Deploying Secure Computing for Real-world Applications

Dan Bogdanov, PhD
Head of Privacy Technology Development
Cybernetica
dan@cyber.ee

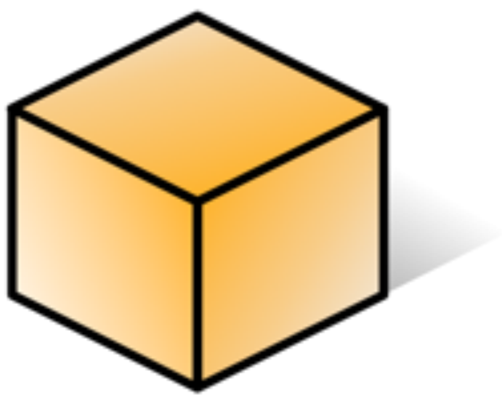
CYBERNETICA

sharemind

The Sharemind Privacy-preserving Computing Platform

Components for Privacy

Encrypted computing



MPC

FHE

Trusted hardware

Privacy policies

Multi-party consensus

Disclosure control

Audit support

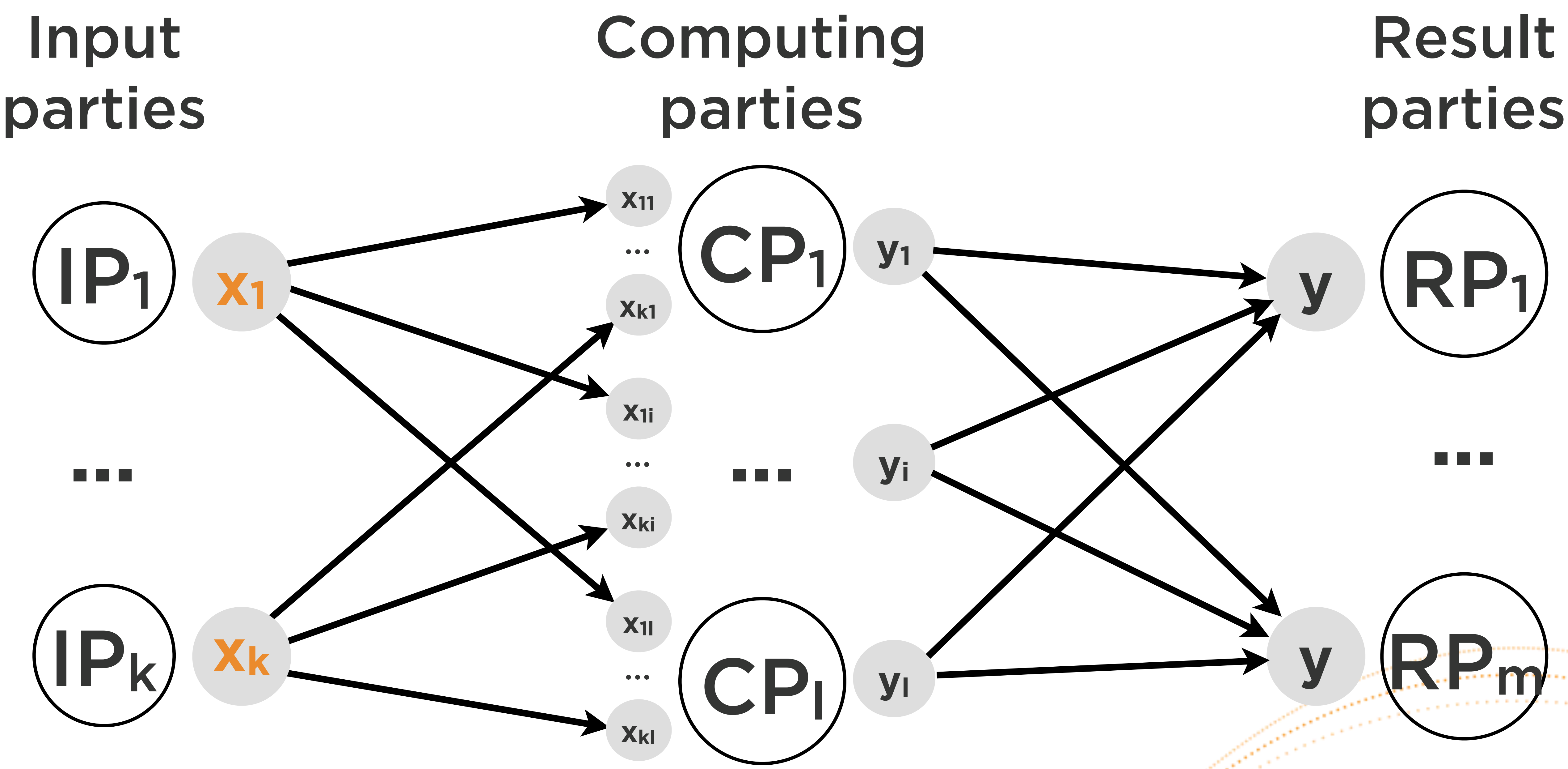
Online verification

