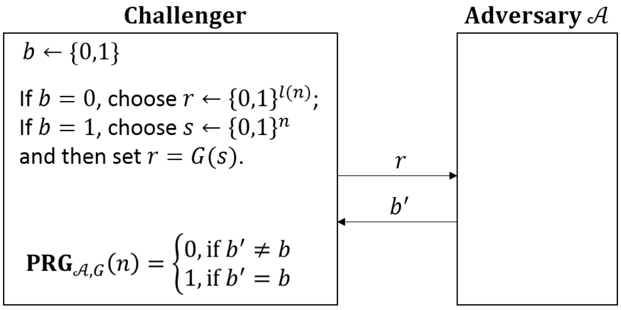
Cryptography: Homework 4

(Deadline: 11:59am, 2019/10/23)

1. (30 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 $\mathsf{PRG}_{\mathcal{A},G}(n)$:



$b \leftarrow \{0,1\}$

If $b = 0$, choose $r \leftarrow \{0,1\}^{l(n)}$;
If $b = 1$, choose $s \leftarrow \{0,1\}^n$
and then set $r = G(s)$.

$$\mathbf{PRG}_{\mathcal{A},G}(n) = \begin{cases} 0, \text{if } b' \neq b \\ 1, \text{if } b' = b \end{cases}$$

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

2. (20 points) Let X_n be a random variable that takes values in $\{0,1\}^n$ for every integer $n \geq 1$. 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 $\{G(X_n)\} \equiv_{\text{c.i.}} \{G(U_n)\}$)