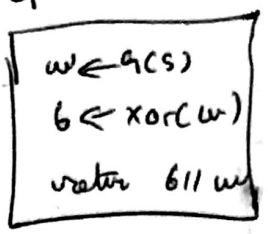
Collabrated w "Biken Maharjen"

Riken Maharjan

Problem 1 (20 points)



To prove

$$L^{G'}_{prg\text{-}real} \approx L^{G'}_{prg\text{-}rand} \quad \text{——— (i)}$$

Suppose $\lambda = |w'|$ ——— (ii)

Thus

$G' : \lambda \longrightarrow (\lambda + 1)$

Now, we will use Hybrid argument to prove (i)

$L^{G}_{prg\text{-}real}$

query ( )
w ← G(s)
b ← xor(w)
return b||w

$\approx$

query ( )
w = query'( )
b ← xor(w)
return b||w

$\diamond$

query'( )
w ← G(s)
return w

∴ Just migrated the code

$\approx$

query ( )
w = query'( )
b ← xor(w)
return b||w

$\diamond$

Random
query'( )
w ← $\{0,1\}^{\lambda}$
return b||w

∴ ~~b~~ because G(s) produce distribution indistinguishable from the random.

$\approx$

query
w ← $\{0,1\}^{\lambda}$
b ← xor(w)
return b||w

∴ just moved the code back

I Skipped some Steps here.

≈ query ()
w ← {0,1}^λ
b ← {0,1}^2
return b || w

∴ as w had pseudorandom distribution. Xoring all the bits of w produced b which was pseudorandom. Hence we replace b Xor(w) with random distribution as both are indistinguishable

≈ query ()
z ← {0,1}^(λ+1)
return z

∴ Just combined them. Independently selecting λ bits and 1 bits is same as selecting λ+1 bits.

$L^{G'}_{prg\text{-}rand}$

Hence $L^{G'}_{prg\text{-}real} \approx L^{G'}_{prg\text{-}random}$

Advantage of A if it tried to distinguish these libraries will be

$$\varepsilon = Pr[A \diamond L^{G'}_{prg\text{-}real}] - Pr[A \diamond L^{G'}_{prg\text{-}rand}]$$

$$= \frac{1}{2^\lambda} - \frac{1}{2^{\lambda+1}}$$

$$= \frac{2-1}{2(2^\lambda)}$$

$$= \frac{1}{2(2^\lambda)}$$

Using def 4.2 from "Jay of cryptography"

$f(\lambda) = \frac{1}{2(2^\lambda)}$

$\lim_{\lambda \to \infty} P(\lambda) \cdot f(\lambda) = 0$

$\lim_{\lambda \to \infty} \frac{\lambda^c}{2(2^\lambda)}$

$= 0$

Hence $f(\lambda)$ or $\frac{1}{2(2^\lambda)}$ is negligible

The advantage is negligible

Problem 2

To prove

$$L^{\bar{G}}_{Prg\text{-}real} \approx L^{\bar{G}}_{Prg\text{-}rand}$$

Note

$|w| = \lambda$

Given

$$L^{G}_{Prg\text{-}real} \approx L^{G}_{Prg\text{-}rand}$$

Note

$|s| = \lambda$

$L^{\bar{G}}_{Prg\text{-}real}$

```
query():
w ← G(s)
w̄ = 1 - w
return (w̄)
```

$\approx\approx$

L

```
query():
w ← query'()
w̄ = 1 - w
return (w̄)
```

$\diamond$

$L^{G}_{Prg\text{-}real}$

```
query'( ):
w ← G(s)
return (w)
```

$\approx\approx$

L

```
query():
w ← query'()
w̄ = 1 - w
return (w̄)
```

$\diamond$

$L^{G}_{Prg\text{-}rand}$

```
query'( ):
w ← {0,1}^λ
return w
```

$\therefore$ Given $L^{G}_{Prg\text{-}real} \approx L^{G}_{Prg\text{-}rand}$

$\approx\approx$

L'

```
query():
w ← {0,1}^λ
w̄ = 1 - w
return(w̄)
```

$\therefore$ Just moving the code

$\approx\approx$

```
query():
w ← {0,1}^λ
w̄ ← {0,1}^λ
return (w̄)
```

$\therefore$ as w was random. $\bar{w}$ would be like one $ coin toss selecting a side opposite of the thing you get on the toss.
for instance coin has head when toss select fail.

