Pseudorandom Generators with Related Key Security

Problem Statement:

In Lecture 05, we discussed the notion of pseudorandom generators. A length-doubling pseudorandom generator is a deterministic function $G : \{0,1\}^n \to \{0,1\}^{2n}$, and for all p.p.t. adversaries $\mathcal{A}$, there exists a negligible function $\mathsf{negl}(\cdot)$ such that for all n,

$$\Pr[\mathcal{A} \text{ wins the PRG security game}] \leq 1/2 + \mathsf{negl}(n).$$

Recall, we discussed that PRGs may not be secure if the adversary sees the outputs on 'related seeds'. In this exercise, we define a special case of PRG security w.r.t. related seeds. Let $G : \{0,1\}^n \to \{0,1\}^\ell$, with $\ell > n$. Consider the following security game between a challenger and an adversary:

Related-PRG

1. The challenger chooses a uniformly random bit $b \leftarrow \{0,1\}$.
   If $b = 0$, the challenger chooses a seed $s \leftarrow \{0,1\}^n$, sets $s' = s \oplus 0\ldots01$,[a] and sends $u_1 = G(s)$, $u_2 = G(s')$.
   If $b = 1$, the challenger chooses two uniformly random strings $u_1, u_2 \leftarrow \{0,1\}^\ell$ and sends u_1, u_2 to $\mathcal{A}$.
2. The adversary sends its guess b', and wins the security game if $b = b'$.

[a] The string s' is same as s, except that the last bit is flipped.

Figure 1: Related Seed PRG Security Game

A length expanding function $G : \{0,1\}^n \to \{0,1\}^\ell$ (with $\ell > n$) is said to satisfy pseudorandomness security with related seeds if, for any prob. poly. time (p.p.t.) adversary $\mathcal{A}$, there exists a negligible function $\mu(\cdot)$ such that for all n,

$$\Pr\left[\mathcal{A} \text{ wins in the Related Seed PRG Security Game}\right] \leq 1/2 + \mu(n).$$

We will show that PRG security does not imply pseudorandomness security with related seeds. Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a secure pseudorandom generator. Construct a new length expanding function G' with appropriate input/output space such that G' is also a secure pseudorandom generator (assuming G is a secure pseudorandom generator), but G' does not satisfy pseudorandomness with related seeds.

1. Construct G'. Your construction should use G as a building block.
2. Show that G' is a secure pseudorandom generator. That is, if there exists a p.p.t. adversary $\mathcal{A}$ and a non-negligible function ϵ such that

   $$\Pr[\mathcal{A} \text{ wins the PRG security game against } G'] = 1/2 + \epsilon,$$

   then there exists a p.p.t. algorithm $\mathcal{B}$ and a non-negligible function ϵ' such that

   $$\Pr[\mathcal{B} \text{ wins the PRG security game against } G] = 1/2 + \epsilon'.$$

3. Show that G' does not satisfy security pseudorandomness security with related keys.

Note: As mentioned in the question, you are allowed to set the input and output domains appropriately. In particular, if the security parameter is n, the input space can be $\{0,1\}^{p(n)}$ for any polynomial $p(\cdot)$. The Related-PRG security game is defined for the case where the input domain is $\{0,1\}^n$. If the input domain was $\{0,1\}^{p(n)}$, then you would appropriately change the security game.

Solution:

1. Let $G' : \{0,1\}^{2n} \to \{0,1\}^{3n}$ be defined as follows:

$$G'(s_1 \mid\mid s_2) = G(s_1) \mid\mid s_2$$

Here, s_1 (resp. s_2) represent the first (resp. last) n bits of the input, $||$ denotes string concatenation.

2. We will prove that G' is a secure pseudorandom generator, assuming G is.

Claim 1. Suppose there exists a p.p.t. adversary $\mathcal{A}$ that breaks the PRG security of G' with probability $1/2+\epsilon$, where ϵ is non-negligible. Then there exists a p.p.t. algorithm $\mathcal{B}$ that breaks the PRG security of G with probability $1/2+\epsilon$.

Proof. The reduction algorithm $\mathcal{B}$ is defined as follows. It receives $u \in \{0,1\}^{2n}$ from the challenger (w.r.t G). It then chooses a uniformly random string $s_2 \leftarrow \{0,1\}^n$, and sends $u||s_2$ to the adversary $\mathcal{A}$. The adversary sends a bit b', which the reduction algorithm forwards to the challenger.

Analysis of $\mathcal{B}'s$ success probability

$$\begin{aligned}
&\Pr\Big[\mathcal{B} \text{ wins the PRG security game against } G\Big]\\
=&\Pr\Big[(\mathcal{B} \text{ outputs } 0) \ \wedge\ b=0\Big] + \Pr\Big[(\mathcal{B} \text{ outputs } 1) \ \wedge\ b=1\Big]\\
=&\Pr\Big[(\mathcal{A} \text{ outputs } 0) \ \wedge\ b=0\Big] + \Pr\Big[(\mathcal{A} \text{ outputs } 1) \ \wedge\ b=1\Big]
\end{aligned}$$

Now consider the following cases:

(a) $b=0$: $\mathcal{B}$ receives $u = G(s) \in \{0,1\}^{2n}$ for some $s \leftarrow \{0,1\}^n$, chooses $s_2 \leftarrow \{0,1\}^n$ and sends $u||s_2$ to $\mathcal{A}$. Note that $u||s_2 = G(s)||s_2 = G'(s||s_2)$. Now since, $s||s_2 \leftarrow \{0,1\}^{2n}$, $\mathcal{A}$ receives $u_{\mathcal{A}} = G'(s')$ for some $s' \leftarrow \{0,1\}^{2n}$.

(b) $b=1$: $\mathcal{B}$ receives $u \leftarrow \{0,1\}^{2n}$, chooses $s_2 \leftarrow \{0,1\}^n$ and sends $u||s_2$ to $\mathcal{A}$, hence $u_{\mathcal{A}} = u||s_2 \leftarrow \{0,1\}^{3n}$

Using these observations, we can conclude that

$$\begin{aligned}
&\Pr\Big[(\mathcal{A} \text{ outputs } 0) \ \wedge\ b=0\Big] + \Pr\Big[(\mathcal{A} \text{ outputs } 1) \ \wedge\ b=1\Big]\\
=&\Pr\Big[\mathcal{A} \text{ gets } u_{\mathcal{A}} = G'(s'),\ s' \leftarrow \{0,1\}^{2n} \ \wedge\ (\mathcal{A} \text{ outputs } 0)\Big] + \Pr\Big[\mathcal{A} \text{ gets } u_{\mathcal{A}} \leftarrow \{0,1\}^{3n} \ \wedge\ (\mathcal{A} \text{ outputs } 1)\Big]\\
=&\Pr\Big[\mathcal{A} \text{ wins the PRG security game against } G'\Big]\\
=&1/2+\epsilon
\end{aligned}$$

□

3. G' does not satisfy pseudorandomness security with related keys. We can construct a polynomial time adversary $\mathcal{A}$ such that, given two strings $(u_1, u_2) \in \{0,1\}^{3n} \times \{0,1\}^{3n}$, $\mathcal{A}$ can win the Related-PRG game with probability close to 1.

The adversary $\mathcal{A}$ checks if u_1 and u_2 are identical, except for the last bit. If $u_1 = u_2 \oplus 0\ldots01$, then $\mathcal{A}$ outputs 0, else $\mathcal{A}$ outputs 1.

Analysis of $\mathcal{A}'s$ winning probability:

$$\begin{aligned}
p_{\mathcal{A}} &= \Pr\Big[\mathcal{A} \text{ wins in the Related Seed PRG Security Game}\Big]\\
&= \Pr\Big[(\mathcal{A} \text{ outputs } 0) \ \wedge \ b = 0\Big] + \Pr\Big[(\mathcal{A} \text{ outputs } 1) \ \wedge \ b = 1\Big]\\
&= \frac{1}{2} + \left(\frac{1}{2} - \Pr\Big[(\mathcal{A} \text{ outputs } 0) \ \wedge \ b = 1\Big]\right)
\end{aligned}$$

In the last step, we use the following observation :
$\Pr\Big[(\mathcal{A} \text{ outputs } 0) \ \wedge \ b = 1\Big] + \Pr\Big[(\mathcal{A} \text{ outputs } 1) \ \wedge \ b = 1\Big] = \Pr\Big[b = 1\Big] = 1/2.$

Finally, note that if the challenger chose $b = 1$ in the security experiment, then the probability that $u_1 = u_2 \oplus 0 \ldots 01$ is $1/2^{3n}$. Therefore, $\Pr\Big[(\mathcal{A} \text{ outputs } 0) \ \wedge \ b = 1\Big] = \frac{1}{2^{3n+1}}$.

Therefore, $p_{\mathcal{A}} = 1 - 1/2^{3n+1}$, and this shows that G' does not satisfy $\mathsf{Related\text{-}PRG}$ security.