The Danish Sugar Beet Auctions

Tomas Toft, Aarhus University

PEC Workshop

Dec. 8th 2012

Joint work within the SIMAP project

- Computer scientists (Aarhus University/Alexandra Institute)
  - Dan Christensen
  - Ivan Damgård
  - Martin Geisler
  - Thomas Jakobsen
  - Mikkel Krøigaard
  - Janus Nielsen
  - Jesper Nielsen
  - Jakob Pagter
  - Michael Schwartzbach
- Economists at (Kgl. Veterinær og Landbohøjskole)
  - Peter Bogetoft
  - Kurt Nielsen

Outline of the Talk

- Trading sugar beet contracts
- The solution
  - The double auction
  - The implementation
  - The cryptography

Some Background

- Around 5000 Danish farmers grow sugar beets
- Farmers own contracts – production rights – allowing a certain amount of production
- All beets are delivered to Danisco, the only Danish sugar producer

- A few years ago, the EU greatly reduced subsidies and Danisco closed one of its factories.
- This resulted in an immediate need for a nation wide market for trading production rights

The Outcome

- Danisco and the association of sugar beet growers (DKS) became partners in a research project with AU and KVL

First large-scale application of secure multiparty computation (MPC)

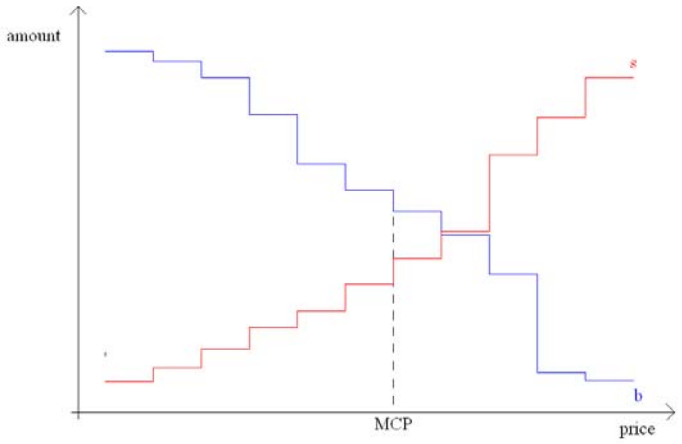
  - 25000 tons of production rights change owner
  - The market price at which trade occurs is computed by three servers, based on encrypted bids that are *never* decrypted

The Double Auction

- Many buyers and sellers trade a commodity
- A double auction (DA) is an exchange where the market clearing price (MCP) is computed based on sealed bids:
  1. Receive sealed bids
  2. Compute MCP based on bids
  3. All trade occurs at MCP and bids are *binding*

Bids and the Market Clearing Price

- The MCP is the intersection between supply and demand
- Bids are supply/demand curves
- Each bidder trades his supply/demand at the MCP
- Discrete version: Price grid
- Need rules for handling excess supply/demand



Who Should be Auctioneer?

- Danisco?
  - No: Bids reveal private information about a farmer’s economy; this can be misused by Danisco
- The farmers themselves/DKS?

