16-124-836
Marcel Zauder

6.1 Distinction between PRGs

$L^{G_1}_{which-PRG}$
QUERY():
$x \leftarrow \{0,1\}^\lambda$
return $G_1(x)$

$\equiv$

$L^{G_1}_{rand-PRG}$
QUERY():
$r \leftarrow \{0,1\}^{\lambda+l}$
return r

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

$\equiv$

$L^{G_2}_{rand-PRG}$
QUERY():
$r \leftarrow \{0,1\}^{\lambda+l}$
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 $s \in \{0,1\}^\lambda$
$x = \text{LOOKUP}(s)$
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.

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

$\diamond$

$L^F_{PRF-real}$
$k \leftarrow \{0,1\}^\lambda$
LOOKUP(x)
return $F(k,x)$

It is obvious that the algorithm combined with $L^F_{PRF-real}$ 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.

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

$\diamond$

$L^F_{PRF-rand}$
T := *empty associated array*
LOOKUP(x)
if $T[x]$ undefined:
$T[x] \leftarrow \{0,1\}^{out}$
return $T[x]$

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:

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

, 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 $(x_1 = y_2) \wedge (x_2 = y_1)$

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 $(x_1 = y_2) \wedge (x_2 = y_1)$

$\diamond$

$L^{F'}_{PRF-real}$
$k \leftarrow \{0,1\}^\lambda$
<u>Lookup(x)</u>
return $(F(k,x) \| F(k,\overline{x}))$

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

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 $(x_1 = y_2) \wedge (x_2 = y_1)$

$\diamond$

$L^{F'}_{PRF-rand}$
T := *empty associated array*
<u>Lookup(x)</u>
if $T[x]$ undefined:
$T[x] \leftarrow \{0,1\}^{out}$
return $T[x]$

The algorithm combined with $L^{F'}_{PRF-rand}$ 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:

$$Bias(A) \ = \mid P[A \diamond L^F_{PRF-Real} \rightarrow 1] - P[A \diamond L^F_{PRF-Rand} \rightarrow 1] \mid = \ 1 - \frac{1}{2^{out}}$$

, which is clearly not negligible.