Securing Auctions

Lab: Artificial Intelligent Laboratory
Prof Boi Faltings

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

1. Background and Introduction

   Auctions are integral part of selling buying item or items. The bidders, bid valuation are very sensitive information and needs to be protected from reaching malicious users. Privacy preserving auctions proposed in the past were theoretically interesting but practically very inefficient for use when there are 100's of bidders. [1] proposed new efficient method for implementing Vickrey auctions using Zero Knowledge Proofs and deniable revelation of secret bids. Thus at the end of auction, only winner knows he is winner and how much he should pay. Nothing else is reveled about the bids of the other agents.

2. Tasks

   i. In this project the student is expected to study [1] and many other privacy preserving auctions.
   ii. Study various and implement various commitment functions referred in the paper.
   iii. Implement cryptographic auction from [1] in JAVA using efficient data structures.
   iv. Stretch goal is to design new schemes enhancing further privacy aspects of the auctions.

3. Pre-requisite

   - ✓ Basic knowledge about cryptography.
   - ✓ Good JAVA Programming skills.

4. Reference:

[1] Micali, Silvio, and Michael O. Rabin. "Cryptography miracles, secure auctions, matching problem verification." *Communications of the ACM* 57.2 (2014): 85-93.