If G is a pseudo random generator with expansion factor l.

Gen: on input 1^n, choose $k \in \{0,1\}^n$ output it's key.

Enc: on input k $c := G(k) \oplus m$

Dec: on input k $m := G(k) \oplus c$

let Π be this construction. The intution is that Π used a uniform pad in place of a pseudo random pad $G(k)$ then the resulting scheme would be identical to the one time pad. So the following equation must be true.

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

If this equation does not hold true then the adversary will be able to distinguish output of G from random string.

Let us show this by reduction. we use A to connect an efficient distinguisher D whose security are directly related.

A is arbitrary PPT adversary

D is takes w as input

Goal to determine if w was chosen uniformly can by computing

$w := G(k)$

Distinguisher D:

D is given as input a string $\{0,1\}^{\ell(n)}$

1. Run $A(1^n)$ to output pair of messages $m_0, m_1 \in \{0,1\}^{\ell(n)}$
2. Choose a uniform bit $b \in \{0,1\}$. set $c := w \oplus m_b$
3. Given c to A and obtain output b.

output 1 if $b' = b$ and output 0, otherwise.

D runs in polynomial time assuming A does.

→ Let us consider a modified encryption scheme.

$\bar{\Pi} = (\bar{Gen}, \bar{Enc}, \bar{Dec})$ which is exactly one time pad except that now, we have a security parameter n.

perfect secrecy implies:

$$Pr[PrivK^{eav}_{A,\bar{\Pi}}(n) = 1] = \frac{1}{2}$$

Analysis of behaviour of D:

1. If w is chosen uniformly view of A when run as a subroutine by D is distributed identically to view of A as in experiment $PrivK^{eav}_{A,\bar{\Pi}}(n)$.

(2) $\Pr_{w \leftarrow \{0,1\}^{\ell(n)}}[D(w)=1] = \Pr\left[\mathrm{PrivK}^{eav}_{A,\Pi}(n)=1\right] = \frac{1}{2}$

2. If w is instead generated by choosing uniform $k \in \{0,1\}^n$ and then setting $w := G(k)$ to view of A when run as a subroutine by D is distributed identically to the view of A in $\mathrm{PrivK}^{eav}_{A,\Pi}(n)$

(3) $\Pr_{k \leftarrow \{0,1\}^n}[D(G(k))=1] = \Pr\left[\mathrm{PrivK}^{eav}_{A,\Pi}(n)=1\right]$

since G is a pseudo random generator,

(4) $\left|\Pr_{w \leftarrow \{0,1\}^{\ell(n)}}[D(w)=1] - \Pr_{k \leftarrow \{0,1\}^n}[D(G(k))=1]\right| \leq \mathrm{negl}(n)$

using (3) and (4),

$$\left|\frac{1}{2} - \Pr\left[\mathrm{PrivK}^{eav}_{A,\Pi}(n)=1\right]\right| \leq \mathrm{negl}(n)$$

$$\Rightarrow \Pr\left[\text{PrivK}^{eav}_{A,\Pi}(n) = 1\right] \leq \frac{1}{2} + \text{negl}(n)$$

This proves that Π has indistinguishable encryptions in the presence of eavesdropper

$\therefore$ proved.