BISS 2015
Course on "Protection of Sensitive Information"

Theory Exam

March 21, 2015

The exam consists of three exercises. The candidate should solve in a satisfactory way (that is, show that s/he has understood the principles of the course) at least two of them. For this purpose, please comment your solution (in case the numerical answer is not correct, I will check that at at least the reasoning is sound). In order to solve the exercises, the slides of the course should be sufficient.

Exercise 1

Consider the following program, which checks whether the binary string $x_1 x_2 \dots x_5$ corresponds to a certain password $k_1 k_2 \dots k_5$.

> `input(`$x_1 x_2 \dots x_5$`);`
> $i = 1$;
> `while` $(i \leq n$ `and` $x_i == k_i)$ do $i = i + 1$;
> `if` $i > n$ `then output(success) else output(fail)`

The input of the program (secrets) are the binary strings $x_1 x_2 \dots x_5$. We assume a uniform distribution on them.

1. What is the Shannon leakage of this program, assuming that the attacker can only observe the outputs are `success` and `fail`?
2. Same question, but now we assume that the attacker can also observe the execution time, namely that he can deduce how many times the operation $i = i + 1$ has been executed.
3. In the second scenario (in which the attacker can count how many times the operation $i = i + 1$ has been executed), rewrite the program so to reduce the leakage to half or less, while keeping the program as efficient as possible. In other words, write a program that is semantically equivalent to the one above, leaks at most half of the one above, and has an average execution time as small as possible.

Exercise 2

Consider the following channel matrix:

	o_1	o_2	o_3	o_4
s_1	$1/2$	$1/2$	0	0
s_2	0	$1/2$	$1/2$	0
s_3	0	0	$1/2$	$1/2$

Assume that $p(s_1) = p(s_3) = \frac{1}{2}x$, and $p(s_2) = 1 - x$, with $0 \leq x \leq 1$. Let S and O be the random variables that represent the input and the output, respectively, of the channel.

1. Please express the prior min-entropy $H_\infty(S)$, the posterior min-entropy $H_\infty(S|O)$, and the leakage $I_\infty(S;O)$ as functions of x.

2. Please compute the min-capacity C_∞ of the channel.

Exercise 3

Consider the geometric method for differential privacy defined in the slides of Lecture 4. Assuming a query that returns a integer answer, prove that the composition of the query with the geometric noise results into a mechanism that is ε-differentially private.