$L^{\bar{G}}_{Prg\text{-}rand}$

$\approx\approx$

```
query():
w̄ ← {0,1}^λ
return(w̄)
```

$\therefore$ w was not used in selecting $\bar{w}$. So useless code was removed

$= Pr[A \diamond L^{\bar{G}}_{Prg\text{-}real} \to 1] - Pr[A \diamond L^{\bar{G}}_{Prg\text{-}rand} \to 1]$

$= \frac{1}{2^{|s|}} - \frac{1}{2^{|s|}}$

$= \frac{1}{2^{\lambda}} - \frac{1}{2^{\lambda}}$

$= 0$

Hence $L^{\bar{G}}_{Prg\text{-}real} \approx L^{\bar{G}}_{Prg\text{-}rand}$

Problem 3

To prove

$$L^{q_3}_{Prg-real} \approx L^{q_3}_{Prg-rand}$$

Given

$$L^{q_1}_{Prg-real} \approx L^{q_1}_{Prg-rand}$$

& $$L^{q_2}_{Prg-real} \approx L^{q_2}_{Prg-rand}$$

$L^{q_3}_{Prg-real}$

```
query():
(s1, s2) := s3
w1 ← q(s1)
w2 ← q(s2)
return (w1 || w2)
```

$\approx$

```
query():
(s1, s2) := s3
z ← query'()
return z
```

$\diamond$

```
query'():
z ← {0,1}^(2λ+2ℓ)
return (z)
```

Random

- ∴ moving code +
- q_1 is indistinguishable from Random.
- q_2 is indistinguishable from Random.
- Hence replace them with Random distribution.
- Also selecting $2\lambda+2\ell$ bits randomly twice is same as selecting $2\lambda+2\ell$ bits randomly once

$\approx$

$L^{q_3}_{Prg-rand}$

```
query()
z ← {0,1}^(2λ+2ℓ)
return (z)
```

$$Pr\left[A \diamond L^{q_3}_{Prg-real}\right] - Pr\left[A \diamond L^{q_3}_{Prg-rand}\right]$$

$$= Re\ \frac{1}{2^{2\lambda}} - \frac{1}{2^{2\lambda+2\ell}}$$

$$= \frac{2^{2\ell} - 1}{2^{2\ell}\left(2^{2\lambda}\right)}$$

← This is negligible

Hence, A's advantage is negligible

4a)

- $Pr[A \diamond L^q_{dn\text{-}real} \to 1] = \frac{q-1}{q} Pr[A \diamond L^q_{dn\text{-}rand\text{-}but\text{-}not} \to 1] + \frac{1}{q} Pr[A \diamond L^q_{dn\text{-}re} \to 1]$

from DDH assumption —(*)

$$Pr[A \diamond L^q_{dn\text{-}rand} \to 1] \approx_c Pr[A \diamond L^q_{dn\text{-}real} \to 1]$$

So plugging this in our (*) gives us

$$\Rightarrow Pr[A \diamond L^q_{dn\text{-}real} \to 1] \approx \frac{q-1}{q} Pr[A \diamond L_{dn\text{-}rand\text{-}but\text{-}not} \to 1] + \frac{1}{q} Pr[A \diamond L^q_{dn\text{-}real} \to 1]$$

Subtracting both side by $\frac{1}{q} Pr[A \diamond L^q_{dn\text{-}rand} \to 1]$

$$\Rightarrow Pr[A \diamond L^q_{dn\text{-}real} \to 1] - \frac{1}{q} Pr[A \diamond L^q_{dn\text{-}real} \to 1] \approx \frac{q-1}{q} Pr[A \diamond L_{dn\text{-}rand\text{-}but\text{-}not} \to 1]$$

$$\Rightarrow \frac{q-1}{q} Pr[A \diamond L^q_{dn\text{-}real} \to 1] \approx \frac{q-1}{q} Pr[A \diamond L_{dn\text{-}rand\text{-}but\text{-}not\text{-}real} \to 1]$$

$$\Rightarrow \boxed{Pr[A \diamond L^q_{dn\text{-}real} \to 1] \approx Pr[A \diamond L_{dn\text{-}ran\text{-}but\text{-}not\text{-}ran} \to 1]}$$

