Cryptography: Homework 2

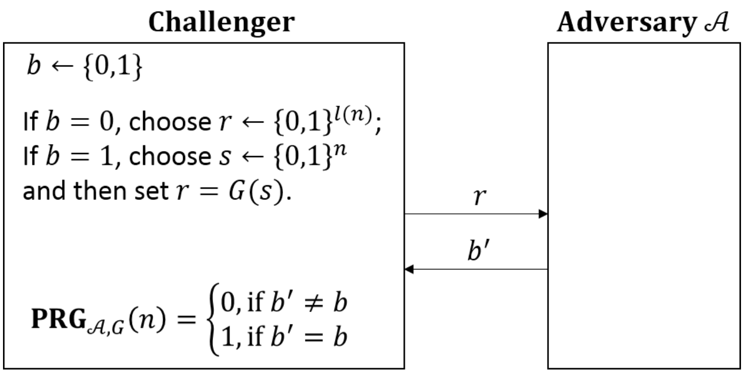
(Deadline: 10am, 2021/10/22)

1. (20 points) Let $f(n), g(n)$ be negligible functions and let $p(n)$ be a polynomial function. Show that $f(n) + g(n)$ and $p(n)f(n)$ are negligible functions.

2. (10 points) Let X_n be a random variable that takes values in $\{0,1\}^n$. Let $G : \{0,1\}^n \to \{0,1\}^{l(n)}$ be a PRG. Show that if $\{X_n\} \equiv_{\text{c.i.}} \{U_n\}$, then $\{G(X_n)\} \equiv_{\text{c.i.}} \{U_{l(n)}\}$.

   (hint: show that $\{G(X_n)\} \equiv_{\text{c.i.}} \{G(U_n)\}$)

3. (20 points) Let $G : \{0,1\}^n \to \{0,1\}^{l(n)}$ be a polynomial-time computable function, where $l(n) > n$ for all $n \geq 1$. Consider the following experiment $\mathsf{PRG}_{\mathcal{A},G}(n)$:



   Show that if G is a PRG, then for any PPT algorithm $\mathcal{A}$, there is a negligible function negl such that $|\Pr[\mathsf{PRG}_{\mathcal{A},G}(n) = 1] - \frac{1}{2}| \leq \text{negl}(n)$.