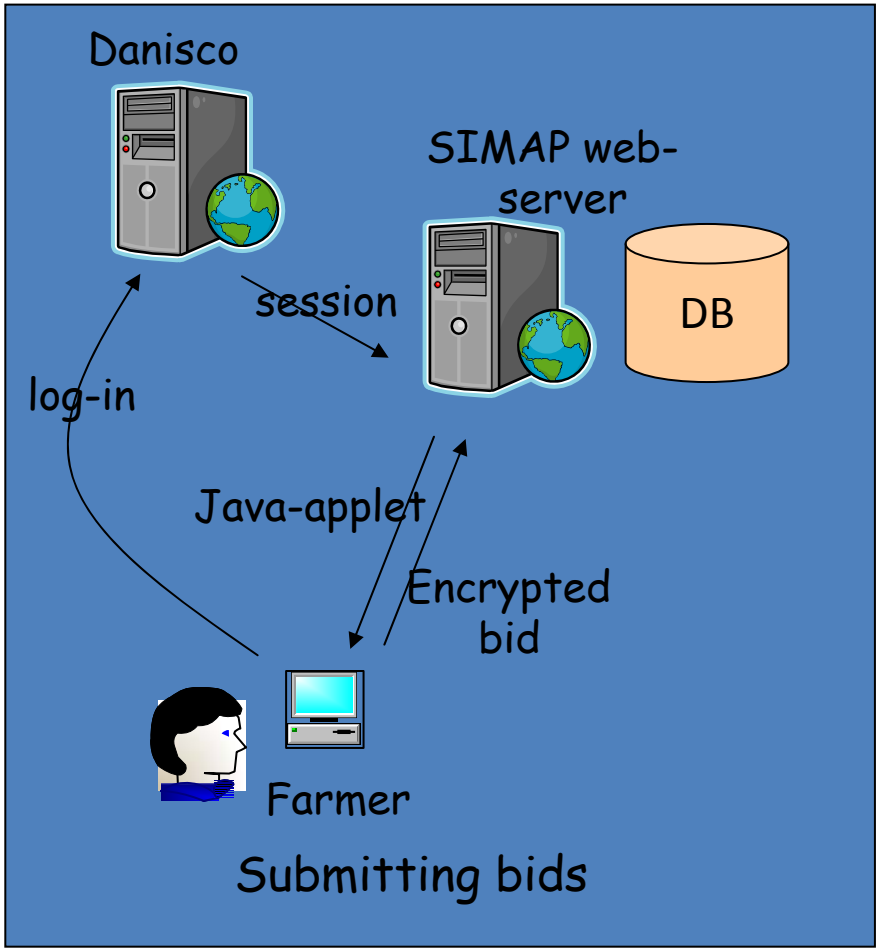
Solution: A “virtual auctioneer” using MPC
Three parties: Danisco, DKS, SIMAP