So they are "approximately" same. Their advantage is close to zero or negligible

Thus $\boxed{L^q_{dn\text{-}real} \approx L^q_{dn\text{-}rand\text{-}but\text{-}not\text{-}real}}$

4)

b)

Claim 2

For a fixed $a, b, c \neq_q ab$

$$Pr\left[(x,y) = (d+be,\ ad+ce)\right] =$$

$$Pr\left[(x-y) = ad^2 + bce + adbe + bce^2\right]$$

$$= \frac{1}{q^2} \quad \because \text{as there is only two variables } d \text{ and } e \text{ and all other variables are fixed.}$$

Hence x, y is also from uniform distribution when $c \neq_q ab$

(30)

From previous Homework we know if we have a cyclic group and prime q elements in the set G.

We can do,

$$x \equiv_q y \iff g^x \equiv_{q+1} g^y \quad \text{(*)} \qquad \text{Proof previous HW}$$

we can use this fact to create $\mathcal{L}$ that exploits this

$\mathcal{L}^q_{\text{multi DH-real}}$

```
Query():
(X_1, ..., X_k) ← G^k
a ← Z_q
Y_1 := X_1^a, ..., Y_k = X_k^a
return (X_1, ..., X_k, Y_1, ..., Y_k)
```

$\approx$

$\mathcal{L}$

```
Query'()
(A, B, C) ← Query''()
g is public
(d_1, ..., d_k) ← Z_q
(e_1, ..., e_k) ← Z_q
∀_i := 1..k
  X_i = (B)^{e_i} (g)^{d_i}
  Y_i = (A)^{d_i} (C)^{e_i}
return (X_1, ..., X_k, Y_1, ..., Y_k)
```

random

Pseudorandom as $C = ab$

$\diamond$

$\mathcal{L}^q_{\text{dh-real}}$

```
Query''()
a ← Z_q
b ← Z_q
c := ab mod q
return (g^a, g^b, g^c)
```

using (*)

$\therefore x = ad + ce$

$$g^x = \left(g^a\right)^d \left(g^c\right)^{e_1}$$

$$g^x \equiv X_i = (A)^{d_i} (C)^{e_i}$$

Same way $Y_i = (A)^{d_i} (C)^{e_i}$

Y_i can be pseudorandom if $C = ab$ (q)

$\approx$ $L_{\diamond}$ $L^{q}_{Ldh\text{-}random\_but\text{-}not\text{-}real}$

```
Query''():
  a ← Zq
  b ← Zq
  c ← Zq - {ab}
  return (g^a, g^b, c)
```

from (4. a)

L

```
Query():
  (A, B, ) ← Query''()
  g in public
  (d_1 ... d_k) ← Z_q
  (e_1 ... e_k) ← Z_q
  ∀ i = 1..k
    x_i = (B)^{e_i} (g)^{d_i}
    y_i = (A)^{d_i} (g)^{e_i}
  return (x_1 ... x_k, y_1 .. y_k)
```

$\approx$ $\diamond$ $L^{q}_{Ldh\text{-}random\text{-}but\text{-}not\text{-}real}$

$\therefore$ both X and Y have random dist as $c \neq ab$

$L^{q}_{multiDH\text{-}random}$

```
Query():
  (X_1, ..., X_k) ← G^k
  (Y_1, ..., Y_k) ← G^k
  return (X_1 ... X_k, Y_1 .. Y_k)
```

$\approx$

$\therefore$ as X and Y both were random we can replace $L^{q}_{\diamond}$ $L^{q}_{Ldh\text{-}random\_but\_not\_real}$ with $L^{q}_{multiDH\text{-}random}$

Hence

$$L^{q}_{multiDH\text{-}real} \approx L^{q}_{multiDH\text{-}random}$$