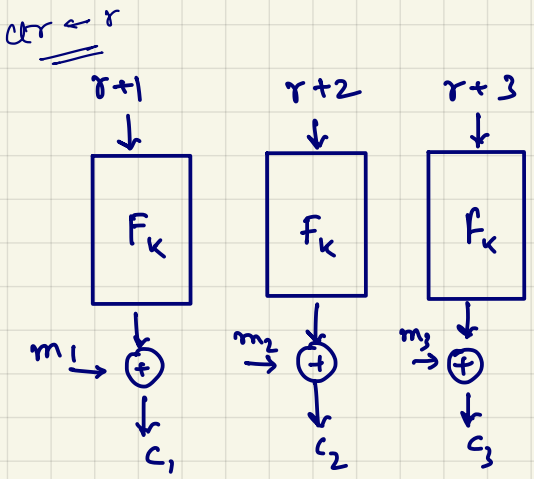
CPA-Secure

Proof of security for randomised-counter mode



Let Π be the encryption scheme for our method,

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

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

∵ Security of CPA in ctr 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.

To prove: $\forall$ PPT MA,

$$\exists\, negl(n) \;|\; Pr\left[Priv^{CPA}_{A,\bar{\Pi}}(n) = 1\right] \leq \frac{1}{2} + negl(n).$$

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

Consider a message m, of l blocks.

∵ The function f is applied to → $ctr_c+1, ctr_c+2, \dots ctr_c+l$

and $l \leq q(n)$.

Here let ctr_i denote random initial seed used by A in i^{th} query and

ctr_c → random seed for challenge text.

The following cases arise –

(1) There doesn't exist i, j and $j' \geq 1$ and $j \leq l_i$ and $j' \leq l_c$

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

∵ A hasn't seen the output of f when f is applied to

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

∵ XORing with random-seed, to message m_b,

$$\therefore P\left[Priv^{CPA}_{K,\bar{\pi}}(n) = 1\right] = \frac{1}{2}$$ [same as one-time pad].

(1)

(2) There 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 now, look at the bounded probability of this happening.

∴ we have,

now there must be some overlap b/w the ranges

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

and $ctr_c + 1, ctr_c + 2 \quad \cdots \quad ctr_c + l_c$

also, let $l_i = l_c$ (to maximise the overlap) . and $l_i + l_c \leq q(n)$

∴ if $ctr_i + j = ctr_c + j'$ for some i, j and j'

then, we can never bound on ctr_i such that

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

$2q(n)-1$ values for ctr_i for overlap to happen.

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

Since, ctr_i is chosen randomly,

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

(event that overlap happens at i^{th} query)

also, $P[\text{overlap}]$ (event that an overlap occurs)

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

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

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

From (1) and (2) we have,

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

∵ we used truly random function f here, if we replace f with F (PRF), for PPTM adversaries A,

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

also, $q(n)$ → polynomial, ∵ $\frac{2q^2(n)}{2^n} \to negl(\cdot)$

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

Hence proved.