Eaves drop

Construction :

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

and a message $m \in \{0,1\}^{l(n)}$ [uniformly distributed]

and G: PRG,

$G: \{0,1\}^n \to \{0,1\}^{l(n)}$.

$Enc_k(m)$: $c = G(k) \oplus m$

$Dec_k(m)$ $m = G(k) \oplus c$

Proof of security :

↓

To prove:

$P[PrivK^{eav}_{A,\pi}(n)=1] \leq \frac{1}{2} + negl(n)$

for a PRG G, we know that, (by definition),

$P[D(G(k))=1] - P[D(w)=1] \leq negl(n)$ — (1)

$G: \{0,1\}^n \to \{0,1\}^{l(n)}$ & $w \in \{0,1\}^{l(n)}$ [uniform distribution]

generated from pseudo random generator.

} Distinguisher can't distinguish b/w a truly random generated output and a output generated by PRG.

consider a PPTM A,

$P[D(w)=1] = P[PrivK^{EAV}_{A,\pi}(n)=1] = \frac{1}{2}$ — (2)

⇒ Since, in a truly random setting there's a $\frac{1}{2}$ chance, uniform distribution for the Adversary A to output either of bit $b \in \{0,1\}$

$P[D(G(k))=1] = P[PrivK^{eav}_{A,\pi}(n)=1]$ — (3)

⇒ if G is a PRG, then we can say that the probability by which the distinguisher recognises $G(k)$ as a pseudo-random string than random string, should be same as the probability of adversary A guessing the message bit b, using the scheme π.

using (1) & (2) in (1), we get

$$P[PrivK^{eav}_{A,\pi}(n)=1] \leq \frac{1}{2} + negl(n)$$

∴ given scheme is provably secure.