CS 601.442/642 – Modern Cryptography Instructor: Abhishek Jain

Reduction Example

1 Pseudorandom Generators

Problem

Let $G : \{0,1\}^n \to \{0,1\}^{3n}$ be a PRG. Consider a function $H : \{0,1\}^n \to \{0,1\}^{6n}$ that works as follows:

$$H(s) : \text{First compute } s_1||s_2||s_3 \coloneqq G(s), \text{ then compute and output } G(s_1)||G(s_3)$$

Prove via reduction that $H(\cdot)$ also a PRG.

Solution

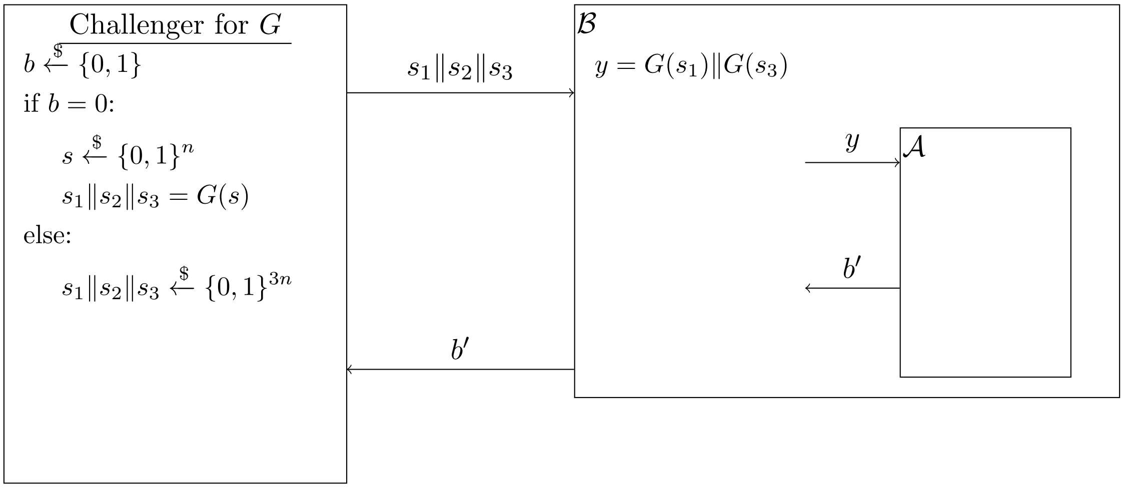
Consider the following hybrids:

- $\mathcal{H}_0 : \{G(s_1)||G(s_3); s \xleftarrow{\$} \{0,1\}^n, s_1||s_2||s_3 = G(s)\}$
- $\mathcal{H}_1 : \{G(s_1)||G(s_3); s_1, s_3 \xleftarrow{\$} \{0,1\}^n\}$
- $\mathcal{H}_2 : \{G(s_1)||R_2; s_1 \xleftarrow{\$} \{0,1\}^n, R_2 \xleftarrow{\$} \{0,1\}^{3n}\}$
- $\mathcal{H}_3 : \{R_1||R_2; R_1, R_2 \xleftarrow{\$} \{0,1\}^{3n}\}$

In order to show that $H(s)$ is a PRG, it suffices to show that $\mathcal{H}_0$ is indistinguishable from $\mathcal{H}_3$. Let us assume for the for the sake of contradiction that $\mathcal{H}_0 \not\approx \mathcal{H}_3$. In other words, let us assume that there exists an adversary $\mathcal{A}$ who can distinguish between $\mathcal{H}_0$ and $\mathcal{H}_3$ with some non-negligible advantage $\mu(n)$. From hybrid lemma, it follows that there must exist $i \in \{0,1,2\}$, such that $\mathcal{A}$ can distinguish between $\mathcal{H}_i$ and $\mathcal{H}_{i+1}$ with non-negligible advantage at least $\mu(n)/4$. We now show that if this is the case, then there exists another adversary $\mathcal{B}$ that can break the security of PRG G.

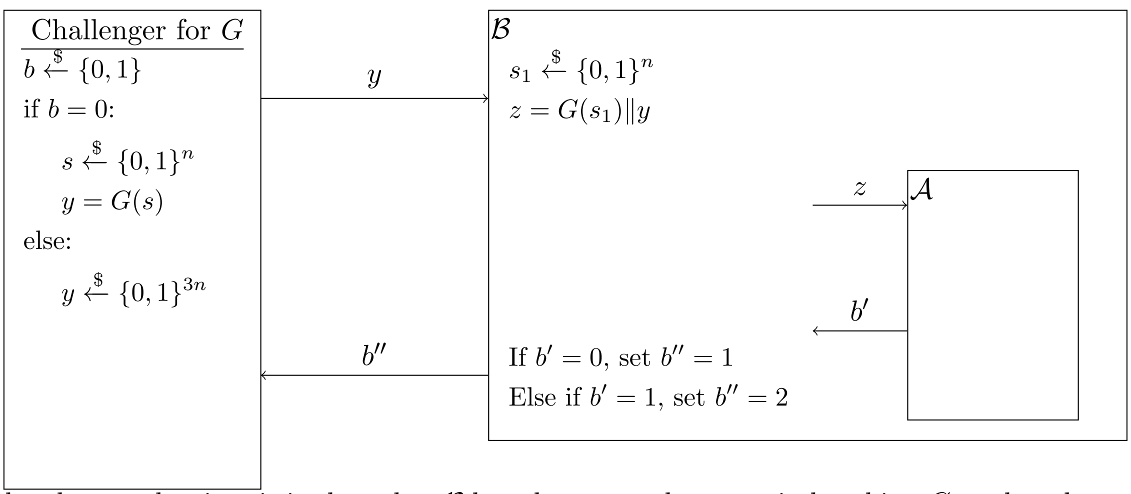
We argue this, by giving a proof via reduction for each $i \in \{0,1,2\}$.

