## LEMMA

THE NEGLIGIBLE FUNCTIONS ARE CLOSED WITH RESPECT TO MULTIPLICATION BY A POLYNOMIAL, I.E. IF $\varepsilon \in \mathcal{NGL}$ AND $p$ IS ANY POLYNOMIAL, THEN $n \longmapsto \varepsilon(n) \cdot p(n)$ IS NEGLIGIBLE.

PROOF

FROM THE HYPOTHESIS $\varepsilon \in \mathcal{NGL}$ WE KNOW THAT FOR EVERY PAIR OF POLYNOMIALS $r, q$ IT HOLDS THAT

$$\varepsilon(n) < \frac{1}{r(n) \cdot q(n)} \qquad \forall n \geq N \qquad (*)$$

FOR A CERTAIN $N \in \mathbb{N}$. PROVING THAT $\varepsilon \cdot p$ IS NEGLIGIBLE AMOUNTS TO CONSIDER ANY POLYNOMIAL $q$ AND PROVE THAT $(\varepsilon \cdot p)(n) < \frac{1}{q(n)}$ FOR EVERY $n \geq M$. NOW:

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

$$(\varepsilon \cdot p)(n) = \underbrace{\varepsilon(n)}_{(*)} \cdot p(n) < \frac{1}{\cancel{p(n)} \cdot q(n)} \cdot \cancel{p(n)}$$

$$= \frac{1}{q(n)} \qquad \forall n \geq N \qquad M = N$$

$\boxtimes$

## THEOREM

IF $G$ IS A PSEUDORANDOM GENERATOR, THEN $\Pi^G$ IS SECURE AGAINST PASSIVE ATTACKS

PROOF

IT IS DONE BY REDUCTION AND IT HAS THE FOLLOWING STRUCTURE

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

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

```
function D_A(x):
    n ← ℓ^{-1}(|x|)
    m_0, m_1 ← A(1^n)
    if |m_0| ≠ |m_1| then return 0
    b ← {0,1}
    c ← m_b ⊕ x
    b* ← A(c)
    return ¬(b ⊕ b*)
```

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

WE WANT TO PROVE THAT

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

$$\boxed{PrivK^{eav}_{A,\Pi^G}(n) \not\approx FlipCoin}$$

$\alpha = \gamma \qquad \Downarrow \qquad \beta = \delta$

$$\boxed{D_A(G(s)) \not\approx D_A(r)}$$

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

(1) WE WANT TO PROVE THAT

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

```
PrivK^{eav}_{A,Π^G}(n)
    (m_0, m_1) ← A(1^n)
    if |m_0| = |m_1| then return 0
    k ← {0,1}^n
    b ← {0,1}
    c ← m_b ⊕ G(k)
    b* ← A(c)
    return ¬(b ⊕ b*)
```

```
s ← {0,1}^n
w ← G(s)
n ← ℓ^{-1}(|w|)
(m_0, m_1) ← A(1^n)
if |m_0| = |m_1| then
    return 0
b ← {0,1}
c ← m_b ⊕ w
b* ← A(c)
return ¬(b* ⊕ b)
```