Teorema 5.6.

Se Π è un Mac sicuro per Messaggi di lunghezza l e Π_H è resistente a collisioni, Allora la costruzione 5.5 (Hash-and-Mac) è un Mac sicuro per messaggi di lunghezza arbitraria.

Dimostrazione:

Sia:

- Π' la costruzione 5.5 Hash and Mac.
- A' un Adv che attacca Π'.

In una esecuzione di $Mac\text{-}Forge_{A',\Pi'}(n)$ sia:

- $K' = \langle K, S \rangle$
- Q l'insieme dei m per cui A' richiede i tag.
- $m^* \notin Q$ il messaggio per il quale A' produce una contraffazione
- Coll l'evento "c'è un $m \in Q$ per cui $H^S(m) = H^S(m^*)$"

Risulta $Pr[Mac\text{-}forge_{A',\Pi'}(n)=1] =$

$$Pr[Mac\text{-}forge_{A',\Pi'}(n)=1 \wedge Coll] + Pr[Mac\text{-}forge_{A',\Pi'}(n)=1 \wedge \overline{Coll}]$$

$$\leq$$

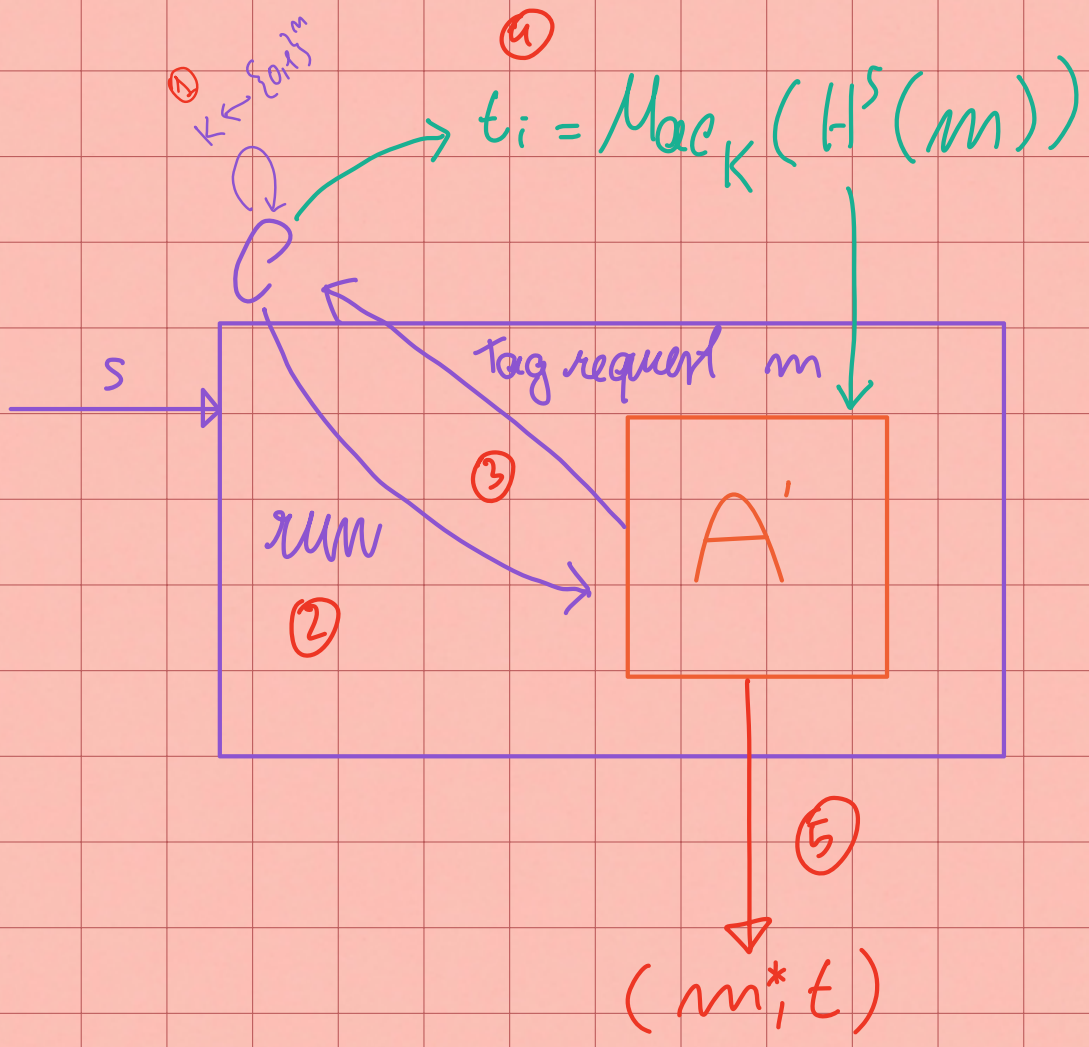
$$Pr[coll] + Pr[Mac\text{-}forge_{A',\Pi'}(n)=1 \wedge \overline{coll}]$$

mostreremo che entrambi i termini sono trascurabili.

$Pr[coll]$:

intuitivamente, questa probabilità è trascurabile perchè Π_H per hp. è resistente a collisioni. Lo mostro formalmente mediante riduzione.

C vuole sfruttare A' che attacca Π' per trovare una collisione in Π_H.



se $\exists i$ t.c. $H^s(m^*) = H^s(m^i) \Rightarrow A$ vince e diamo in output (m^*, t)

C'è come se fosse l'oracolo $Mac_K(\cdot)$ per A', quindi A' pensa di stare giocando nell'esperimento $Mac\text{-}forge_{A',\Pi'}(n)$.

