CS 276: Homework 4

Due Date: Friday September 27th, 2024 at 8:59pm via Gradescope

1 Carter-Wegman Message Authentication Code

The Carter-Wegman MAC is built from a PRF and a hash function as follows. Let p be a large prime. Let n be the security parameter. Let $F : \mathcal{K}_F \times \{0,1\}^n \to \mathbb{Z}_p$ be a secure PRF, and let $H : \mathcal{K}_H \times \mathcal{M} \to \mathbb{Z}_p$ be a hash function. Next:

1. MAC takes a key $(k_H, k_F) \in \mathcal{K}_H \times \mathcal{K}_F$ and a message $m \in \mathcal{M}$. Then MAC samples $r \xleftarrow{\$} \{0,1\}^n$ and computes:

$$v = H(k_H, m) + F(k_F, r)$$

   Finally MAC outputs (r, v).

2. Verify takes a key $(k_H, k_F) \in \mathcal{K}_H \times \mathcal{K}_F$, a message $m \in \mathcal{M}$, and a tag $(r, v) \in \{0,1\}^n \times \mathbb{Z}_p$. Then Verify checks that $v = H(k_H, m) + F(k_F, r)$. If so, Verify outputs 1 (accept). If not, Verify outputs 0 (reject).

Now we will consider two possible choices for H:

1. H_1 takes a key $k_H \xleftarrow{\$} \mathbb{Z}_p$ and an input $m = (m_1, \ldots, m_\ell) \in \mathbb{Z}_p^\ell$, where ℓ is polynomial in n. Then

$$H_1(k_H, m) = k_H^\ell + \sum_{i=1}^{\ell} k_H^{\ell-i} \cdot m_i$$

2. $H_2(k_H, m) = k_H \cdot H_1(k_H, m)$

Question: Prove that the Carter-Wegman MAC is insecure if it is constructed with $H = H_1$, but it is secure if it is constructed with $H = H_2$.

The following definition of MAC security will be useful.

Definition 1.1 (MAC Security [KL14]) *A MAC is secure if for any non-uniform PPT adversary $\mathcal{A}$,*

$$\Pr[\mathsf{MAC\text{-}Forge}_{\mathcal{A}}(n) \to 1] \leq \mathsf{negl}(n)$$

<u>$\mathsf{MAC\text{-}Forge}_{\mathcal{A}}(n)$</u>:

1. ***Setup:*** *The challenger samples k uniformly from the key space. $\mathcal{A}$ is given 1^n.*

2. ***Query:*** *The adversary submits a message $m^{(i)}$; then the challenger computes a tag $t^{(i)} \leftarrow \mathsf{MAC}(k, m^{(i)})$ and sends it to the adversary. The adversary may submit any polynomial number of message queries.*

   Let $\mathcal{Q} = \{(m^{(1)}, t^{(1)}), \ldots, (m^{(q)}, t^{(q)})\}$ be the set of messages $m^{(i)}$ submitted in the query phase along with the tags $t^{(i)}$ computed by MAC.

3. ***Forgery:*** *The adversary outputs a message-tag pair (m^*, t^*). The output of the game is 1 if $(m^*, t^*) \notin \mathcal{Q}$ and $\mathsf{Verify}(k, m^*, t^*) = 1$. The output is 0 otherwise.*

Solution

Theorem 1.2 *The Carter-Wegman MAC construction is insecure if $H = H_1$.*

Proof. Here is an adversary $\mathcal{A}$ that breaks the security of the scheme:

1. The adversary submits a query $m^{(1)} = (0, \ldots, 0, 1) \in \mathbb{Z}_p^\ell$ and receives the tag $t^{(1)} = (r, v)$, where $r \xleftarrow{\$} \{0,1\}^n$ and $v = k_H^\ell + 1 + F(k_R, r)$.
2. The adversary outputs $m^* = (0, \ldots, 0, 2)$ and $t^* = (r, v + 1)$.

Note that $(m^*, t^*) \notin \mathcal{Q}$ because $m^* \neq m$. Furthermore, (m^*, t^*) will pass verification. $\mathsf{Verify}(k, m^*, t^*)$ outputs 1 if

$$H_1(k_H, m^*) + F(k_F, r) = v + 1$$

This does occur because

$$\begin{aligned} H_1(k_H, m^*) + F(k_F, r) &= k_H^\ell + 2 + F(k_R, r) \\ &= v + 1 \end{aligned}$$

This adversary wins the MAC security game with probability 1, so the MAC construction is insecure.

