CSC 591, Homework 3

Fatema Olia - 200253671
folia@ncsu.edu
November 19, 2018

1.

1. This MAC is not secure. We can show an adversary A_{forge} that wins the MAC game as follows:

   Adversary A_{forge}:
   1. Training Phase:
      - query with message $m_1 = m_a||m_b$ and obtain $t_1 = F_k(0||m_a)||F_k(1||m_b)$
      - query with message $m_2 = m_b||m_c$ and obtain $t_2 = F_k(0||m_b)||F_k(1||m_c)$
   2. Challenge Phase:
      - parse t_1 as $t_{1L}||t_{1R}$ and t_2 as $t_{2L}||t_{2R}$
      - query with message $m* = m_b||m_b$ and $t* = t_{2L}||t_{1R}$

   Analysis:
   In the challenge phase the adversary A_{forge} submits $m* = m_b||m_b$ and $t* = t_{2L}||t_{1R}$.
   Since $t_{2L} = F_k(0||m_b)$ and $t_{1R} = F_K(1||m_b)$, $\therefore t* = F_k(0||m_b)||F_k(1||m_b)$
   Thus, the MAC verifies and $Pr[A_{forge} wins] = 1$.

2. This MAC is not secure. We can show an adversary A_{forge} that wins the MAC game as follows:

   Adversary A_{forge}:
   1. Challenge Phase:
      - choose message $m*$
      - choose $r = \langle 1 \rangle||m*$
      - set $t* = 0^n$
      - output $m*$ and $(r, t*)$

Analysis:

In the challenge phase the adversary A_{forge} chooses $r = \langle 1 \rangle || m^*$. (Since $\langle 1 \rangle$ is $n/2$-bit and m^* is $n/2$-bit then the value chosen is from $\{0,1\}^n$)

Then the adversary sets $t^* = 0^n$, this is because for m^* we have

$t^* = F_k(r) \oplus F_k(\langle 1 \rangle || m^*)$

$\therefore t^* = F_k(\langle 1 \rangle || m^*) \oplus F_k(\langle 1 \rangle || m^*)$

Thus, the MAC verifies and $Pr[A_{forge} wins] = 1$.

2.

3. This construction is not collision resistant. We can show a hash function h_s for which there exists a collision.

   Consider a collision resistant hash function h'_s. We can show the construction of h_s as follows:

   $$h_s(x) = \begin{cases} 1 & \text{if } x = 2||x_1 \\ 1||h'_s(x) & \text{otherwise} \end{cases}$$

   Where x_1 is a fixed value.

   Since h'_s is a collision resistant hash function and only $x = 2||x_1$ maps to 1^n then even h_s is collision resistant. Thus it can be used for this modification of the Merkle-Damgard transform. The adversary A_{coll} can defeat the function as follows:

   Adversary A_{coll}:

   - Output the two values as $m_1 = x_1||x_2$ and $m_2 = x_2$

   Analysis:

   - Hash of $m_1 = h_s(h_s(2||x_1)||x_2) = h_s(1||x_2)$
   - Hash of $m_2 = h_s(1||x_2)$

   Thus, there is a collision for m_1 and m_2. $\therefore$ $Pr[A_{coll}$ finds collision$] = 1$

4. If h_s is a collision resistant hash function then this modified Merkle-Damgard construction is also collision resistant.

   Proof:

   Assumption:

   1. Towards a contradiction, assume $\exists$ a PPT adversary A_{coll} that can find a collision in the modified Merkle-Damgard construction such that:

      $Pr[A_{coll}$ finds collision$] = p(n)$ which is non-negligible.

2. There is a PPT adversary A_h that finds a collision in function h_s with negligible probability

Reduction:

Consider the modified Merkle-Damgard construction as H_s.

The adversary A_h runs adversary A_{coll} to find a collision in h_s as follows:

- A_{coll} outputs two messages (m, m') where $m \neq m'$
- Using $B = l(m)$ and $B' = l(m')$, A_h checks:

 if $B \neq B'$:

 A_h outputs $(z_b||B, z'_b||B')$

 if $B = B'$:

 Let $I_i = z_i||m_i$ denoted the ith input to h_s. Similarly $I'_i = z'_i||m'_i$. Let N be the largest index for which $I_N \neq I'_N$.

