Se G è un generatore pseudocasuale, allora Π^G è sicuro contro attacchi passivi.

In breve: si crea un distinguitore D che usi l'attaccante A e si mostra così che la probabilità di vittoria in $PrivK$ e in D coincidono: la probabilità di $PrivK$ in caso di generatore realmente casuale è $\frac{1}{2}$, si ricava quella in caso di GP.

Si considera prima di tutto lo schema $\hat{\Pi}$ del tutto simile a Π^G ma in cui $\hat{Gen}$ produce in output una chiave k completamente casuale di lunghezza $l(n)$ e la cifratura è: $c = k \oplus m$. Per la sicurezza di one time pad sappiamo che:

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

A questo punto vi sono due scenari:

- Se w è stato scelto in modo uniforme e casuale in $\{0,1\}^{l(n)}$, l'attaccante A usato dal distinguitore D sarà distribuito nello stesso modo di $PrivK^{eav}_{A,\hat{\Pi}}(n)$.
- Se w è uguale a $G(k)$ con $k \leftarrow \{0,1\}^n$ scelto in modo casuale e uniforme, l'attaccante A usato dal distinguitore D sarà distribuito nello stesso modo di $PrivK^{eav}_{A,\Pi^G}(n)$.

Ne consegue che:

$$Pr(PrivK^{eav}_{A,\hat{\Pi}}(n) = 1) = Pr(D(w) = 1) = \frac{1}{2}$$

Dove $\hat{\Pi}$ coicide con OTP.

$$Pr(PrivK^{eav}_{A,\Pi^G}(n) = 1) = Pr(D(G(k)) = 1) = \frac{1}{2} + \epsilon(n)$$

Dove $\epsilon(n)$ è trascurabile, questo deriva dall'assunzione che G è un GP. Quindi si avrà:

$$|Pr(D(w) = 1) - Pr(D(G(k)) = 1)| = \epsilon(n)$$

In cui $\epsilon(n)$ è trascurabile e quindi Π^G sicuro contro attacchi passivi.