WE WERE TRYING TO PROVE THE EQUALITY

$$\Pr\left(\text{MacForge}^{B^A,\Pi}(n)=1\right) = \Pr\left(\text{MacForge}^{A,\Pi^H}(n)=1 \wedge \neg \text{coll}_A\right) \quad (*)$$

TO DO THAT, WE FIRST OF ALL HAVE TO BUILD $B^A$ WITH A AS A SUBROUTINE. REMEMBER: A IS ADVERSART FOR $\Pi^H$, WHILE $B^A$ SHOULD BE AN ADVERSARY FOR $\Pi$.

function $B^A(1^n)$ // THIS IS SUPPOSED TO HAVE ACCESS TO AN ORACLE FOR $\text{Mac}^H_k(\cdot)$

- WE FIRST OF ALL GENERATE A (PUBLIC) SEED S BY CALLING $\text{Gen}^H(1^n)$.
- WE CAN CALL THE ADVERSART A ON $1^n$
- WHILE RUNNING, A MAY CALL THE ORACLE FOR $\text{Mac}^H_k(\cdot)$. IF THE PARAMETER OF THE QUERY IS m, WE PASS $H^s(m)$ TO OUR OWN ORACLE, WHICH OF COURSE RETURNS A TAG t WHICH IS FORWARDED TO A.
- A FINALLY OUTPUTS $\langle m^*, t^* \rangle$, AND UNFORTUNATELY, WE CANNOT PASS THEM AS A RESULT. SO, WE HAVE TO PASS $m^*$ TO H, THIS WAY OBTAINING $H^s(m^*)$. WE CAN THEN RETURN $\langle H^s(m^*), t^* \rangle$

WE HAVE TO PROVE THAT EQUALITY (*) HOLDS. WE DO THAT BY SHOWING THAT THE TWO PROBABILISTIC EVENTS UNDER CONSIDERATIONS ARE THE SAME PROBABILISTIC EVENTS

$\Rightarrow$) SUPPOSE THAT $B^A$ WINS AGAINST $\Pi$. THIS MEANS THAT ALSO A WINS, BECAUSE $\text{Mac}^H$ IS DEFINED AS $\text{Mac}^H_{\langle s,k\rangle}(m) = \text{Mac}_k(H^s(m))$. MOREOVER, IF $B^A$ WINS, $H^s(m^*)$ IS DIFFERENT FROM ANY OF THE QUERIES $B^A$ MADE. SO THIS ALSO IMPLIES THAT $\neg\text{coll}_A$ HOLDS, BECAUSE A COLLISION IN THE SENSE OF $\text{coll}_A$ IS PRECISELY WITNESSED BY $m \neq m^*$ SUCH THAT $H^s(m) = H^s(m^*)$

$\Leftarrow$) SUPPOSE NOW THAT A WINS AND FURTHER SUPPOSE THAT $\text{coll}_A$ DOES NOT HOLDS. THIS IMPLIES THAT $m^*$ AS PRODUCED BY A IS DIFFERENT FROM ALL THE m's ON WHICH A QUERIES ITS ORACLE, AND THAT $H^s(m^*) = H^s(m)$ FOR ANY SUCH m (BECAUSE OF $\neg\text{coll}_A$). SO WE ARE IN PRESENCE OF A SUCCESSFUL ATTACK IN THE SENSE OF $B^A$.

WE THEN HAVE TWO PROBABILISTIC EVENTS WHICH HOLD IN PRECISELY THE SAME SITUATIONS, SO (*) MUST HOLD. ⊠