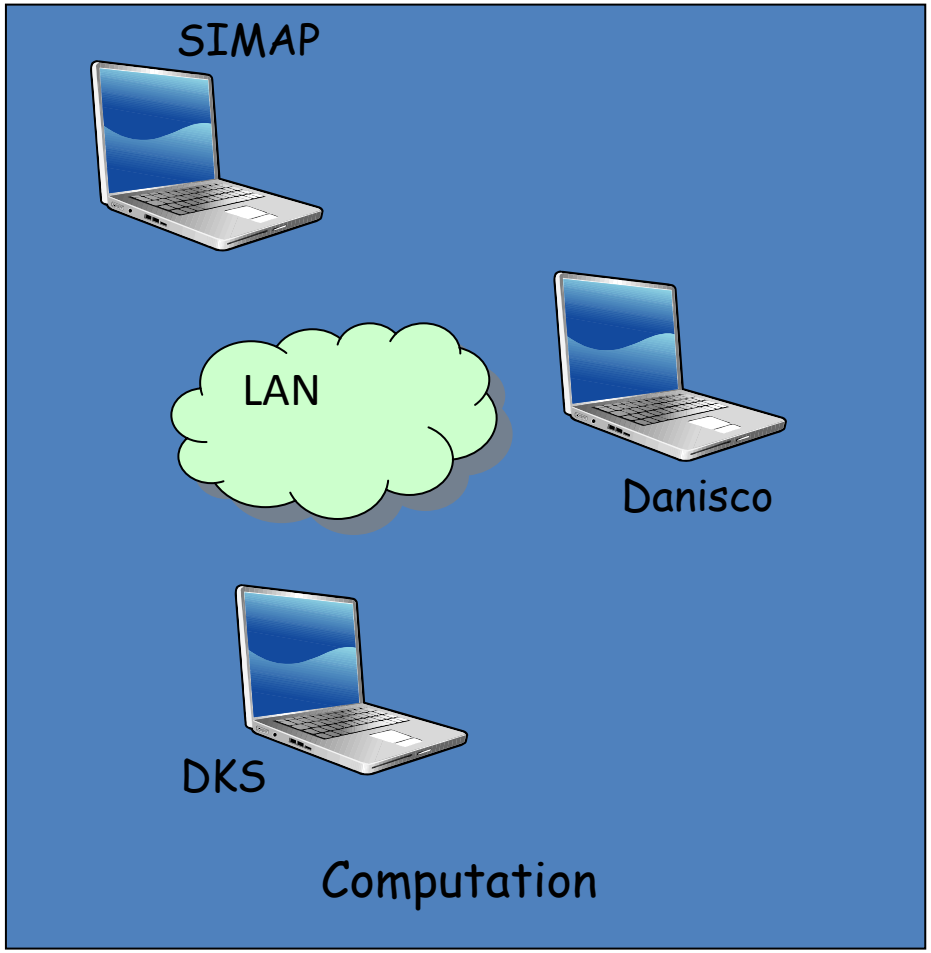
  - No: Too expensive

Why Use MPC

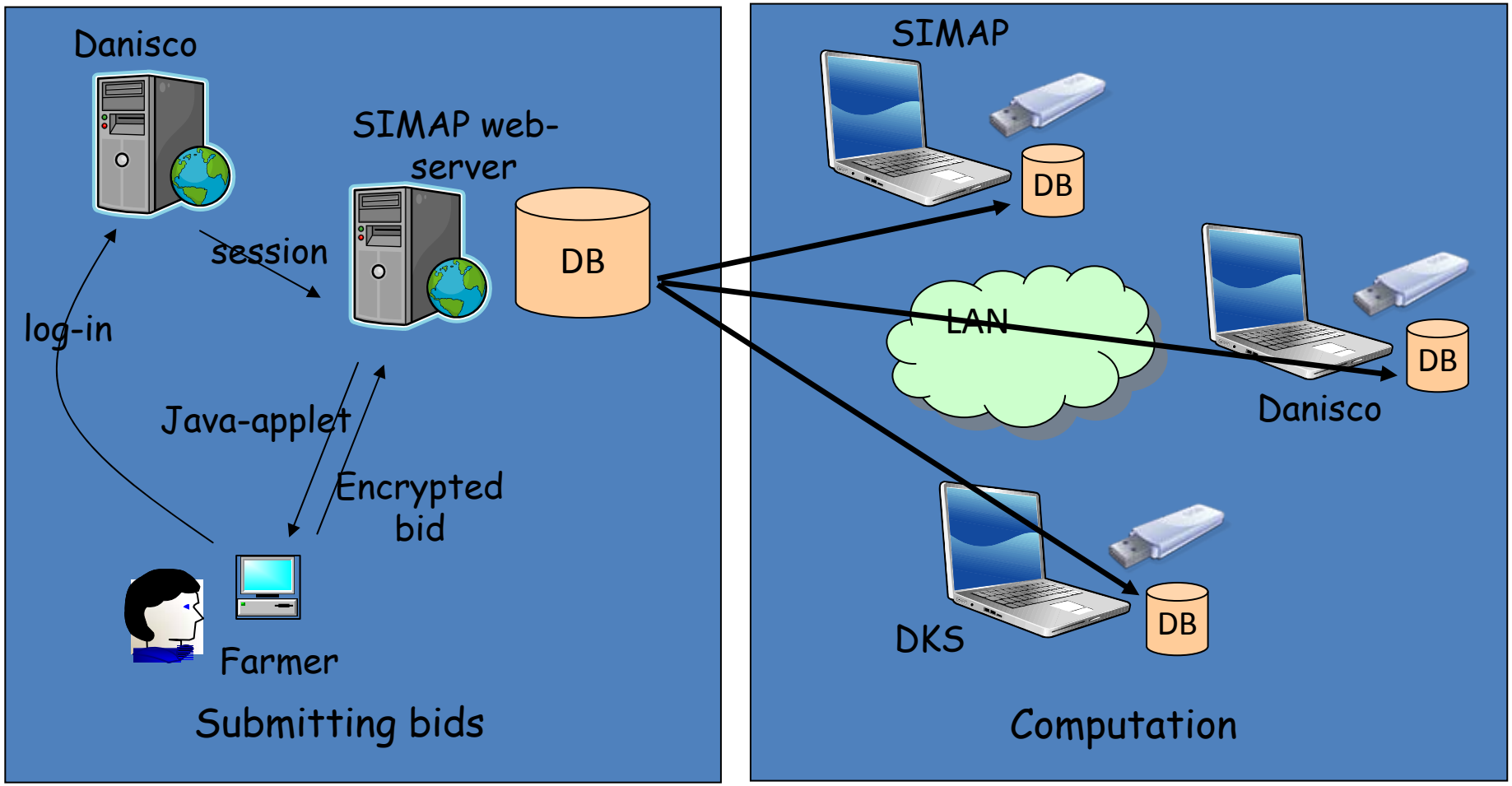
- No party holds data in the clear
  - No one has to take full responsibility
  - Simpler security policy
  - Easily communicated security policy
- Responsibility implies compensation
- Multiple parties with conflicting interests: negotiations for a security policy could block everything
- Use secure hardware device?
  - Single point of trust; needs security policy (administration, backup, …)
- MPC-costs are low once the solution is there (consultancy house must be be paid every time)

