Contents

1. Computational Indistinguishability in the presense of eavesdropper 1
2. Pseudorandom Generator 1

1. Computational Indistinguishability in the presense of eavesdropper

1.1 Let $\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n, b)$ represents the experiment $\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n)$, where the fixed bit b is used rather than being selected uniformly.

Show that a private key encryption scheme $\Pi(n)$ has an indistinguishable encryption in the presence of an eavesdropper, if for all PPT adversaries $\mathcal{A}$, there is a negligible function $\varepsilon()$ such that, for all n,

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

2. Pseudorandom Generator

2.1 Define $G(s) = s \parallel \bigoplus_{i=0}^{n-1} s_i$, where n is the length of string s and s_i represent the i^{th} bit of s. Show that G is not a pseudo-random generator.

2.2 Define $G(s) = s \parallel s$, where $s \in \{0, 1\}^n$. Prove that G is not a pseudorandom generator.

2.3 Let $G(s) = s \parallel \mathrm{reverse}(s)$, where $\mathrm{reverse}(s)$ denotes the reverse of string s. Show that G is not a pseudorandom generator.