Privacy Preserving Auctions
Shh... Others do not know what I am bidding for!

Lab: Artificial Intelligent Laboratory
Prof Boi Faltings

Semester Project/Master Thesis
No of Students 1.
Supervisor for the project: Sujit Gujar. {firstname.lastname@epfl.ch}

1. Background and Introduction

Many times, there are multiple auctions are running simultaneously. It is very important to keep it secret who are agents bidding for which of the object. Bidders have preferences that are combinatorial in nature. Like, if a bidder may be interested in item 2 from auctioneer 2 only if he gets item 1 from auctioneer 1. Or may be he is interested only one of the two items. Such problems can be addressed in Distributed Constraint Optimization (DCOP) framework. [1] proposed an algorithm, DPOP, that solves the DCOP correctly and works quite fast in practice. [2] proposed various schemes to execute DPOP privately, namely P-DPOP, P3/2-DPOP, P2-DPOP. Though winners can be determined using P*-DPOP, payment computation is challenge.

2. Tasks
i. In this project, student is expected to study P*-DPOP algorithms.
ii. Study FRODO [3], an open source platform, that has implementations of DPOP and P*DPOP and some other algorithms for solving DCOP.
iii. Implement two different payment schemes for such distributed auctions using FRODO.
iv. Prove privacy properties of the new payment schemes.
v. Stretch Goal: Come up with more innovative payment schemes other than the two different suggested by the supervisor.

3. Pre-requisite

✓ Preliminary knowledge about cryptography.
✓ Preliminary knowledge of Game Theory
✓ Good JAVA Programming skills.

4. Reference: