Homework 5

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

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

Using G, construct a new PRG G' such that

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

(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. Note that B is a fixed constant.)

Solution.

2. **New Pseudorandom Function Family.** (7+8+10) Let G be a length-doubling PRG $G\colon \{0,1\}^B \to \{0,1\}^{2B}$. Recall the basic GGM PRF construction presented below.

- Define $G(x) = (G_0(x), G_1(x))$ where $G_0, G_1 : \{0,1\}^B \to \{0,1\}^B$
- We define $g_{\mathsf{id}}(x_1, x_2, \dots x_n)$ as $G_{x_n}(\dots G_{x_2}(G_{x_1}(\mathsf{id}))\dots)$ where $\mathsf{id} \xleftarrow{\$} \{0,1\}^B$.

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

(a) (7 points) Why is the above-mentioned GGM construction not a pseudorandom function family from the domain $\{0,1\}^*$ to the range $\{0,1\}^B$? (Note that $\{0,1\}^*$ means that the length of the input to the PRF is arbitrary)
Solution.

(b) (8 points) Given a length-doubling PRG $G\colon \{0,1\}^B \to \{0,1\}^{2B}$, 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) (10 points) Consider the following function family $\{h_1, \dots, h_\alpha\}$ from the domain $\{0,1\}^*$ to the range $\{0,1\}^B$. We define $h_{\mathsf{id}}(x) = g_{\mathsf{id}}(x, [\ |x|\ ]_2)$, for $k \in \{1, 2, \dots, \alpha\}$. Show that $\{h_1, \dots, h_\alpha\}$ is not a secure PRF from $\{0,1\}^*$ to the range $\{0,1\}^B$.

(*Note*: The expression $[|x|\,]_2$ represents the length of x in n-bit binary expression.)

Solution.

3. **Variant of Pseudorandom Function Family.** (15 points) Let G be a length-doubling PRG $G\colon \{0,1\}^B \to \{0,1\}^{2B}$ and $G' : \{0,1\}^B \to \{0,1\}^T$ be a PRG where $T \geqslant B$. The following construction is suggested to construct a PRF family from $\{0,1\}^* \to \{0,1\}^T$. (Note that $\{0,1\}^*$ means that the length of the input to the PRF is arbitrary)

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

   Prove that the above-mentioned PRF construction is <u>not</u> secure when $G' = G$. (Note that when $G' = G$, then $T = 2B$).

   Solution.

4. **OWF.** (10 points) Let $f : \{0,1\}^n \to \{0,1\}^n$ be a one-way function. Define $g : \{0,1\}^{2n} \to \{0,1\}^{2n}$ as
$$g(x_1, x_2) = f(x_1) || x_1 \oplus x_2$$

where $x_1 \in \{0,1\}^n$ and $x_2 \in \{0,1\}^n$. Show that g is also a one-way function.
Hint. Suppose there exists an efficient adversary $\mathcal{A}$ that inverts the function g . You should now construct a new efficient adversary $\mathcal{A}'$ that uses $\mathcal{A}$ as a subroutine to invert the function f.
Solution.

5. **Encryption using Random Functions.** (15+10 points) Let $\mathcal{F}$ be the set of all functions $\{0,1\}^n \to \{0,1\}^n$. Consider the following private-key encryption scheme.

- $\mathsf{Gen}()$: Return $\mathsf{sk} = F$ uniformly at random from the set $\mathcal{F}$
- $\mathsf{Enc}_{\mathsf{sk}}(m)$: Return (c, r), where r is chosen uniformly at random from $\{0,1\}^n$, $c = m \oplus F(r)$, and $\mathsf{sk} = F$.
- $\mathsf{Dec}_{\mathsf{sk}}(\widetilde{c}, \widetilde{r})$: Return $\widetilde{c} \oplus F(\widetilde{r})$.

(a) (15 points) Suppose we want to ensure that even if we make 10^{15} calls to the encryption algorithm, all randomness r that are chosen are distinct with probability $1 - 2^{-101}$. What value of n shall you choose?
Solution.

(b) (10 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.

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

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

Prove that the encryption scheme is not secure.
Solution.

7. **Birthday Paradox.** (10 points) Recall that the Birthday Paradox states that if we throw $m = c\sqrt{n}$ balls into n bins, then the probability that there exists a collision (i.e., a bin with at least two balls) is $\geqslant 0.99$, where $c > 0$ is an appropriate constant. Purdue university has 12 colleges. How many Purdue students in a room will ensure with probability $\geqslant 0.99$ that there exists at least a pair of students of the same gender who are from the same college and also celebrate their birthday at the same month.

8. **PRF.**(10 points) Suppose the set of functions $F_{\mathsf{id}}\colon \{0,1\}^n \to \{0,1\}^n$ forms a secure PRF when id is chosen uniformly at random from the set $\{0,1\}^n$.

   We are now constructing a new PRF family $G_{\mathsf{id}}\colon \{0,1\}^{2n} \to \{0,1\}^{2n}$, where $\mathsf{id} \in \{0,1\}^n$. This new function is defined as follows.

$$G_{\mathsf{id}}(x_1, x_2) := \big(\ F_{\mathsf{id}}(x_1)\ ,\ x_1 \oplus F_{\mathsf{id}}(x_2)\ \big)$$

   Is this new PRF secure or not?

   (If you think that it is secure, then prove that it is secure. If you think that it is insecure, then prove why this construction is insecure. You get no points for writing Yes/No.)

Collaborators :