Homework 5

1. **Stretching PRG Output.** (10 points) Suppose we are given a length-doubling PRG $G$ such that

$$G : \{0, 1\}^B \rightarrow \{0, 1\}^{2B}$$

Using $G$, construct a new PRG $G'$ such that

$$G' : \{0, 1\}^B \rightarrow \{0, 1\}^{100B}$$

(Remark: We do not need a security proof. You should only use the PRG $G$ to construct the new PRG $G'$. In particular, you should not use any other cryptographic primitive like one-way function etc.)

**Solution.**
2. **New Pseudorandom Function Family.** Let $G$ be a length-doubling PRG $G : \{0,1\}^B \rightarrow \{0,1\}^{2B}$. Recall the basic GGM PRF construction presented below.

- Define $G(x) = (G_0(x), G_1(x))$ where $G_0, G_1 : \{0,1\}^B \rightarrow \{0,1\}^B$
- We define $g_{id}(x_1, x_2, \ldots, x_n)$ as $G_{x_n}(\ldots G_{x_2}(G_{x_1}(id))\ldots)$ where $id \overset{\$}{\leftarrow} \{0,1\}^B$.

Recall that in the class we studied that $g_{id}$ is a PRF family for $\{0,1\}^n \rightarrow \{0,1\}^B$, for a fixed value of $n$ when the key $id$ is picked uniformly at random from the set $\{0,1\}^B$.

(a) (6 points) Why is the above-mentioned GGM construction not a pseudorandom function family from the domain $\{0,1\}^*$ to the range $\{0,1\}^B$?

**Solution.**
(b) (13 points) Given a length-doubling PRG \( G : \{0, 1\}^B \rightarrow \{0, 1\}^{2B} \), construct a PRF family from the domain \( \{0, 1\}^n \) to the range \( \{0, 1\}^{100B} \).

(Remark: Again, in this problem, do not use any other cryptographic primitive like one-way function etc. You should only use the PRG \( G \) in your proposed construction.)

Solution.
(c) (6 points) Consider the following function family \{h_1, \ldots, h_\alpha\} from the domain \{0,1\}^* to the range \{0,1\}^B. We define \( h_{id}(x) = g_{id}(x, \lfloor |x| \rfloor_2) \), for \( k \in \{1,2,\ldots,\alpha\} \). Show that \{h_1, \ldots, h_\alpha\} is not a secure PRF from \{0,1\}^* to the range \{0,1\}^B.

(Note: The expression \( \lfloor |x| \rfloor_2 \) represents the length of \( x \) in \( n \)-bit binary expression.)

Solution.
3. **Variant of Pseudorandom Function Family.** Let $G$ be a length-doubling PRG $G: \{0, 1\}^B \rightarrow \{0, 1\}^{2B}$, recall the GGM construction taught in class to construct PRF family from $\{0, 1\}^* \rightarrow \{0, 1\}^T$

- Define $G(x) = (G_0(x), G_1(x))$ where $G_0, G_1 : \{0, 1\}^B \rightarrow \{0, 1\}^B$
- Let $G' : \{0, 1\}^B \rightarrow \{0, 1\}^T$ be a PRG.
- We define $g_{id}(x_1, x_2, \ldots, x_n)$ as $G'(G_{x_n}(\ldots G_{x_2}(G_{x_1}(id))\ldots))$
  where $id \leftarrow \{0, 1\}^B$.

(15 points) Prove that the above-mentioned PRF construction is not secure when $G' = G$.

**Solution.**
4. **OWF.** (15 points) Let \( f : \{0,1\}^n \rightarrow \{0,1\}^n \) be a one-way function. Define \( g : \{0,1\}^n \rightarrow \{0,1\}^{n+1} \) as
\[
g(x) = f(x) \|
\]
where \( x \in \{0,1\}^n \). Show that \( g \) is also a one-way function.

**Hint.** Suppose there exists an efficient adversary \( A \) that inverts the function \( g \). You should now construct a new efficient adversary \( A' \) that uses \( A \) as a subroutine to invert the function \( f \).

**Solution.**
5. **Encryption using Random Functions.** Let \( \mathcal{F} \) be the set of all functions \( \{0, 1\}^n \rightarrow \{0, 1\}^n \). Consider the following private-key encryption scheme.

- **Gen()**: Return \( \text{sk} = F \) uniformly at random from the set \( \mathcal{F} \)
- **Enc_{sk}(m)**: Return \((c, r)\), where \( r \) is chosen uniformly at random from \( \{0, 1\}^n \), \( c = m \oplus F(r) \), and \( \text{sk} = F \).
- **Dec_{sk}(\tilde{c}, \tilde{r})**: Return \( \tilde{c} \oplus F(\tilde{r}) \).

(a) (12 points) Suppose we want to ensure that even if we make \( 10^9 \) calls to the encryption algorithm, all randomness \( r \) that are chosen are distinct with probability \( 1 - 2^{-100} \). What value of \( n \) shall you choose?

**Solution.**
(b) (8 points) Conditioned on the fact that all randomness $r$ in the encryption schemes are distinct, prove that this scheme is secure.

Solution.
6. **Attack on an Encryption Scheme.** (15 points) Let $\mathcal{F}$ be the set of all function $\{0,1\}^n \to \{0,1\}^n$. Consider the following private-key encryption scheme.

- **Gen()**: Return $sk = F$ chosen uniformly at random from the set $\mathcal{F}$
- **Enc_{sk}(m)**: Return $m \oplus F(m)$, where $sk = F$

We have knowingly not defined the decryption scheme because it might not be efficient to decrypt this scheme even given $sk = F$! However, the encryption algorithm itself has an issue.

Prove that the encryption scheme is not secure.

**Solution.**
Collaborators: