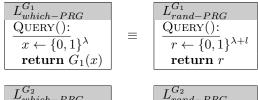
6.1 Distinction between PRGs



$$\frac{L_{which-PRG}^{G_2}}{QUERY():} \\
\frac{QUERY():}{x \leftarrow \{0,1\}^{\lambda}} \\
\mathbf{return} \ G_2(x)$$

$$\equiv \frac{L_{rand-PRG}^{G_2}}{QUERY():} \\
r \leftarrow \{0,1\}^{\lambda+l} \\
\mathbf{return} \ r$$

Because we know that G_1 (respectively G_2) is secure those two libraries are equivalent and indistinguishable.

Because it is obvious that these so created "random" PRGs of G_1 and G_2 are the same this indistinguishability is also guaranteed for the starting libraries.

6.2 Find the key

We consider the following distinguisher:

Distinguisher A pick $s \in \{0,1\}^{\lambda}$ x = LOOKUP(s)get key k y = F(k,s)return x = y

First we will pick a random seed and put in either the Lookup and the F library. The distinguisher will get the key by its property stated in the exercise, with probability p, which is also given to the F function. In the end we will check both outputs.

$$\begin{array}{c|c} \textbf{Distinguisher } A \\ \textbf{pick } s \in \{0,1\}^{\lambda} \\ x = \text{LOOKUP}(s) \\ \textbf{get key } k \\ y = F(k,s) \\ \textbf{return } x = y \end{array} \diamond \begin{array}{c} L_{PRF-real}^{F} \\ k \leftarrow \{0,1\}^{\lambda} \\ \hline L_{PRF-real}^{F} \\ k \leftarrow \{0,1\}^{\lambda} \\ k \leftarrow \{0,1\}^{\lambda} \\ L_{PRF-real}^{F} \\ k \leftarrow \{0,1\}^{\lambda} \\ L_{PRF-real}^{F} \\ k \leftarrow \{0,1\}^{\lambda} \\ L_{PRF-real}^{F} \\ k \leftarrow \{0,1\}^{\lambda} \\ k \leftarrow \{0,1\}^{\lambda}$$

It is obvious that the algorithm combined with $L_{PRF-real}^F$ will always output 1, if the right key was found with probability p, because the LOOKUP and F function are doing exactly the same and therefore their output will be equal.

$$\begin{array}{c} \textbf{Distinguisher A} \\ \textbf{pick } s \in \{0,1\}^{\lambda} \\ x = \text{LOOKUP}(s) \\ \textbf{get key } k \\ y = F(k,s) \\ \textbf{return } x = y \end{array} \Leftrightarrow \begin{array}{c} L_{PRF-rand}^{F} \\ T := empty \ associated \ array \\ \hline \textbf{LOOKUP}(x) \\ \textbf{if } T[x] \ undefined: \\ T[x] \leftarrow \{0,1\}^{out} \\ \textbf{return } T[x] \end{array}$$

This combination will only return 1 if the entry in T will be exactly the same as the F function output. The probability for this will be $\frac{1}{2^{out}}$. For the advantage, we get:

$$Bias(A) = |P[A \diamond L_{PRF-Real}^F \rightarrow 1] - P[A \diamond L_{PRF-Rand}^F \rightarrow 1]| = p - \frac{1}{2^{out}}$$

, which is clearly not negligible, because p is non-negligible.

6.3 Build a distinguisher

We consider the following distinguisher:

```
Distinguisher A

pick s \in \{0, 1\}^{\lambda}

\overline{s} = s \oplus 1^{\lambda}

x_1 \| y_1 = \text{Lookup}(s)

x_2 \| y_2 = \text{Lookup}(\overline{s})

return (x_1 = y_2) \land (x_2 = y_1)
```

First we will pick a random seed and calculate its complement. Both seeds are then encrypted the PRF F'.

```
Distinguisher A

pick s \in \{0,1\}^{\lambda}

\overline{s} = s \oplus 1^{\lambda}

x_1 \| y_1 = \text{LOOKUP}(s)

x_2 \| y_2 = \text{LOOKUP}(\overline{s})

return (x_1 = y_2) \land (x_2 = y_1)
```

It is obvious that our algorithm will always return 1 if we use $L_{PRF-real}^{F'}$, because first it will compute $(F(k, \overline{s}) || F(k, \overline{s}))$ and compare it with $(F(k, \overline{s}) || F(k, \overline{s}))$ which is the same as $(F(k, \overline{s}) || F(k, \overline{s}))$.

$$\begin{array}{c} Distinguisher \ A \\ \textbf{pick} \ s \in \{0,1\}^{\lambda} \\ \overline{s} = s \oplus 1^{\lambda} \\ x_1 \| y_1 = \text{Lookup}(s) \\ x_2 \| y_2 = \text{Lookup}(\overline{s}) \\ \textbf{return} \ (x_1 = y_2) \land (x_2 = y_1) \end{array}$$

$$L_{PRF-rand}^{F'}$$

$$T := empty \ associated \ array$$

$$\frac{\text{Lookup(x)}}{\text{if} \ T[x] \ \text{undefined:}}$$

$$T[x] \leftarrow \{0,1\}^{out}$$

$$\text{return} \ T[x]$$

The algorithm combined with $L_{PRF-rand}^{F'}$ will only return 1 if for s and \overline{s} the strings saved in T consist of the same two "stringparts" but in the opposite different sequence. The probability for this is $\frac{1}{2^{out}}$

For the advantage, we get:

$$Bias(A) = |P[A \diamond L_{PRF-Real}^F \rightarrow 1] - P[A \diamond L_{PRF-Rand}^F \rightarrow 1]| = 1 - \frac{1}{2^{out}}$$

, which is clearly not negligible.