CS 427

HW 3

Zongyan Lu

1. G is a secure PRG.

Define $G'(s) = G(s) \oplus G(0^\lambda)$.

prove G' is also secure PRG.

For equation. $G'(s) = G(s) \oplus G(0^\lambda)$

Take $G(0^\lambda)$ at both side

$G(0^\lambda) \cdot G'(s) = G(s) \oplus G(0^\lambda) \oplus G(0^\lambda)$

$\Rightarrow G(s) = G'(s) \oplus G(0^\lambda)$.

By definition. Since G is secure PRG.

The output of $G(s)$ and $G(0^\lambda)$ are uniform distribution.

And we know, the outputs of PRG are indistinguishable from the uniform distribution.

So, $G'(s)$ supposes be Secure PRG

2. Define $G'(s) = G(s) \| G(G(s))$.

Show G' is not secure PRG, even if G is.

```
$\mathcal{L}^{G}_{\text{prg-real}}$
Query():
    $s \leftarrow \{0,1\}^\lambda$
    return $G(s)$
```

```
$\mathcal{L}^{G}_{\text{prg-rand}}$
Query():
    $r \leftarrow \{0,1\}^{\lambda+l}$
    return $r$
```

```
$\mathcal{L}^{G'}_{\text{prg-real}}$
Query():
    $s \leftarrow \{0,1\}^\lambda$
    $x := G(s)$
    $y := G(s)$
    $z := G(y)$
    return $x \| z$
```

```
$\mathcal{L}^{G'}_{\text{prg-rand}}$
Query():
    $x := \{0,1\}^{\lambda+l}$
    $z := \{0,1\}^{\lambda+2l}$
    return $x \| z$
```

Construct an attack

```
A:
    x||y := Query().
    return G(x) ≟ y.
```

→ link to G'-prg-real.
$Pr[\text{output true}] = 1$.

→ link to G'-prg-rand.
$pr[\text{output true}] = \frac{1}{2^{\lambda+2l}}$

— So, the difference of possibilities for two cases. is not negligible.

So, G' is not secure.

Also, for the quation. Even G(s) is secure.
It is impossible to prove G(s) and G(G(s)) are both pseudo-random.
Because they relational.

3. F is secure PRF.

$F'(k,x) = \overline{F(k,x)}$ (flip every bit).
prove F' is also PRF

```
L^F_prf-real
    k ← {0,1}^λ
    Lookup(x ∈ {0,1}^in):
        return F(k,x)
```

```
L^F_prf-rand
    T := empty array
    Lookup(x ∈ {0,1}^in):
        if T[x] undef
            T[x] ← {0,1}^out
        return T[x].
```

Based on the equation, we get.

Want to show:

```
k ∈ {0,1}^λ.
Lookup(x):
```

~

```
L^F̄_prf-rand
    T := empty array
```

```
  y = F(k,x)
  ret $\overline{y}$
```

≈

```
T := empty array
Lookup(x∈{0,1}^in):
  if T[x] undef.
    T[x] ← {0,1}^out
  return $\overline{T[x]}$
```

```
k ← {0,1}^λ
Lookup(x):
  y = F(k,x)
  ret $\overline{y}$
```

≡

```
T := empty array.
Lookup(x ∈ {0,1}^in):
  if T[x] undef.
    T[x] ← {0,1}^λ
  return $\overline{T[x]}$
```

≈

```
Lookup(x):
  y := Lookup_F(x)
  ret $\overline{y}$
```

◇

```
$\mathcal{L}^F_{prf\text{-}real}$
k ← {0,1}^λ
Lookup(x∈{0,1}^in):
  return F(k,x)
```

≈

```
T ← Empty
Lookup(x):
  if T[x] undef
    T[x] ← $
  y := T[x]
  ret $\overline{y}$
```

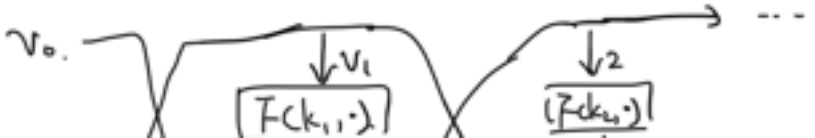
≡

```
T ← Empty.
Lookup(x):
  if T[x] undef
    T[x] ← $
  ret $\overline{T[x]}$
```

So, the F' is a secure PRF.

4. Show:

2-round keyed Feistel cipher cannot be a secure PRP.



```
F_T((k₁,k₂), v₀||v₁):
  for i=1 to 2
    v_{i+1} := F(k_i, v_i) ⊕ v_{i-1}
```

```
    return $v_r \| v_{r+1}$
```

Theoritically. 2 Round Feistel:

$$(L, R) \longrightarrow (R, f(R) \oplus L).$$
$$\longrightarrow (f(R) \oplus L, f(f(R) \oplus L) \oplus R).$$

$\mathcal{L}_{\text{Feistel cipher-rand}}$

```
Query(L.R.):
    $A := f(R) \oplus L$
    $B := f(f(R) \oplus L) \oplus R.$
    return $(A, B)$
```

$\mathcal{L}_{\text{Feistel cipher-real.}}$

```
Query(L.R):
    return $\{0,1\}^\lambda$
```

Construct an attack.

$A.$

```
$L \leftarrow \{0,1\}^\lambda$
$R \leftarrow \{0,1\}^\lambda$
$L' \leftarrow \{0,1\}^\lambda$
$(A_1, B_1) = \text{Query}(L, R)$
$(A_2, B_2) = \text{Query}(L', R).$
return $A_1 \oplus A_2 \overset{?}{=} L \oplus L'$
```

Case 1:

$A \diamond \mathcal{L}_{\text{Feistel cipher-rand}}$

Query 1:

$$(L, R) \to (\overset{A_1}{f(R) \oplus L}, \overset{B_1}{f(f(R) \oplus L) \oplus R})$$

Query 2:

$$(L', R) \to (\overset{A_2}{f(R) \oplus L'}, \overset{B_2}{f(f(R) \oplus L') \oplus R})$$

So, $A_1 \oplus A_2 = (f(R) \oplus L) \oplus (f(R) \oplus L')$

$$= f(R) \oplus f(R) \oplus L \oplus L'$$

$$= \underline{L \oplus L'} \longrightarrow \text{So, the output always } \underline{\underline{1.}}$$

Case 2:

$A \diamond \mathcal{L}_{\text{Feistel cipher-real.}}$

Output as $\frac{1}{2^\lambda}$

So, these two cases are not negligible.

So. the 2round feistel cipher does not secure.