CBC - MAC ↴

For proving the security of CBC-MAC, we follow this outline ↴

1. Show that basic CBC-MAC is secure under prefix free inputs.

2. define a function f^n CBC, which is computed similiar to MAC.

3. Show that CBC is a PRF, if f is PRF
   - → Show that CBC is keyed with RF g. is indistinguishable from a RF.
   - → Show that CBC keyed with PRF does not affect distinguishability (only negl(·))

Proof:

$$CBC_K : (\{0,1\}^n)^+ \longrightarrow \{0,1\}^n$$

$$CBC_K(\underbrace{x_1}_{x_i\text{'s} \to n\text{-bit}} \cdots x_\ell) = F_K(F_K \cdots (F_K(x_1) \oplus x_2) \oplus \cdots \oplus x_\ell)$$

instead of key K on PRF, we use g as

$$\boxed{CBC_g(x_1 \cdots x_\ell) = g(g(\cdots g(x_1) \oplus x_2) \oplus x_3) \oplus x_\ell)}$$

To prove:

$$\left| \Pr\left[D^{CBC_g(\cdot)}(1^n) = 1 \right] - \Pr\left[D^{f(\cdot)}(1^n) = 1 \right] \right| \leq \frac{q^2 n^2}{2}$$

⇒ This means the CBC keyed with g is indistinguishable from a random function.

Proof -

Let $P = \{x_1 \cdots\cdots x_q\}$ $\quad x_i \leftarrow (\{0,1\}^n)^*$

& $\max |x_i| = \ell$.

for $t_1, \cdots\cdots t_q \in \{0,1\}^n$

$$P[x_i = t_i] = \frac{1}{2^n}.$$

$$\therefore P[\forall i \, ; x_i = t_i] = \frac{1}{2^{nq}}$$

Here we define (q, ℓ, δ) - smooth CBC as,

$$\boxed{\Pr[\forall i, \ CBC_g(x_i) = t_i] \geq \frac{(1-\delta)}{2^{nq}}}$$

$\because$ we prove that, CBC_g° is (q, ℓ, δ) smooth if

$$\delta = \frac{q^2 \ell^2}{2^n}.$$

for $x \in P$, we have, $(x \in (\{0,1\}^n)^m)$

$$g(x) = (I_1 \ \cdots\cdots \ I_m)$$

$$I_1 = x_1$$

$$I_2 = CBC_g(x_1) \oplus x_2$$

$$\vdots$$

$$I_m = CBC_g(x_1 \cdots x_{m-1}) \oplus x_m$$

Now, for $x_1, x_2 \in P$, we have

(a) A collision in x_1 if $I_i = I_j$, for $i \neq j$

$(coll_1)$

(b) a collision b/w x_i & x_j if $I_i = I_j'$

but $(x_1, x_2 \cdots x_i) \neq (x_1', x_2' \cdots x_j')$

$(coll_2)$

$$coll = coll_1 \cup coll_2$$

Since, g is a RF, $CBC_g(x_1) \cdots\cdots CBC_g(x_q)$ are uniform and independent, $\because$ if no collisions, happen, Prob of all $x_i \to t_i \ \forall i = \frac{1}{2^{nq}}$

$$\Pr[\forall i : CBC_g(x_i) = t_i \mid \overline{coll}] = \frac{1}{2^{nq}}$$

Now,

$$coll_{i,j} = coll_1(x_1) \cup coll_1(x_2) \cup coll_2(x_1, x_2)$$

$$\Pr[coll] \leq \sum_{i<j} \Pr[coll_{i,j}]$$

[using Union Bound]

$$\Rightarrow \quad \Pr[\text{col}] \le \frac{q(q-1)}{2} \max \Pr[\text{col} \mid i, j]$$

$$< \frac{q^2}{2} \max \{ \Pr[\text{col}\ i, j] \}$$

$\Rightarrow$ max collission prob is possible when x_i & x_j are at max lengths

Let $x_i = X$
$x_j = x'$

$$X = (x_1, x_2 \ldots x_\ell) \to (I_1 \ldots)$$
$$x' = (x_1', x_2' \ldots x_\ell') \to (I_1' \ldots)$$

and let t be the biggest value such that,

$$(x_1, x_2 \ldots x_t) = (x_1' \ldots x_t')$$
$$\Rightarrow (I_1, I_2 \ldots I_t) = (I_1', \ldots I_t')$$

$2\ell-t-2$ step procedure

step $i = 1$ to $t-1$
choose uniform $g(I_i)$

step $i = t$
$\to$ choose $g(I_t)$

Step $i = t+1$ to $\ell-1$
$\to$ choose $g(I_i)$

step $i = \ell$ to $2\ell-t-2$
choose $g(I_i')$

define,

coll(k) = collision in ith step

$$\Pr[\text{coll}(i,j)] = \Pr[\cup \text{coll}(k)]$$

$$\leq \Pr[\text{coll}(1)]$$

$$+ \sum_{k=2}^{2\ell-t-2} [\text{coll}(k) \mid \overline{\text{coll}}(k-1)]$$

$$= \frac{1}{2^n}\left(k(t-1) + 2t + (2\ell - 2t - 2)k + 1\right)$$

where,

$k(t-1) \Rightarrow$ only collision with itself

$(2\ell - 2t - 2)k \Rightarrow$ remaining steps can have $k+1$ ways of colli.

$$\Rightarrow 2^{-n} \sum_{\cancel{k}\,k=2}^{2\ell-t-1} k < 2\ell^2 2^{-n}$$

$$\therefore P[\forall i: CBC_g(x_i) = t_i] \geq \Pr[E \mid \overline{\text{coll}}] \cdot \Pr[\overline{\text{coll}}]$$

$$= 2^{-nq}(1 - \Pr(\text{coll}))$$

$$\Rightarrow 2^{-nq}\left(1 - \frac{q^2\ell^2}{2^n}\right)$$

$$= 2^{-nq}(1-\delta)$$

as needed.

similar to CPA-proof, we can say that it is indistinguishable.

$\therefore$ CBC-MAC is secure.