 A_h outputs (I_N, I'_N)

Analysis:

Case $B \neq B'$:

This means that if $H_s(m) = H_s(m')$ then the last step of the construction collided, i.e. $h_s(z_b||B) = h_s(z'_b||B')$. Since $B \neq B'$ then the inputs to h_s are different and thus if A_h outputs $(z_b||B, z'_b||B')$ then $Pr[A_h$ finds collision$] = Pr[A_{coll}$ finds collision$]$

Case $B = B'$:

Since $B = B'$ but $m \neq m'$ there is an i where $m_i \neq m'_i$. Thus, N exists. By maximality of N we have $I_{N+1} = I'_{N+1}$ and $z_N = z'_N$. This means (I_N, I'_N) are in collision in h_s. Thus, $Pr[A_h$ finds collision$] = Pr[A_{coll}$ finds collision$]$

Since $Pr[A_{coll}$ finds collision$] = p(n)$, thus $Pr[A_h$ finds collision$] = p(n)$. But we know that h_s is collision resistant. Thus $p(n)$ has to be negligible. Thus our original assumption was wrong and the modified Merkle-Damgard construction is collision resistant.

3.

5. The scheme is not a one-time-secure signature scheme. An adversary A_{forge} can win the digital signature game as follows:

Adversary A_{forge}:

1. Training Phase:

   - query the oracle with $m_1 = i$ (where $1 < i < n$) and receive $\sigma_1 = f^{(n-i)}(x)$

2. Challenge Phase:

   - choose $m^* = i - 1$ and $\sigma^* = f^{(1)}(\sigma_1)$

Analysis:

We know the value of the public key is $y = f^{(n)}(x)$.

According to the digital signature scheme, the values (m^*, σ^*) sent in the challenge phase can be verified as follows:

$$\begin{aligned} f^{(m^*)}(\sigma^*) &= f^{(i-1)}(f^{(1)}(\sigma_1)) \\ &= f^{(i)}(f^{(n-i)}(x)) \\ &= f^{(n)}(x) \\ &= y \end{aligned}$$

Thus, $Pr[A_{forge}$ wins digital signature game$] = 1$

6. If f is a one way permutation then no PPT adversary given a signature on i can output a forgery on any message $j > i$, except with negligible probability.

Proof:

Assumption:

1. Towards a contradiction, assume $\exists$ a PPT adversary A_{forge} that outputs a forgery for $j > i$ with the following probability:

   $Pr[A_{forge}$ wins digital signature game$] = p(n)$ which is non-negligible.

2. There is a PPT adversary A_{owf} that reverses one way function f with negligible probability.

Reduction:

The adversary A_{owf} has access to an oracle that gives public key $y = f^{(n)}(x)$ and the signature. A_{owf} runs A_{forge} to try and break f as follows:

- A_{forge} queries with $i \in \{1...n\}$. A_{owf} accepts i and forwards it to the oracle which returns the digital signature $\sigma_i = f^{(n-i)}(x)$ where x is chosen by the oracle.

- A_{owf} returns σ_i to A_{forge}
- A_{forge} challenges with a pair (m^*, σ^*) where $m^* = i + c$ and $\sigma * = f^{(n-i-c)}(x)$ and $0 < c \leq n - i$.
- A_{owf} verifies the signature. If verified, A_{owf} can run the function f for input σ^* for $c - 1$ iterations.

  $f^{(c-1)}(\sigma^*) = f^{(n-i-c-c+1)}(x)$

  $\therefore f^{(c-1)}(\sigma^*) = f^{(n-i+1)}(x)$

  Thus A_{owf} has inverted the function on the left hand side. Similarly A_{owf} can find the inverse of all values between $i - c$ and i.

Analysis:

Since A_{owf} can use the output of A_{forge} to reverse the one way function:

$Pr[A_{owf}$ reverses $f] = Pr[A_{forge}$wins digital signature game$] = p(n)$

However, since f is a one way function. $Pr[A_{owf}$ reverses $f] = negl(n)$. Thus our original assumption was incorrect.

Thus $Pr[A_{forge}$wins digital signature game$] = negl(n)$.