Anish Banerjee, Shankh Gupta
Problem Set - 1
COL759: Cryptography
August 2023

Problem 1: Perfect 2 time security

Solution:

Problem 2 : Secure/Insecure PRGs and PRFs

Solution:

(a) PRGs

i. $\mathcal{G}' = \left\{G'_n : \{0,1\}^{2n} \to \{0,1\}^{3n}\right\}_{n\in\mathbb{N}}$, where

$$G'_n(s_1 \mid\mid s_2) = G_n(s_1) \wedge G_n(s_2).$$

The given PRG is **insecure**. As discussed in class and Quiz 2, a secure PRG G can disclose some of the bits of the seed s. For convenience we take n to be even but a similar logic can be used for the odd case too. Suppose $G : \{0,1\}^n \to \{0,1\}^{3n}$ is such that it reveals the first $n/2$ of its bits:

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

where $G'' : \{0,1\}^{n/2} \to \{0,1\}^{5n/2}$ is a secure PRG. It can be proved that G is secure if G'' is secure. Now,

$$G'(s_1 \mid\mid s_2) = G_n(s_{11} \mid\mid s_{12}) \wedge G_n(s_{21} \mid\mid s_{22}) = s_{11} \wedge s_{21} \mid\mid G''(s_{12}) \wedge G''(s_{22})$$

which reveals the bits of $s_{11} \wedge s_{21}$. The advantage of the adversary which exploits this will be close to 1.

ii. $\mathcal{G}' = \left\{G'_n : \{0,1\}^{2n} \to \{0,1\}^{3n}\right\}_{n\in\mathbb{N}}$, where

$$G'_n(s_1 \mid\mid s_2) = G_n(s_1) \oplus G_n(s_2).$$

(b) PRFs

i. $\mathcal{F}' = \left\{F'_n : \{0,1\}^n \times \{0,1\}^{2n} \to \{0,1\}^n\right\}_{n\in\mathbb{N}}$ where

$$F'_n(k,(x_1,x_2)) = F_n(k,x_1) \oplus F_n(k,x_2).$$

The given family $\mathcal{F}'$ is **insecure**. Consider a PPT attacker $\mathcal{A}$ who sends $\mathsf{poly}(\lambda)$ distinct (x_i, x_i) queries to the challenger. If the challenger chooses $b = 0$ then it will end up sending

$$F_n(k,x_i) \oplus F_n(k,x_i) = 0^n$$

for each of the queries. The attacker outputs 0 if all the responses are 0 and 1 otherwise. Advantage of the attacker is close to 1, precisely $1 - 2^{-n\mathsf{poly}(\lambda)}$.

ii. $\mathcal{F}' = \{F'_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n\}_{n\in\mathbb{N}}$ where

$$F'_n(k,x) = F_n(k,x) \oplus x.$$

The given family is secure. Given an adversary $\mathcal{A}$ which breaks PRF security of $\mathcal{F}'$, we can construct an adversary $\mathcal{B}$ which breaks the security of $\mathcal{F}$ (Fig. 1)

Problem 2(b)(ii)

- Challenger picks a uniformly random bit $b \leftarrow \{0,1\}$ and a seed $s \leftarrow \{0,1\}^n$.
- The adversary $\mathcal{A}$ makes polynomially many queries to $\mathcal{B}$, who passes them to the challenger. Challenger replies as in the PRF Game.
- Upon receiving the response y_i of each query, $\mathcal{B}$ sends $y_i \oplus x_i$ to $\mathcal{A}$
- After polynomially many queries, $\mathcal{B}$ forwards the response send by $\mathcal{A}$ (b') and wins if $b = b'$.

Figure 1: Reduction for Problem 2(b)(ii)

Problem 3 : PRG Security does not imply Related-Key-PRG Security

Solution:

Problem 4 : Constructing PRFs from PRGs

Solution: We will use a tree construction similar to the one given in the book for proving (Fig. 2)

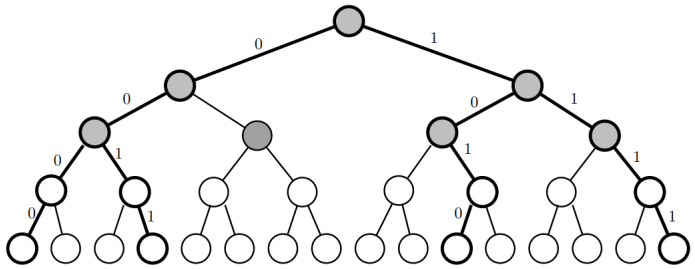

Figure 4.16: Evaluation tree for Hybrid 2 with $\ell = 4$. The shaded nodes are assigned random labels, while the unshaded nodes are assigned derived labels. The highlighted paths correspond to inputs 0000, 0011, 1010, and 1111.

Figure 2: Tree construction in the book

(a) Construct $\log n$ hybrid worlds in the following way: in Hybrid world j, the challenger samples 2^j random bitstrings $s_1, s_2, s_3 \ldots s_j \leftarrow \{0,1\}^n$. Then it applies