

LEMMA

THE NEGLIGIBLE FUNCTIONS ARE CLOSED WITH RESPECT TO MULTIPLICATION BY A POLYNOMIAL, I.E. IF $\epsilon \in \text{Neg}_c^s$ AND p IS ANY POLYNOMIAL, THEN $n \mapsto \epsilon(n) \cdot p(n)$ IS NEGLIGIBLE.

PROOF

FROM THE HYPOTHESIS $\epsilon \in \text{Neg}_c^s$ WE KNOW THAT FOR EVERY PAIR OF POLYNOMIALS r, q IT HOLDS THAT

$$\epsilon(n) < \frac{1}{r(n) \cdot q(n)} \quad \forall n \in \mathbb{N} \quad (*)$$

FOR A CERTAIN $N \in \mathbb{N}$. PROVING THAT $\epsilon \cdot p$ IS NEGLIGIBLE AMOUNTS TO CONSIDER ANY POLYNOMIAL q AND PROVE THAT

$$(\epsilon \cdot p)(n) < \frac{1}{q(n)} \quad \text{FOR EVERY } n \in \mathbb{N}. \text{ NOW:}$$

WE CAN EXPLOIT (*) AND PICK $r = p$. THIS WAY

$$(\epsilon \cdot p)(n) = \frac{\epsilon(n) \cdot p(n)}{1} < \frac{1}{p(n) \cdot q(n)} \cdot p(n) = \frac{1}{q(n)} \quad \forall n \geq N \quad M=N$$

THEOREM

IF G IS A PSEUDORANDOM GENERATOR, THEN Π^G IS SECURE AGAINST PASSIVE ATTACKS

PROOF

IT IS DONE BY REDUCTION AND IT HAS THE FOLLOWING STRUCTURE

$$[\exists A \in \text{PPT. BRK}(A, \Pi^G)] \Rightarrow [\exists D \in \text{PPT. BRK}(D, G)]$$

WE BUILD, THEN, OUT OF ANY SUCCESSFUL ADVERSARY A FOR Π^G , A DISTINGUISHER D_A WHICH USES A AS A SUBROUTINE

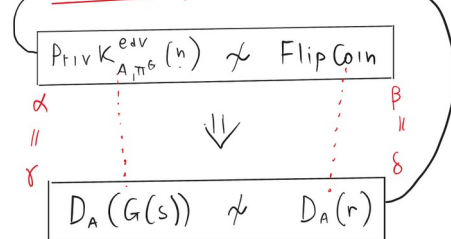
function $D_A(x)$:

$n \leftarrow \ell^{-1}(|x|)$
 $m_0, m_1 \leftarrow A(1^n)$
 if $|m_0| \neq |m_1|$ then return 0
 $b \leftarrow \{0, 1\}$
 $c \leftarrow m_b \oplus x$
 $b^* \leftarrow A(c)$
 return $\neg(b \oplus b^*)$

IF A WORKS IN POLYNOMIAL TIME, THEN D_A WORKS IN PPT TOO!

WE WANT TO PROVE THAT

$$\text{BRK}(A, \Pi^G) \Rightarrow \text{BRK}(D_A, G)$$



THE REST OF THE PROOF IS ABOUT RELATING $\text{PrivK}_{A, \Pi^G}^{adv}(n)$ WITH $D_A(G(s))$ AND Flip Coin WITH $D_A(r)$.

① WE WANT TO PROVE THAT

$$\Pr(\text{PrivK}_{A, \Pi^G}^{adv}(n) = 1) = \Pr(D_A(G(s)) = 1)$$

$\text{PrivK}_{A, \Pi^G}^{adv}(n)$
 $(m_0, m_1) \leftarrow A(1^n)$
 if $|m_0| \neq |m_1|$ then return 0
 $k \leftarrow \{0, 1\}^n$
 $b \leftarrow \{0, 1\}$
 $c \leftarrow m_b \oplus G(k)$
 $b^* \leftarrow A(c)$
 return $\neg(b \oplus b^*)$

$s \leftarrow \{0, 1\}^n$
 $w \leftarrow G(s)$
 $n \leftarrow \ell^{-1}(|w|)$
 $(m_0, m_1) \leftarrow A(1^n)$
 if $|m_0| \neq |m_1|$ then return 0
 $b \leftarrow \{0, 1\}$
 $c \leftarrow m_b \oplus w$
 $b^* \leftarrow A(c)$
 return $\neg(b^* \oplus b)$