Offline audit

sharemind

CYBERNETICA

Secure Computing Model



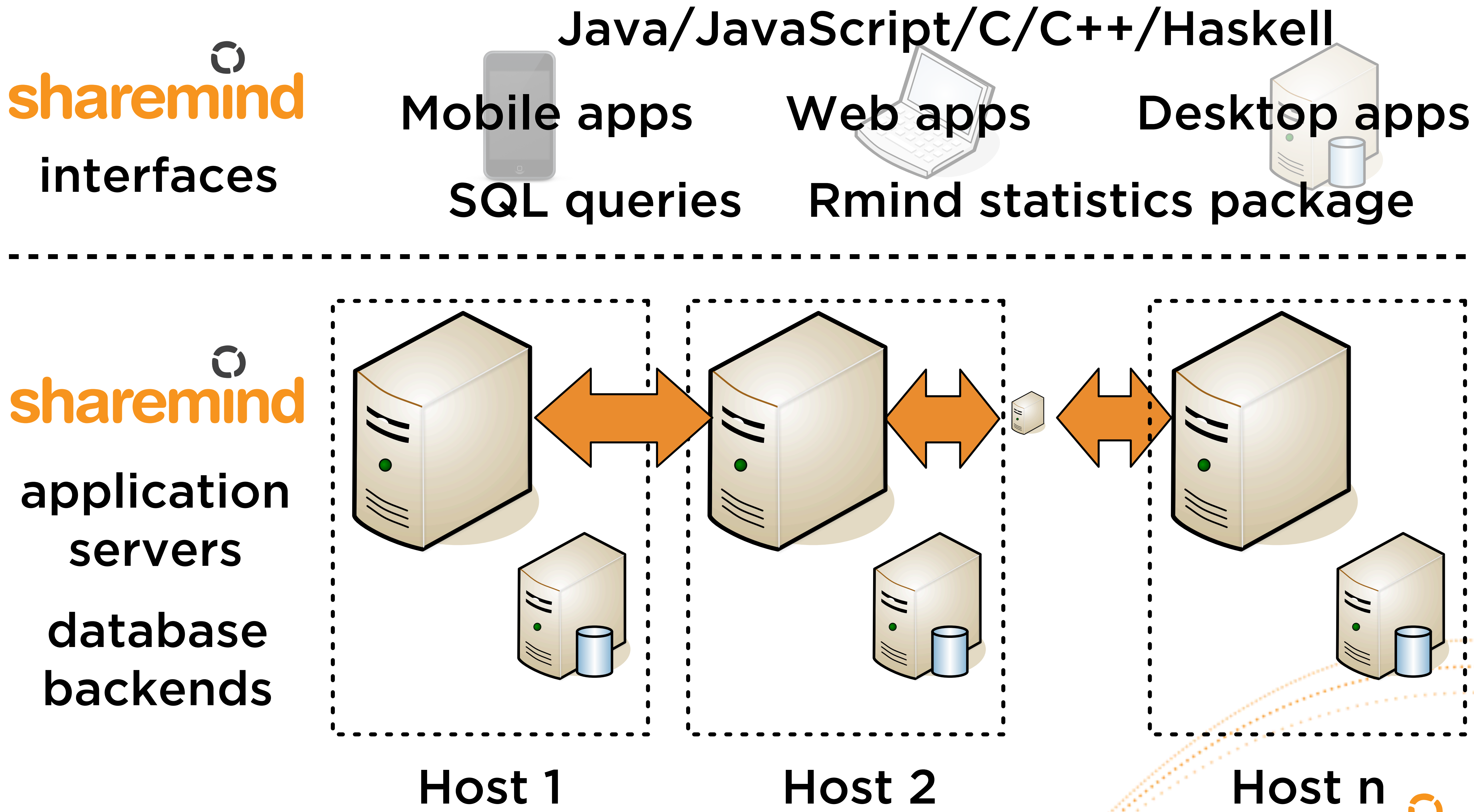
Step 1:
upload and
storage of inputs

Step 2:
Sharemind
servers

Step 3:
publishing
of results

sharemind
CYBERNETICA

Programmable Architecture



sharemind
CYBERNETICA

Sharemind's Protocols

Name	num of input parties	num of computing parties	num of result parties	Technology	Status
shared3p	any	3	any	LSS/MPC	In commercial use
shared2p	any	2	any	LSS/MPC	Under development
sharednp	any	3 or more	any	LSS/MPC	Under development

More are being planned

sharemind
CYBERNETICA

Student A

Score: 25

Student B

Score: 33

1. Pick random number $a_1 = 57$
2. Pick random number $a_2 = 13$
3. Find $a_3 = 25 - 57 - 13 \equiv 55 \bmod 100$
4. Send a_k to Server k, $(k \in \{1, 2, 3\})$

1. Pick random number $b_1 = 44$
2. Pick random number $b_2 = 57$
3. Find $b_3 = 33 - 44 - 57 \equiv 32 \bmod 100$
4. Send b_k to Server k, $(k \in \{1, 2, 3\})$

