Assignment-1

2020111013

⑥ Construction CBCMAC

Let PRF $F_n : \{0,1\}^n \to \{0,1\}^n$

For a given message $m \in \{0,1\}^{l(n)}$ & keys $k_1, k_2 \in \{0,1\}^n$, the scheme is as follows

1) Divide the message into d blocks of length n
2) For each block, calculate $t_i = F_{k_1}(t_{i-1} \oplus m_i)$
   where $t_0 = 0^n$, Finally we'll have t_d
3) ~~calculate~~ Calculate $t = F_{k_2}(t_d)$

For verification, check if tag as input & calculated tag are same.

Proof of Security

Let $f : \{0,1\}^n \to \{0,1\}^n$, $f \to$ uniformly random

We define CBC_k as $CBC_k : (\{0,1\}^n)^+ \to \{0,1\}^n$

$$CBC_k(x_1 \dots x_d) = F_k(F_k \cdots (F_k(x_1) \oplus x_2) \oplus \cdots \oplus x_d)$$

RTP $\quad Pr[D^{CBC_{F_k}(\cdot)}(1^n) = 1] - Pr[D^{f(\cdot)}(1^n) = 1] \le \frac{q^2 n^2}{2}$

We are using CBC key with a PRF

Let $P = \{X_1, X_2 \dots X_q\}$ $\quad X_i \in (\{0,1\}^n)^*$

$|X_i| = l$

$\forall t_i \in \{0,1\}^n$, $1 \le i \le q$

$Pr[X_i = f_i] = \frac{1}{2^n}$ $\quad$ {f is uniformly random}

$Pr[\bigwedge_i X_i = f_i] = \frac{1}{2^{nq}}$

for $X_i \in P$

$$I_1 = X_1$$
$$I_2 = CBC_{F_k}(x_1) \oplus x_2$$
$$I_i = CBC_{F_k}(x_1, x_2 \cdots x_{i-1}) \oplus x_i$$

Let us consider the event collision which is defined as if there is collision in X_i ($\exists i \neq j \mid I_i = I_j$) or collision between X_i & X_j

$\downarrow$ collision1 $\quad$ $(\exists i,j \; ; \; I_i = I_j')$ $\downarrow$ collision2

$\because f$ is a random function

$CBC_f(X_i) \; \forall \; 1 \leq i \leq q$ will be uniformly distributed & independent

If there are no collisions

$$Pr[X_i \to t_i] = \frac{1}{2^{nq}} \; \forall i$$

$$Pr[\forall i : CBC_{F_k}(X_i) = t_i \mid \overline{Collision}] = \frac{1}{2^{nq}}$$

Let $Coll_{i,j} = Coll_1(X_i) \cup Coll_1(X_j) \cup Coll_2(X_i, X_j)$

$$Pr[collision] \leq \sum_{i<j} Pr[Coll_{i,j}]$$
$$\leq \frac{q(q-1)}{2} \cdot \max(Pr[coll_{i,j}])$$
$$< \frac{q^2}{2} \cdot \max(Pr[coll_{i,j}])$$

Max collision will happen at maximum length

Let X & X' be of length l

Let t be max value s.t

$$(X_1, X_2, X_3 \cdots X_t) = (X_1', X_2' \cdots X_t')$$
$$\Rightarrow (I_1, I_2 \cdots I_t) = (I_1', I_2' \cdots I_t')$$

Procedure

For steps, $i = 1$ to $(t-1) \rightarrow$ choose uniform $F_k(I_i)$

$i = t \rightarrow$ " " $F_k(I_t)$

$i = t+1$ to $(l-1) \rightarrow$ " " $F_k(I_i)$

$i = l$ to $(2l-t-2) \rightarrow$ " " $F_k(I_i')$

Let collision (k) be collision at k^{th} step

$$Pr[coll(i,j)] = Pr[\bigcup_i collision(i)]$$

$$\leq Pr[coll(1)] + \sum_{k=2}^{2l-t-2} Pr[collision(k) \mid \overline{collision(k-1)}]$$

$$= \frac{1}{2^n}\left(k\cdot(t-1) + 2t + k(2l-2t-2)+1\right) = 2^{-n}\sum_{k=2}^{2l-t-2} < 2q^2 l^2 \cdot 2^{-n}$$

The first 2 terms represent coll w/ itself

Last term represent last $k+1$ steps that can have coll^n.

$$\boxed{\therefore Pr[\forall i : CBC_F(X_i) = t_i] \geq Pr[\forall i\ CBC_F(X_i) = t_i \mid \overline{Coll}] \cdot Pr(\overline{coll}) = 2^{-nq}(1 - Pr[coll]) = 2^{-nq}\left(1 - \frac{q^2 l^2}{2^n}\right) = 2^{-nq}(1-\delta)}$$

$\therefore$ The given CBC is a <u>smooth CBC</u>

$\because$ Smooth CBC's imply indistinguishability

$\therefore$ Since message was prepared with length, we know that the inputs can't be prefix free.

$\therefore$ CBCMAC is secure