Se F è pseudocasuale, allora il MAC Π^F è sicuro.

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

Si considera prima di tutto un MAC $\hat{\Pi}$ del tutto simile a Π^F ma in cui viene utilizzata una funzione f_n realmente casuale al posto di F_k pseudocasuale. In questo scenario è chiaro che il valore di $t = f_n(m)$ è uniformemente distribuito in $\{0,1\}^n$ dal punto di vista dell'avversario A, quindi:

$$Pr(MacForge_{A,\hat{\Pi}}(n)) \ \leq \ \frac{1}{2^n}$$

È possibile costruire un distinguitore D che utilizzi l'avversario A di $MacForge_{A,\hat{\Pi}}(n)$. Per come è costruito D si ha che:

$$Pr(MacForge_{A,\hat{\Pi}}(n) = 1) = Pr(D^{f_n(\cdot)}(1^n) = 1) \ \leq \ \frac{1}{2^n}$$

$$Pr(MacForge_{A,\Pi^F}(n) = 1) = Pr(D^{F_k(\cdot)}(1^n) = 1) = \epsilon(n)$$

Quindi:

$$|Pr(D^{f_n(\cdot)}(1^n) = 1) - Pr(D^{F_k(\cdot)}(1^n) = 1)| \ \geq \ \frac{1}{2^n} - \epsilon(n)$$

Avendo assunto che F sia una funzione pseudocasuale il lato destro della disequazione dovrà essere trascurabile quindi $\epsilon(n)$ sarà una funzione trascurabile, confermando la sicurezza di Π^F.