Homework 5

Collaborators:

Practice Questions

These are practice questions. They will **NOT** be graded. We have also provided the final answers. However, it is up to you to understand how or why the given solution is correct.
You do not need to submit these on Gradescope. However, you may find it easier to just include them in the pdf. In that case, please do not mark these questions on Gradescope.

1. **Birthday Paradox. (0 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.
   An international university has 12 colleges. Moreover, the students of this university come from 121 different countries around the world. How many students (from the university) in a room will ensure with probability $\geqslant 0.99$ that there exists at least one pair of students such that they are from the same country, the same college, and they celebrate their birthday in the same month.

   Solution.
   $\lceil 132c \rceil$

2. **Encryption using Random Functions. (0 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) **(0 points)** Suppose we want to ensure that even if we make 10^{30} calls to the encryption algorithm, all randomness r that are chosen are distinct with probability $1-2^{-401}$. What value of n shall you choose?

Solution.

We have proved in class that the probability that all k samples chosen uniformly at random from a set S are distinct is roughly equal to $\exp(\frac{-k^2}{2|S|})$. In this question, $|S| = 2^n$ and $k = 10^{30}$. We need to have:

$$\exp\left(-\frac{10^{60}}{2^{n+1}}\right) \geqslant 1 - 2^{-401} \approx \exp\left(-2^{-401}\right) \tag{1}$$

$$\iff \left(-\frac{10^{60}}{2^{n+1}}\right) \geqslant \left(-2^{-401}\right) \tag{2}$$

$$\iff 10^{60} \leqslant 2^{n-400} \tag{3}$$

$$\iff 60 \log_2(10) \leqslant n - 400 \tag{4}$$

$$\iff n \geqslant 400 + 60 \log_2(10) \approx 599.316 \tag{5}$$

$$\iff n \geqslant 600 \tag{6}$$

(b) **(0 points)** Conditioned on the fact that all randomness r in the encryption schemes are distinct, prove that this scheme is secure.

Solution.

We assume that $r_i \neq r_j$ for all $i \neq j$. Note that F is chosen uniformly at random from the set of all functions that map a string of n bits to a string of n bits. Therefore, the values $F(r_1), \ldots, F(r_q)$ are independent and have uniform distribution. This implies that $c_1 = m_1 \oplus F(r_1), \ldots, c_q = m_q \oplus F(r_q)$ are all uniform and independent of each other. This means that the encryption of $m_1, m_2, \ldots, m_{q-1}$ does not reveal any information about the encryption of m_q. This scheme is like the one-time pad, because it is equivalent to XORing the sequence $m_1 \ldots m_q$ with uniformly random sequence $F(r_1) \ldots F(r_q)$ to get $c_1 \ldots c_q$. Formally, for any messages $m_1, \ldots, m_q$ and ciphertexts $c_1, \ldots, c_q$, the probability below equals $(1/2^n)^q$, which does not depend on the messages.

$$\Pr[C_1 = c_1, \ldots, C_q = c_q \mid M_1 = m_1, \ldots, M_q = m_q] \tag{7}$$

$$= \Pr[m_1 \oplus F(r_1) = c_1, m_2 \oplus F(r_2) = c_2, \ldots, m_q \oplus F(r_q) = c_q] \tag{8}$$

$$= \Pr[F(r_1) = m_1 \oplus c_1, F(r_2) = m_2 \oplus c_2, \ldots, F(r_q) = m_q \oplus c_q] \tag{9}$$

$$= \Pr[F(r_1) = m_1 \oplus c_1] \times \cdots \times \Pr[F(r_q) = m_q \oplus c_q] = \left(\frac{1}{2^n}\right)^q \tag{10}$$

Homework Questions

These are homework questions and will be graded. Please make sure to clearly mark each problem on Gradescope.

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

$$G' : \{0,1\}^B \to \{0,1\}^{2026B}$$

(Remark: You do not need to provide 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, such as a one-way function.)

Solution.

2. **New Pseudorandom Function Family. (7+8+10 points)** 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 $g_{\mathsf{id}}(x_1, x_2, \ldots x_n)$ as $G_{x_n}(\ldots G_{x_2}(G_{x_1}(\mathsf{id}))\ldots)$ 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 $\{0,1\}^{2026B}$.
(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 $\{h_1, \ldots, h_\alpha\}$ from the domain $\{0,1\}^*$ to the range $\{0,1\}^B$. We define $h_{\mathsf{id}}(x) = g_{\mathsf{id}}(x, [\,|x|\,]_2)$, for $\mathsf{id} \in \{1, 2, \ldots, \alpha\}$. Show that $\{h_1, \ldots, h_\alpha\}$ is not a secure PRF from $\{0,1\}^*$ to the range $\{0,1\}^B$.

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

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 $g_{\mathsf{id}}(x_1, x_2, \ldots x_n)$ as $G'(G_{x_n}(\ldots G_{x_2}(G_{x_1}(\mathsf{id}))\ldots))$ where $\mathsf{id} \xleftarrow{\$} \{0,1\}^B$.

   Prove that the above-mentioned PRF construction is not 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

$$g(x_1, x_2) = f(x_1 \oplus 1^n) \mid\mid x_1 \oplus x_2$$

where $x_1 \in \{0,1\}^n$, $x_2 \in \{0,1\}^n$, $\cdot \mid\mid \cdot$ denotes the concatenation operation, and 1^n denotes the n-bit all 1s string. 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. **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.

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

   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 just writing Yes/No.)

   Solution.

6. **One Way Function (12 points)** In this problem, we will show that a one-way function cannot have a small range.

   (a) **(6 points)** First, we need an inequality. Prove that

   $$p_1^2 + p_2^2 + \cdots + p_k^2 \geqslant \frac{1}{k},$$

   where $p_1, \ldots, p_k \geqslant 0$ such that $p_1 + \cdots + p_k = 1$.
   Hint: The Cauchy-Schwarz inequality says that for non-negative x_i and y_is, the following inequality holds.

   $$\sum_{i=1}^{k} x_i y_i \leqslant \sqrt{\left(\sum_{i=1}^{k} x_i^2\right)\left(\sum_{i=1}^{k} y_i^2\right)}$$

   Solution.

(b) **(6 points)** Let $f\colon \{0,1\}^n \to \{0,1\}^\ell$ be a function. The honest challenger samples $x \xleftarrow{\$} \{0,1\}^n$ and sends the challenge $y = f(x)$ to us. We, on input y, run the following algorithm

1: Sample $r \xleftarrow{\$} \{0,1\}^n$
2: Compute $t = f(r)$
3: If $y == t$: return $\widetilde{x} = r$
4: Else: return $\widetilde{x} = 0$.

Prove that the probability of our algorithm successfully inverting the one-way function f is $\geqslant \frac{1}{2^\ell}$ (over the random choice of $x \xleftarrow{\$} \{0,1\}^n$ by the honest challenger). Equivalently, prove that

$$\Pr_{x,r \xleftarrow{\$} \{0,1\}^n} \left[f(\widetilde{x}) = f(x) \right] \geqslant \frac{1}{2^\ell}.$$

(Remark: It is not necessary that the size of the preimage of $y \in \{0,1\}^\ell$ is the same as the size of the preimage of another $y' \in \{0,1\}^\ell$.)

Solution.