Theorem 1.3 *The Carter-Wegman MAC construction is secure if $H = H_2$.*

Proof. Consider the following hybrids:

- $\mathcal{H}_0$ is the $\mathsf{MAC\text{-}Forge}_{\mathcal{A}}(n)$ security game:
  1. The challenger samples $k_H \xleftarrow{\$} \mathbb{Z}_p$ and $k_F \xleftarrow{\$} \mathcal{K}_F$. $\mathcal{A}$ is given 1^n.
  2. $\mathcal{A}$ gets query access to $\mathsf{MAC}((k_H, k_F), \cdot)$. Upon receiving query m, the challenger samples $r \xleftarrow{\$} \{0,1\}^n$, computes
     $$v = H(k_H, m) + F(k_F, r)$$
     and returns $t = (r, v)$. Then the challenger appends $(m, (r, v))$ to $\mathcal{Q}$.
  3. $\mathcal{A}$ outputs $(m^*, (r^*, v^*))$. If $(m^*, (r^*, v^*)) \notin \mathcal{Q}$, and $v^* = H(k_H, m^*) + F(k_F, r^*)$, then the output of the hybrid is 1. Otherwise the output is 0.
- $\mathcal{H}_1$ is the same as $\mathcal{H}_0$, except $F(k_F, r)$ is replaced with a truly random function R that maps $\{0,1\}^n \to \mathbb{Z}_p$.
  1. The challenger samples $k_H \xleftarrow{\$} \mathbb{Z}_p$ and the truly random function $R : \{0,1\}^n \to \mathbb{Z}_p$. $\mathcal{A}$ is given 1^n.
  2. $\mathcal{A}$ may submit queries to MAC. Upon receiving query m, the challenger samples $r \xleftarrow{\$} \{0,1\}^n$, computes
     $$v = H(k_H, m) + R(r)$$
     and returns $t = (r, v)$. Then the challenger appends $(m, (r, v))$ to $\mathcal{Q}$.

3. $\mathcal{A}$ outputs $(m^*, (r^*, v^*))$. If $(m^*, (r^*, v^*)) \notin \mathcal{Q}$, and $v^* = H(k_H, m^*) + R(r^*)$, then the output of the hybrid is 1. Otherwise the output is 0.

Claim 1.4 $\left|\Pr[\mathcal{H}_0 \to 1] - \Pr[\mathcal{H}_1 \to 1]\right| = \mathsf{negl}(n)$

Proof. This follows from the PRG security of F.

Claim 1.5 $\Pr[\mathcal{H}_1 \to 1] = \mathsf{negl}(n)$

Proof.

1. In $\mathcal{H}_1$, with overwhelming probability, the challenger never samples the same r-value twice. If every query i uses a unique $r^{(i)}$, then $R(r^{(i)})$ will be a fresh random value. Additionally $(v^{(1)}, \ldots, v^{(q)})$ will be independent of each other, k_H, and the messages $(m^{(1)}, \ldots, m^{(q)})$. In particular, k_H will be uniformly random in the adversary's view and independent of the adversary's final output $(m^*, (r^*, v^*))$.

2. If r^* does not match any $r^{(i)}$-value that was previously sampled by the challenger, then $R(r^*)$ will be uniformly random and independent of the adversary's view. So

$$\begin{aligned}\Pr_R[v^* = H(k_H, m^*) + R(r^*)] &= \Pr_R[R(r^*) = v^* - H(k_H, m^*)] \\ &= \frac{1}{p} = \mathsf{negl}(n)\end{aligned}$$

3. Let us consider the case where $r^* = r^{(i)}$ for some query $i \in [q]$, but $m^* \neq m^{(i)}$. Next $v^* = H(k_H, m^*) + R(r^*)$ only if:

$$\begin{aligned}v^* &= H(k_H, m^*) + R(r^{(i)}) \\ 0 &= H(k_H, m^*) - H(k_H, m^{(i)}) + H(k_H, m^{(i)}) + R(r^{(i)}) - v^* \\ &= \sum_{j=1}^{\ell} k_H^{\ell+1-j} \cdot (m_j^* - m_j^{(i)}) + v^{(i)} - v^* \\ &= \sum_{j'=1}^{\ell} k_H^{j'} \cdot (m_{\ell+1-j'}^* - m_{\ell+1-j'}^{(i)}) + v^{(i)} - v^*\end{aligned}$$

Let

$$f(X) = \sum_{j'=1}^{\ell} X^{j'} \cdot (m_{\ell+1-j'}^* - m_{\ell+1-j'}^{(i)}) + v^{(i)} - v^*$$

The degree of $f(X)$ is ≥ 1 because for some index j', $m_{\ell+1-j'}^* \neq m_{\ell+1-j'}^{(i)}$. Then $v^* = H(k_H, m^*) + R(r^*)$ only if:

$$0 = f(k_H)$$

However, k_H is uniformly random given the description of f, so $\Pr_{k_H}[f(k_H) = 0] \leq \frac{\ell}{p} = \mathsf{negl}(n)$. This shows that the $\Pr[\mathcal{H}_1 \to 1] = \mathsf{negl}(n)$.

Corollary 1.6 $\Pr[\mathsf{MAC\text{-}Forge}_{\mathcal{A}}(n) \to 1] = \mathsf{negl}(n)$

Therefore, the MAC scheme is secure.

■

References

[KL14] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography, Second Edition*. Chapman & Hall/CRC, 2nd edition, 2014.