Isaac Kim
CS 487
Professor Baldimtsi
Mar 31, 2023

Homework 4

1. $MAC'(k,m) = MAC(k,m)||MAC(k,m)$.

Verification works as follows: Let $t = MAC(k,m)$ and $t' = MAC'(k,m)$. Then $Vrfy'(m,t') = 1$ if and only if $t' = t||t$ and $Vrfy(m,t) = 1$

Contrapositive: If MAC' is *not* secure, then MAC is *not* secure. This means that there exists an adversary A' such that the probability that A' can successfully forge a message with a valid tag is $p(n)$, where $p(n)$ is some non-negligible value.

Reduction: Using A', we can construct an adversary A that breaks MAC.
Step 1. A generates a tag t and makes t' such that $t' = t||t$ and $|t'| = 2t$
Step 2. A runs A' and gives $t' = t||t$ to A'
Step 3. A' can then successfully forge a valid message m for t' with probability $p(n)$ such that $Vrfy'(m,t') = 1$
Step 4. In doing so, A' forges $t' = MAC'(k,m) = MAC(k,m)||MAC(k,m) = t||t$
Step 5. A can then output (m,t). The probability that $Vrfy(m,t) = 1$ is equal to $p(n)$

Hence, A is a good adversary for MAC.

2.1) Let $m_0 = x_0 \oplus w_0$, $m_1 = x_1 \oplus w_1$, $m_0 = 000, m_1 = 0000$. Then, it must follow that $x_0 = w_0$ and $x_1 = w_1$. Note that $m_0 \neq m_1$. Then, $H(m_0) = H(x_0) \oplus H(w_0) = 0^n = H(x_1) \oplus H(w_1) = H(m_1)$. Then, $H(m_0) = H(m_1)$, but $m_0 \neq m_1$. Hence, H is not collision resistant.

2.2) Let $x_\alpha = x_1||x_2$, and $x_\beta = x_2||x_1$, $x_1 \neq x_2$. Note that $x_\alpha \neq x_\beta$. Then, $H_s^a(x_\alpha) = H_s(x_1) \oplus H_s(x_2) = H_s(x_2) \oplus H_s(x_1) = H_s^a(x_\beta)$. Then, $H_s^a(x_\alpha) = H_s^a(x_\beta)$ but $x_\alpha \neq x_\beta$. Hence, H_s^a is not collision resistant.

3) $H_s^b(x) = H_s^1(x)||H_s^2(x)||H_s^3(x)$.

Consider the case where only H_s^1 is collision resistant. Then, $H_s^b(x)$ is also collision resistant. To show this, we will show equivalently by contrapositive that if H_s^b is *not* collision resistant, then $H_s^1(x)$ is *not* collision resistant.

This implies that there exists an adversary A_b for H_s^b such that the probability that A_b can output $x, x', x \neq x'$ with $H_s^b(x) = H_s^b(x')$ is $p(n)$, where $p(n)$ is a non-negligible value.

Let A_1 be an adversary for H_s^1. A_1 runs A_b, and A_b outputs $x, x', x \neq x'$. Since A_b is a good adversary for H_s^b, with probability $p(n)$, it holds that $H_s^b(x) = H_s^1(x)||H_s^2(x)||H_s^3(x) = H_s^1(x')||H_s^2(x')||H_s^3(x') = H_s^b(x')$. This implies that $H_s^1(x) = H_s^1(x')$. Then, A_1 can output $x, x', x \neq x'$ since $H_s^1(x) = H_s^1(x')$. The probability of success for A_1 is the same as the probability of success for A_b, namely $p(n)$. Hence, A_1 is a good adversary for H_s^1. The proof for cases where H_s^2 or H_s^3 are the only collision resistant functions is similar.

4)
a) If H_s is collision resistant, then H_s' is collision resistant. Contrapositive: If H_s' is *not* collision resistant, then H_s is *not* collision resistant.

Let A' be an adversary for H_s' that can find a collision for $y = H_s'(x_1, x_2, ..., x_{2^h})$. Let a, b be the children of the root node y and a', b' be the children of the root node y', $a \neq a', b \neq b'$.

Let A' find a collision x, x' such that $x = x_1, x_2, ..., x_{2^h}, x' = x_1', x_2', ..., x_{2^h}', x \neq x'$. Note that $y = H_s'(x_1, x_2, ..., x_{2^h}) = H_s(a||b)$ and $y' = H_s'(x_1', x_2', ..., x_{2^h}') = H_s(a'||b')$. Since this is a collision,

$$y = H_s'(x) = H_s'(x_1, x_2, ..., x_{2^h}) = H_s'(x_1', x_2', ..., x_{2^h}') = H_s'(x') = y' \rightarrow H_s(a||b) = H_s(a'||b').$$

Hence, A' has also found a collision for H_s.

b) Consider $y_1 = H_s'(x_1, x_2) = H(x_1||x_2), y_2 = H_s'(x_1, x_2, x_1, x_2) = H(H(x_1||x_2)||H(x_1||x_2)), y_3 = H_s'(y_1, y_1)$. Then, for $y_1, h_1 = 1$, for $y_2, h_2 = 2$ and for $y_3, h_3 = 1$. Then, $y_2 = H_s'(x_1, x_2, x_1, x_2) = H(H(x_1||x_2)||H(x_1||x_2)) = H_s'(y_1, y_1) = y_3$, but $h_2 = 2 \neq 1 = h_3$. Hence, if h is not fixed, this construction is not secure.