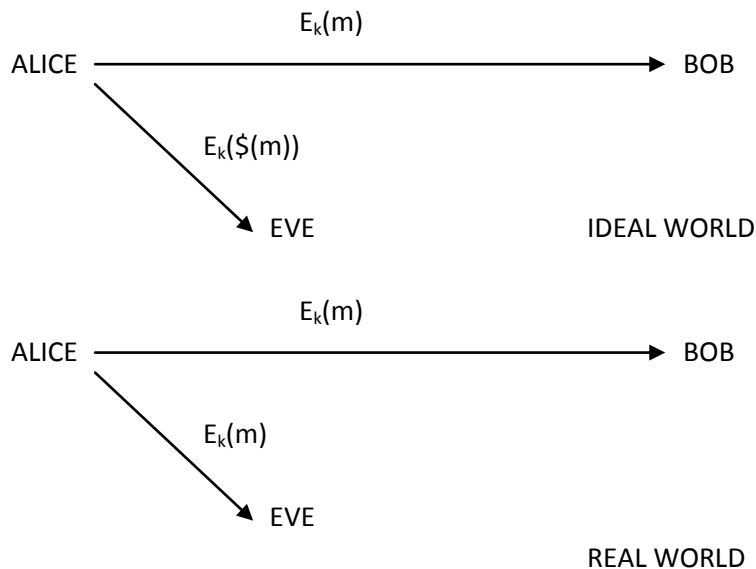


Definition of Security for Encryption:

Initial Conditions Assumed:

- Eve would learn that the message was sent
- Eve would learn length



$\$(X)$: A Random String of the same length as X
 It is non deterministic

SECURE ENCRYPTION SCHEME

Definition: An encryption Scheme is (t, q, ϵ) real or random (R-O-R) if $\forall A$ running in time $\leq t$ and making at most q bits total queries,

$$\text{Adv } A = |\Pr[A^{E_k} = 1 | k \leftarrow U_{\text{keys}}] - \Pr[A^{E_k \cdot \$} = 1 | k \leftarrow U_{\text{keys}}]|$$

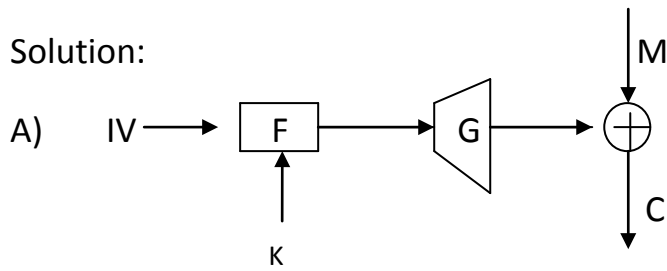
(Also called

Real or Random Advantage)

Problem:

$$\text{A PRF is } F: \{0,1\}^{128} * \{0,1\}^{128} \longrightarrow \{0,1\}^{128}$$

Hence the largest KeyStream which can be sent is only 128 bits.



Here G is an expansion function (GGM)

B) Theorem: $PRG \cdot PRF = PRF$

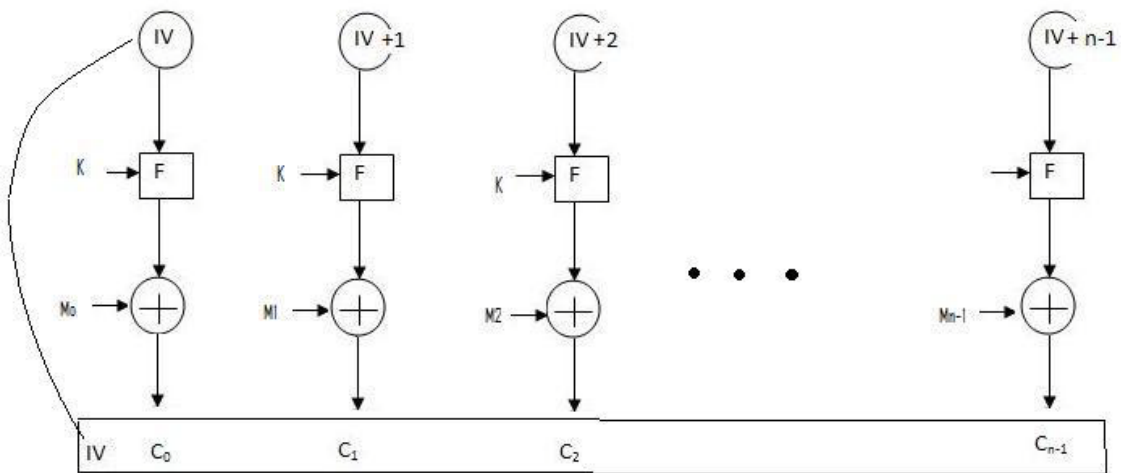
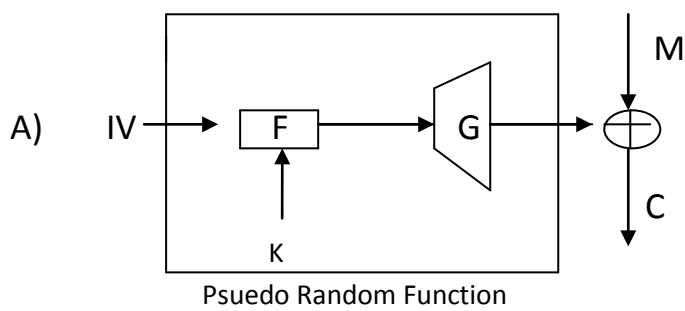


