THEOREM

IF F IS A PRF, THEN THE MAC Π^F IS SECURE.

PROOF SKETCH.

- THIS REQUIRES BUILDING AN IDEALIZED MAC $\tilde{\Pi}$, WHICH IS A VARIATION ON Π^F IN WHICH $\tilde{Gen}$ INSTEAD OF SAMPLING K UNIFORMLY AT RANDOM, GENERATES A FUNCTION FROM $\{0,1\}^n$ TO ITSELF AT RANDOM. OF COURSE, THEN $\hat{Mac}(m, f) = f(m)$
- WE CAN PROVE THAT $\tilde{\Pi}$ IS SECURE, BECAUSE GUESSING THE VALUE OF $Mac(k, m)$ WITHOUT KNOWING ANYTHING ABOUT $f(m)$ IS SIMPLY IMPOSSIBLE (UNLESS WITH NEGLIGIBLE PROBABILITY).
- WE HAVE SOMEHOW TO "COMPARE" Π^F AND $\hat{\Pi}$, AND PROVE THAT THEY DO NOT BEHAVE SO DIFFERENTLY, UNLESS F IS NOT PSEUDORANDOM
- AS USUAL, THEN, WE BUILD A DISTINGUISHER D_A FOR F USING AN ADVERSART A FOR Π^F AS A SUBROUTINE, AND FOLLOWING THE IDEA THAT D_A SHOULD CALL A IN SUCH A WAY AS TO PRETEND A IS RUNNING AS PART OF $MacForge_{A,\Pi^F}$
- IN DOING SO, WE GET THESE TWO EQUATIONS:

$$Pr\left(D_A^{F_k(\cdot)}(1^n) = 1\right) = Pr\left(MacForge_{A,\Pi^F}(n) = 1\right) \qquad (*)$$

$$Pr\left(D_A^{f(\cdot)}(1^n) = 1\right) = Pr\left(MacForge_{A,\tilde{\Pi}}(n) = 1\right) = \varepsilon(n) \qquad (**)$$

- IF, NOW Π^F IS NOT SECURE, NAMELY

$$Pr\left(MacForge_{A,\Pi^F}(n) = 1\right) = \eta(n) \qquad \eta \text{ NOT NEGLIGIBLE}$$

THEN WE WOULD HAVE THAT

$$\left| Pr\left(D_A^{f(\cdot)}(1^n) = 1\right) - Pr\left(D_A^{F_k(\cdot)}(1^n) = 1\right) \right| \overset{\text{BY } (*) \text{ AND } (**)}{=}$$

(**) (*)+HYPOTHESIS

$$= \left| \underset{\in NGL}{\varepsilon(n)} - \underset{\notin NGL}{\eta(n)} \right|$$

THIS CANNOT BE IN NGL, NAMELY F CANNOT BE PSEUDORANDOM, CONTRADICTING THE HYPOTHESIS!

$\boxtimes$

THEOREM

IF Π IS A SECURE MAC AND H IS A COLLISION-RESISTANT HASH FUNCTION, THEN Π^H IS SECURE ITSELF AS A MAC.

PROOF

- AS A RECAP, Π^H IS DEFINED AS $(Gen^H, Mac^H, Vrfy^H)$ WHERE $Mac^H(\langle s,k \rangle, m) = Mac(k, H_s(m))$
- BEFORE DOING THE ACTUAL REDUCTION, LET US ANALYSE THE SITUATION FROM THE POINT OF VIEW OF AN ADVERSARY A FOR Π^H. A CAN QUERY THE ORACLE FOR $Mac_k^H(\cdot)$ AND, AT SOME POINT, OUTPUTS $\langle m^*, t^* \rangle$
- LET US DEFINE THE FOLLOWING PROBABILISTIC EVENT:

$$coll_A = \text{“} H_s(m^*) = H_s(m) \text{ FOR SOME } m \neq m^*, m \in Q \text{”}$$

- WE CAN NOW DO SOME EASY PROBABILISTIC REASONING:

$$Pr\left(MacForge_{A,\Pi^H}(n) = 1\right) =$$

$$= Pr\left(MacForge_{A,\Pi^H}(n) = 1 \wedge coll_A\right) + Pr\left(MacForge_{A,\Pi^H}(n) = 1 \wedge \neg coll_A\right)$$

$Pr(A) = Pr(A \wedge B) + Pr(A \wedge \overline{B})$

$$\leq \underbrace{Pr(coll_A)}_{\text{WE WILL PROVE THAT THIS IS NEGLIGIBLE BY A REDUCTION AND EXPLOITING THE COLLISION RESISTANCE OF H}} + \underbrace{Pr\left(MacForge_{A,\Pi^H}(n) = 1 \wedge \neg coll_A\right)}_{\text{WE WILL PROVE THAT THIS IS NEGLIGIBLE BY ANOTHER REDUCTION, AND EXPLOITING THE SECURITY OF } \Pi.}$$

(I) IN THE FIRST REDUCTION, WE BUILD AN ADVERSART C_A FOR THE HASH FUNCTION USING A AS A SUBROUTINE. OUR OBJECTIVE IS TO PROVE THAT

$$Pr\left(HashColl_{C_A,H}(n) = 1\right) = Pr(coll_A)$$

C_A IS DEFINED AS FOLLOWS:

- FIRST, IT PRODUCES A KEY $\langle s,k \rangle$ BY CALLING Gen^H.
- THEN, IT CALLS A ON 1^n AND WAITS UNTIL A PRODUCES A RESULT
- WHENEVER A QUERIES THE ORACLE FOR Mac^H ON m, C PROCEEDS AS FOLLOWS:
  - IT FIRST CALLS H_s ON m AND Mac_k ON THE OBTAINED RESULT
  - IT KEEPS TRACK OF THE MESSAGE m IN AN INTERNAL "DATABASE", CALL IT $\mathbb{D}$, ALSO KEEPING TRACK OF $H_s(m)$
  - FINALLY, IT FORWARDS THE RESULT TO A
- AFTER PERFORMING SOME QUERIES, A FINALLY PRODUCES A PAIR $\langle m^*, t^* \rangle$
- WE THROW AWAY t^*, AND WE COMPUTE $H_s(m^*)$, CHECKING IN $\mathbb{D}$, WHETHER ANY OTHER MESSAGE $m \neq m^*$ IS SUCH THAT $H_s(m) = H_s(m^*)$. IF WE FIND ONE, WE OUTPUT $\langle m, m^* \rangle$, OTHERWISE WE OUTPUT NOTHING

- FROM THE WAY WE HAVE DESIGNED C_A, IT IS EASY TO REALISE THAT

$$Pr\left(HashColl_{C_A,H}(n) = 1\right) = Pr(coll_A)$$

(II) IN THE SECOND REDUCTION, WE INSTEAD WANT TO BUILD AN ADVERSARY B_A FOR Π USING A AS A SUBROUTINE. OUR OBJECTIVE IS, OF COURSE, TO BUILD B_A IN SUCH A WAY THAT

$$Pr\left(MacForge_{B_A,\Pi}(n) = 1\right) = Pr\left(MacForge_{A,\Pi^H}(n) = 1 \wedge \neg coll_A\right)$$

WE HAVE TO DESIGN B_A USING AS A SUBROUTINE. WE WILL DO IT ON FRIDAY.