Problem 1-1. Hash Function Properties

Let $h : \{0,1\}^{\leq 2n} \to \{0,1\}^n$ be a hash function that is collision resistant. Let $h' : \{0,1\}^{\leq n+1} \to \{0,1\}^{n+1}$ be the hash function given by the rule

$$h'(x) = \begin{cases} 0||x & \text{if } x \in \{0,1\}^n \\ 1||h(x) & \text{otherwise} \end{cases}$$

(a) Prove that h' is not one-way.

Definition 1 *A function $f : X_n \to Y_n$ is said to be one-way if for every efficient adversary $\mathcal{A}$, the probability that $\mathcal{A}$, on input n and $y = f(x)$ for a random $x \in X_n$, outputs any x' such that $f(x') = y$, is negligible.*

(b) Prove that h' is collision resistant.

Definition 2 *A function $f : X_n \to Y_n$ is said to be collision resistant (CR) if for every efficient adversary $\mathcal{A}$, the probability that $\mathcal{A}$ on input n, outputs any distinct $x, x' \in X_n$ such that $f(x) = f(x')$, is negligible.*

(c) Prove that h' is target collision resistant if h is target collision resistant. For this problem part, assume that h has the form $h\colon \{0,1\}^{\leq n+1} \to \{0,1\}^n$.

Definition 3 *A function $f : X_n \to Y_n$ is said to be target collision resistant (TCR) if for every efficient adversary $\mathcal{A}$, the probability that $\mathcal{A}$ on input n and a random $x \in X_n$, outputs $x' \in X_n$ such that $x' \neq x$ and $f(x) = f(x')$, is negligible.*

Problem 1-2. Message Authentication

(a) Let MAC be a secure message authentication code. Suppose Alice and Bob send authenticated messages to each other. Namely, every time one of them sends a message M they send it together with $\mathsf{MAC}(K, M)$ where K is their shared secret key. On day 1, Alice asks Bob if he wants to go to the movies, and Bob replies "yes". On day 2, Alice asks Bob if he wants to go to ice cream and Bob replies "no". On day 3, Alice asks Bob if he wants to rob a bank and Bob replies "no". Can an adversary Eve observing the communication on the first two days, corrupt Bob's message on the third day (in an authenticated way)? If so, how would you use a secure MAC so that the adversary cannot corrupt Bob's message?

(b) Recall that the CMAC construction we saw in class is a sequential construction. Namely, to MAC a very long message that consists of L blocks (each of 128 bits), we need to do L sequential steps. Consider the following parallel construction: Let $F : K \times X \to \{0,1\}^k$ be a pseudorandom function (PRF). Let

$$\mathsf{MAC}(K, (M_1, \ldots, M_L)) = \oplus_{i=1}^{L} F(K, M_i),$$

where each $M_i \in X$. Is this a secure MAC (i.e., existentially unforgeable against adaptive chosen message attacks)?

Problem 1-3. Message Signing

Let $(\mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$ be a signature scheme with message space $\{0,1\}^k$ (where k is the security parameter), and let H be a seeded hash function with domain $\{0,1\}^*$ and range $\{0,1\}^k$. Consider the new signature scheme $(\mathsf{Gen}', \mathsf{Sig}', \mathsf{Ver}')$, with message space $\{0,1\}^*$, defined via the following "hash-then-sign" paradigm:

- Gen' runs Gen to generate a pair (sk, vk) and samples a seed s for H. It outputs $sk' = (sk, s)$ and $vk' = (vk, s)$.
- Sig' takes as input a secret key $sk' = (sk, s)$ and a message M, and outputs a $\mathsf{Sig}(sk, H_s(M))$, i.e., it signs the hashed message $H_s(M)$.
- Ver', given the verification key $vk' = (vk, s)$, a message M, and a signature σ, outputs 1 if and only if $\mathsf{Ver}(vk, H_s(M), \sigma) = 1$.

(a) Suppose that $(\mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$ is secure (existentially against adaptive chosen message attack) then which of the following properties of H do we need to ensure that $(\mathsf{Gen}', \mathsf{Sig}', \mathsf{Ver}')$ is also secure?

1. One-wayness.
2. Target collision resistance
3. Collision resistance.

Problem 1-4. Pseudo-Random Functions

Let F be a pseudorandom function (PRF) that takes messages in $\{0,1\}^n$ to messages in $\{0,1\}^n$.

(a) We wish to use F to construct a PRF that takes messages in $\{0,1\}^{2n}$ to messages in $\{0,1\}^{2n}$. Suppose the key to F is also in $\{0,1\}^n$.

Below are four proposals of such a PRF, where $x_0, x_1, K, K_0, K_1 \in \{0,1\}^n$ and where we use $||$ to denote concatenation. Notice that the constructions 1, 3, and 4 use a key in $\{0,1\}^n$ whereas the second construction uses a key in $\{0,1\}^{2n}$.

1. $G_1(K, x_0||x_1) = F(K, x_0)||F(K, x_1)$.
2. $G_2(K_0||K_1, x_0||x_1) = F(K_0, x_0)||F(K_1, x_1)$.
3. $G_3(K, x_0||x_1) = F(K', 0^n)||F(K', 1^n)$, where $K' = F(F(K, x_0), x_1)$
4. $G_4(K, x_0||x_1) = F(F(K, x_0), x_1)||F(F(K, x_0), x_1 \oplus 1^n)$.

Only one of the above four proposals is a secure PRF. Which one is the secure one? For each of the three others, show an attack that distinguishes it from a truly random function (recall the definition of a PRF given in the lecture).