Figure 1: CTR^F Mode
(Counter Mode of Operation)

CTR^F Mode : Pick IV randomly at boot time only

CTR^F \$ Mode : Pick IV randomly per message.

Theorem :

If F is a (t, q, ϵ) – secure PRF , then CTR^f is $(t-O(q), \min(q, |ctr|), \epsilon)$ R-or-R secure

PROOF:

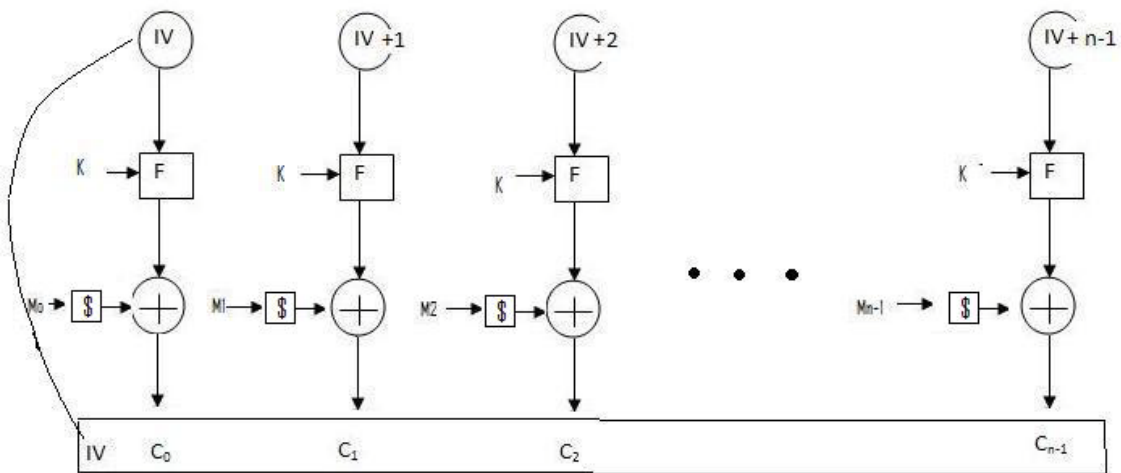


Figure 2

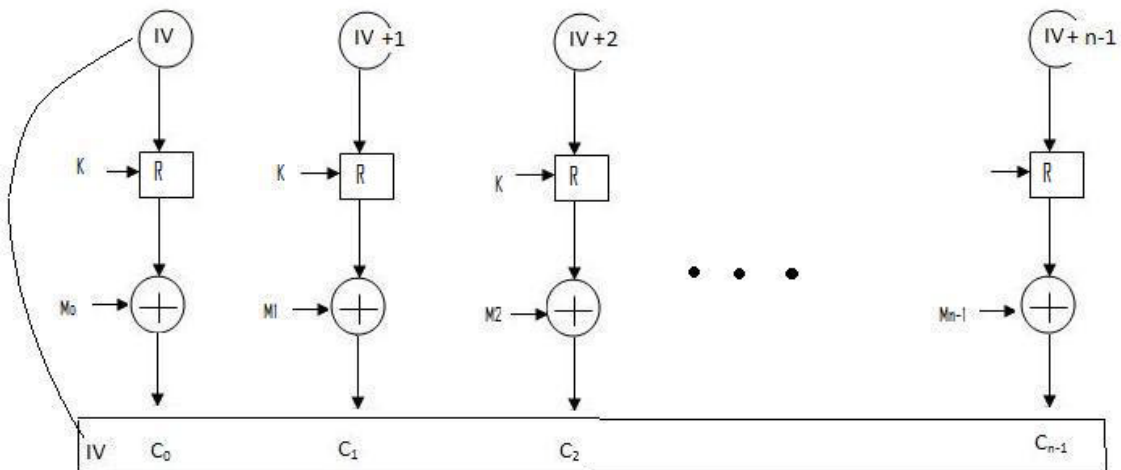


Figure 3

BY DPI – PRF :

$$(CTR)^R \sim (CTR)^{Fk}$$

In figure3, R is a random generator and produces a random output. In figure 2, \$ again outputs a true y random output thus by logic

$$CTR^R = CTR^{Fk} \bullet \$$$

$$\text{Therefore } CTR^{Fk} \sim CTR^{Fk} \bullet \$$$

Hence Proved