Cryptography: Homework 7

(Deadline: 10am, 2021/11/26)

1. (20 points) Let (Gen, H) be a collision-resistant hash function. Is $(\mathsf{Gen}, \hat{H})$ defined by $\hat{H}^s(x) = H^s(H^s(x))$ necessarily collision resistant?

2. (30 points) Let $g^s : \{0,1\}^{2n} \to \{0,1\}^{n-1}$ be a collision-resistant hash function. For every integer i, we denote with $\langle i \rangle \in \{0,1\}^n$ the n-bit binary representation of i (e.g., $\langle 1 \rangle = 0^{n-1}1$).

   - Let $h^s : \{0,1\}^{2n} \to \{0,1\}^n$ be a function such that

   $$h^s(x) = \begin{cases} \langle 1 \rangle, & \text{if } x = \langle 2 \rangle \| 0^n; \\ 1 \| g^s(x), & \text{otherwise.} \end{cases}$$

   Show that h^s is collision-resistant.

   - Consider a modification to the Merkle-Damgård transform where instead of using a fixed IV, set $z_0 = L$ and then compute $z_i = h^s(z_{i-1} \| x_i)$ for $i = 1, \ldots, B$ and output z_B. Suppose that h^s is collision-resistant. Determine whether the H^s obtained with this modified transform is collision-resistant. Prove your answer.