Server 1

$a_1 = 57$
$b_1 = 44$
$c_1 = a_1 + b_1 = 101$
$\equiv 1 \bmod 100$

Server 2

$a_2 = 13$
$b_2 = 57$
$c_2 = a_2 + b_2 = 70$
$\equiv 70 \bmod 100$

Server 3

$a_3 = 55$
$b_2 = 32$
$c_3 = a_3 + b_3 = 87$
$\equiv 87 \bmod 100$

Student C

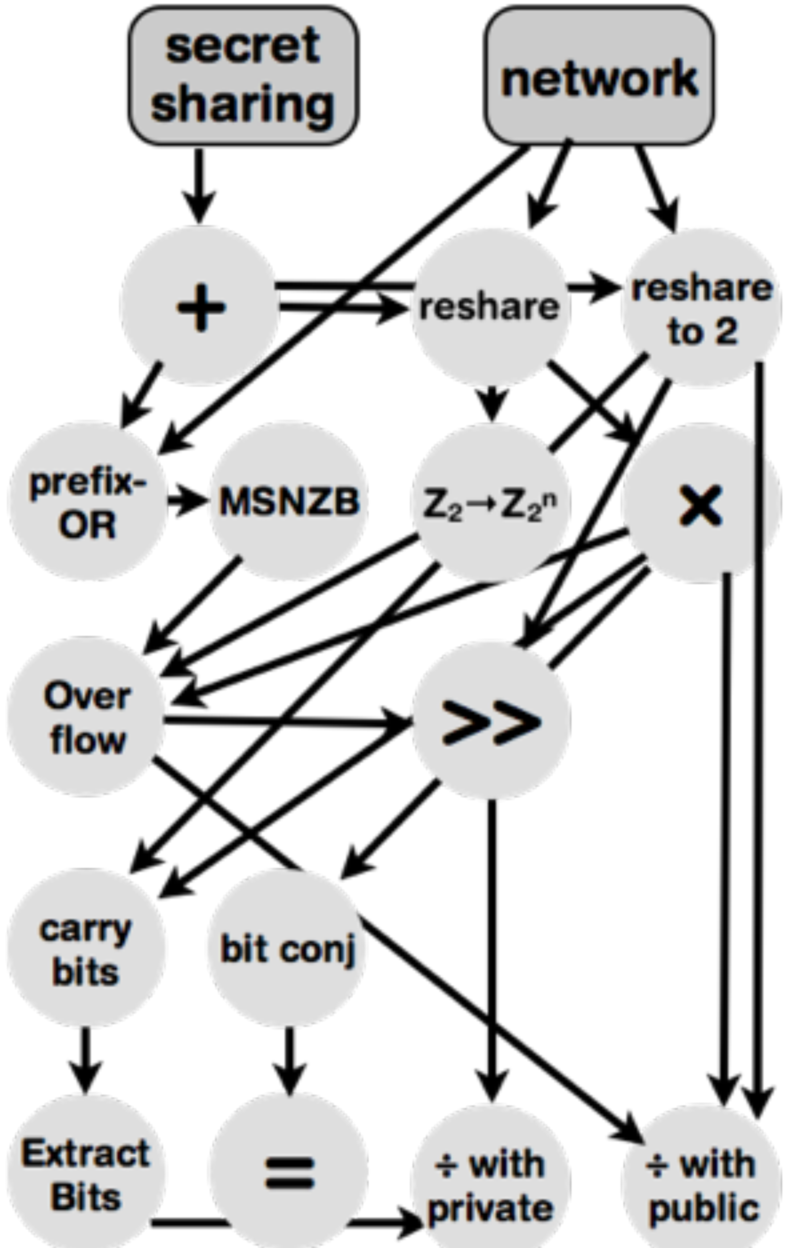
C calculates $c = 1 + 70 + 87 = 158 \equiv 58 \bmod 100$

C learns that the sum of A's and B's score is 58 without learning the scores of either student.

sharemind

CYBERNETICA

Getting More Operations



- *(continued example)*
- Addition derives from the homomorphic property of additive secret sharing.
- Further operations require network communication.
- The challenge is finding non-trivial ways to simplify the more complex protocols to make them efficient and keep them composable.

Dan Bogdanov, Margus Niitsoo, Tomas Toft, Jan Willemson. **High-performance secure multi-party computation for data mining applications**. International Journal of Information Security 11(6), pp 403-418. Springer. 2012.

sharemind CYBERNETICA

Coding for Sharemind Analytics with Sharemind

Demo Contents

- Programming SMC using SecreC
- Parallel operations
- Security protocol polymorphism
- Usability of SMC
- The Rmind statistics tool

Dan Bogdanov, Peeter Laud, Jaak Randmets. **A Domain-Specific Language for Low-Level Secure Multiparty Computation Protocols.** In Proceedings of 22nd ACM Conference on Computer and Communications Security. 2015.

Requirements specification based on the interviews. Usable and Efficient Secure Multiparty Computation project deliverable D1.2. http://usable-security.eu/files/d12final.pdf

Expert Feedback on Prototype Application. Usable and Efficient Secure Multiparty Computation project deliverable D1.4. http://usable-security.eu/files/D1.4-web.pdf

