Cryptography & Security

Jesper Buus Nielsen
The Crypto Group

1 professor: Ivan Damgård
1 lektor: Louis Salvail
1 adjunkt: Jesper Buus Nielsen
1 postdoc: Nikos Triandopoulos
       Jakob Pagter
              Innovation manager, Alexandra institute
8 PhD students: Jakob Funder, Martin Geisler, Mikkel Krøigård, Carolin Lunemann, Gert Læssøe Mikkelsen, Claudio Orlandi, Miroslava Sotakova, Rune Thorbek

More on http://www.brics.dk/Activities/Cryptology
Digital Sealed-Bid Auctions

- Want to sell goods via fully digital auctions
- Want to keep the bids secure
  - No single point must know anything but the result

Need for secure bids:

- Seller might use knowledge of bidders’ previous valuations to set high minimal price
  - Bad for bidders
- Bidders might use knowledge of other bidders’ previous valuations to give lower bids
  - Bad for seller

More on
http://www.brics.dk/Activities/Cryptology
Secure Distributed Computing

- The main tool is secure distributed computing via secret sharing
- Allows a set of input clients to use a set of partially trusted servers to perform a computation on their secret inputs and to make only the output public
- No single server will know anything but the output
  - I.e., no single point of attack!

More on http://www.brics.dk/Activities/Cryptology
Secret Sharing

Example with three servers:

- A secret $s \in \{0, \ldots, 9\}$ to be stored on three servers
- Pick three random numbers $s_1, s_2, s_3 \in \{0, \ldots, 9\}$ for which
  \[
  s = s_1 + s_2 + s_3 \mod 10
  \]
  and send $s_n$ to server number $n$

More on
http://www.brics.dk/Activities/Cryptology
Secret Sharing

\[ 8 + 3 + 4 \mod 10 = 15 \mod 10 = 5 \]

More on [http://www.brics.dk/Activities/Cryptology](http://www.brics.dk/Activities/Cryptology)
Want servers to securely compute sharing of \( 5 + 7 \mod 10 = 2 \)

Leaks no information about operands as there is no communication!

More on http://www.brics.dk/Activities/Cryptology
Multiplication

\[(8+4+3)(6+2+9) = \]
\[8 \cdot 6 + 8 \cdot 2 + 8 \cdot 9 + 4 \cdot 6 + 4 \cdot 2 + 4 \cdot 9 + 3 \cdot 6 + 3 \cdot 2 + 3 \cdot 9 = 255\]

More on

http://www.brics.dk/Activities/Cryptology
And so on…

- Can develop fairly efficient protocols for many other primitives common in programming languages, like: <, =, a[i], &&, ||, …
- In all cases the protocols compute sharings of the shared inputs without leaking any information on the inputs to any individual server
- In the end the shares of *only* the results are made public

More on http://www.brics.dk/Activities/Cryptology
Double Auctions

- Some uniform mass commodity
  - European CO₂-contracts, Electricity, …
- Each seller for each price specifies how much it is willing to sell at that price
- Each buyer for each price specifies how much it is willing to buy at that price
- For each price the total demand and supply is computed
- The result is the market clearing price: the price at which total demand equals total supply
- Only MCP should be revealed, not individual curves

More on http://www.brics.dk/Activities/Cryptology
To optimize the Danish market for sugar beet production we implemented a digital double auction for contracts on growing sugar beets

- Motivation: EU subsidizing receding
- Goal: Move production to most efficient farmers

3 Servers run by:
- DKS (Danske Sukkerroedyrkere)
- Danisco
- Alexandra institute + Crypto group @ DAIMI

1200 input clients (farmers)

More on http://www.brics.dk/Activities/Cryptology
A Digital Double Auctions (2/2)

- This year the auction moved 25000 tons of production rights
  - Significantly restructured the Danish market in an hour
  - Would have been impossible using the previous bilateral mechanism
- A survey showed that 80% of the farmers found it important that the auction was guaranteeing the privacy of the bids

More on
http://www.brics.dk/Activities/Cryptology
Ad Hoc Digital Auctions

- Some agents meet on the Internet and want to run an auction to sell some good
- They exchange public signature keys
- The agents run a protocol among themselves to find a winner $W$ and a price $P$ and all sign $(W,P)$ to create a verifiable result called a *contract*
- The seller will sell to $W$ at price $P$

More on [http://www.brics.dk/Activities/Cryptology](http://www.brics.dk/Activities/Cryptology)
Ad Hoc Digital Auctions

- If efficient enough online auctions can e.g. be used to implement true microeconomics
  - Markets for goods at the scale of routing a packet and doing some relatively simple computation

More on http://www.brics.dk/Activities/Cryptology
Your Computer

http://www.brics.dk/Activities/Cryptology
Sell Your Cycles (1/2)

- A lot of projects, like SETI@home, is willing to use your excess computing power for free.
- What if you could sell 50% of your power those 100 days where you do nothing and then have access to the equivalent of 50 of your own machines on day 101 when you really have to crunch numbers?

More on
http://www.brics.dk/Activities/Cryptology
Sell Your Cycles (2/2)

- Currently being explored by the crypto group at Brown university
- Involves selling jobs of the form \((x,F)\) to other computes and getting back \(y=F(x)\)
- Payment and fairness is handled using electronic cash
- Distributing the jobs and pricing them is an obvious place to use *ad hoc* digital auctions

More on [http://www.brics.dk/Activities/Cryptology](http://www.brics.dk/Activities/Cryptology)
Sell your Connectivity

Routing in *ad hoc* networks and peer-to-peer networks is another obvious candidate

- Micro payments for relaying packages

Auctions can be used to find the optimal pricing/route

More on
http://www.brics.dk/Activities/Cryptology
Problem

Computing a sharing of the signed result can easily be done using secure distributed computing.

Revealing the shares of the result is hard as the losers might defect to hide the results:
- Hides information on their bids
- Could even provoke a “rematch”

More on [http://www.brics.dk/Activities/Cryptology](http://www.brics.dk/Activities/Cryptology)
After a secure computation the agents hold shares of the signed result. 

Time to make the shares public.

Damn, I lost!

More on http://www.brics.dk/Activities/Cryptology
Solution (1/2)

First run a secure distributed computation to compute sharings, one of them of the contract.

I won!

http://www.brics.dk/Activities/Cryptology
The End

More on
http://www.brics.dk/Activities/Cryptology
Solution (2/2)

By using the right auction mechanism and selecting the position of the contract at random with the right distribution the protocol becomes a Nash equilibrium

- When the parties are assumed to be greedy-then-paranoid

Still cryptographic secure in the usual sense even if the assumption on the parties’ rationality fails

More on
http://www.brics.dk/Activities/Cryptology