

SWS — Trusted Intermediary

Informal Problem Statement

Lambert Meertens

September 27, 2005

Rock–Paper–Scissors

Rules of the game. In the game of *Rock–Paper–Scissors* (also known as *Roshambo*) two players are pitted against each other. They play a sequence of rounds. In each round, each player secretly selects one of three possible moves: ROCK, PAPER and SCISSORS, whereupon they simultaneously reveal their moves to each other. If they selected the same move, the round is a tie. Otherwise, one of the two wins, where the winner is determined as follows:

- PAPER beats ROCK;
- SCISSORS beats PAPER;
- ROCK beats SCISSORS.

Communication architecture. There are two communication channels, one from each player to the other:



The events (messages) they carry are ROCK, PAPER and SCISSORS. The picture does not express the requirement of simultaneity.

An UGLI Problem

In late 2004 the dynamic software company UGLI (Utrecht Gaming and Leisure Industries) released **Ro!Sham!Bo**TM, a computerized version of the game in which a human player plays against the computer.

In the original version, the program wrote its move on the screen while waiting for the human player to enter their move. The accompanying instructions stated: “Don’t look at the screen before you enter your move. That is cheating and is not fun.”

When sales foundered, UGLI did some market research, including in-depth interviews with (ex) players of **Ro!Sham!Bo**TM. Apart from the fact that almost nobody read those instructions, it turned out that everybody cheated. The temptation was just too much. However, as had already been noted in the unread instructions, cheating is not fun. In fact, it makes playing the game extremely boring.

In the next release, in Spring 2005, the program wrote its move “behind” an opaque pane, invisible to the human player. Only when the human player’s move was entered was the pane made transparent, revealing the program’s move. This solved the cheating problem. However, after a small initial spike, sales again dropped. Further market research showed that the human players did not trust the program. They suspected that the program could quickly alter its move before revealing it. And, they told the researchers: “playing against a cheating program is not fun”.

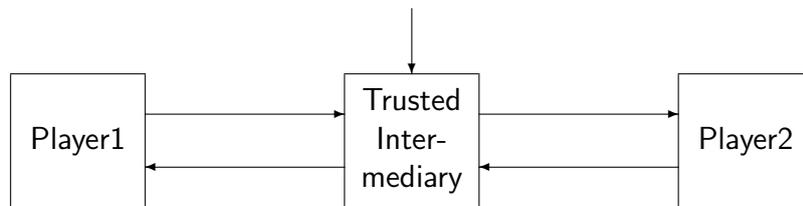
The Trusted-Intermediary Approach

Cheating made impossible. The think tank at UGLI now have devised the following solution. There will be a *Trusted Intermediary*, a third agent mediating between the two players. Unlike the heavily guarded top-secret specification of the **Ro!Sham!Bo**TM program, the specification of this Trusted Intermediary (TI) will be open source. Everyone will be welcome to inspect it and convince themselves no cheating is going on.

The role of TI. Instead of directly communicating to each other, the players reveal their moves to TI. Once a player has revealed their move to TI, they are committed to that move: the player cannot back out. Then, informally, TI does nothing but copy the output it receives from each player to the other player.

However, it will not copy to a player until it has received the move from that player. So there is no way a player can have advance knowledge in choosing the next move.

The New Communication Architecture



The extra input descending upon the Trusted Intermediary is a channel for RESET events, in order to be able to start over in case one player defects while the other has already revealed a move.

Assignment

The assignment is to specify the Trusted Intermediary in at least two truly different ways, and prove them equivalent. Since the specifications and proofs will be open source and are meant to inspire trust in UGLI's next Ro!Sham!Bo™ release, they should of course be crystal clear in all respects.