Instructions

- You are allowed to work in groups of size at most 2.
- The assignments must be typed in Latex, and the resulting pdf must be submitted on Gradescope.
- The bonus questions are somewhat challenging, and you are recommended to attempt them only after solving all the other problems.
- **Plagiarism policy**: You should not discuss your solutions with other group members. Sharing your solutions with other group members is strictly not allowed, and if there are significant similarities in two or more submissions, all relevant group members will be penalized.

  You can refer to resources online, but you should write your solutions in your own words (and also cite the resources used).

Notations

- In class, when we discussed PRGs, we talked about a function G that maps n bits to $\ell \cdot n$ bits. Strictly speaking, we have a family of functions $\{G_n : \{0,1\}^n \to \{0,1\}^{\ell \cdot n}\}_{n \in \mathbb{N}}$. In fact, the domain and co-domain for G_n can be $\{0,1\}^{\ell_{\text{in}}(n)}$ and $\{0,1\}^{\ell_{\text{out}}(n)}$ for some polynomials $\ell_{\text{in}}, \ell_{\text{out}}$ such that $\ell_{\text{out}}(n) > \ell_{\text{in}}(n)$. For notational brevity, we often skip the n in subscript.

  Similarly, for PRFs, we have a family of functions $\{F_n : \mathcal{X}_n \times \mathcal{K}_n \to \mathcal{Y}_n\}_{n \in \mathbb{N}}$.

Questions

1. (10 marks)

   Let $\mathcal{D}_0, \mathcal{D}_1$ be two distributions where $\mathsf{SD}(\mathcal{D}_0, \mathcal{D}_1) \leq \epsilon$. Consider the distributions $\mathcal{D}'_b$ defined as follows:

   $$\mathcal{D}'_b \equiv \{ \text{ output } t \text{ samples chosen independently from } \mathcal{D}_b \}$$

   Show an upper bound on $\mathsf{SD}(\mathcal{D}'_0, \mathcal{D}'_1)$.

   (Hint: hybrid technique + triangle inequality.)

2. (10 marks) **Weak PRPs**

   Let $\mathcal{P} = \{P_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n\}_{n \in \mathbb{N}}$ be a family of keyed permutations. We say that $\mathcal{P}$ is a weak pseudorandom permutation if for any p.p.t. adversary $\mathcal{A}$, there exists a negligible function $\mu(\cdot)$ such that for all n,

   $$\Pr[\mathcal{A} \text{ wins the weak PRP game}] \leq 1/2 + \mu(n)$$

   where the weak PRP game is defined in Figure 1 below.

Weak PRP Security Game

1. **Setup Phase** Challenger picks a bit $b \leftarrow \{0,1\}$. If $b = 0$, it picks a key $k \leftarrow \{0,1\}^n$, and sets $P_0 \equiv P(\cdot, k)$. If $b = 1$, it sets a uniformly random permutation P_1 from the set of all permutations mapping $\{0,1\}^n$ to $\{0,1\}^n$.
2. **Query Phase** The adversary is allowed polynomially many queries. For each query, the adversary does not send any input; the challenger picks a uniformly random string $x \leftarrow \{0,1\}^n$ and sends $(x, P_b(x))$ to $\mathcal{A}$.[a]
3. **Guess** The adversary sends its guess b', and wins the security game if $b = b'$.

[a] Note that the same bit b chosen during setup is used for all queries.

