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**. Consider the PRG game between $\mathcal{A}$ and G' challenger where on input y, $\mathcal{A}$ outputs the last bit of y. Let $L(x)$ denote the last bit of x. Note that if G is secure, then $\Pr[L(G(s) = 0)]$ will be close to 1/2. Otherwise, if it is $1/2 + \epsilon$ we can create an adversary breaking G with non-negligible advantage ϵ($\mathcal{A}$ always outputs 0). So, if we take $\Pr[L(G(s)) = 0] = 1/2 + \mathsf{negl}(\lambda)$

$$\Pr[b' = 0|b = 0] = \Pr[L(G(s_1) \wedge G(s_2)) = 0]$$

$$\leq \Pr[L(G(s_1)) = 0 \wedge L(G(s_2)) = 0] + \Pr[L(G(s_1)) = 1 \wedge L(G(s_2)) = 0] + \Pr[L(G(s_1)) = 0 \wedge L(G(s_2)) = 1]$$

$$\approx 3/4 + \mathsf{negl}(\lambda)$$

and

$$\Pr[b' = 0|b = 1] = 1/2$$

Thus the $\mathsf{PRGAdv}[\mathcal{A}, \mathcal{G}] \approx 1/4$ which is non-negligible.

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

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

This is a **secure** PRG. We prove the security by a hybrid argument.

- **World0** The challenger sends $G_n(s_1) \oplus G_n(s_2)$ to the attacker
- **HybridWorld** The challenger sends $G_n(s_1) \oplus \mathsf{random}_1$ to the attacker
- **World1** The challenger sends $\mathsf{random}_1 \oplus \mathsf{random}_2$ to the attacker

Claim: If any adversary $\mathcal{A}$ can distinguish between World0 and HybridWorld then we can construct $\mathcal{B}$ which breaks the PRG security of G.
The reduction $\mathcal{B}$ receives y from the PRG challenger. It samples $s \leftarrow \{0,1\}^n$ and sends $G(s) \oplus y$ to $\mathcal{A}$. The advantage of $\mathcal{A}$ in distinguishing between World0 and HybridWorld will be equal to the advantage of $\mathcal{B}$ in breaking PRG security of G.
Similarly we can also claim that:

Claim: If any adversary $\mathcal{A}$ can distinguish between HybridWorld and World1 then we can construct $\mathcal{B}$ which breaks the PRG security of G.
The reduction $\mathcal{B}$ receives y from the PRG challenger. It samples $r \leftarrow \{0,1\}^n$ and sends $r \oplus y$ to $\mathcal{A}$. The advantage of $\mathcal{A}$ in distinguishing between HybridWorld and World1 will be equal to the advantage of $\mathcal{B}$ in breaking PRG security of G.
Now we can choose any reduction randomly to break the PRG security of G. Also note that we cannot use a similar argument in part i. because $\mathsf{random}_1 \wedge \mathsf{random}_2$ is not truely random

(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 (Fig. 2)

