CPA - Secure encryption scheme

CPA :- Chosen Plain text Attack

CPA - secure encryption scheme using PRF

Let F be a pseudorandom function. Define a private key encryption scheme for messages of length as follows:

- Gen :- on input 1^n, choose $k \leftarrow \{0,1\}^n$ & message $m \in \{0,1\}^n$, choose $r \leftarrow \{0,1\}^n$ uniformly at random & output the ciphertext.

$$c = \langle r, F_k(r) \oplus m \rangle$$

- Dec :- on input a key $k \in \{0,1\}^n$ and ciphertext $c = \langle r, s \rangle$, output the plaintext message

$$m = F_k(r) \oplus s$$

To prove :- If F is a PRF, then above CPA scheme with length parameter $l(n) = n$ that has indistinguishable encryptions under a chosen plaintext attack.

Proof :- Let $\tilde{\pi} = (\tilde{Gen}, \tilde{Enc}, \tilde{Dec})$ be encryption scheme that is exactly the same as $\pi = (Gen, Enc, Dec)$ except f_n (truly random function is used instead of F_k).

We claim that for every adversary A, that makes at most $q(n)$ queries to it's encryption oracle, we have

$\Pr[\mathrm{PrivK}^{cpa}_{A,\pi} = 1] = \frac{1}{2} + \frac{q(n)}{2^n}$ —(1)

[Every time a message m is encrypted, a random $r \leftarrow \{0,1\}^n$ is chosen & ciphertext is ~~set~~ set equal to $\langle r, f_n(r) \oplus m \rangle$. Let r_c denote random string used when generating the challenge ciphertext

$c = \langle r_n, f_n(r_c) \oplus m_b \rangle$

There are 2 subcases:-

1.) The value r_c is used by encryption oracle to answer at least one of A's queries - In this case A may easily determine which of the messages was encrypted. However, since A makes at most $q(n)$ queries to it's oracle and each oracle query is answered using a value r chosen uniformly at random, the probability of this event is at most $q(n)/2^n$.

2.) The value of r_c is never used by the encryption oracle to answer any of A's queries. In this case A leaves nothing about value of $f_n(r_c)$. That means for A, the value is chosen uniformly at random. Probability that A outputs $b' = b$ in this case is exactly $1/2$

Let $\varepsilon(n) \stackrel{def}{=} \Pr[\mathrm{PrivK}^{cpa}_{A,\pi}(n) = 1] - \frac{1}{2}$ —(2)

Let Repeat denote a event that r_c is used by encryption oracle to answer at least one of A's queries.

$$\Pr[\mathrm{Priv}^{cpa}_{A,\pi}(n)=1] = \Pr[\mathrm{Priv}K^{cpa}_{A,\pi}(n)=1 \wedge \mathrm{Repeat}]$$

$$+ \Pr[\mathrm{Priv}K^{cpa}_{A,\pi}(n)=1 \wedge \overline{\mathrm{Repeat}}]$$

$$\leq \Pr[\mathrm{Repeat}] + \Pr[\mathrm{Priv}K^{cpa}_{A,\pi}(n)=1 \mid \overline{\mathrm{Repeat}}]$$

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

Let D be the distinguisher with input 1^n.

* If D's oracle is PRF, the view of A when as a sub-routine by D is distributed identically to the view of A in exp. $\mathrm{Priv}^{cpa}_{A,\pi}(n)$

$\Rightarrow \Pr[D^{F_k(\cdot)}(1^n)=1] = \Pr[\mathrm{Priv}K^{cpa}_{A,\pi}(n)=1]$

* If D's oracle is a random function, then view of A, when run as a sub-routine by D is distributed identically to the view of A in the experiment $\mathrm{Priv}K^{cpa}_{A,\pi}(n)$

$\Pr[D^{f_n(\cdot)}(1^n)=1] = \Pr[\mathrm{Priv}K^{cpa}_{A,\pi}(n)=1]$

$\because$ F is PRF & D runs in probabilistic polynomial time, there exists a negligible function negl such that

$\Pr[D^{F_k(\cdot)}(1^n)=1] - \Pr[D^{f_n(\cdot)}(1^n)=1] \leq negl(n)$

Using eqn (1) & (2)

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

$$= \left| \Pr[\text{PrivK}^{cpa}_{A,\pi}=1] - \Pr[\text{PrivK}^{cpa}_{A,\tilde{\pi}}=1] \right|$$

$$\geq \Pr[\text{PrivK}^{cpa}_{A,A}=1] - \Pr[\text{PrivK}^{cpa}_{A,\tilde{\pi}}=1]$$

$$\geq \frac{1}{2} + \epsilon(n) - \frac{1}{2} - \frac{q(n)}{2^n}$$

$$= \epsilon(n) - \frac{q(n)}{2^n}$$

$$\Rightarrow \epsilon(n) \leq \text{negl}(n) + \frac{q(n)}{2^n}$$

$\because q(n)$ is a polynomial

$\Rightarrow \epsilon(n)$ is negligible, completing the proof.