Dan Bogdanov, Liina Kamm, Sven Laur, Ville Sokk. **Rmind: a tool for cryptographically secure statistical analysis.** Cryptology ePrint Archive, Report 2014/512. 2014. (to appear) http://eprint.iacr.org/2014/512.pdf

sharemind

CYBERNETICA

Secure Computing for Governmental Statistics

It's a Good Time to be in IT

Software developer shortage transcends international boundaries

Shortage brings demand for overseas engineers

The Myth of America's Tech-Talent Shortage

Computer science graduates struggle to find work despite IT skills shortage

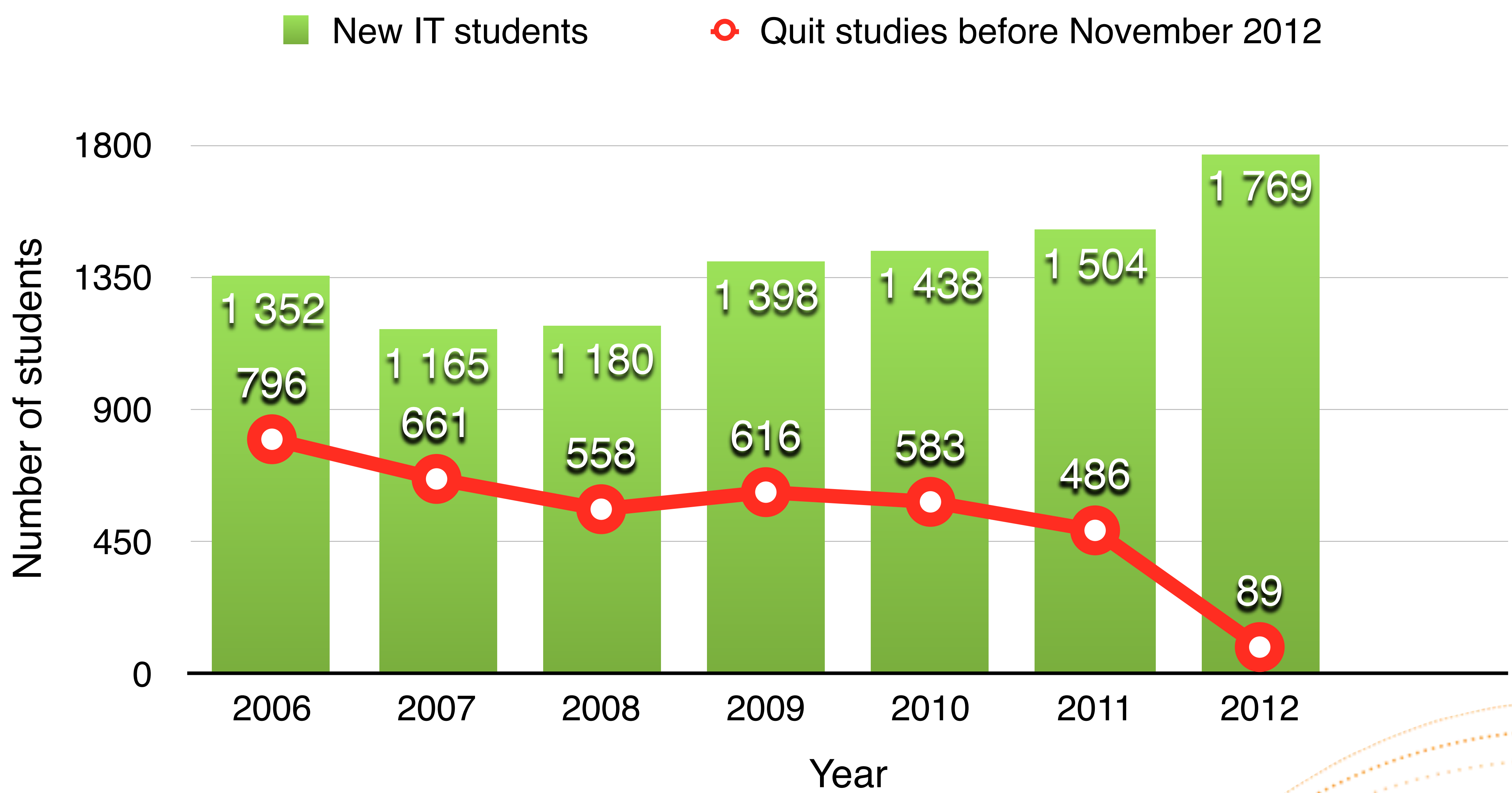
The fact that up to 900 000 jobs in the ICT sector remain unfilled because of a skills gap gives the clearest indication possible of what needs to be done," says Manuel Kohnstamm, Liberty Global's senior vice president and chief policy officer.

