CPA security

Wednesday, 22 February 2023 8:34 PM

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

Let ctr_c be the initial value of the counter

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

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

$$Pr\left[PrivK^{cpa}_{A,\widetilde{\Pi}}(n) = 1 \right] \leq \frac{1}{2} + negl(n)$$

Let n be security parameter and ctr_c be the initial ctr. When ciphertext is encrypted f_n is applied to value $ctr_c + 1, \ldots ctr_c + l_c$ where $l_c \leq q(n)$

Now for an oracle when the i^{th} query is answered f_n is applied to $ctr_i + 1, \ldots ctr_i + l$

Case-1

There do not exist any $i, j, j' > 1$ for which $ctr_i + j = ctr_c + j'$

In such a case the probability that A outputs $b' = b$ is case $= 1/2$ because we can obtain this by xoring a random stream

Case-2

There exist $i, j, j' \geq 1$ with $j \leq l_i$ and $j' \leq l_c$ for which $ctr_i + j = ctr_c + j'$. In this case A may easily determine which of its message was encrypted to give the challange ciphertext

Let $Overlap_i$ denote the event $ctr_i + 1 \ldots ctr_i + q(n)$ overlaps the sequence $ctr_c + 1, \ldots ctr_c + q(n)$ and let overlap denote the event that $Overlap_i$. Since there are at most $q(n)$ queries

$$Pr[Overlap] \leq \sum_{i=1}^{q(n)} Pr[Overlap_i]$$

Overlap Occurs when

$$ctr_c + 1 - q(n) \leq ctr_i \leq ctr_c + q(n) - 1$$

and ctr_i can be chosen b/w $\{0,1\}^n$ uniformly.

and Overlap can be from $2q(n) - 1$

$$Pr[Overlap_i] = \frac{2q(n) - 1}{2^n}$$

$$\therefore \quad Pr[Overlap] \leq \frac{2q(n)^2}{2^n}$$

$$Pr\left[PrivK^{cpa}_{A,\widetilde{\Pi}}(n) = 1 \right] = Pr\left[PrivK^{cpa}_{A,\widetilde{\Pi}}(n) = 1 \wedge overlap \right]$$

$$+ \; Pr\left[PrivK^{cpa}_{A,\widetilde{\Pi}}(n) = 1 \wedge \overline{overlap} \right]$$

$$\leq Pr[Overlap] + Pr\left[PrivK^{cpa}_{A,\widetilde{\Pi}}(n) = 1 \mid \overline{Overlap} \right]$$

$$\leq \frac{2q(n)^2}{2^n} + \frac{1}{2}$$

$\therefore \widetilde{\Pi}$ is CPA secure.

now this implies Π is secure since $F_k(\cdot)$ is a Pseudo Random function

$$Pr\left[PrivK^{cpa}_{A,\Pi}(n) = 1 \right] \geq \frac{1}{2} + negl(n)$$