Figure 1: The Weak PRP Security Game

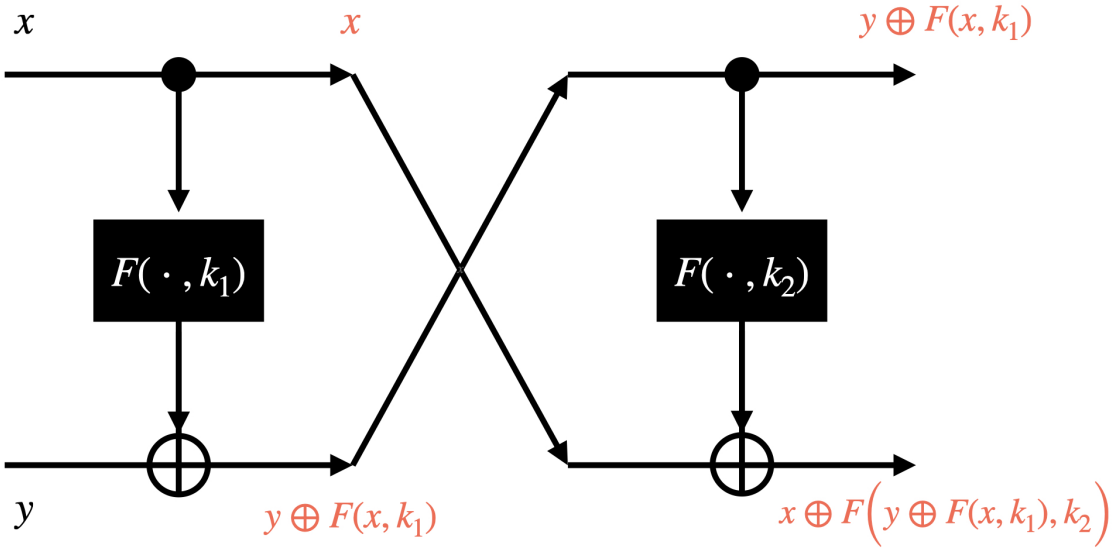

Figure 2: Attempt 2 for constructing a PRP

It is similar to the regular PRP game, the challenger picks a bit, and depending on the bit, it either uses a pseudorandom permutation or a truly random permutation. However, for each query, the adversary does not get to choose the inputs. Instead, every time the adversary asks for an input/output pair, the challenger chooses a uniformly random input x, and outputs $(x, P(x))$ (where P is the random or pseudorandom permutation).

In class, we discussed a few attempts for building a secure PRP from a secure PRF. Recall Attempt 2, but with two different keys.

Formally, let $\mathcal{F} = \{F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n\}_{n\in\mathbb{N}}$ be a secure PRF family. Consider the family of keyed permutations $\mathcal{P} = \{P_n : \{0,1\}^{2n} \times \{0,1\}^{2n} \to \{0,1\}^{2n}\}_{n\in\mathbb{N}}$ where P_n is shown pictorially in Figure 2. We discussed that this is not a secure PRP.

Show that this construction is a weak PRP.

3. (20 marks) **Composing PRGs and PRFs**

   1. (10 marks) Let $\mathcal{F} = \{F_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n\}_{n\in\mathbb{N}}$ be a family of secure pseudorandom functions, and let $\mathcal{G} = \{G_n : \{0,1\}^n \to \{0,1\}^{2n}\}_{n\in\mathbb{N}}$ be a family of secure pseudorandom generators. Consider the following function family:

$$\mathcal{F}' := \left\{ \begin{array}{c} F'_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^{2n} \\ F'_n(x,k) = G_n\left(F_n(x,k)\right) \text{ for all } x,k \in \{0,1\}^n \end{array} \right\}_{n\in\mathbb{N}}$$

      Show that $\mathcal{F}'$ is a family of secure pseudorandom functions, assuming $\mathcal{F}$ is a secure PRF family and $\mathcal{G}$ is a secure PRG family.

      Start with the contrapositive: suppose there exists a p.p.t. adversary $\mathcal{A}$ that makes $q(n)$ PRF queries, and wins the PRF security game against $\mathcal{F}'$ with advantage $\epsilon(n)$. Here $q(n)$ is some polynomial, and $\epsilon(n)$ is a non-negligible function.

(a) Formally define the hybrid worlds that you will consider for this proof. The number of hybrids may need to depend on $q(n)$.

(b) Suppose you define hybrid worlds $H_1, H_2, \ldots, H_t$. Let p_0 and p_1 denote the probability of adversary $\mathcal{A}$ outputting 0 in world-0/world-1 respectively, and let $p_{\text{hyb},i}$ denote the probability of outputting 0 in hybrid i. Show that if $p_{\text{hyb},i}$ and $p_{\text{hyb},i+1}$ are far-apart, there exists a p.p.t. reduction algorithm that breaks the security of _____. Similarly, show that p_0 and $p_{\text{hyb},1}$ should be close, and $p_{\text{hyb},t}$ and p_1 should be close.

2. (10 marks) If we apply the PRG first, and then use the resulting string as an input for the PRF, then the resulting function family may not be a secure PRF family!

