MPC Goes Live
- and the Partisia Spinouts

Kurt Nielsen and Jakob Pagter
Theory ◯ Practice

- Economics
  - Revelation
  - Theory
  - 1979 -

- Computer Science
  - MPC
  - Theory
  - 1979 -

- SCET 2004
- SIMAP
- COBE
- CFEM
- Practice
- Big Data by Security

- MPC is cool!

- Partisia
- Energiauktion
- Sepior

- Spinouts

University of Toronto
The Revelation Principle
- Economics and Computer Science meet on common ground

**Economics (assume)**
- Myerson (1979) Revelation principle (Cited by 1841 and Nobel prize)
- Direct revelation as good as anything
- Need impartial social planner

**Computer Science (build)**
- Shamir (1979) How to share a secret (Cited by 8793)
- Started the construction of an impartial social planner

Economics (assume)

**Old**

Type 1

“Input 2”

Old

**New**

Old

OUTCOME 3

Computer Science (build)

**Old**

Type 1

Impartial social planner

“Input 2”

New

Old

OUTCOME 3

“Type 1”

New

Old

OUTCOME 3
... and what turned out to be a sweet startup case

MPC GOES LIVE
The Business Case
MPC Goes Live
(and the industrial game around …)

Danisco Sugar finally sold

<table>
<thead>
<tr>
<th>Exchange</th>
<th>MCP (DDK)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2008 (January)</td>
<td>1</td>
</tr>
<tr>
<td>2008 (August)</td>
<td>3</td>
</tr>
<tr>
<td>2009 (August)</td>
<td>501</td>
</tr>
<tr>
<td>2010 (August)</td>
<td>800</td>
</tr>
<tr>
<td>2011 (August)</td>
<td>650</td>
</tr>
</tbody>
</table>

Funding
• SCET
• SIMAP

Economic study
• Large gain

Problem became larger
Growers: YES to auction

Problem solved!!

Danisco sugar sold!

Danisco: OK let’s try

Danisco: NO need
• They are free to trade

Auction ready

Large gain from auctions:
• Double profit
• Fill up factories
What About MPC?

“The secure approach contributed to our decision to use Partisia Contract Exchange. It turned out, however, to be of greater importance for the growers than I initially thought”

Klaus Sørensen, daily manager of the Danish Sugar beet growers’ organization

“Partisia Contract Exchange was an important element to ensure a fast adjustment to the new market situation that was a result of the EU sugar reform.”

Lars M. Petersen, Head of Department, Danisco Sugar
PARTISIA AND SPINOUTS
Partisia – A Commercial Platform

R&D Public-private bridge
- Extended collaboration
- Subcontractor

Team of 9 people
- Computer Scientists
- Economists

• Projects and project sale
• Initial business dev

• Business dev
• Scale up

More focus, people and risk (capital)
Products and Collaborations

- Double auctions
- High stake auctions
- Energiauktion.dk
- Sepior
- Secure statistics +

- Direct sale
- Consortium
- Joint venture
- Spinout
- R&D - prototypes

Revenue (some since 2008)

Pre-revenue (Private & public funding)
Prospects and Startup Challenges

“MPC processor speed” (by all means)

- Key management
- Authentication
- Auctioneer
- Collaborative statistics
- Big Data analytics
- Monitoring
- Info brokers

- Replace existing trust institutions
- New solutions - new opportunities
- Perceived trust
- All new services
- No competition no market
- Reduced use of MPC
- Regulation
SPINOUTS
Energy Procurement
– made simple and secure

1. Request auction
2. Learning your type
3. Submit bids
4. Finding best price
5. Accept = contract

STRONG SECURITY AND AUTOMATION
Sepior

• Using MPC for “blind” encryption
• Initial funding from SEED Capital + business angels
• Public funding:
  – Markedsmodningsfonden
  – H2020 SME Instrument
• Currently 7 FTEs
Sepior - Why

• Cloud Application Security Brokers (CASB)
  – Visibility, Compliance, Data Security, Threat protection
  – Encryption feature of Data Security at several incumbents: CipherCloud, SkyHigh, CloudLock etc.

• “While some 84% of respondents say they’re worried about cloud security, about 39% are encrypting all files they send to the cloud” – Sophos Dec. 2015

• New EU Data Regulation - encryption can relieve e.g. breach notification
Sepior - What

Must be secure
• Cryptographic security
• Satisfactory trust model

Must be convenient
• Basically unchanged UX for SaaS users
• Easy integration across devices, users, and applications
• Easy user management
• Ease of operation

“Making it easy for SaaS providers to encrypt their customers' data in a way so that the customers retain full control over the encryption keys”
Sepior - How I

**Distributed Trust**
- Basic trust paradigm based on MPC (going back to Shamir ‘78)
- Trust that T of N not compromised
- On-prem security in cloud-native fashion
- Potentially ”subpoena-proof”

**API-based integration**
- Cloud-native integration model
- API and SDK-based
- Cross-user, -end-point, -application, -platform
End-customer

- Sepior SDK
- SaaS-application.

KeyServer_{1@IaaS_1}

share_1

KeyServer_{2@IaaS_2}

share_2

KeyServer_{N@IaaS_N}

share_N

key = share_1 + share_2 + ... + share_N

---

Stream-cipher leveraging AES-CTR
Threshold-model
Use MPC for pro-active security, key rotation, and server-side crypto
Performance “≈” cost of communication
(plus PRNG and redundancy)

Parten
SaaS-service (cloud-side)

Enc_key(data)
Outlook

BIG DATA BY SECURITY
Big Data by Security
Better security → Better data → Better services

- Tax authority
  - Personal data
  - Company data
- Accountancy
  - Personal data
  - Company data
- Statistics Denmark
  - Personal data
  - Company data
- Banks
  - Personal data
  - Company data
- Loans on auction
- Credit rating as-a-Service
- Benchmarking as-a-Service
- Testing environment

MANY CONFIDENTIAL DATA

Users
- Companies
- Persons

-Better services
E.g. Include Data from Statistics Denmark

Step 1

Step 2

Firms

Customer
- Log in
- Request analysis

X Control

Y Control

Service provider

Peer performance
as motivation...

"Trustworthy peer mapping"
CONCLUDING REMARKS
Concluding Remarks

• MPC an early stage technology:
  – Some good PoCs
  – Very few scalable solutions

• MPC an early stage business:
  – Few “paid for” services
  – First private money invested
  – Early stage competition
  – Potential disruptive effect
Secure Multiparty Computation
- to become a component in a "combinatorial innovation" world...