Se Π è un MAC sicuro, allora Π^* è anch'esso un MAC sicuro.

In breve: si definiscono due eventi *Repeat* e *NewBlock* e si espande la probabilità di forgiatura per il nuovo schema, si valutano poi i risultati con il teorema del compleanno e la similarità ad una forgiatura per schema a lunghezza fissa.

Lo scopo è dimostrare che: $Pr(MacForge_{A,\Pi^*}(n) = 1) = negl(n)$.
Definiamo l'evento **Repeat** = "l'oracolo in $MacForge_{A,\Pi^*}(n)$ produce due valori r identici". Questo significa che A genera un blocco e la verifica va a buon fine perchè lo stesso k viene ripetuto uguale.
Definiamo l'evento **NewBlock** = "viene prodotto in output un tag (composto da vari sotto-tag) che contiene almeno un sotto-tag diverso da quelli per cui si è interrogato l'oracolo". Questo significa che il blocco in output è valido, ma non necessariamente corretto.

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

$Pr(MacForge_{A,\Pi^*}(n) = 1 \ \wedge \ \textbf{Repeat} \ \wedge \ \textbf{NewBlock}) +$
$Pr(MacForge_{A,\Pi^*}(n) = 1 \ \wedge \ \textbf{Repeat} \ \wedge \ \neg \textbf{NewBlock}) +$
$Pr(MacForge_{A,\Pi^*}(n) = 1 \ \wedge \ \neg \textbf{Repeat} \ \wedge \ \textbf{NewBlock}) +$
$Pr(MacForge_{A,\Pi^*}(n) = 1 \ \wedge \ \neg \textbf{Repeat} \ \wedge \ \neg \textbf{NewBlock}) \ \leq$

$Pr(\textbf{Repeat}) +$
$Pr(MacForge_{A,\Pi^*}(n) = 1 \ \wedge \ \textbf{NewBlock}) +$
$Pr(MacForge_{A,\Pi^*}(n) = 1 \ \wedge \ \neg \textbf{Repeat} \ \wedge \ \neg \textbf{NewBlock}) +$

$Pr(\textbf{Repeat})$ è trascurabile in quanto questo evento per il teorema del compleanno ha probabilità: $\frac{O(q^2)}{2^{\frac{n}{4}}}$ dove q è un polinomio.
$Pr(MacForge_{A,\Pi^*}(n) = 1 \ \wedge \ \neg \textbf{Repeat} \ \wedge \ \neg \textbf{NewBlock})$ ha probabilità 0 in quanto non c'è possibilità di vincere se non avviene una ripetizione ne l'attaccante forgia messaggio e tag che non sia stato prima "richiesto" all'oracolo.
$Pr(MacForge_{A,\Pi^*}(n) = 1 \ \wedge \ \textbf{NewBlock})$ è di fatto trascurabile in quanto ha la stessa probabilità di forgiare un tag per uno schema Mac a lunghezza fissa Π, che abbiamo assunto essere sicuro, quindi con probabilità trascurabile.