Prof. Dr. Johannes Blömer
Nils Löken

May 9th, 2016
submission due: May 17th, 2016: 11 a.m.

Cryptography - Provable Security

SS 2016

Handout 5

Exercises marked (*) and (**) will be checked by tutors.
We encourage submissions of solutions by small groups of up to four students.

Exercise 1 (4 points)**:**
(**) Show that the following function $f_{\text{add}} : \{0,1\}^* \to \{0,1\}^*$ is not one-way. To define the value of f_{add} at $z \in \{0,1\}^*$, we write z as $z = x||y$ with $|x| = \lceil |z|/2 \rceil$ and $|y| = \lfloor |z|/2 \rfloor$ and interpret x and y as the binary representations of two natural numbers. Then $f_{\text{add}}(z) = x+y$.

Exercise 2:
Assume that f is a one-way function. Define $g : \{0,1\}^* \to \{0,1\}^*$ as follows: For $z \in \{0,1\}^*$ write $z = x||y$, where $|x| = \lceil |z|/2 \rceil$ and $|y| = \lfloor |z|/2 \rfloor$, then $g(z) = (f(x)||y)$. Prove that the function g is also one-way. Observe that g fully reveals half of its input bits, but is nevertheless still one-way.

Exercise 3:
Prove that if there exists a one-way function, then there exists a one-way function f such that for every n, $f(0^n) = 0^n$. Provide a full formal proof of your answer. Note that this demonstrates that for infinitely many values x, the function f is easy to invert. Why does this not contradict one-wayness?

Exercise 4 (4 points)**:**
(**) Assume that f is a one-way function. Prove that for every polynomial p and all n sufficiently large it holds that

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

Exercise 5:
Show that if a one-to-one function has a hard-core predicate, then it is one-way.

Exercise 6 (4 points)**:**
(**) Prove Corollary 5.12 using Theorem 5.11.