Review Questions

October 12, 2022

1. Let $f : \{0,1\}^n \to \{0,1\}^n$ be a one-way function. Let $g : \{0,1\}^{2n} \to \{0,1\}^n$ be s.t. for every $x_1||x_2 \in \{0,1\}^{2n}$, $|x_1| = |x_2|$, $g(x_1||x_2) = f(x_1)$. Then is g also a one-way function?

2. Let $f : \{0,1\}^n \to \{0,1\}^n$ be a one-way function. Define:

$$g(x_1||x_2) = \begin{cases} 0^{2n}, \ if \ x_2 = 0^n \\ f(x_1)||0^n, \ otherwise \end{cases}$$

   Is g also a one-way function?

3. Let f be a one-way function. Is $f(f)$ also a one-way function?

4. Let G_1 and G_2 be PRGs. Is $G(s_1||s_2) = G_1(s_1)||G_2(s_2)$ also a PRG? Prove or give a counterexample. What about $G(s_1||s_2||s_3) = G_1(s_1)||G_2(s_2)||G_3(s_3)$, where G_3 is also a PRG ?

5. Let $\{F_k\}_k$ be a family of PRFs. Is $\{F'_k\}_k$ also a family of PRFs, where $F'_k(x_1||x_2) = F_{k_1}(x_1)||F_{k_2}(x_2)$ and $k = k_1||k_2$. Prove or give a counterexample.

6. Let $\{F_k\}_k$ be a family of PRFs. Is $\{F'_k\}_k$ also a family of PRFs, where $F'_k(x) = F_{k_1}(x) \oplus k_2$ and $k = k_1||k_2$. Prove or give a counterexample.

7. Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a pseudorandom generator with n-bit stretch. Prove that G is a one-way function.