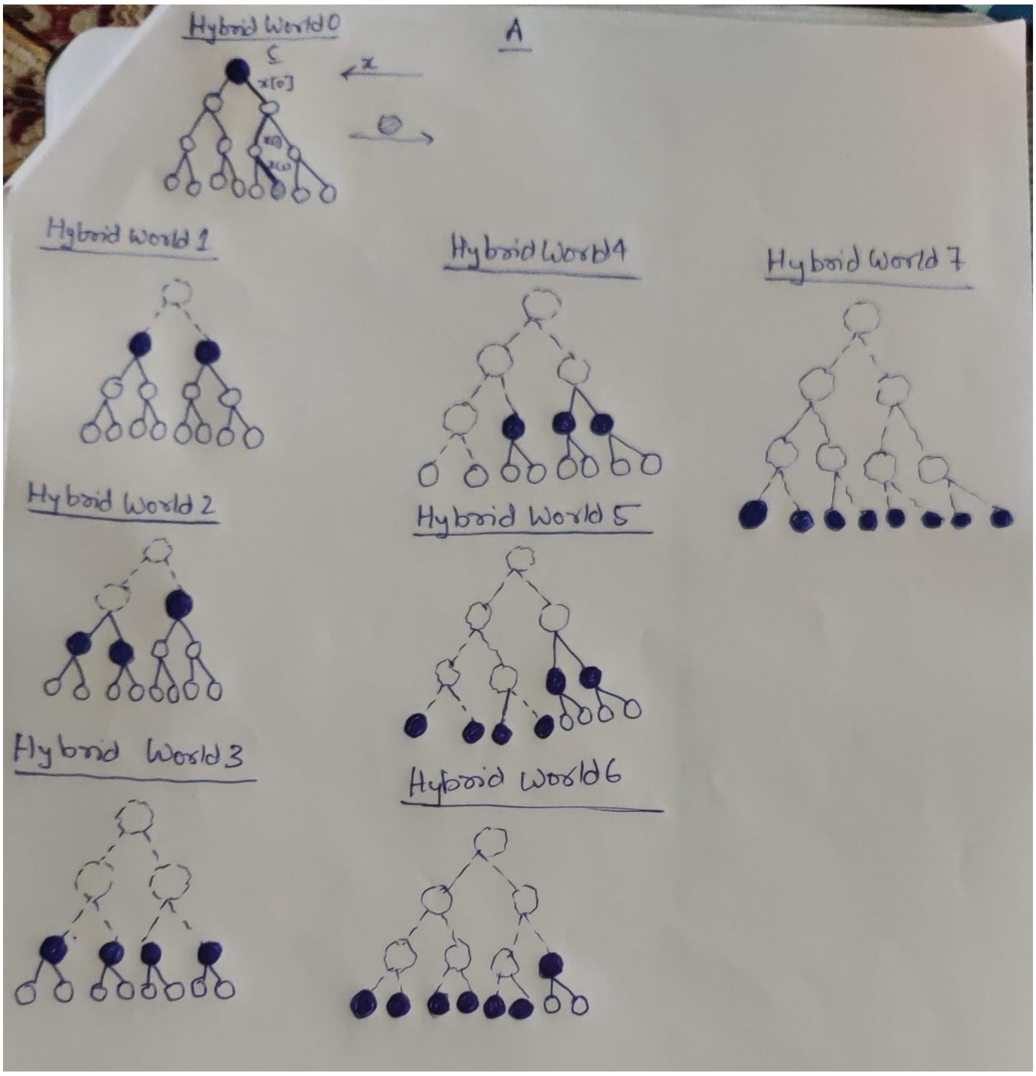

Figure 2: Construction of Hybrid worlds for the case $\log n = 3$. The randomly generated nodes are shadedand the nodes which can be ignored are dotted

(a) Construct n hybrid worlds in the following way: In Hybrid j, the challenger builds an evaluation tree whose nodes are labeled as follows:

- The first j nodes (as appearing in the level order traversal of the tree) can be ignored.
- The next $j+1$ nodes are labelled with random values.
- Remaining nodes are derived from their parents.

In response to a query $x \in \{0,1\}^{\log n}$ in Hybrid j, the challenger sends to the adversary the label of the leaf addressed by x.

Observe that Hybrid 0 corresponds to the case $b = 0$ in the PRF game when the challenger sends $F_k(x)$ and Hybrid l corresponds to $b = 1$ when the challenger uses a truly random function.

Claim: If there exists an adversary $\mathcal{A}$ which can distinguish between Hybrid i and Hybrid $i+1$ then we can construct an adversary $\mathcal{B}$ which breaks the PRG security of G.

Problem 4(a)

- Challenger picks a uniformly random bit $b \leftarrow \{0,1\}$ and a seed $s \leftarrow \{0,1\}^n$. If $b = 0$, he sends $y = G(s)$ to $\mathcal{B}$ otherwise he sends a $y = r \leftarrow \{0,1\}^{2n}$.
- $\mathcal{B}$ constructs the evaluation tree.
  - The first $i+1$ nodes can be ignored
  - The next i nodes are randomly generated
  - The next two nodes are made by splitting y sent by the challenger into two halves
  - Remaining nodes are generated using the algorithm from their parents.
- The adversary $\mathcal{A}$ makes polynomially many queries to $\mathcal{B}$. In response to a query $x \in \{0,1\}^{\log n}$, $\mathcal{B}$ sends the label of the leaf addressed by x (This traveral is shown in the HybridWorld0 of Fig. 3)
- After polynomially many queries, $\mathcal{B}$ forwards the response send by $\mathcal{A}$ (b') and wins if $b = b'$.

