[**Solutions**] Lecture 5: Pseudorandom Functions + PRG Exercises

Name: ______________________________ Unity ID: ______________________________

Q4. Practice with PRF

Q4a

Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ a secure PRF. Let $F' : \{0,1\}^{2n} \times \{0,1\}^{2n} \to \{0,1\}^{2n}$ function defined as follows:

$$F'_k(x) = F_{k_1}(x_1)||F_{k_2}(x_2)$$

is it secure? If yes, prove it by a reduction. If no, show a formal attack.
(Assume we parse $k = k_1||k_2$ and $x = x_1||x_2$))

Q4b

Let $F' : \{0,1\}^{2n} \times \{0,1\}^n \to \{0,1\}^n$ function defined as follows:

$$F'_k(x) = F_{k_1}(x_1) \oplus k_2$$

is it secure? If yes, prove it by a reduction. If no, show a formal attack.

Q5. Prove or disprove the security of a PRG.

Let $M : \{0,1\}^n \to \{0,1\}^{2n}$ and $G : \{0,1\}^n \to \{0,1\}^{2n}$ be two secure PRF.
Let $Q : \{0,1\}^n \to \{0,1\}^{4n}$ be the following PRG.

$$Q(s) := M(s)||M(\bar{s})$$

(where $\bar{s}$ means we negated all the bits of s).
Prove or disprove that Q is a secure PRG.

Solution 4a: Formal Attack.

<u>Algorithm A</u>

- Prepare input
  1. $x^0 = x_0^1||x_0^2 = 0^{2n}$.
  2. $x^1 = x_1^1||x_1^2 = 0^n||1^n$.

  Note that $x_0^1 = x_1^1 = 0^n$ and $x_1^2 = 0^n \neq 1^n = x_2^2$, and so $x^0 \neq x^1$. (In this case, it is fine to either instantiate x^0 and x^1 as specific strings or be more generic and pick any strings where $x_0^1 = x_1^1$ and $x_2^0 \neq x_2^1$.)
- Query oracle $\mathcal{O}$ with input x^0, x^1.
- On receipt of $\mathcal{O}(x^0) = y^0$, parse as $y^0 = y_1^0||y_2^0$.
- On receipt of $\mathcal{O}(x^1) = y^1$, parse as $y^0 = y_1^1||y_2^1$.
- If $y_1^1 = y_1^0$ output 1. Else, 0.

<u>Analysis of A's success</u>
Case $\mathcal{O} = F'$.

1. $\mathcal{O}(x^0) = y^0 = y_1^0||y_2^0 = F'_{k_1}(0^n)||F'_{k_2}(0^n)||$.
2. $\mathcal{O}(x^1) = y^1 = y_1^1||y_2^1 = F'_{k_1}(0^n)||F'_{k_2}(1^n)||$.
3. Then $y_1^1 = y_0^1$ with probability 1.
4. $A^{F(\cdot)}() = 1$ with probability 1.

Case $\mathcal{O} = TF$.

1. $\mathcal{O}(x^0) = y^0 = y_1^0||y_2^0$. Note y_1^0 is a uniformly random bitstring of length n.
2. $\mathcal{O}(x^1) = y^1 = y_1^1||y_2^1$. Note y_1^1 is a uniformly random bitstring of length n.
3. Then $y_1^1 = y_0^1$ with probability $\frac{1}{2^n}$.
4. $A^{TF(\cdot)}() = 1$ with probability $\frac{1}{2^n}$.

We see that

$$|Pr[A^{TF(\cdot)}() = 1] - Pr[A^{F(\cdot)}() = 1]| = |1 - \frac{1}{2^n}|$$

which is not negligible. Hence, F' is not a secure PRF.

Solution 4b: SECURITY PROOF BY REDUCTION.

Theorem. If F is a secure PRF then F' is a secure PRF.

Proof. By contradiction. We will prove the following statement.

If F' is **not** a secure PRF then also F is not a secure PRF.

Step 1. Write formally what it means that F' is not a secure PRF? It means that there exist a PPT algorithm $A^{'}$ such that: A' can distinguish between F' and a truly random function TF with probability $q(n)$, where $q(n)$ is non-negligible.

