Homework 2 (40 + 6 points)
Due on 11:59pm Nov. 20th.
Solution must be typed, preferably using LaTeX.
It can be submitted via email to rachel.lin@cs.ucsb.edu or in class.
You can collaborate with one other student in class. Please acknowledge your collaborator and all public resources that you use.

Part 1 — Computational Indistinguishability (6 points)

Task (a) — Properties of Computational Indistinguishability (6 points)

Let \( \{X_n\}, \{Y_n\} \) and \( \{Z_n\} \) be distribution ensembles satisfying the following: (1) for every \( n \in \mathbb{N} \), distributions \( X_n, Y_n \) and \( Z_n \) are over domain \( \{0, 1\}^n \) and are efficiently samplable, and (2) \( \{X_n\} \approx \{Y_n\} \) and \( \{Y_n\} \approx \{Z_n\} \), where “\( \approx \)” denotes computational indistinguishability.

Decide whether the following pairs of distribution ensembles are computationally indistinguishable or not.

(i) \( \{X_n \oplus 1^n\} \) and \( \{Y_n \oplus 1^n\} \).

Here \( \oplus \) is the XOR operation and \( 1^n \) is the \( n \)-bit all 1 string.

(ii) \( \{X_n||Y_n\} \) and \( \{Y_n||Z_n\} \).

Here, \( A_n||B_n \) is the distribution of \( a||b \), when sampling \( a \) from \( A_n \) and \( b \) from \( B_n \) independently.

(iii) \( \{M(X_n, Y_n)\} \) and \( \{M(Y_n, Z_n)\} \).

Here, \( M \) is a randomized algorithm that on input \( (a, b) \), samples a random bit \( i \xleftarrow{} U_1 \), and outputs \( a \) if \( i = 0 \) and \( b \) if \( i = 1 \). Moreover, \( M(A_n, B_n) \) is the distribution of \( M(a, b) \), when \( a \) is sampled from \( A_n \) and \( b \) is sampled from \( B_n \) independently.

For each of the above questions,
- (1 pts) Answer Yes, they are computationally indistinguishable, or No.
- (1 pts) If you answer is Yes, argue why the ensembles are indistinguishable, using the two properties “closure under efficient computation” and “transitivity” introduced in class. If your answer is No, describe a distinguisher that can distinguish the two ensembles.

Part 2 — Pseudo-Random Generators (PRG) (10 points)

Task (a) — The Relation between PRG and OWF (4 points)

Let \( G \) be a length-doubling PRG. Show that \( G \) is a OWF.
- **(2 pts)** Argue informally why this is the case.
- **(2 pts)** Prove this formally.

**Task (b) — An alternative definition for PRG.**

Given an efficiently-computable function $G$ with $|G(x)| = l(|x|)$, consider the following experiment $\text{Exp}_{A}^{n}$ defined for an adversary $A$ and parameter $n$:

**Experiment $\text{Exp}_{A}^{n}$**: Proceed in the following three steps.

- Sample a random bit $b \overset{\$}{\leftarrow} U_{1}$.
- If $b = 0$, sample a random $x \overset{\$}{\leftarrow} U_{n}$ and set $y = G(x)$.
  If $b = 1$, sample a random $y \overset{\$}{\leftarrow} U_{l(n)}$.
- Output $b' \overset{\$}{\leftarrow} A(y)$

Say that $G$ is a PRG if for every non-uniform PPT adversaries $A$, there is a negligible function $\varepsilon$, such that,

$$Pr[b = b'] \leq 1/2 + \varepsilon(n)$$

(i) **(2 pts)** Describe formally the definition of PRG introduced in class.

(ii) **(2 pts)** Argue informally why the above definition is equivalent to the definition introduced in class.

(iii) **(2 pts)** Prove formally this equivalence.

**Part 3 — Pseudo-Random Functions (PRF)**

**Task (a) — Properties of PRF**

Call function $F : \{0,1\}^{k} \times \{0,1\}^{n} \rightarrow \{0,1\}^{n}$ a keyed function, and denote $F_{K}(x) = F(K, x)$. Furthermore, assume that $F$ is a PRF.

(i) Consider the keyed function $F' : 0,1^{k} \times \{0,1\}^{2n} \rightarrow \{0,1\}^{n}$ such that

$$F'_{K}(x_1|x_2) = F_{K}(x_1) \oplus F_{K}(x_2)$$

for all $x_1, x_2 \in \{0,1\}^{n}$ and $K \in \{0,1\}^{k}$. Is $F'$ a PRF?

