CS 171: Discussion Section 7 (March 4)

1 One-way Functions

Let $f : \{0,1\}^n \to \{0,1\}^n$ be a one-way function (OWF), and

$$\text{let } g(x) = f(x) \oplus x$$

Is $g(x)$ necessarily a one-way function? Prove your answer. Note: In your answer, you may use a secure OWF $h : \{0,1\}^{n/2} \to \{0,1\}^{n/2}$.

2 Composed Hash Functions

We will show how to compose mulitiple hash functions to increase their compression factor. Let (Gen_1, H_1) and (Gen_2, H_2) be two fixed-length collision-resistant hash functions (CRHFs), where:

- $H_1^{s_1}$ maps $\mathcal{X} \to \mathcal{Y}$, for any seed $s_1 \leftarrow \mathsf{Gen}_1(1^n)$,
- $H_2^{s_2}$ maps $\mathcal{Y} \to \mathcal{Z}$, for any seed $s_2 \leftarrow \mathsf{Gen}_2(1^n)$, and
- $|\mathcal{X}| > |\mathcal{Y}| > |\mathcal{Z}|$

Define a new hash function $(\mathsf{Gen}_{\mathsf{comp}}, H_{\mathsf{comp}})$ to be the composition of H_2 and H_1:

1. $\mathsf{Gen}_{\mathsf{comp}}(1^n)$: Sample $s_1 \leftarrow \mathsf{Gen}_1(1^n)$ and $s_2 \leftarrow \mathsf{Gen}_2(1^n)$, and output $s = (s_1, s_2)$.
2. $H^s_{\mathsf{comp}}(x)$: Let $x \in \mathcal{X}$. Output $H_2^{s_2}(H_1^{s_1}(x))$.

Prove that $(\mathsf{Gen}_{\mathsf{comp}}, H_{\mathsf{comp}})$ is a secure collision-resistant hash function.