Step 2. Reduction Write an algorithm A that uses A' to distinguish the output of F. Algorithm A has access to an oracle $\mathcal{O}$ and its goal is to distinguish if $\mathcal{O} = F$ or $\mathcal{O} = TF$ (where TF stands for truly random function).
$\underline{A(1^n)}$

- A gets access to $\mathcal{O}$ where $\mathcal{O}$ is either F or a truly random function TF.
- A picks $k_2 \leftarrow_{\$} \{0,1\}^n$
- A activates A'.
  1. On each query x_i by A', forward to $\mathcal{O}$. Receive $\mathcal{O}(x_i) = y_i$.
  2. Calculate $y_i' = y_i \oplus k_2$. Forward y_i' to A'.
- Finally, when A' outputs b, output the same.

Step 3. Analysis of Success probability of the reduction A.

Case 1. $\mathcal{O} = F$

1. A gets $F_k(x_i)$ for each query x_i.
2. Then $y_i' = F_2(x_i) \oplus k_2$.

This looks exactly like the view A' would see with $\mathcal{O} = F'$.
Case 2. $\mathcal{O} = TF$

1. A gets $y_i \leftarrow_{\$} \{0,1\}^n$.
2. Since k_2 is also uniform at random, $y_i' = y_i \oplus k_2$ is uniform at random.

Then this is the same view for A' seeing a truly random function.
We know by assumption that

$$|Pr[A^F(1^n) = 1] - Pr[A^{TF}(1^n) = 1] = q(n)$$

We conclude that A, outputting the same as A' distinguishes with probability $q(n)$. However, by assumption, $q(n)$ is non-negligible and A is an adversary for F, a PRF. This is a contradiction, so F' must be a secure PRF.

Question 4a: Formal Attack.

1. Construct a PRG $M(s)$ (that uses a PRG G as building block) as follows:

   $\underline{M(s)}$

   - Parse s as $s_1 \ldots s_n$
   - If $s_1 = 0$, output $G(s)$ otherwise output $G(\bar{s})$.

   We note that M is a secure PRG, since G is a PRG.

2. Instantiate Q with PRG M. Recall that Q should work with any PRG. When instantiating Q with M we obtain the following behaviour:

   $Q(s) = M(s)||M(\bar{s})$
   If $s_1 = 0$, then $M(s)||M(\bar{s}) = G(s)||G(s) = G(s)||G(s)$
   if $s_1 = 1$, then $M(s)||M(\bar{s}) = G(\bar{s})||G(\bar{s})$

3. The last step is to show when Q is instantiated with M, the output of Q is easily distinguishable from a truly random string. There exists a PPT distinguisher D that works as follows:

   Algorithm $\underline{D(y)}$

   - Parse $y = y_L||y_R$
   - Decision: If $y_L = y_R$ then output 1, otherwise output 0.

Analysis of D's success
Case 1: $y = Q(s)$**.**
if y is the output of Q, then $Pr[D(y) = 1|y = Q(s)] = 1$.

Case 2: $y \leftarrow_\$ \{0,1\}^{4n}$**.**
if y is the output of a truly uniform distribution, $Pr[D(y) = 1|y \leftarrow_\$ \{0,1\}^{2n}] = \frac{2^{2n}}{2^{4n}} = \frac{1}{2^{2n}}$

We see that:

$$|Pr[D(y) = 1|y = Q(s)] - Pr[D(y) = 1|y \leftarrow_\$ \{0,1\}^{2n}]| = |1 - \frac{1}{2^{2n}}|$$

which is not negligible. Hence, Q is not a secure PRG.

TEMPLATE: SECURITY PROOF BY REDUCTION.

Theorem. If F is a secure PRF then F' is a secure PRF.

Proof. By contradiction. We will prove the following statement.

If F' is **not** a secure PRF then also F is not a secure PRF.

Step 1. Write formally what it means that F' is not a secure PRF? It means that there exist a PPT algorithm $A^{'}$ such that:

Step 2. Reduction Write an algorithm A that uses A' to distinguish the output of F. Algorithm A has access to an oracle $\mathcal{O}$ and its goal is to distinguish if $\mathcal{O} = F$ or $\mathcal{O} = TF$ (where TF stands for truly random function).

$\underline{A}$

- ...
- ...
- Output

Step 3. Analysis of Success probability of the reduction A.

Case 1. $\mathcal{O} = F$

Case 2. $\mathcal{O} = F$

TEMPLATE FOR FORMAL ATTACK.

Algorithm A

- Prepare input ...
- Query oracle $\mathcal{O}$ with input ...
- ...
- ...
- Output ...

Analysis of A's success

Case $\mathcal{O} = F$.

Case $\mathcal{O} = TF$.

hence,