Multiparty Computation Goes Live

Ivan Damgård, Jesper Buus Nielsen

Aarhus University

SIMAP

Secure Information Management and Processing

Research project at Aarhus University, Denmark, aimed at developing

- programming language for multiparty computation, SMCL, where you can easily specify which secure computation you want

- compiler that maps source code to software executing MPC protocols, that can be directly run by the players.

- new protocols that are efficient for the type of secure computing needed in practical applications, typically integer arithmetic.

MPC in Real Life

This year, SIMAP will launch the first real-life application of MPC:

A nation-wide market for trading production rights for sugar beets.

• Sugar beet production is big in Denmark, but under pressure due to reduction of EU support

• Need to move production to where it is best done

• Sugar beet contracts should be bought and sold on a nation-wide auction.

Basic idea: use MPC to find a fair price per ton of beets

• Buyers and sellers submit bids in encrypted form
bid = “buy this much if price is p1, so much if price in p2, etc.. “

• MPC among 3 players, representing the interested parties is used to find *market clearing price*: price at which supply =demand. All trading done at clearing price.

• Secure MPC needed because bids are private information: need to prevent strategic behavior where knowledge of other people’s bids is (mis)used.

In practice

- Up to 5000 bidders
- Work with 4000 possible price values.
- Computation done on (up to) 32 bit integers.
- Protocol based on Shamir secret sharing, with honest-but-curious security.
- After bids are in, can do MPC for entire auction in about 10 seconds.
- Goes live in November/December this year

Interested in working on the theory or practice of this?

We are looking for new postdocs/PhD's in the area!

We're hiring at Århus University from beginning of 2008

For information, contact me, or Ivan Damgård (ivan@daimi.au.dk)