Se F è una funzione pseudocasuale, allora Π^F è un cifrario sicuro contro attacchi CPA.

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 ricavabile espandendo $PrivK$ con l'evento *Repeat*, si ricava quella in caso di FP.

Si considera prima di tutto lo schema $\hat{\Pi}$ del tutto simile a Π^F ma in cui $\hat{Gen}$ sceglie una funzione casuale f_n tra tutte quelle da $\{0,1\}^n$ a $\{0,1\}^n$ ed $\hat{Enc}$ usa f_n al posto di F_k per cifrare.
È possibile costruire un distinguitore D che utilizzi l'avversario A di $PrivK^{CPA}_{A,\hat{\Pi}}$ generando un r ogni volta che A ha intenzione di effettuare una chiamata all'oracolo, ritornandogli poi il risultato di $O(r)$. A questo punto possono succedere due cose:

- Dopo una chiamata all'oracolo, A ottiene un risultato che contiene lo stesso valore random r utilizzato per cifrare m_b, questo porta A ad una vittoria certa. A può effettuare al massimo un numero polinomiale $q(n)$ di richieste all'oracolo, ognuna delle quali ritorna un valore random lungo n scelto uniformemente, portando ad una probabilità che due r coincidano di: $\frac{q(n)}{2^n}$.
- Dopo una chiamata all'oracolo, il valore r ritornato non è mai stato ritornato prima, questo lascia ad A la stessa probabilità di tirare a caso tra m_0 ed m_1: $\frac{1}{2}$.

Definiamo l'evento **Repeat** = "r appartenente al challenge-chipertext passato ad A viene ritornato anche da (almeno) una chiamata all'oracolo". Quindi abbiamo:
$Pr(PrivK^{CPA}_{A,\hat{\Pi}}(n) = 1) =$
$Pr(PrivK^{CPA}_{A,\hat{\Pi}}(n) = 1 \;\wedge\; \textbf{Repeat}) + Pr(PrivK^{CPA}_{A,\hat{\Pi}}(n) = 1 \;\wedge\; \neg\,\textbf{Repeat}) \;\leq$
$Pr(\textbf{Repeat}) + Pr(PrivK^{CPA}_{A,\hat{\Pi}}(n) = 1 \;\wedge\; \neg\,\textbf{Repeat}) \;\leq$
$\frac{q(n)}{2^n} + \frac{1}{2}$

Sappiamo ora che: $Pr(PrivK^{CPA}_{A,\hat{\Pi}}(n) = 1) \;\leq\; \frac{1}{2} + \frac{q(n)}{2^n}$
Mentre per un cifrario che utilizza F_k sappiamo che: $Pr(PrivK^{CPA}_{A,\Pi^F}(n) = 1) \;\leq\; \frac{1}{2} + \epsilon(n)$ dove $\epsilon(n)$ non sappiamo se sia trascurabile o meno.
Per come è costruito il distinguitore D è chiaro che:

$$Pr(PrivK^{CPA}_{A,\hat{\Pi}}(n) = 1) \;=\; Pr(D^{f_n}(1^n) = 1)$$

$$Pr(PrivK^{CPA}_{A,\Pi^F}(n) = 1) \;=\; Pr(D^{F_k}(1^n) = 1)$$

Avendo assunto essere F una funzione pseudocasuale, allora vale che:

$$|Pr(D^{f_n}(1^n) = 1) - Pr(D^{F_k}(1^n) = 1)| \;\leq\; negl(n)$$

Sostituendo con i valori che abbiamo noti:

$negl(n) \;\geq$
$|Pr(D^{f_n}(1^n) = 1) - Pr(D^{F_k}(1^n) = 1)| \;=$
$|Pr(PrivK^{CPA}_{A,\hat{\Pi}}(n) = 1) - Pr(PrivK^{CPA}_{A,\Pi^F}(n) = 1) \;\geq$
$\frac{1}{2} + \epsilon(n) - \frac{1}{2} - \frac{q(n)}{2^n} =$
$\epsilon(n) - \frac{q(n)}{2^n}$
Quindi: $\epsilon(n) \;\leq\; negl(n) + \frac{q(n)}{2^n}$ è trascurabile.