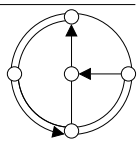
ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich



WS 2005-2006

Roger Wattenhofer, Nicolas Burri,
Pascal von Rickenbach, and Yves Weber

Mobile Computing
Exercise 8

Assigned: January 23, 2006
Due: January 30, 2006

Distributed Shuffling and Card Dealing

So far we have implemented the multi hop-layer that allows communication using other players as relay stations and a lobby to create, join, and search for games. Therefore, we now start thinking about the implementation of game specific functions.

A vital function of our distributed hearts game is the shuffling and dealing of the 52 cards. Since we usually don't trust other players, this task can not be done by one player alone. Therefore, we need a distributed algorithm for shuffling and dealing where not any single player can cheat.

The assignment of this exercise is to invent such an algorithm and to write down the protocol. The guidelines are pretty straightforward:

- Only the four players should be involved. There is no common trusted party.
- No single player can manipulate the protocol. If a player tries to cheat, at least one other player can see that.
- Keep your protocol as simple as possible. This includes the time required for shuffling and dealing, the amount of messages exchanged, and of course the implementation difficulty.
- We assume that no two players cooperate to gain a common benefit. Such a scenario can not be prevented easily since the two players can always pass information about their cards to each other after the cards are shuffled and dealt.

You may also make certain assumptions to keep the implementation complexity low. For example, you may assume that two nodes may communicate in a secure manner, i.e. the communication is end-to-end encrypted and the players that forward the multi-hop messages can not peek at the payload.

NOTE: There is no need to implement your algorithm at the moment!