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

$\underline{\mathsf{MAC\text{-}Forge}_{\mathcal{A}}(n)}$:

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.*

References

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