What causes this composition to fail — is it the underlying PRF $\mathcal{F}$, or the underlying PRG $\mathcal{G}$?

We will show that there exists secure PRG family $\mathcal{G}'$ such that the resulting composition does not give a secure PRF family. Let $\mathcal{G} = \{G_n : \{0,1\}^n \to \{0,1\}^{3n}\}_{n\in\mathbb{N}}$ be a secure PRG family. Construct a PRG family $\mathcal{G}' = \{G'_n : \{0,1\}^{2n} \to \{0,1\}^{3n}\}_{n\in\mathbb{N}}$ such that the following properties hold:[1]

(a) $\mathcal{G}'$ is a secure PRG, assuming $\mathcal{G}$ is a secure PRG. For this part, you must present a formal reduction, and analyse the success probability of your reduction algorithm.

(b) Let $\mathcal{F} = \{F_n : \{0,1\}^{3n} \times \{0,1\}^n \to \{0,1\}^{3n}\}$ be any keyed function family. Consider the following function family:

$$\mathcal{F}' := \left\{ \begin{array}{c} F'_n : \{0,1\}^{2n} \times \{0,1\}^n \to \{0,1\}^{3n} \\ F'_n(x,k) = F_n\left(G'_n(x), k\right) \text{ for all } x \in \{0,1\}^{2n}, k \in \{0,1\}^n \end{array} \right\}_{n\in\mathbb{N}}$$

Show that this is **not** a secure PRF family.

4. (10 marks) **CBC mode and** No-Query-Semantic-Security

Recall the following variant of CBC mode, defined in Lecture 10 (Section 3.2). It uses a secure PRP $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$.

- KeyGen : choose a random key $k \leftarrow \{0,1\}^n$.
- $\mathsf{Enc}(m,k)$: Parse $m = (m_1 \,||\, \ldots \,||\, m_\ell)$. Let $\mathsf{ct}_1 = F(m_1, k)$. For each $i > 1$, compute $\mathsf{ct}_i = F(m_i \oplus \mathsf{ct}_{i-1}, k)$.
- $\mathsf{Dec}(\mathsf{ct},k)$: Parse $\mathsf{ct} = (\mathsf{ct}_1 \,||\, \ldots \,||\, \mathsf{ct}_\ell)$. Let $m_1 = F^{-1}(\mathsf{ct}_1, k)$. For each $i > 1$, compute $m_i = F^{-1}(\mathsf{ct}_i, k) \oplus \mathsf{ct}_{i-1}$.

Show that the above scheme satisfies No-Query-Semantic-Security, assuming F is a secure pseudorandom permutation. As discussed in class, this proof will involve a sequence of hybrid worlds. Carefully define the hybrid worlds, and discuss why the consecutive hybrids are indistinguishable.

5. (Bonus Question: 2 marks)

Luby-Rackoff with two keys: Consider the Luby-Rackoff PRP construction, but with two keys instead of three. That is, given a PRF $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$, consider the keyed permutation $P : \{0,1\}^{2n} \times \{0,1\}^{2n} \to \{0,1\}^{2n}$ defined as follows:

$$P(\cdot, (k_1, k_2)) = P_1(\cdot, k_1) \circ \mathsf{swap} \circ P_1(\cdot, k_2) \circ \mathsf{swap} \circ P_1(\cdot, k_2)$$

where $P_1((x,y),k) = (x, y \oplus F(x,k))$. Is this a secure PRP? Either show an attack, or prove security (assuming F is a secure PRF).

[1] Note that both properties must hold simultaneously.

6. (Bonus Question: 3 marks)

   Let $f : \{0,1\}^n \to \{0,1\}^m$ be a OWF (as defined in Lecture 08). Consider the function $g : \{0,1\}^n \to \{0,1\}^{m-1}$, where $g(x)$ is computed by evaluating $f(x)$ and then removing the first bit from the output (i.e. if $f(x) = y_1, y_2, \ldots, y_m$ then $g(x) = y_2, \ldots, y_m$). If f is a OWF, then is g a OWF?

   Either give a reduction showing that one-wayness of f implies one-wayness of g, or give a counter example — assuming f is a OWF, construct a new function f' such that f' is still a OWF, but removing the first bit results in a function that is not a OWF.