EE 720: Introduction to Number Theory and Cryptography (Autumn 2023)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Assignment 2: 20 points — Date: August 18, 2023

1. [5 points] For a negligible function negl, prove that $p(n)\mathsf{negl}(n)$ is also negligible for any positive polynomial p.

2. [5 points] Let $G : \{0,1\}^n \to \{0,1\}^{l(n)}$ be a pseudorandom generator with expansion factor $l(n) > n$. **Prove or disprove** that the following functions are pseudorandom generators where $s \in \{0,1\}^n$ and s_i is the ith bit of s. The $\|$ denotes the string concatenation operator.
   (a) $G_1(s) = G(s)\|0$.
   (b) $G_2(s) = G(s_1, s_2, \ldots, s_{|s|-1})\|s_{|s|}$.
   (c) $G_3(s) = G(s\|0)$.

3. [10 points] A private-key encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is **EAV-secure**, if for all PPT adversaries $\mathcal{A}$ there is a negligible function negl such that, for all n,

$$\Pr\left[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1\right] \leq \frac{1}{2} + \mathsf{negl}(n).$$

   Let $\mathsf{out}_{\mathcal{A}}\left(\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n,b)\right)$ denote the output b' of $\mathcal{A}$ when m_b is encrypted. Suppose that a private-key encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is EAV-secure.

   Prove that for all PPT adversaries $\mathcal{A}$ there is a negligible function negl such that, for all n,

$$\left|\Pr\left[\mathsf{out}_{\mathcal{A}}\left(\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n,0)\right) = 1\right] - \Pr\left[\mathsf{out}_{\mathcal{A}}\left(\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n,1)\right) = 1\right]\right| \leq \mathsf{negl}(n).$$