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

Prof. Christian Cachin
Luca Zanolini

Exercise 6

6.1 Distinction between PRGs (4 pts)

A frequently asked question in online discussions on cryptography is whether it's possible to determine which PRG implementation was used by looking at output samples.

Let G_1 and G_2 be two PRGs with matching input/output lengths. Define two libraries $\mathcal{L}_{\text{which-prg}}^{G_1}$ and $\mathcal{L}_{\text{which-prg}}^{G_2}$ as follows:

```
$\mathcal{L}_{\text{which-prg}}^{G_1}$
QUERY():
    $s \leftarrow \{0,1\}^\lambda$
    return $G_1(x)$
```

```
$\mathcal{L}_{\text{which-prg}}^{G_2}$
QUERY():
    $s \leftarrow \{0,1\}^\lambda$
    return $G_2(x)$
```

Prove that if G_1 and G_2 are both secure PRGs, then $\mathcal{L}_{\text{which-prg}}^{G_1}$ and $\mathcal{L}_{\text{which-prg}}^{G_2}$ are indistinguishable — that is, it is infeasible to distinguish which PRG was used simply by receiving output samples.

6.2 Find the key (3 pts)

In this problem, you will show that it is hard to extract the key of a PRF simply by querying the PRF. Let F be a candidate PRF and suppose there exists a program $\mathcal{A}$ such that:

$$P[\mathcal{A} \diamond \mathcal{L}_{\text{prf-real}}^{F} \Rightarrow k \mid \mathcal{L}_{\text{prf-real}}^{F} \text{ uses } k]$$

is non-negligible.

As stated, k refers to the private variable within $\mathcal{L}_{\text{prf-real}}^{F}$. Prove that if such an $\mathcal{A}$ exists, then F is not a secure PRF. Use $\mathcal{A}$ to construct a distinguisher that violates the PRF security definition.

6.3 Build a distinguisher (3 pts)

Let F be a secure PRF. Let $\bar{x}$ denote the bitwise complement of the string x. Define the new function:

$$F'(k,x) = F(k,x)||F(k,\bar{x}).$$

Show that F' is **not** a secure PRF. Describe a distinguisher and compute its advantage.