CPA-secure

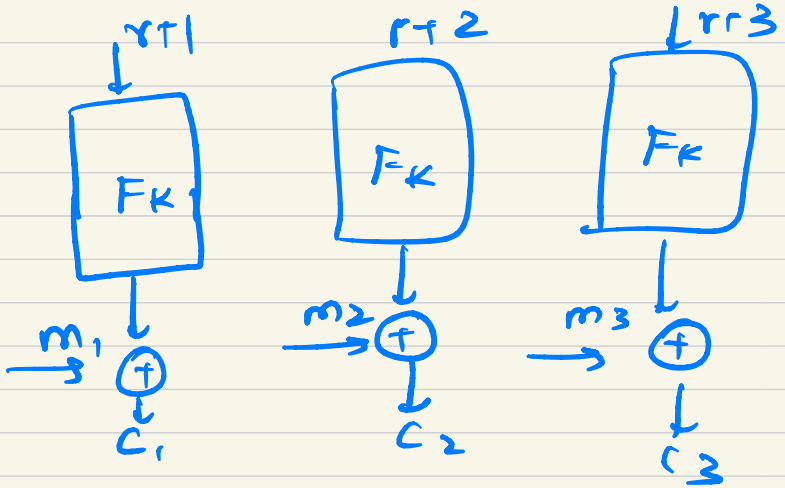
proof of security for randomised-counter mode:

Let Π be the encryption scheme for our method,

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

Let,

$\Pi = (\overline{Gen}, \overline{Enc}, \overline{Dec})$ be the similiar encryption scheme such that, instead of PRF in Π we use a truly random function f.



∵ security of CPA in this mode relies on the fact that $ctr+i$ is distinct, and thus $f(ctr+i)$ is distinct, and thus the security boils down to the fact that, $ctr+i$, was previously used.

PTP:

$$\forall \text{ PPTM } A \quad \exists \cdot negl(n) \mid$$

$$Pr[Priv^{CPA}_{A,\Pi}(n) = 1] \leq \frac{1}{2} + negl(n)$$

proof: Let $q(n)$ denote the bound on queries made by A.

consider a message m, of e blocks.

∵ The function f is applied to

→ $ctr_c + 1, ctr_c + 2, \ldots ctr_c + l$

and $l \leq q(n)$

there let ctr_i denote random initial seed used by A in ith query and,

$ctr_c \rightarrow$ random seed for challenge text

The following cases arise

① sure donot exist i, j and $j' \geq 1$ and $j \leq l_i$ and $j' \leq l_c$

$ctr_i + j = ctr_c + j'$

$\therefore$ A hasn't seen the output of f when f is applied to

$ctr_c + 1, ctr_c + 2, \ldots, ctr_c + l_c$

$\therefore$ XORing with random-seed, to message m_b,

$$\therefore P\left[Priv^{CPA}_{K_A, \pi}(n) = 1 \right] = 1/2$$

(same as one-time pad)

② exists i, j and j' such that,

$$ctr_i + j = ctr_c + j'$$

↓

Now adversary knows that,

$$f(ctr_i + j) = f(ctr_c + j')$$

∵ could determine which of the 2 messages (m_0 or m_1) was encrypted, some information is leaked.

∴ we have,

now there must be some overlap blw the ranges,

$ctr_i+1, ctr_i+2 \cdots ctr_i+l_i$

and

$ctr_i+1, ctr_i+2 \cdots ctr_i+l_c$

also,

let $l_i = l_c$ (to maximise the overlap)

and l_i & $l_c \leq q(n)$

∵ if $ctr_i[T_j] = ctr_{c'}[T_j]$ for some i, j and j'.

then, we can hence bound on ctr_i such that.

$$ctr_{c'} - (q(n)-1) \le ctr_i \le ctr_{c'} + (q(n)-1)$$

max blocks A could query in $q(n)$ time.

$2q(n)-1$

values for ctr_i for overlap to happen.

Since, ctr_i is chosen randomly,

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

↳ event that overlap happens at ith query.

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

↓

(event that an overlap occurs)

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

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

From (1) and (2) we have,

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

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