eve^{COA} breaking Π , then, you can build Eve^{PRF} that breaks the PRF security as follows.

(Intuition: $\because$ there is no encryption oracle, the "deterministic" component that helps with CPA doesn't help in COA)

Challenger^{PRF}

$k \leftarrow \mathcal{K}$
 random fn $R: \mathcal{D}_1 \times \mathcal{Y}^n \rightarrow \mathcal{D}_2 \times \mathcal{Y}^n$

$b \leftarrow \mathcal{D}_1$
 $F^0 = R$
 $F^1 = f_k$



Eve^{PRF}

$b' \leftarrow \mathcal{D}_1$
 $r \leftarrow \mathcal{R}$

$\leftarrow m_0, m_1$

$c_b = (r, y_b \oplus m_b, y_b)$

$\leftarrow b''$

Eve^{COA}

If $b'' = b'$ output 1
 Else output 0.

(A correct intuitive explanation of above reduction would have itself earned you full marks.)

Analysis is simple (complete it): If Eve^{COA} wins $\Rightarrow b' = b''$

$\Rightarrow$ Eve^{PRF} says it is PRF

Else Eve^{PRF} says it is random.

Write down probabilities to show Eve^{COA}'s advantage turns to Eve^{PRF}'s.

b) $\{f_k: \mathcal{D}_1 \times \mathcal{Y}^n \rightarrow \mathcal{D}_2 \times \mathcal{Y}^n\}_{k \in \mathcal{K}}$ be a PRF. Define Π for $\mathcal{M} = \mathcal{D}_1 \times \mathcal{Y}^n$:

- $\text{Gen}(1^n)$: $k \leftarrow \mathcal{K}$
- $\text{Enc}(k, m)$: output $c = f_k(1^n) \oplus m$.
- $\text{Dec}(k, c)$: compute & output $m := f_k(1^n) \oplus c$.

Solution: This is a deterministic encryption scheme

$\Rightarrow$ not CPA-secure.

(can query encryption oracle on challenge 'messages' & get the same ciphertext as the challenge ciphertext.)

COA: It is COA secure. If you mentioned that $G(k) = f_k(1^n)$ is a PRG if $\{f_k\}$ is a PRF & said that Π is computational OTP which is known to be secure, you get full marks.