1. Let $\mathcal{A}$ distinguish between $\mathcal{H}_0$ and $\mathcal{H}_1$ non-negligible advantage at least $\mu(n)/4$. We now construct another adversary $\mathcal{B}$ that breaks the security of G as follows:



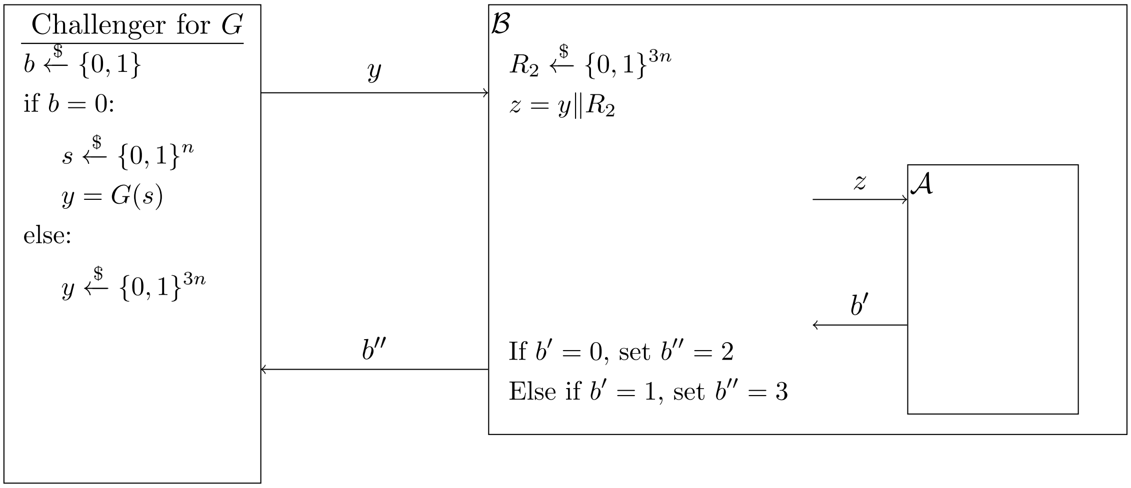
From the above reduction, it is clear that $\mathcal{B}$ has the same advantage in breaking G as the advantage that $\mathcal{A}$ has in distinguishing between $\mathcal{H}_0$ and $\mathcal{H}_1$, which is at least $\mu(n)/4$. Since $\mu(n)/4$ is non-negligible, this would mean $\mathcal{B}$ can break G. However, we know that G is a secure PRG, and hence, no such adversary can exist. Therefore our assumption was incorrect and $\mathcal{H}_0 \approx \mathcal{H}_1$.

2. Let $\mathcal{A}$ distinguish between $\mathcal{H}_1$ and $\mathcal{H}_2$ non-negligible advantage at least $\mu(n)/4$. We now construct another adversary $\mathcal{B}$ that breaks the security of G as follows:



From the above reduction, it is clear that $\mathcal{B}$ has the same advantage in breaking G as the advantage that $\mathcal{A}$ has in distinguishing between $\mathcal{H}_1$ and $\mathcal{H}_2$, which is at least $\mu(n)/4$. Since $\mu(n)/4$ is non-negligible, this would mean $\mathcal{B}$ can break G. However, we know that G is a secure PRG, and hence, no such adversary can exist. Therefore our assumption was incorrect and $\mathcal{H}_1 \approx \mathcal{H}_2$.

3. Let $\mathcal{A}$ distinguish between $\mathcal{H}_2$ and $\mathcal{H}_3$ non-negligible advantage at least $\mu(n)/4$. We now construct another adversary $\mathcal{B}$ that breaks the security of G as follows:



From the above reduction, it is clear that $\mathcal{B}$ has the same advantage in breaking G as the advantage that $\mathcal{A}$ has in distinguishing between $\mathcal{H}_2$ and $\mathcal{H}_3$, which is at least $\mu(n)/4$. Since $\mu(n)/4$ is non-negligible, this would mean $\mathcal{B}$ can break G. However, we know that G is a secure PRG, and hence, no such adversary can exist. Therefore our assumption was incorrect and $\mathcal{H}_2 \approx \mathcal{H}_3$.

We have shown that $\mathcal{H}_0 \approx \mathcal{H}_1 \approx \mathcal{H}_2 \approx \mathcal{H}_3$. Hence, our assumption must be wrong and there does not exist any adversary $\mathcal{A}$ who can distinguish between $\mathcal{H}_2$ and $\mathcal{H}_3$ with non-negligible advantage $\mu(n)$. Hence $H(\cdot)$ is a secure PRG.