Assignment - 1

2020111013

④ Construction of CPA secure Encryption Scheme

Let the PRF be $F_k : \{0,1\}^n \to \{0,1\}^n$. Let the random seed be $r \in \{0,1\}^n$
Given a key $k \in \{0,1\}^n$ & $m \in \{0,1\}^l$, The encryption scheme is as follows

1) Divide m into d blocks of size $n \to m_1, m_2 \cdots m_d$
2) For each block, calculate the value of $x_i = F_k(r+i)$ and then subsequently calculate $c_i = x_i \oplus m_i$ $(1 \le i \le d)$
3) The ~~final~~ final ciphertext will be $c = r \| c_1 \| c_2 \| \cdots \| c_d$

Proof of Security

~~In in order~~ RTP $\to \Pr[\mathrm{PrivK}^{cpa}_{A,\Pi}(n) = 1] \le negl(n)$

Let the no. of queries made by A be q which is bounded by $q(n)$, since A is PPTM

Let the message m have l blocks. Let l_i be no. of blocks used by A on i^{th} query.
$\therefore l \le q(n)$

Since we are ~~a~~ using randomized counter mode, ~~to~~ the random seed ~~to~~ used for each block will be different.

Let ctr_i denote the random initial seed used by A in the i^{th} query & let ctr_c represent the random seed for the challenge text.

Let overlap represent the event of $ctr_i + j = ctr + j'$

Case I $\quad \nexists\, i, j, j' \ge 1,\ j \le d_i,\ j' \le d$ s.t. $ctr_i + j = ctr + j'$ (no overlap)

$\because$ A has never seen the output of $F_k(ctr + i)\ \forall\ 1 \le i \le d$

$\therefore$ In order for A to guess the correct initial seed, A would have to correctly guess the output of the PRF output of $F_k(ctr+i)$, which is negligible.

$$\Pr[\mathrm{PrivK}^{cpa}_{A,\Pi}(n) \wedge \overline{\text{overlap}}] = \frac{1}{2} \quad -①$$

$\therefore$ There is no overlap & ~~$\Pr[\mathrm{PrivK}^{cpa}_{A,\Pi}(n) = 1] \le \frac{1}{2} + negl(n)$~~

Case II

$\exists\, i, j, j' \geq 1$ s.t $ctr_i + j = ctr + j'$ (overlap)

In this case, there is an overlap $\Rightarrow F_k(ctr_i + j_0) = F_k(ctr + j')$

$\downarrow$

adversary can ~~get~~ decrypt block

$\boxed{\text{Let overlap represent the event of } ctr_i + j = ctr + j'}$

Let $l_i = l_c$, $l_i, l_c \leq q(n)$

For overlap $= 1$,

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

These bounds represent the maximum & minimum number of block A can query in $q(n)$ time. $\therefore$ Total no. of values for ctr_i to overlap $= 2q(n) - 1$

Total possible ctr_i would be 2^n {n-bit}

$$\therefore P[\text{overlap}_i] = \frac{2q(n) - 1}{2^n}$$

$$\therefore P[\text{overlap}] \leq \sum_{1}^{q(n)} \frac{2q(n) - 1}{2^n}$$

$$\therefore P[\text{overlap}] \leq \frac{2q^2(n)}{2^n}$$

$$\therefore P[\text{PrivK}^{cpa}_{A,\pi}(n) = 1 \wedge \text{overlap}] \leq \frac{2q^2(n)}{2^n} \quad - (2)$$

From (1) & (2)

$$\Pr[\text{PrivK}^{cpa}_{A,\pi}(n) = 1] = \Pr[\text{PrivK}^{cpa}_{A,\pi}(n) = 1 \wedge \text{overlap}] + \Pr[\text{PrivK}^{cpa}_{A,\pi}(n) = 1 \wedge \overline{\text{overlap}}]$$

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

$\rightarrow$ polynomial

$\rightarrow$ exponential

$\therefore \frac{2q^2(n)}{2^n} \rightarrow negl(n)$ $\boxed{\therefore \Pr[\text{PrivK}^{cpa}_{A,\pi}(n) = 1] \leq \frac{1}{2} + negl(n)}$