Secure Auctions

Advisor(s): Lukas Helminger

Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology, Austria

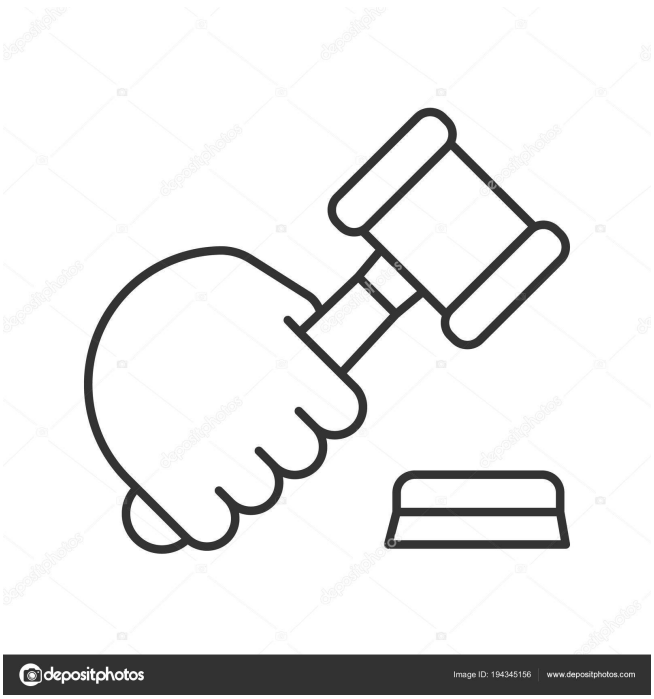
Motivation

Auctions are a centreal process of buying and selling goods or services in our economy. The transformation of this formerly analog process to the digital world leads to security challanges. In the first large scale commerical deployment of a MPC protocol, Danish researchers created a bidding platform for sugar beet production contractors (2009). Despite this success there are many open issues concerning secure auctions.

The goal of this project is to get an overview of the sate-of-the-art in this field and to implement a component of a secure auction.

Goals and Tasks

- Get familiar with the required background
- Review the state-of-the-art
- Implement a component of a secure auction



Literature

- P. Bogetoft et al.
  Secure Multiparty Computation Goes Live
  Financial Cryptography and Data Security, 13th International Conference, FC 2009, Accra Beach, Barbados, February 23-26, 2009. Revised Selected Papers
  https://doi.org/10.1007/978-3-642-03549-4_20

Deliverables

- Project files
- Thesis or project report (pdf)
- Poster (pdf)
- Presentation (pdf)

Schedule

- Start immediately
- Reading related work and taking first steps
- Intermediate presentation or poster
- Implementing
- Thesis writing
- Final presentation

Studies

☒ CS ☒ ICE ☒ SEM

Prerequisites

- Programming: C, C++, Java, Python
- Interest in public key crypto

Advisor / Contact

lukas.helminger@iaik.tugraz.at