University of Bristol

Background Chapter

Secure two party computation

Author: Nicholas Tutte (nt1124)
Supervisor: Prof. Nigel Smart

Abstract

1 Background Chapter

1.1 Problem definition

Secure multi-party computation(SMPC) is a fundamental problem in Cryptography. We have a set of parties who wish to cooperate to compute some function on inputs distributed across the parties. However, these parties distrust one another and do not wish their inputs to be known to the other parties. We shall be focusing on the case where there are only two parties(S2PC), but most two party approaches can be generalised to the multi-party case.

A commonly used example is the Millionaires problem. A group of rich persons wish to find out who among them is the richest, but do not wish to tell each other how much they are worth. Here the parties are the rich (and somewhat vain) individuals. Their inputs are their net worths and the function will return the identifier of the individual with the highest input. Finally no party should be able to divine anything about anothers inputs, apart from what the can infer from their own input and the output.

So for example Whilst this is not exactly an inspiring application, it does explain convey the problem concisely. We shall cover further applications later in 1.4.

Throughout we will assume that we can establish a secure and authenticated channel of communication to all other parties in the computation. That is we assume communications between two parties cannot be eavesdropped upon or altered, and that we can detect attempts to impersonate another party.

1.2 Formal ideal model

Formally speaking any solution developed to the problem of secure two party computation should be equivalent to the following model, which we refer to as the *ideal*.

The obvious solution to our problem would be to find an external individual, trusted by both parties. Such a trusted individual could receive the inputs from each party, compute the function and then inform both parties of the output of the function.

This model is held up as the ideal to which any SMPC protocol should aspire to, both in terms of functionality and in terms of security.

1.3 Security levels

1.4 Applications

At first it might appear that SMPC lacks applications beyond those like the trivial example provided in 1.1. In fact as this is often the first example given leads many to dismiss SMPC as of limited usefulness. Here we shall provide a number of other active applications either already in use or in the process of emerging.

1.4.1 Secret Auctions - Netherlands Beets

1.4.2 Legal cases - Database queries

1.4.3 Distributed encryption

1.4.4 Secret sharing

1.5 Yao Garbled Circuits

1.6 Oblivious Transfer

References

[1] Trading Sugar Beet Quotas,
Secure Multiparty Computation in Practice,
ECRIM News 73,
Ivan Damgard and Tomas Toft.