Tutorial 5: Hash Functions and MACs

Submission Guidelines All problems must be solved in class today. Searching on the internet for solutions is strictly discouraged.

1. Let F be a PRF. Show that the following constructions of MAC are insecure. Let $\mathcal{K} = \{0,1\}^n$ and $m = m_1 \| \cdots \| m_\ell$ with $m_i \in \{0,1\}^n$ for $i \in [1, \ell]$.
   (a) Send $t = F_k(m_1) \oplus \cdots \oplus F_k(m_\ell)$.
   A: If t is the tag for $m_1 \| m_2 \| \cdots \| m_\ell$, t would be a valid forgery for $m_2 \| m_1 \| m_3 \| \cdots \| m_\ell$ since changing the order of message blocks does not change the value of the tag given by $F_k(m_1) \oplus \cdots \oplus F_k(m_\ell)$.
   (b) Pick $r \xleftarrow{\text{U}} \{0,1\}^n$, compute $t = F_k(r) \oplus F_k(m_1) \oplus \cdots \oplus F_k(m_\ell)$ and send (r, t).
   A: Same attack (as in the previous part) works here. (r, t) remains a valid tag for any permutation of $m_1, m_2, \ldots, m_\ell$.

2. If a message m is authenticated by sending $t = F_k(m)$ along with m, the security is implied if F is a PRF. Does security hold when F is a weak PRF?

   A: Security may not hold when F is a weak PRF. The proof does not go through, since an adversary would have no control over the points on which F_k is evaluated. In the CMA game, Mac queries are allowed and the adversary must be able to query on messages of its choice.

   Intuitively, if m, m' are two 'related' messages, then $F_k(m), F_k(m')$ are not guaranteed to be pseudorandom. Only when $m.m'$ are independent and uniformly distributed is the distribution of $F_k(m), F_k(m')$ computationally indistinguishable from random.

3. Let $\mathsf{H}_1, \mathsf{H}_2 : \{0,1\}^m \to \{0,1\}^n$ be two hash functions. Define a hash function $\mathsf{H} : \{0,1\}^m \to \{0,1\}^{2n}$ as $\mathsf{H}(x) = \mathsf{H}_1(x) \| \mathsf{H}_2(x)$. Prove that if at least one of $\mathsf{H}_1, \mathsf{H}_2$ is collision resistant, then H is collision resistant.

   A: If x, x' is a collision for H, then $\mathsf{H}(x) = \mathsf{H}(x')$ i.e., $\mathsf{H}_1(x) \| \mathsf{H}_2(x) = \mathsf{H}_1(x') \| \mathsf{H}_2(x')$ i.e., $\mathsf{H}_1(x) = \mathsf{H}_1(x')$ and $\mathsf{H}_2(x) = \mathsf{H}_2(x')$. That means x, x' is a collision for both H_1 and H_2. So, if atleast of $\mathsf{H}_1, \mathsf{H}_2$ is collision resistant, then so is H.

4. Show that for a hash function, collision resistance implies second pre-image resistance and second pre-image resistance implies pre-image resistance.

   A: Let $\mathsf{H} : X \to Y$ be a hash function. Denote by $\mathsf{CR}, \mathsf{SPR}, \mathsf{PR}$ collision resistance, second pre-image resistance and pre-image resistance (and the corresponding games) respectively.

   We first show (ε, t)-CR implies (ε', t')-SPR. Suppose $\mathscr{A}'$ is an adversary that finds second-preimages. Then we can build a collision finding adversary $\mathscr{A}$. $\mathscr{A}$ gets the description of H. It then picks $x \xleftarrow{\text{U}} X$ and provides H, x to $\mathscr{A}'$. $\mathscr{A}'$ returns $x \in X$. Now, $\mathscr{A}$ returns x, x' to its challenger. If $x \neq x'$ and $\mathsf{H}(x) = \mathsf{H}(x')$, then $\mathscr{A}'$ wins and so does $\mathscr{A}$. So the probability of $\mathscr{A}$ winning is equal to that of $\mathscr{A}'$ winning. Consequently, $\varepsilon = \varepsilon'$ and clearly, $t = t'$.

