Se Π è sicuro e H è resistente alle collisioni, allora Π^{HM} è sicuro.

In breve: si definisce l'evento *Coll* e si espande la probabilità di forgiatura per il nuovo schema, si valutano poi i risultati in base all'assunzione di resistenza di H alle collisioni e al fatto che Π sia sicuro quindi abbia forgiatura trascurabile.

Si considera un avversario A' per Π^{HM} e si prende in considerazione l'esperimento $MacForge_{A',\Pi^{HM}}(n)$.
Definiamo l'evento **Coll** = "dato $m^* \notin \mathbb{Q}$ il messaggio prodotto da A' in output, esiste un $m \in \mathbb{Q}$ tale che $H^s(m) = H^s(m^*)$".

$Pr(MacForge_{A',\Pi^{HM}}(n) = 1) =$
$Pr(MacForge_{A',\Pi^{HM}}(n) = 1 \ \wedge \ \textbf{Coll}) +$
$Pr(MacForge_{A',\Pi^{HM}}(n) = 1 \ \wedge \ \neg \textbf{Coll}) \ \leq$
$Pr(\textbf{Coll}) + Pr(MacForge_{A',\Pi^{HM}}(n) = 1 \ \wedge \ \neg \textbf{Coll})$

$Pr(\textbf{Coll})$ è trascurabile, in quanto è possibile costruire un avversario C che determini le collisioni nella funzione hash H che abbia come probabilità di successo $Pr(\textbf{Coll})$. C crea un oracolo per A' combinando Mac ed H come in $HMAC$, così facendo A' ha la stessa distribuzione di $MacForge_{A',\Pi^{HM}}$ e C produce una collisione solo quando l'evento **Coll** si verifica:

$$Pr(HashColl_{C,H}(n) = 1) = Pr(\textbf{Coll})$$

$Pr(MacForge_{A',\Pi^{HM}}(n) = 1 \ \wedge \ \neg \textbf{Coll})$ è trascurabile, in quanto è possibile costruire un avversario A, per Π basandoci su A'. Questo avversario effettua l'hashing del messaggio su cui A' vuole interrogare l'oracolo, e passa l'output al reale oracolo, il quale invierà la risposta direttamente ad A'. Quando A' ha trovato la coppia $(m*, t)$ viene passata in output da A dopo aver fatto l'hash di $m*$. Si hanno quindi due probabilità distinte:

$$Pr(MacForge_{A,\Pi}(n) = 1)$$

$$Pr(MacForge_{A',\Pi^{HM}}(n) = 1)$$

Questi due valori non sono uguali perchè i messaggi in cui A' interroga l'oracolo ed $m*$, passato in output come risultato da A', possono essere diversi (quindi avere successo per A') ma dopo l'hashing possono coincidere (avere una collissione e quindi un fallimento per A). Tuttavia però se al secondo elemento si aggiunge il vincolo "$\neg$ **Coll**" le due probabilità si eguaglierebbero e dato che abbiamo assunto Π sicuro il valore è trascurabile:
$Pr(MacForge_{A',\Pi^{HM}}(n) = 1 \ \wedge \ \neg \textbf{Coll}) = Pr(MacForge_{A,\Pi}(n) = 1) = negl(n)$

Confermando così che $Pr(MacForge_{A',\Pi^{HM}}(n) = 1)$ è trascurabile e Π^{HM} sicuro.