CPA - Secure Scheme

$r, m, k \in \{0,1\}^n$

Construction: Enc: $c := \langle r, f_k(r) \oplus m \rangle$

Dec: $m := f_k(r) \oplus s$; $c = \langle r, s \rangle$

Proof:

consider the 2 set of encryption schemes,

$S_1 = (Gen, Enc, Dec)$

$S_2 = (\overline{Gen}, \overline{Enc}, \overline{Dec})$

where S_1 and S_2 are completely identical, except the fact that we use a truly random function f in S_2 and a pseudo random function f_k in S_1. for a PPTM adversary A,

$\therefore$ To prove: $\exists$ negl(n) such that, $\left| P\left[PrivK^{CPA}_{A,S_1}(n) = 1 \right] - P\left[PrivK^{CPA}_{A,S_2}(n) = 1 \right] \right| \leq negl(n)$.

Proof: Let $q(n)$ be the upper bound on the number of operations carried by adversary A to the encryption oracle.

Let D be a PPTM adversary, with access to a random oracle O. Then,

① D is truly random

→ This setting is similar to A's getting using the scheme S_2

$\therefore P_{f \leftarrow Func}\left[D^{f(\cdot)}(1^n) = 1 \right] = Pr\left[PrivK^{CPA}_{A,S_2}(n) = 1 \right]$ — ①

② D is PRF

⇒ If key k, is chosen uniformly then,

$$P_{k \leftarrow \{0,1\}^n}\left[D^{f_k(\cdot)}(1^n) = 1 \right] = P\left[PrivK^{CPA}_{A,S_1}(n) = 1 \right] \quad — ②$$

$\therefore$ F is pseudo random, $\therefore$ we know that $\exists$ negl(n) such that

$$\left| Pr\left[D^{f_k(\cdot)}(1^n) = 1 \right] - Pr\left[D^{f(\cdot)}(1^n) = 1 \right] \right| \leq negl(n)$$

$\therefore$ from ① & ② we get

$$\boxed{\left| P\left[PrivK^{CPA}_{A,S_1}(n) = 1 \right] - P\left[PrivK^{CPA}_{A,S_2}(n) = 1 \right] \right| \leq negl(n).}$$

② consider a uniformly sampled string $r \in \{0,1\}^n$, then for almost $q(n)$ queries then there could be following 2 cases,

(1) Adversary A has not seen string r yet. [repeat]

→ Here, A learns nothing about $f(r)$, and is uniformly distributed. $\therefore$ Prob. that A outputs $b = b'$ is $= 1/2$ (truly random case)

② Adversary A has seen string r before [repeat]

$$\Rightarrow P\left[PrivK^{CPA}_{A,S_2}(n)=1\right] = P\left[PrivK^{CPA}_{A,S_2}(n)=1 \wedge \text{repeat}\right] + P\left[PrivK^{CPA}_{A,S_2}(n)=1 \wedge \overline{\text{repeat}}\right]$$

$$\leq P[\text{repeat}] + P\left[PrivK^{CPA}_{A,S_2}(n)=1 \mid \text{repeat}\right]$$

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

∵ if we put a PRF in place of random function we get,

$$P\left[PrivK^{CPA}_{A,S_1}(n)=1\right] \leq \frac{1}{2} + \frac{q(n)}{2^n} + negl(n)$$

$q(n)$ is bounded by a polynomial

∵ $\frac{q(n)}{2^n} \rightarrow$ negligible

$$P\left[PrivK^{CPA}_{A,S_1}(n)=1\right] \leq \frac{1}{2} + negl'(n)$$