2022201041

Use the PRF to build a secure MAC.

A MAC is Message Authentication Codes. The components of the authentication

protocol involves :

1. A key generation algorithm that returns a secret key ‘k’

2. A MAC generating algorithm that returns a tag for a given message ‘m’ where the

tag ‘t’ = MAC k(m)

3. A verification algorithm that returns a bit b = Verify k(m1, t1), given a message m1

and a tag t1.

4. If the message is not modified then with high probability, the value of b is true

otherwise false.

A MAC(Gen, MAC, Verify) is secure if for all probabilistic polynomial-time adversaries A:

Pr[MAC-Game(n) = 1] <= negl(n)

If F is a PRF, then the below mentioned scheme gives a secure fixed length MAC :

1. Gen(1n) chooses k to be a random n-bit string

2. MACk(m) = Fk(m) = t (the tag)

3. Verifyk(m, t) = Accept, iff t = F k(m)

CONSTRUCTION 4.5

Let F be a (length preserving) pseudorandom function. Define a fixed-length MAC for messages of length n as follows:

- Mac: on input a key $k \in \{0,1\}^n$ and a message $m \in \{0,1\}^n$, output the tag $t := F_k(m)$.
- Vrfy: on input a key $k \in \{0,1\}^n$, a message $m \in \{0,1\}^n$, and a tag $t \in \{0,1\}^n$, output 1 if and only if $t \stackrel{?}{=} F_k(m)$.

CONSTRUCTION 4.7

Let $\Pi' = (\mathsf{Mac}', \mathsf{Vrfy}')$ be a fixed-length MAC for messages of length n. Define a MAC as follows:

- Mac: on input a key $k \in \{0,1\}^n$ and a message $m \in \{0,1\}^*$ of (nonzero) length $\ell < 2^{n/4}$, parse m as d blocks $m_1, \ldots, m_d$, each of length $n/4$. (The final block is padded with 0s if necessary.) Choose a uniform message identifier $r \in \{0,1\}^{n/4}$.

  For $i = 1, \ldots, d$, compute $t_i \leftarrow \mathsf{Mac}'_k(r \| \ell \| i \| m_i)$, where i, ℓ are encoded as strings of length $n/4$.† Output the tag $t := \langle r, t_1, \ldots, t_d \rangle$.
- Vrfy: on input a key $k \in \{0,1\}^n$, a message $m \in \{0,1\}^*$ of nonzero length $\ell < 2^{n/4}$, and a tag $t = \langle r, t_1, \ldots, t_{d'} \rangle$, parse m as d blocks $m_1, \ldots, m_d$, each of length $n/4$. (The final block is padded with 0s if necessary.) Output 1 if and only if $d' = d$ and $\mathsf{Vrfy}'_k(r \| \ell \| i \| m_i, t_i) = 1$ for $1 \leq i \leq d$.

† Note that i and ℓ can be encoded using $n/4$ bits because $i, \ell < 2^{n/4}$.

A Message Authentication Code (MAC) is a cryptographic checksum that provides integrity and authenticity of a message. It ensures that the message has not been altered during transmission and that it comes from a trusted sender. A secure MAC should have the following properties:

1. Message integrity: A MAC guarantees that the message has not been altered during transmission. Any changes made to the message after it has been sent will cause the MAC to fail.
2. Authentication: A MAC ensures that the message comes from a trusted sender. Only someone with the secret key can generate a valid MAC for a given message.
3. Non-repudiation: A MAC provides proof of origin and prevents the sender from denying that they sent the message. If a message has a valid MAC, the sender cannot deny sending it.
4. Unforgeability: A MAC is designed to be computationally infeasible to forge or generate a valid MAC for a message without knowing the secret key.

These properties make MACs secure and reliable for protecting the integrity and authenticity of messages.