Figure 3: Reduction for Problem 4(a)

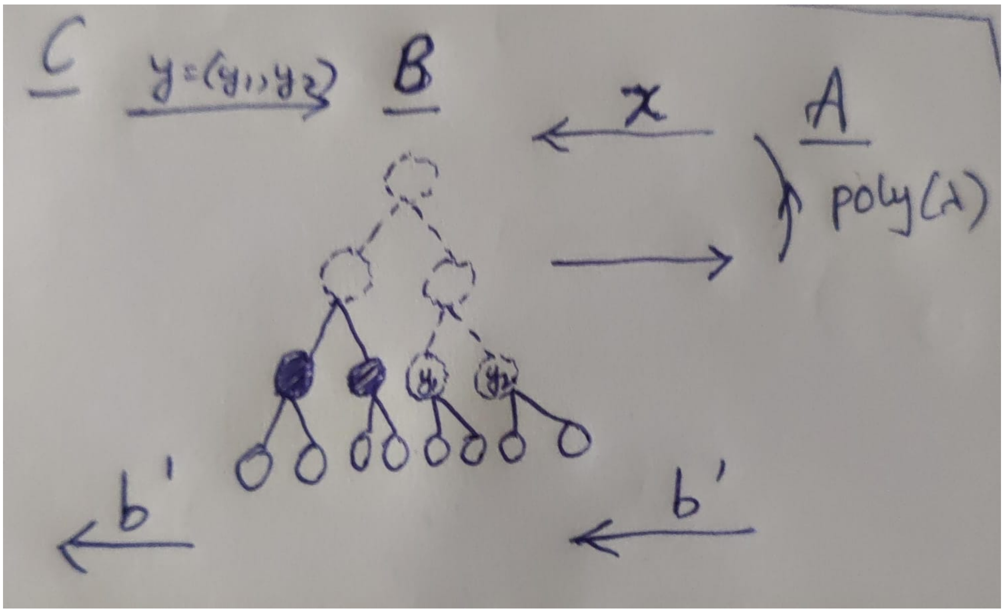

Figure 4: Reduction for distinguishing between HybridWorld2 and HybridWorld3

Proof: Consider the reduction Fig. 3

From the construction, it can be checked that:

$$\Pr[b' = 0 | b = 0] = \Pr[\mathcal{A} \text{ outputs } 0 \text{ in HybridWorld } i] = p_i$$

$$\Pr[b' = 0 | b = 0] = \Pr[\mathcal{A} \text{ outputs } 0 \text{ in HybridWorld } i+1] = p_{i+1}$$

Thus,

$$\mathsf{PRGAdv}[\mathcal{B}, \mathcal{G}] = |p_i - p_{i+1}|$$

Finally for the combined reduction, we choose any one of the reductions at random.

$$\mathsf{PRGAdv}[\mathcal{B}^c, \mathcal{G}^c] = \frac{|p_l - p_0|}{\log n}$$

(b) In the above construction, $\mathcal{B}$ will need to sample $O(2^d)$ random bitstrings in some hybrids, where d is the depth of the tree. If $d = \log n$ then $\mathcal{B}$ samples $O(n)$ bitstrings. However, if $d = n$ then he has to sample exponentially many strings, making him inefficient. So, we cannot use the same reduction when $x \in \{0,1\}^n$.

(c) The given construction is insecure. Consider an adversary $\mathcal{A}$ which plays the following game $\mathcal{G}$:

- $\mathcal{A}$ sends x to the Challenger and receives y_1
- $\mathcal{A}$ sends $x||1$ to the Challenger and receives y_2
- $\mathcal{A}$ finds $G(y_1) = (s_0, s_1)$ and checks if $s_1 = y_1$. If so it returns $b' = 0$ else $b' = 1$

Now,

$$\mathsf{PRFAdv}[\mathcal{A}, \mathcal{G}] = |\Pr[b' = 0|b = 0] - \Pr[b' = 0|b = 1]|$$

From construction we have,

$$\Pr[b' = 0|b = 0] = 1$$

and

$$\Pr[b' = 0|b = 1] = \Pr[G(y_1) = (s_0, s_1) \wedge s_1 = y_1] = 2^{-n}$$

Thus the $\mathsf{PRFAdv}[\mathcal{A}, \mathcal{G}] = 1 - 2^{-n}$