INFO-F-??? - Course Report
Secure computation

Université Libre de Bruxelles

Hakim Boulahya

June 2, 2018

1 Introduction

In this paper we will propose formal definitions of secure computation, also refered as secure multiparty computation. We will also gives known example in the litterature that are defined following the logical of secure computation. We will then gives techniques and protocols that allow to resolve secure computations.

2 Secure computation

A secure multi-part computation problem, is a problem where a computation, or a result, must be computed but the input that each party must used is confidential and not share between all parties. Such problem can be defined as a function $f(\cdot)$, that takes n parameters. The idea is to be able to compute the function $f(x_0, .., x_n)$ where the input x_i can only be accessed by the party i. The final results is accessible to everyone.

cite f(.)

3 Problems

There exists multiple problems that used the secure computation definition. For example the millionaires problem, is the problem that for two millionaires they both want to know which one of them is the richer, but they don't want to know the difference. In this problem, the computation function is the usual comparison $<$, and the inputs are the incomes of the individuals.

Another problem is the Oblivious Transfer introduced by Rabin during in 1982 [**?**].

cite mill problem

References