BISS 2015
Course on “Protection of Sensitive Information”

Implementation Exam

March 18, 2015

The exam consists of three coding exercises. The candidate should write a program for at least two of them. Please comment your solution (in case the program does not produce the correct answer, 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.

Program 1

Write a program that takes in input a channel matrix $m \times n$, and an input distribution (a discrete probability distribution on the m possible input values), and

1. checks that the matrix is a correct channel matrix (i.e., the rows represent probability distributions),
2. computes and outputs the Shannon leakage of the channel.

Please test the program on a couple of channel matrix of your choice, one deterministic and one (strictly) probabilistic.

Program 2

Write a program that takes in input a channel matrix $m \times n$, and an input distribution (a discrete probability distribution on the m possible input values), and a gain function on a finite number k of guesses. Note that the domain of the gain function is finite (it has $k \times n$ possible pairs), and therefore a gain function g can be represented simply by tabulating all possible results. The program should:

1. check that the matrix is a correct channel matrix (i.e., the rows represent probability distributions),
2. compute and outputs the g-leakage leakage of the channel.

Please test the program on a couple of channel matrix of your choice, one deterministic and one (strictly) probabilistic.

Program 3

Consider a database of patients of a hospital. Each record contains the name of the person, the age, and whether the patient has a certain disease or not. Consider a query of the form "How many people in the database are at most 50 years old, and have the disease?". Write a program that implements an ε-differentially private mechanism for this query, using the method of the geometric noise described in the slides of Lecture 4.