MAC

Wednesday, 22 February 2023 8:34 PM

we implemented a radom ctr mode. and now we prove that is CPA secure.

. . .

Let $\Pi = (Gen, Enc, Dec)$

$\tilde{\Pi} = (\tilde{Gen}, \tilde{Enc}, \tilde{Dec})$ but with $F_k(\cdot)$ substituted with $f(\cdot)$. for $\tilde{\Pi}$ we can now prove

$$Pr\left[MacF^{cpa}_{A,\tilde{\Pi}}(n) = 1\right] \leq \text{negl}(n)$$

Let $t = (r, t_1, \ldots, t_d)$, we have the cases

1.) The identifier r appearing in t_0 output be A is different from all other r_i's. Since f_n is truly random $\therefore$ probability of guess is at most 2^{-n}.

2.) The identifier r is appearing in the tag t output by A appears in exactly one of the MAC tags obtained by A from the oracle. Let m' be the message that A query for which reply t' had r.

a) if $len(m) = len(m')$ in such a case one of the block is diff. f_n was never applied the diff block here prob. of guessing 2^{-n}

b) if $len(m) \neq len(m')$ then one block would be defn. different. Thus the prob of guessing is is 2^{-n}

3.) The prob of two or more macs having the same t is $\binom{n}{2} 2^{-n/4} = \frac{O(n^2)}{2^{n/4}} = \text{negl}(n)$

Thus

$$\left| Pr\left[D^{F_k(\cdot)}(1^n) = 1\right] - Pr\left[D^{f_n(\cdot)}(1^n) = 1\right] \right| \geq \varepsilon(n) - \text{negl}(n)$$