   Now we show that (ε, t)-SPR implies (ε', t')-PR with $\varepsilon' \leq 2\varepsilon + \frac{|Y|}{|X|}$ and $t = t' + O(1)$. Suppose that $\mathscr{A}'$ is a PR-adversary. We build an SPR-adversray $\mathscr{A}$ that does the following: receives H and $x \in X$ chosen uniformly at random from its challenger. It sends $\mathsf{H}, \mathsf{H}(x)$ to $\mathscr{A}'$ which in turn outputs $x' \in X$ and halts. $\mathscr{A}$ just sends the same x' to its challenger. It remains to analyse the probability of $\mathscr{A}$ winning.

Let $Y_1 \subseteq Y$ contain points $y \in Y$ having exactly one pre-image under H. That is,

$$Y_1 = \{y \in Y : |\mathsf{H}^{-1}(y)| = 1\}.$$

Note that Y_1 is fixed given H. Clearly $|Y_1| \le |Y|$. For a subset $Z \subset Y$, define $|h^{-1}(Z) = \{x \in X : h(x) = Z\}|$. Since $|Y_1| \le |Y|$, we have

$$\Pr[x \in \mathsf{H}^{-1}(Y_1) : x \xleftarrow{\mathrm{U}} X] \le \frac{|Y|}{|X|}.$$

We now have

$$\begin{aligned}
\Pr[\mathscr{A} \text{ wins}] &= \Pr\left[(x \ne x') \wedge (\mathsf{H}(x) = \mathsf{H}(x'))\right] \\
&= \Pr\left[(x \ne x') \wedge (\mathsf{H}(x) = \mathsf{H}(x')) \wedge (x \notin \mathsf{H}^{-1}(Y_1))\right] + \Pr\left[(x \ne x') \wedge (\mathsf{H}(x) = \mathsf{H}(x')) \wedge (x \in \mathsf{H}^{-1}(Y_1))\right] \\
&= \Pr\left[(x \ne x') \wedge (\mathsf{H}(x) = \mathsf{H}(x')) \wedge (x \notin \mathsf{H}^{-1}(Y_1))\right] \qquad \left(\text{since } x = x' \text{ if } x \in \mathsf{H}^{-1}(Y_1)\right) \\
&= \Pr\left[(x \ne x') | (\mathsf{H}(x) = \mathsf{H}(x')) \wedge (x \notin \mathsf{H}^{-1}(Y_1))\right] \cdot \Pr\left[(\mathsf{H}(x) = \mathsf{H}(x')) \wedge (x \notin \mathsf{H}^{-1}(Y_1))\right] \\
&= \left(1 - \frac{1}{|\mathsf{H}^{-1}(\mathsf{H}(x))|}\right) \cdot \Pr\left[(\mathsf{H}(x) = \mathsf{H}(x')) \wedge (x \notin \mathsf{H}^{-1}(Y_1))\right] \\
&\ge \frac{1}{2} \Pr\left[(\mathsf{H}(x) = \mathsf{H}(x')) \wedge (x \notin \mathsf{H}^{-1}(Y_1))\right] \qquad \left(\text{since } |\mathsf{H}^{-1}(\mathsf{H}(x))| \ge 2 \text{ when } x \notin \mathsf{H}^{-1}(Y_1)\right) \\
&\ge \frac{1}{2} \left(\Pr\left[(\mathsf{H}(x) = \mathsf{H}(x'))\right] - \Pr\left[(x \in \mathsf{H}^{-1}(Y_1))\right]\right) \\
&\ge \frac{1}{2} \left(\Pr[\mathscr{A}' \text{ wins}] - \frac{|Y|}{|X|}\right).
\end{aligned}$$