CS 171: Problem Set 6

Due Date: March 14th, 2024 at 8:59pm via Gradescope

1 One-Way Functions

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

$$g(x) = f(f(x))$$

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

Tip: Your answer should have one of the following forms. Only one of them is possible:

- Prove that if f is a OWF, then g is also a OWF.
- (1) Construct a function f. (2) Prove that f is a one-way function. (3) Then prove that when g is constructed from this choice of f, g is not a one-way function.

Also, you may cite without proof any theorems proven in discussion or lecture.

2 Concatenated Hash Functions

Let $\mathcal{H}_1 = (\mathsf{Gen}_1, H_1)$ and $\mathcal{H}_2 = (\mathsf{Gen}_2, H_2)$ be two fixed-length hash functions that take inputs of length $3n$ bits and produce outputs of length n bits. Only one of $\mathcal{H}_1$ and $\mathcal{H}_2$ is collision resistant; the other one is not collision-resistant, and you don't know which is which.

Next, we define two new hash functions $\mathcal{H}_3 = (\mathsf{Gen}_3, H_3)$ and $\mathcal{H}_4 = (\mathsf{Gen}_4, H_4)$ below:

$\underline{\mathcal{H}_3}$:

1. $\mathsf{Gen}_3(1^n)$: Sample $s_1 \leftarrow \mathsf{Gen}_1(1^n)$ and $s_2 \leftarrow \mathsf{Gen}_2(1^n)$. Output $s = (s_1, s_2)$.
2. $H_3^s(x)$: Output $H_1^{s_1}(x)||H_2^{s_2}(x)$.

Note that $H_3^s : \{0,1\}^{3n} \to \{0,1\}^{2n}$.

$\underline{\mathcal{H}_4}$:

1. $\mathsf{Gen}_4(1^n)$: Sample $s_1 \leftarrow \mathsf{Gen}_1(1^n)$ and $s_2 \leftarrow \mathsf{Gen}_2(1^n)$. Output $s = (s_1, s_2)$.
2. $H_4^s(x)$: Let $x = (x_1, x_2) \in \{0,1\}^{3n} \times \{0,1\}^{3n}$. Output $H_1^{s_1}(x_1)||H_2^{s_2}(x_2)$.

Note that $H_4^s : \{0,1\}^{6n} \to \{0,1\}^{2n}$.

Question: For each of $\mathcal{H}_3$ and $\mathcal{H}_4$, determine whether the hash function is collision-resistant, and prove your answer.

3 Hard-Concentrate Predicates

Let $f : \{0,1\}^n \to \{0,1\}^n$ be an efficiently computable one-to-one function. Prove that if f has a hard-concentrate predicate[1], then f is one-way.

[1]Hard-concentrate predicates are defined in Katz & Lindell, 3rd edition, definition 8.4 under the name *hard-core predicate*.