Assignment-1

2020111013

(5) Construction of MAC

PRF F_k is defined as $F_k : \{0,1\}^n \rightarrow \{0,1\}^n$

Given a key $k \in \{0,1\}^n$ and a message $m \in \{0,1\}^l$, where l is the length of the message. The algorithm for generating the MAC tag is as follows:

1) Divide m into d blocks of length $n/4$ $\rightarrow m_1, m_2 \cdots m_d$.
m_d is padded with 0's if necessary.

2) Using a uniform random meassage identifier $r \in \{0,1\}^{n/4}$, generate a tag t_i for every message block m_i as

$$t_i = F_k(r \| d \| i \| m_i) \quad \forall i \in [1,d], \; i \in \mathbb{N}$$

3) Return the final tag as

$$t = r \| t_1 \| t_2 \| t_3 \cdots \| t_d$$

For the vrfy function, given a message m & tag t, calculates the value of $Mac_k(m)$ and compares with t. If both tags are same, it outputs 1 else it outputs 0.

Proof of Security

Let the set of q messages that have been queried by the A be Q and let $m' \notin Q$.

In order to prove our scheme is secure, we need to prove that

$$Pr[Mac\text{-}forge_{A,\Pi}(n) = 1] \leq negl(n)$$

The experiment is such that, if the adversary, for a non-queried message is able to find a matching tag with the tags of the queried messages, then output 1, else 0.

Let us define 2 events,

repeat → same random identifier r is used in two of the tags returned by the MAC in $Mac\text{-}forge_{A,\Pi}(n)$

NewBlock → Atleast one of the blocks $r||d||i||m_i$ was never previously authenticated by A's queries

Using these, we can write

$$Pr[Mac\text{-}forge_{A,\Pi}(n)=1] = Pr[Mac\text{-}forge_{A,\Pi}(n)=1 \wedge repeat] + Pr[Mac\text{-}forge_{A,\Pi}(n)=1 \wedge \overline{repeat} \wedge NewBlock] + Pr[Mac\text{-}forge_{A,\Pi}(n)=1 \wedge \overline{repeat} \wedge \overline{NewBlock}]$$

↳ (1)

Now we prove that if repeat doesnt occur, then NewBlock has to occur, and if repeat occurs, newBlock still occurs.

We know that $m' \neq m$, where $m \in Q$, $m' \notin Q$. let their lengths be l & l'.

Case I : $l = l'$ (Here repeat = 1)

$\because m \neq m'$

$\Rightarrow \exists\ i \in [1, l]$ s.t $m_i \neq m_i'$ $(i \in \mathbb{N})$

Let $x_i = r||d||i||m_i$

$\Rightarrow x_i \neq x_i'$ for some i

$\Rightarrow F_k(x_i) \neq F_k(x_i') \Rightarrow t_i \neq t_i'$ for some $i \Rightarrow$ NewBlock occurs

Case II $l \neq l'$

Since the lengths are different, two cases arise

Case 2.1 $\max(l, l') - \min(l, l') < \frac{n}{4}$

Here the last block of one the messages will be different as they will have different amounts of zero padding

Case 2.2 $\max(l, l') - \min(l, l') > \frac{n}{4}$

In this case, the longer message will have a completely new block which would've never been authenticated before.

∴ The tags generated will be different and a new block occurs

And if repeat doesn't occur, then the identifiers would be r & r' ⇒ which will bring about point of difference & NewBlock occurs.

$$\therefore Pr[Mac\text{-}forge_{A,\Pi}(n)=1 \wedge \overline{repeat} \wedge NewBlock] = 0$$

&

$$Pr[Mac\text{-}forge_{A,\Pi}(n)=1 \wedge \overline{repeat} \wedge NewBlock] = Pr[Mac\text{-}forge_{A,\Pi}(n)=1 \wedge NewBlock]$$

From ①

$$Pr[Mac\text{-}forge_{A,\Pi}(n)=1] \leq Pr[repeat] + Pr[Mac\text{-}forge_{A,\Pi}(n)=1 \wedge NewBlock]$$

$\{ Pr[Mac\text{-}forge_{A,\Pi}(n)=1 \wedge repeat] \leq Pr[repeat] \}$

Let the no. of queries be $q = q(n)$ ⇒ polynomial function

r is of length $\frac{n}{4}$ ⇒ total possible $r = 2^{n/4}$

Out of q queries, the probability of repeat is exactly the probability of $r_i = r_j$ for $i \neq j$; $i, j \in [1, q]$

$\uparrow i$ $\quad$ $\uparrow$ choosing j

$$\therefore Pr[repeat] \leq \left(\frac{q}{2^{n/4}}\right) \cdot \left(\frac{q-1}{2^{n/4}}\right)$$

$$\therefore Pr[repeat] \leq \frac{q^2}{2^{n/4}}$$

$\because q$ is polynomial & $2^{n/4}$ is exponential ⇒ $\frac{q^2}{2^{n/4}}$ is negligible

$$\Rightarrow Pr[repeat] \leq negl(n) \quad — ②$$

For $Pr[Mac\text{-}forge_{A,\Pi}(n)=1 \wedge NewBlock]$, since the tag exists a new tag that has not been authenticated, & since the tag is generated through PRF, the probability of guessing the tag would be the same as probability of guessing output of PRF, which is negligible.

$$\therefore Pr[Mac\text{-}forge_{A,\Pi}(n)=1 \wedge NewBlock] \leq negl(n) \quad — ③$$

From ~~(2)~~ (1), (2), (3)

$\therefore \Pr[\text{Mac-forge}_{A,\Pi}(n) = 1] \leq \text{negl}(n)$

$\therefore$ ~~Our scheme~~ The constructed scheme is secure.