C riesce a trovare una collisione per H^s esattamente quando A vince quindi

$$Pr[\text{Hash-coll}_{G,\Pi_H}(n)=1] = Pr[\text{coll}]$$

per hp. H^s è collision-resistent quindi

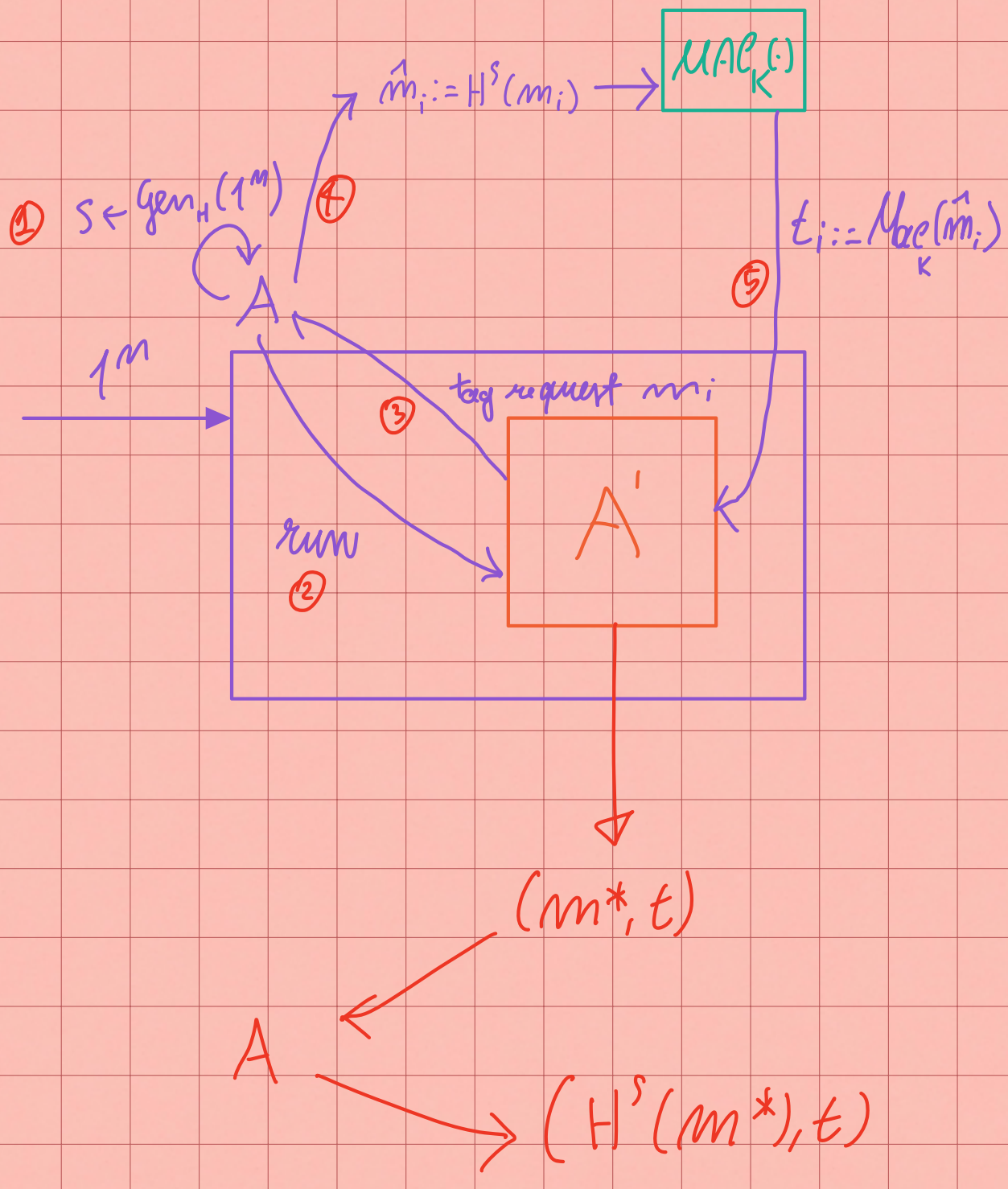
$$negl(n) \geq Pr[\text{coll}]$$

$$Pr[\text{Mac-forge}_{A',\Pi'}(n)=1 \wedge \overline{\text{coll}}]:$$

Per intuire questa quantità è trascurabile per via della sicurezza per hp. del Mac.

Lo mostriamo con un'altra riduzione

A attacca Π in $\text{Mac-forge}_{A,\Pi}(n)$ usando A' come subroutine.



La vista di A' quando eseguita come subroutine di A è distribuita identicamente alla "vista" di A' quando esegue in $Mac\text{-}forge_{A',\Pi'}(n)$.

Quando entrambi gli eventi

"$\text{Mac-forge}_{A',\Pi'}(n)=1$" e "$\overline{\text{Coll}}$" si verificano, A dà in output una falsificazione.

Infatti, poichè Coll non si verifica, $H^s(m^*)$ non è stata una query di A ad $\text{Mac}_k(\cdot)$. Quindi:

$$\Pr[\text{Mac-forge}_{A,\Pi}(n)=1] = \Pr[\text{Mac-forge}_{A',\Pi'}(n)=1 \wedge \overline{\text{Coll}}].$$

Vista l'assunzione che Π è un Mac sicuro, segue che $\exists\, \text{negl}(n)$ t.c.

$$\Pr[\text{Mac-forge}_{A,\Pi}(n)=1] \leq \text{negl}(n)$$

$$\Downarrow$$

$$\Pr[\text{Mac-forge}_{A,\Pi'}(n)=1 \wedge \overline{\text{Coll}}] \leq \text{negl}(n)$$