Implementation Architecture

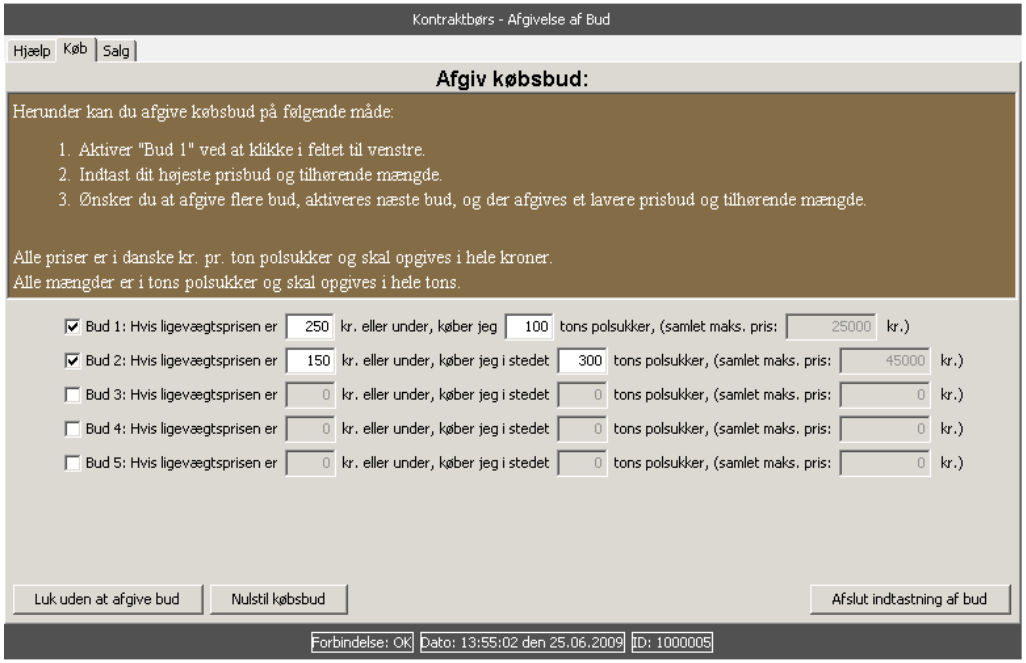




Implementation Architecture

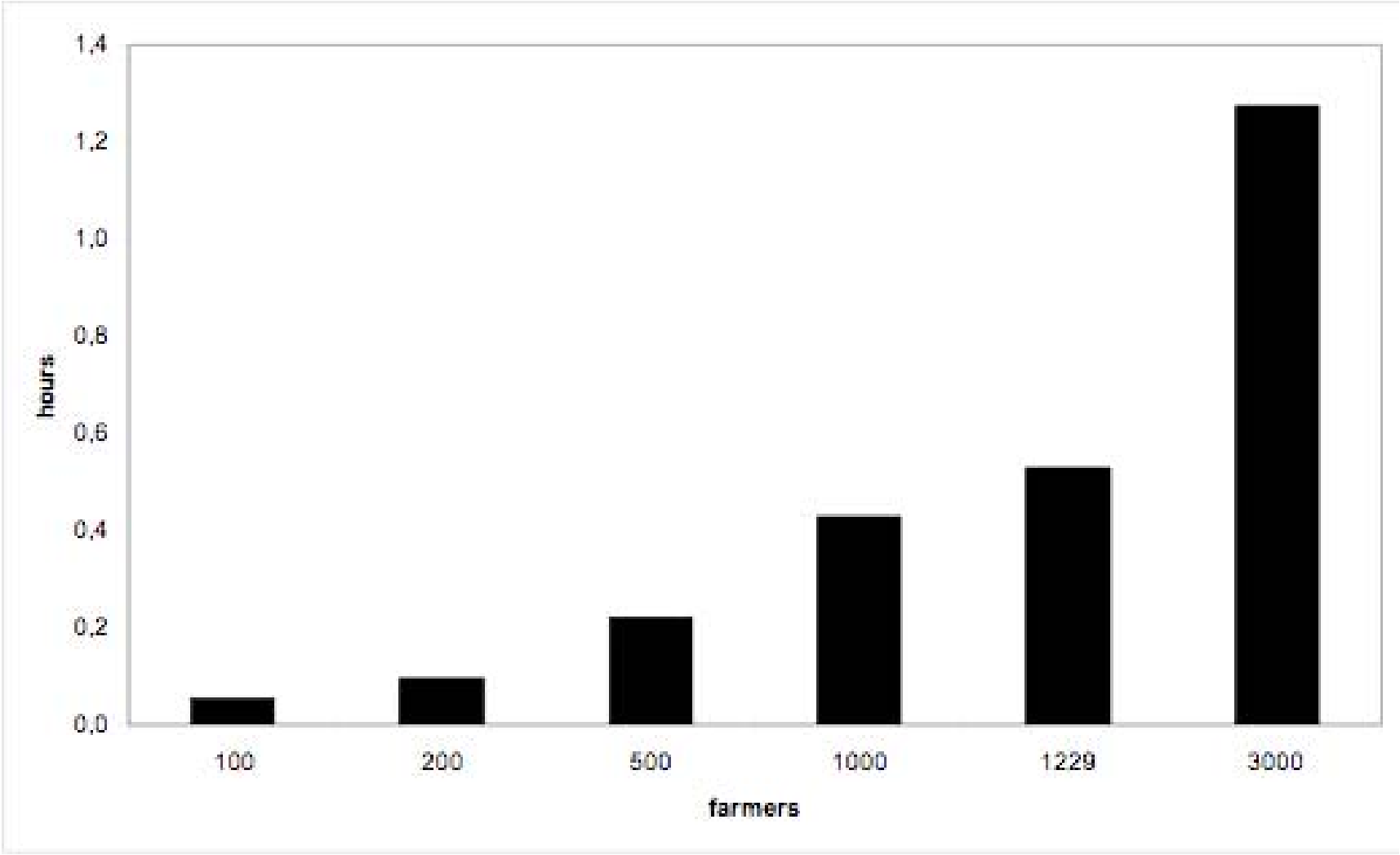


Submitting Bids

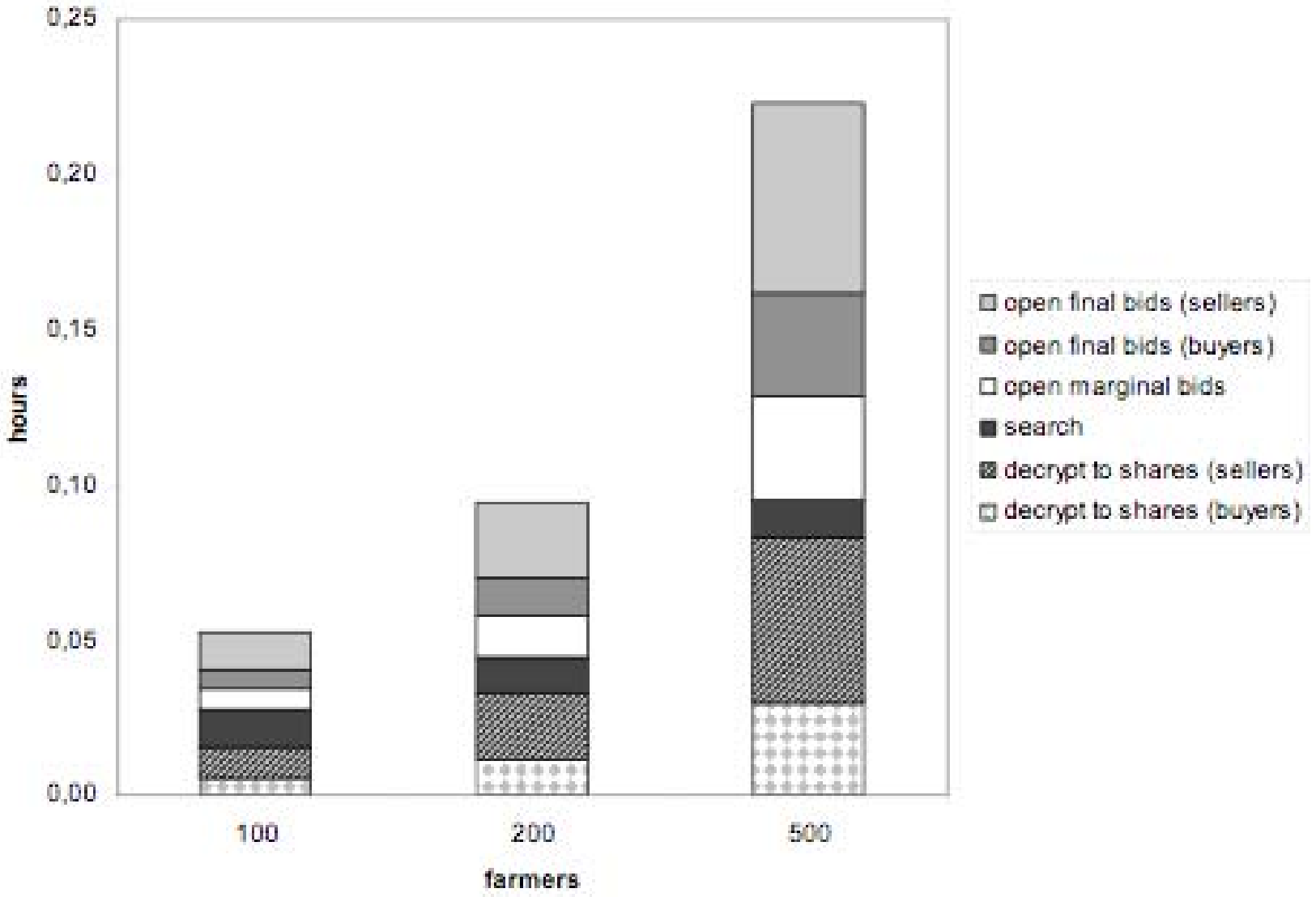


- Supply/demand curves are simplified
  - number of price changes limited to at most five
- Farmers must understand both auction and interface

Performance (I)



Performance (II)



The Cryptography

- MPC based on secret sharing
  - Addition (homomorphic property)
  - Multiplication (protocol)
  - More efficient than homomorphic encryption
- Honest-but-curious servers
  - Servers execute protocol correctly
  - No one learns the bids in the clear (i.e., no one is responsible)
  - The threat of an active attack was low

The MPC Double Auction

- Aggregate supply and demand curves
  - Many additions
- Find the intersection: Compare supply and demand
  - Complex protocol using addition/multiplication
  - Trick: Reveal random values related to secret ones; e.g., seeing $r+x$ does not reveal x

In Conclusion (I)

- MPC applications are possible
  - Sufficiently efficient and convenient for real life
  - The auction has been run every year since 2008
- Questionnaire:
  - 81% of farmers said that the auction simplified trading contracts
  - 78% of farmers said that confidentiality of bids was important
  - 86% of farmers said that they were happy with the confidentiality provided

In Conclusion (II)

- More information
  - The SIMAP project (www.alexandra.dk/uk/projects/Pages/SIMAP.aspx)
  - Trading Sugar Beet Quotas – Secure Multiparty Computation in Practice (ERCIM NEWS, April 2008; ercim-news.ercim.eu/en73)
  - Multiparty Computation goes Live (Financial Cry
- SIMAP spinoff company: Partisia (partisia.com)

Thank you!