THEOREM

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

PROOF

⋮

$$PrivK^{eav}_{A,\Pi^G}(n) \not\approx \text{Flip Coin}$$

LAST FRIDAY $\qquad\Downarrow\qquad$ TODAY!

$$D_A(G(s)) \not\approx D_A(r)$$

$$1/2 = Pr\left(PrivK^{eav}_{A,OTP} = 1\right) \quad = \quad Pr(D_A(r) = 1)$$

$k \leftarrow \{0,1\}^{\ell(n)}$		$w \leftarrow r$
$(m_0, m_1) \leftarrow A(1^n)$		$n \leftarrow \ell^{-1}(\lvert w \rvert)$
$b \leftarrow \{0,1\}$		$(m_0, m_1) \leftarrow A(1^n)$
$c \leftarrow m_b \oplus k$	$=$ EQUIVALENT	$b \leftarrow \{0,1\}$
$b^* \leftarrow A(c)$		$c \leftarrow m_b \oplus w$
return $\neg(b^* \oplus b)$		$b^* \leftarrow A(c)$
		return $\neg(b^* \oplus b)$

$\boxtimes$

EXERCISE 2.6

$$\exists B \in PPT.\ BRK^{LB}(B, \Pi) \Rightarrow \exists A \in PPT.\ BRK^{EAV}(A, \Pi)$$

LET US BUILD THE ADVERSARY A USING B AS A SUBROUTINE

```
function A^FIRST(1^n)
    w ← {0,1}^(ℓ(n)-1)
    return (w0, w1)
function A^SECOND(c)
    return B(c)
```

$$Pr\left(B(Enc(k,m)) = lastbit(m)\right) \not\approx \text{Flip Coin}$$

$$\Downarrow$$

$$Pr\left(PrivK^{eav}_{A,\Pi}(n) = 1\right) \not\approx \text{Flip Coin}$$

THE TWO EQUIVALENCES CAN BE EASILY PROVED BY EXAMINING THE PSEUDOCODE OF A AND B

EXERCISE 2.7

Π SECURE
Θ SECURE $\implies$ $\Pi \# \Theta$ SECURE

$$\exists A.\ BRK(A, \Pi \# \Theta) \Rightarrow \exists B.\ BRK(B, \Pi) \vee \exists B.\ BRK(B, \Theta)$$

THIS IS QUITE DIFFICULT!

$\Pi \# \Theta$ SECURE $\Rightarrow$ Π SECURE $\wedge$ Θ SECURE

$$\exists A.\ BRK(A, \Pi) \vee \exists A.\ BRK(A, \Theta) \Rightarrow \exists B.\ BRK(B, \Pi \# \Theta)$$

THIS IS "A BIT" EASIER BECAUSE ONE CAN PROCEED AS FOLLOWS

$$\exists A.\ BRK(A, \Pi) \Rightarrow \exists B.\ BRK(B, \Pi \# \Theta)$$
$$\exists A.\ BRK(A, \Theta) \Rightarrow \exists B.\ BRK(B, \Pi \# \Theta)$$

THE FIRST ONE, FOR EXAMPLE, CAN BE PROVED BY BUILDING AN ADVERSARY FOR $\Pi \# \Theta$ FROM AN ADVERSARY FOR Π

```
function B^FIRST(1^n)
    (m0^Π, m1^Π) ← A^FIRST(1^n)
    return <m0^Π · m, m1^Π · m>   // m IS ANY FIXED MESSAGE
function B^SECOND(c)
    <c^Π, c^Θ> ← c
    return A^SECOND(c^Π)
```

WHAT IS MISSING (EXERCISE!) IS THAT

$$Pr\left(PrivK^{eav}_{A,\Pi}(n) = 1\right) = \frac{1}{2} + \eta(n) \qquad \eta \text{ IS NOT NEGLIGIBLE}$$

$$\Downarrow$$

$$Pr\left(PrivK^{eav}_{B,\Pi\#\Theta}(n) = 1\right) = \frac{1}{2} + \xi(n) \qquad \xi \text{ IS NOT NEGLIGIBLE}$$

LEMMA

Π^G IS NOT SECURE AGAINST MULTIPLE ENCRYPTIONS

PROOF

LET US DEFINE AN ADVERSARY A AGAINST Π^G, SHOWING THAT

$$Pr\left(PrivK^{mult}_{A,\Pi^G}(n) = 1\right) = \frac{1}{2} + \eta(n) \qquad \text{WHERE } \eta \text{ IS NOT NEGLIGIBLE}$$

```
function A^FIRST(1^n):
    return <(0^ℓ(n), 0^ℓ(n)), (0^ℓ(n), 1^ℓ(n))>
function A^SECOND(c):
    (c1, c2) ← c
    if c1 = c2 then
        return 0
    else
        return 1
```

WE CAN EXPLICITLY ANALIZE THE PROBABILITY $Pr\left(PrivK^{mult}_{A,\Pi^G}(n) = 1\right)$:

$$Pr\left(PrivK^{mult}_{A,\Pi^G}(n) = 1\right) =$$
$$\frac{1}{2} Pr\left(PrivK^{mult}_{A,\Pi^G}(n) = 1 \mid b = 0\right) +$$
$$\frac{1}{2} Pr\left(PrivK^{mult}_{A,\Pi^G}(n) = 1 \mid b = 1\right)$$
$$\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot 1 = \frac{1}{2} + \frac{1}{2} = 1$$

$\boxtimes$

· CONSIDER. $F(k, x) = x$

IS THERE ANY HOPE THAT F IS PSEUDORANDOM?

NO, THERE IS NO HOPE!

A DISTINGUISHER D COULD FOR EXAMPLE:

- QUERY THE ORACLE ON 0^n
- OUTPUT 1 IF THE RESULT OF THE QUERY IS 0^n AND 0 OTHERWISE

$$Pr\left(D^{F_k(\cdot)}(1^n) = 1\right) = 1$$
$$Pr\left(D^{f(\cdot)}(1^n) = 1\right) = 1/2^n$$

THUS:

$$\left| Pr\left(D^{F_k(\cdot)}(1^n) = 1\right) - Pr\left(D^{f(\cdot)}(1^n) = 1\right) \right| = \underbrace{1 - 1/2^n}_{\text{THIS IS NOT NEGLIGIBLE}}$$