Institute of Computer Science, University of Bern
Cryptography, HS 2019

Prof. Christian Cachin
Luca Zanolini, Ignacio Amores Sesar

Exercise 5

5.1 A searching adversary (3 pts)

Let $G : \{0,1\}^\lambda \to \{0,1\}^{\lambda+\ell}$ be an injective (i.e., 1-to-1) PRG. Consider the following distinguisher:

$\mathcal{A}$
$x :=$ QUERY()
for all $s' \in \{0,1\}^\lambda$:
if $G(s') = x$ then return 1
return 0

1. What is the advantage of $\mathcal{A}$ in distinguishing $\mathcal{L}^G_{\text{prg-real}}$ and $\mathcal{L}^G_{\text{prg-rand}}$? Is it negligible?
2. Does this contradict the fact that G is a PRG? Why or why not?
3. What happens to the advantage if G is not injective?

5.2 Lucky gambler (2 pts)

Let $G : \{0,1\}^\lambda \to \{0,1\}^{\lambda+\ell}$ be an injective (i.e., 1-to-1) PRG. Consider the following distinguisher:

$\mathcal{A}$
$x :=$ QUERY()
$s' \leftarrow \{0,1\}^\lambda$
return $G(s) = x$

What is the advantage of $\mathcal{A}$ in distinguishing $\mathcal{L}^G_{\text{prg-real}}$ and $\mathcal{L}^G_{\text{prg-rand}}$? Is it negligible?

Hint: When computing $\Pr[\mathcal{A} \diamond \mathcal{L}^G_{\text{prg-rand}} \to 1]$, separate the probabilities based on whether x is a possible output of G or not.

5.3 PRGs (2 pts)

Let $G : \{0,1\}^\lambda \to \{0,1\}^{3\lambda}$ be a secure length-tripling PRG. For each function below, state whether it is also a secure PRG. If the function is a secure PRG, give a proof. If not, then describe a successful distinguisher and explicitly compute its advantage. When we write $a||b||c := G(s)$, each of a, b, c have length λ.

$A(s)$:
$x\|\|y\|\|z = G(s)$
return $G(x)\|\|G(z)$

$B(s)$:
$x\|\|y\|\|z = G(s)$
return $x\|\|y$

$C(s)$:
$x = G(s)$
$y = G(s)$
return $x\|\|y$

$D(s)$:
$x = G(s)$
$y = G(o^\lambda)$
return $x\|\|y$

$E(s)$:
$x = G(s)$ $y = G(o^\lambda)$ return $x \oplus y$

$F(s_L \| s_R)$:
$x = G(s_L)$ $y = G(s_R)$ return $x \oplus y$

$H(s_L \| s_R)$:
$x = G(s_L)$ $y = G(s_R)$ return $x \| y$

Note that $F : \{0,1\}^{2\lambda} \to \{0,1\}^{3\lambda}$ and $H : \{0,1\}^{2\lambda} \to \{0,1\}^{6\lambda}$.

5.4 Breaking a PRG candidate (3 pts)

1. Let f be any function. Show that the following function G is **not** a secure PRG, no matter what f is. Describe a successful distinguisher and explicitly compute its advantage:

$G(s)$:
return $s \| f(s)$

2. Let $G : \{0,1\}^\lambda \to \{0,1\}^{\lambda+\ell}$ be a candidate PRG. Suppose there is a polynomial-time algorithm V with the property that it inverts G with non-negligible probability. That is,

$$P[V(G(s)) = s] > \textit{negl}(\lambda).$$

Show that if an algorithm V exists with this property, then G is not a secure PRG. In other words, construct a distinguisher contradicting the PRG-security of G and show that it achieves non-negligible distinguishing advantage.

Note: Don not assume anything about the output of V other than the property shown above. In particular, V might very frequently output the "wrong" thing.