Exercise 1 – Foundations of Cryptography 89-856/653

Due Date: 17th March 2019

Honour code: You are expected to solve all exercises on an *individual* basis. It is *highly recommended* that you spend a considerable amount of effort on the exercises before discussing the solutions with anyone. If you do discuss the exercises, the actual solutions must be written by yourself. You may also *not* use solutions that can be obtained from other sources (e.g., the Internet). I cannot enforce most of these rules, but have a strong expectation that you will abide by them.

Exercise 1: Show that the addition function $f(x, y) = x + y$ (where $|x| = |y|$ and x and y are interpreted as natural numbers) is not one-way.

Exercise 2: Prove that if there exist one-way functions, 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 3: A function f is said to be length regular if for every $x, y \in \{0, 1\}^*$ such that $|x| = |y|$, it holds that $|f(x)| = |f(y)|$. Show that if there exist one-way functions, then there exist length-regular one-way functions. Provide a full (formal) proof of your answer.

> **Hint:** Let f be a one-way function and let $p(\cdot)$ be a polynomial such that for every x, $|f(x)| \leq p(|x|)$ (justify the existence of this p). Define $f'(x) = f(x)10^{p(|x|)-|f(x)|}$. Prove that f' is length-regular and one-way.

Exercise 4: Prove that if there exist collections of one-way functions, then there also exist one-way functions. Can you say the same for 1–1 one-way functions? Explain.

Exercise 5: Assume that $\mathcal{P} \neq \mathcal{NP}$. Show that there exists a function that is easy to compute and hard to invert by deterministic algorithms in the worst case, but is not one-way.

Exercise 6: Let $x \in \{0, 1\}^n$ and denote $x = x_1 \cdots x_n$. Prove that if there exist one-way functions, then there exists a one-way function f such that for every i there exists an algorithm A_i such that,

$$\Pr_{x \leftarrow U_n}[A_i(f(x)) = x_i] \geq \frac{1}{2} + \frac{1}{2n}$$

We note that $x \leftarrow U_n$ means that x is chosen according to the uniform distribution over $\{0, 1\}^n$. (This exercise demonstrates that it is not possible to claim that every one-way function hides at least one *specific* bit of the input.)