(ii) Consider the keyed function $F'' : 0,1^{2k} \times \{0,1\}^{2n} \rightarrow \{0,1\}^{n}$ such that

$$F''_{K_1||K_2}(x_1|x_2) = F_{K_1}(x_1) \oplus F_{K_2}(x_2)$$

for all $x_1, x_2 \in \{0,1\}^{n}$ and $K_1, K_2 \in \{0,1\}^{k}$. Is $F''$ a PRF?
(iii) Consider the keyed function $F''' : 0,1^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ such that
\[
F'''_K(x) = F_K(x) \oplus x
\]
for all $x \in \{0,1\}^n$ and $K \in \{0,1\}^k$. Is $F'''$ a PRF?

For each of the above questions,

- (1 pts) Answer Yes or No.

- (1 pts) If you answer is Yes, argue informally why the function is a PRF, given that $F$ is. If your answer is No, describe informally a distinguisher that can distinguish the function from the random function.

**Task (b) — From PRF to PRG** (6 points)

Let $F : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a PRF. Construct a PRG $G$, such that, for all input $x$, the output length $|G(x)| = 100|x|$ (i.e., on input an $n$-bit $x$, the output $y = G(x)$ has $100n$ bits).

(i) (2 pts) Describe your candidate PRG $G$.

(ii) (2 pts) Argue informally why your candidate function $G$ is a PRG, given that $F$ is a PRF.

(iii) (2 pts) Prove formally the security of your candidate function $G$, by arguing contra-positive and giving security reduction.

**Task (c) — From PRF to PRF** (10 points)

Suppose we have constructed a PRF function $F : \{0,1\}^k \times \{0,1\}^m \rightarrow \{0,1\}^l$, where the input and output length $m = m(k)$ and $l = l(k)$ are polynomial in $k$. Show that now, for any polynomial $l'(k)$, we can construct a PRF $F'$ with the same key and input lengths $m = m(k)$ $l = l(k)$, but with output length $l' = l'(k)$.

(i) (2 pts) Case 1: If $l'(n) \leq l(n)$, how to construct $F'$ from $F$?

(ii) (2 pts) Case 2: If $l'(n) > l(n)$, how to construct $F'$ from $F$? You may use PRG in your construction

(iii) (4 pts) Argue informally why your function $F'$ is a PRF.

(iv) (2 pts) Prove formally that your construction $F'$ for Case 2 is a PRF, by arguing contra-positive and giving security reduction.
Part 4 — Secret Key Encryption

Task (a) — Malleability of a Secret Key Encryption

In class, we showed that the following encryption scheme \( \Pi = (\text{Gen}, \text{Enc}, \text{Dec}) \) is multi-message secure. Let \( F : \{0, 1\}^k \times \{0, 1\}^n \rightarrow \{0, 1\}^l \).

- \( \text{Gen}(1^k) \): Sample a PRF key \( K \leftarrow U_k \). Output \( K \).

- \( \text{Enc}(K, m) \): Sample a random string \( r \leftarrow U_n \), and compute \( z = m \oplus F(K, r) \). Output \( c = (r, z) \).
  (The message space is \( \{0, 1\}^l \).)

- \( \text{Dec}(K, c) \): Parse \( c = (r, z) \). Output \( m = z \oplus F(K, r) \).

Suppose that the goal of the adversary is not to distinguish the ciphertexts of different messages. Instead, given a ciphertext \( c \) of some hidden message \( m \) under some hidden key \( k \), the adversary wants to create another ciphertext \( c' \) that when decrypted using \( k \), yields \( m \oplus 1^n \). Describe an adversarial strategy for achieving this.

This shows that it might be easy to “maul” the ciphertext of one message into a ciphertext of a related message, even if the encryption is multi-message secure.

Part 5 — Bonus Tasks

Task (a) — The insecurity of PRF under leakage.

Construct a keyed function \( F : \{0, 1\}^{k+1} \times \{0, 1\}^n \rightarrow \{0, 1\}^n \) with the following properties: (1) \( F \) is a PRF, (2) however, if the adversary learns the last bit of the secret key of the PRF, then the PRF is no longer secure. You may assume other PRF function to construct \( F \).

This in particular shows that leaking even one bit of the secret key can completely destroy the security of a PRF.

(i) (2 pts) Describe your candidate PRF function \( F \).

(ii) (2 pts) Argue informally why your candidate function is a PRF and describe a distinguisher that given the last bit of the secret key can distinguish \( F \) from a random function.

(iii) (2 pts) Prove formally the security of your candidate function \( F \), by arguing contra-positive and giving security reduction.

Hint: You can email me to get a hint for this question.