Secure Two Party Computation

Preliminary presentation

Nick Tutte

Prof. Nigel Smart

February, 2015

Presentation overview

My project focuses on Secure Multiparty Computation, in particular the two party case using Yao Garbled Circuits. By the end of this presentation you should know,

- What is Secure Multiparty Computation?
- What can it be used for?
- What the “Secure” means in this context.
- A grounding in Yao Garbled Circuits.
- How much progress I’ve made so far.

What is Secure Multiparty Computation

In the problem of Secure Multiparty Computation we have a set of parties, each of whom has a secret input. The parties wish to co-operate to compute a function upon their collective inputs without revealing said inputs.

Applications of Secure Multiparty Computation

- The Millionaires problem.
- Distributed secrets.
- Sugar Beets.

Desired security properties

Before we go any further we need to define what properties we want an SMC protocol to fulfil before we consider it Secure.

- Privacy, the only knowledge parties gain from participating is the output.
- Correctness, the output is indeed that of the intended function.
- Independence of inputs, no party can choose it's inputs as the function of other parties inputs.
- Fairness, corrupt parties receive their outputs if and only if the honest parties also receive their outputs.

The Ideal Model

Security Definitions

We say that an OT protocol is secure if parties participating cannot learn any more by taking part then they would if they had used the Ideal Mode.

Oblivious Transfer

A key component we will need later is Oblivious transfer(OT).

Receiver	**Sender**
Inputs : $b \in \{0, 1\}$	Inputs : X_1, X_2
Outputs : X_b	Outputs : $\emptyset$

Figure : Definition of the functionality of a one-out-of-two OT protocol.

Security levels for OTs