Prof. Dr. Johannes Blömer
Nils Löken

May 12th, 2017
submission due: May 23rd, 2017: 11 a.m.

Cryptography - Provable Security

SS 2017

Handout 5

Exercises marked (*) will be checked by tutors.

Exercise 1 (4 points):
(*) Consider the function $f_{\text{add}} : \{0,1\}^* \to \{0,1\}^*$, that, on input $z = x||y \in \{0,1\}^*$ outputs $x + y$, where x, y are bitstrings interpreted as non-negative integers with length $|x| = \lceil |z|/2 \rceil$ and $|y| = \lfloor |z|/2 \rfloor$, respectively. Show that f_{add} is not a one-way function.

Exercise 2:
Given a one-way function $f : \{0,1\}^* \to \{0,1\}^*$, define function $g : \{0,1\}^* \to \{0,1\}^*, z \mapsto f(x)||y$, where $z = x||y \in \{0,1\}^*$ with $|x| = \lceil |z|/2 \rceil$ and $|y| = \lfloor |z|/2 \rfloor$. Prove that g is a one-way function despite revealing half of its input bits.

Exercise 3:
Assuming that one-way function exist, show that there is a one-way function f such that for all $n \in \mathbb{N}$ $f(0^n) = 0^n$. Note that f is easy to invert for infinitely many inputs. Why does the one-way property hold for f nonetheless?

Exercise 4 (4 points):
(*) Given a one-way function f, prove that for every polynomial p and all n sufficiently large

$$|\{f(x) : x \in \{0,1\}^n\}| > p(n).$$

Exercise 5:
Show that every bijective function that has a hard-core predicate is also a one-way function.

Exercise 6 (4 points):
(*) Let $f : \{0,1\}^* \to \{0,1\}^*$ be a one-way function. Consider the encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ with

- $\text{Gen}(1^n)$: output $k \leftarrow \{0,1\}^n$,
- $\text{Enc}_k(m)$ with $m \in \{0,1\}^*$ of appropriate length: pick $r \leftarrow \{0,1\}^n$, output $c = \langle r, m \oplus f(r||k) \rangle$.

Describe the corresponding Dec algorithm and show that Π is indeed an encryption scheme. Then show that Π is not necessarily CPA-secure.
Hint: Exercise 2.