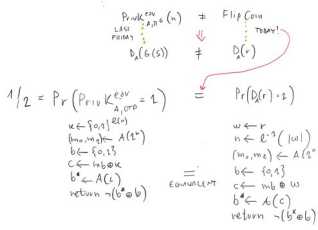


THEOREM
IF \mathcal{E} IS A PSEUDORANDOM GENERATOR, THEN \mathcal{E} IS
SECURE AGAINST MESSAGE ATTACK



EXERCISE 26

\exists B C PPT. BRK(B, Π) \Rightarrow \exists A C PPT. BRK(A, Π)
LET US BUILD THE ADVERSARY A USING B AS A SUBROUTINE

```

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

$$\Pr(B(\text{Enc}(k, m)) = \text{Outbit}(m)) \stackrel{!}{=} \text{Flip Coin}$$

$$\Pr(\text{PRNG}_{A, \Pi}^{\text{EXP}}(n) = 1) \stackrel{!}{=} \text{Flip Coin}$$

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

EXERCISE 27

Π SECURE \Rightarrow $\Pi \# \emptyset$ SECURE
 \emptyset SECURE

$$\exists A. \text{BRK}(A, \Pi \# \emptyset) \Rightarrow \exists B. \text{BRK}(B, \Pi)$$

$$\exists B. \text{BRK}(B, \Pi) \Rightarrow \exists B. \text{BRK}(B, \emptyset)$$

THIS IS QUITE DIFFICULT!

$$\Pi \# \emptyset \text{ SECURE} \Rightarrow \Pi \text{ SECURE} \wedge \emptyset \text{ SECURE}$$

$$\exists A. \text{BRK}(A, \Pi) \Rightarrow \exists B. \text{BRK}(B, \Pi \# \emptyset)$$

$$\exists A. \text{BRK}(A, \emptyset) \Rightarrow \exists B. \text{BRK}(B, \Pi \# \emptyset)$$

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

$$\exists A. \text{BRK}(A, \Pi) \Rightarrow \exists B. \text{BRK}(B, \Pi \# \emptyset)$$

$$\exists A. \text{BRK}(A, \emptyset) \Rightarrow \exists B. \text{BRK}(B, \Pi \# \emptyset)$$

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

```

function B^FIRST(1^n)
  (m_0, m_1) ← A^FIRST(1^n)
  return (m_0, m_1, m) // m IS ANY FIXED MESSAGE
function B^SECOND(c)
  (c^0, c^1) ← c
  return A^SECOND(c^0)
  
```

WHAT IS MISSING (EXERCISE!) IS THAT
 $\Pr(\text{PRNG}_{A, \Pi}^{\text{EXP}}(n) = 1) = \frac{1}{2} + \eta(n)$ η IS NOT NEGLIGIBLE
 $\Pr(\text{PRNG}_{B, \Pi \# \emptyset}^{\text{EXP}}(n) = 1) = \frac{1}{2} + \tilde{\eta}(n)$ $\tilde{\eta}$ IS NOT NEGLIGIBLE

LEMMA

$\Pi \# \emptyset$ IS NOT SECURE AGAINST MULTIPLE ENCRYPTIONS
PROOF

LET US DEFINE AN ADVERSARY A AGAINST $\Pi \# \emptyset$, SHOWING THAT
 $\Pr(\text{PRNG}_{A, \Pi \# \emptyset}^{\text{MULT}}(n) = 1) = \frac{1}{2} + \eta(n)$ WHERE η IS NOT NEGLIGIBLE

```

function A^FIRST(1^n):
  return ((0^n, 0^n), (0^n, 1^n))
function A^SECOND(c):
  (c_1, c_2) ← c
  if c_1 = c_2 then
    return 0
  else
    return 1
  
```

WE CAN EXPLICITLY ANALYZE THE PROBABILITY
 $\Pr(\text{PRNG}_{A, \Pi \# \emptyset}^{\text{MULT}}(n) = 1)$:

$$\Pr(\text{PRNG}_{A, \Pi \# \emptyset}^{\text{MULT}}(n) = 1) = \frac{1}{2} \Pr(\text{PRNG}_{A, \Pi \# \emptyset}^{\text{MULT}}(n) = 1 | b = 0) + \frac{1}{2} \Pr(\text{PRNG}_{A, \Pi \# \emptyset}^{\text{MULT}}(n) = 1 | b = 1)$$

$$\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot 1 = \frac{1}{2} + \frac{1}{2} = 1$$

CONSIDER $F(x, x) = x$
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

$$\Pr(D^{F(\cdot)}(0^n) = 1) = 1$$

$$\Pr(D^{F(\cdot)}(1^n) = 1) = \frac{1}{2}$$

THUS:

$$|\Pr(D^{F(\cdot)}(0^n) = 1) - \Pr(D^{F(\cdot)}(1^n) = 1)| = 1 - \frac{1}{2}$$

THIS IS NOT NEGLIGIBLE