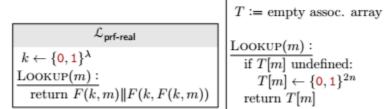
CS427

Homework 6

 $\mathcal{L}_{prf-rand}$

1. Libraries:



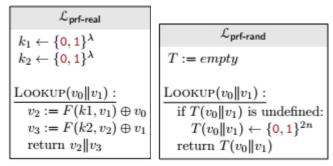
Calling program:

```
F'
m \leftarrow \{0, 1\}^{\lambda}
z := Lookup(m)
a||b := Lookup(z)
if b == F(k, z)
return 1
return 0
```

Advantage:

```
Pr[F' \diamond prf-real == 1] == 1
Pr[F' \diamond prf-rand == 1/2^{\lambda}
1-1/2^{\lambda}, non-negligible
```

2. Libraries



Calling Program:

```
\frac{\text{Call}()}{x \leftarrow \{0, 1\}^{\lambda}}
y \leftarrow \{0, 1\}^{\lambda}
a, b := Lookup(x, y)
w, z := Lookup(a, y)
if (x == w)
return 1
return 0
```

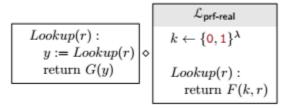
Advantage:

```
Pr[Call \Diamond prf-real == 1] = 1
Pr[Call \Diamond prf-rand == 1] == 1/2^{\lambda}
1 - 1/2^{\lambda}, non-negligible
```

3. Starting function:

$$k \leftarrow \{0,1\}^{\lambda}$$
 $Lookup(r) :$
 $return \ G(F(k,r))$

First, we will factor out the F function into a separate subroutine. This does not change how the library operates.



Second, we will swap prf-real for prf-rand, which will have no effect on the operation of the library.

```
 \begin{array}{c} \mathcal{L}_{\mathsf{prf-rand}} \\ Lookup(r) : \\ y := Lookup(r) \\ \mathsf{return} \ G(y) \\ \end{array} \diamond \begin{array}{c} \mathcal{L}_{\mathsf{prf-rand}} \\ T := undefined \\ \\ Lookup(r) : \\ \mathsf{If} \ (\mathsf{T}[r] == undefined) : \\ T[r] \leftarrow \{\mathtt{0},\mathtt{1}\}^{\lambda} \\ \mathsf{return} \ T[r] \end{array}
```

Now, we can inline the subroutine, changing nothing about the operation of the library.

```
T := undefined
\frac{Lookup_F(r) :}{\text{If } (T[r] == undefined):}
T[r] \leftarrow \{0, 1\}^{\lambda}
y := T[r]
return G(y)
```

Next, we can add T' and apply G to it. This means G is called once and stored in T'[r], instead of calling G every time the library is run. This changes nothing about how the library operates.

```
T := undefined
T' := undefined
\frac{Lookup_F(r) :}{\text{If } (T[r] == undefined):}
T[r] \leftarrow \{0, 1\}^{\lambda}
T'[r] := G(T[r])
\text{return } T'[r]
```

Then, we can omit T because it is not serving any purpose anymore. This does not change how the library operates.

```
T' := undefined
\frac{Lookup_F(r) :}{\text{If } (T'[r] == undefined):}
y \leftarrow \{0, 1\}^{\lambda}
T'[r] := G(y)
\text{return } T'[r]
```

Now we can factor out the lines within the if statement into a subroutine, which changes nothing about the operation of the library.

Through the security of prg, we can swap prg-real for prg-rand, which changes nothing about the operation of the library.

Finally, we can inline the prg-rand subroutine, and end up with our final function, which is

indistinguishable from our starting function.

```
T := undefined \frac{Lookup(r)}{\text{if T'}[r] == undefined:} T'[r] \leftarrow \{\mathbf{0}, \mathbf{1}\}^{\lambda + \ell} \text{return } T'[r]
```