http://careers.ieee.org/article/European_Job_Outlook_0414.php

sharemind

CYBERNETICA

IT Training has a Failure Rate

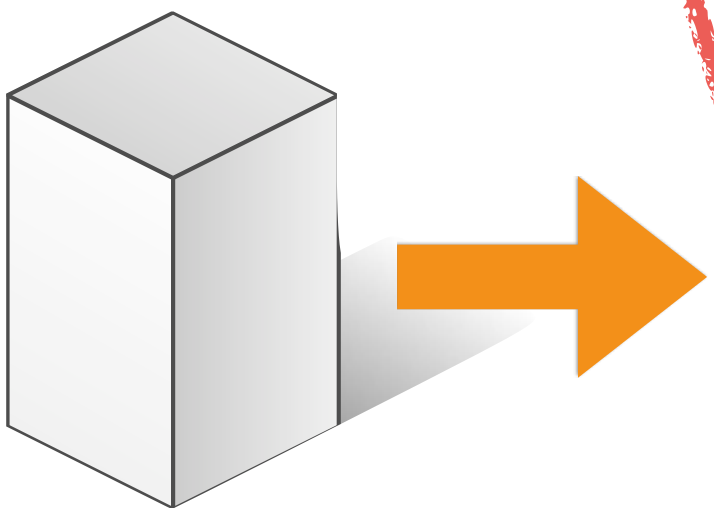


By 2012, a total of 43% of students enrolled in in the four largest IT higher learning institutions in Estonia during 2006-2012 had quit their studies.
Source: Estonian Ministry of Education and Research, CentAR.

sharemind
CYBERNETICA

Government has the Data

Tax records

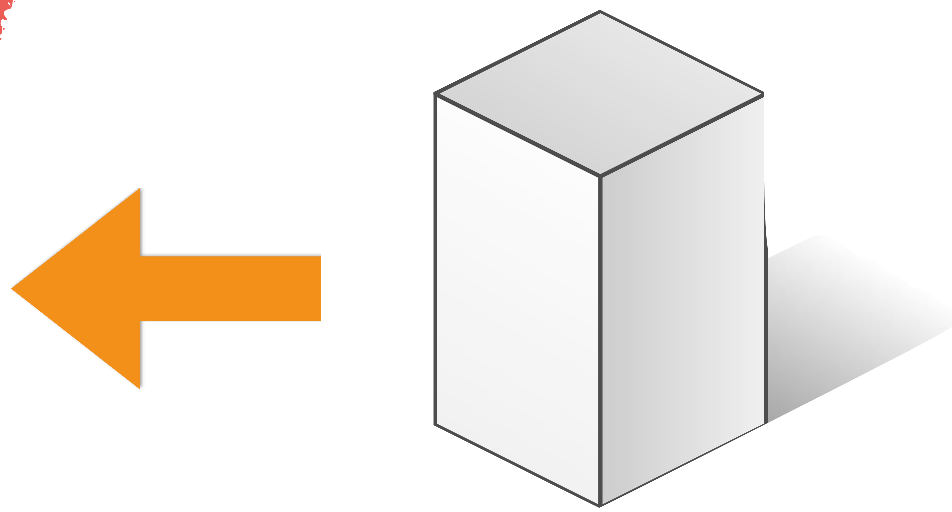


Has the student worked?
In which period?
In an IT company?

How is working related to not graduating on time?

Barriers
Data Protection
Tax Secrecy

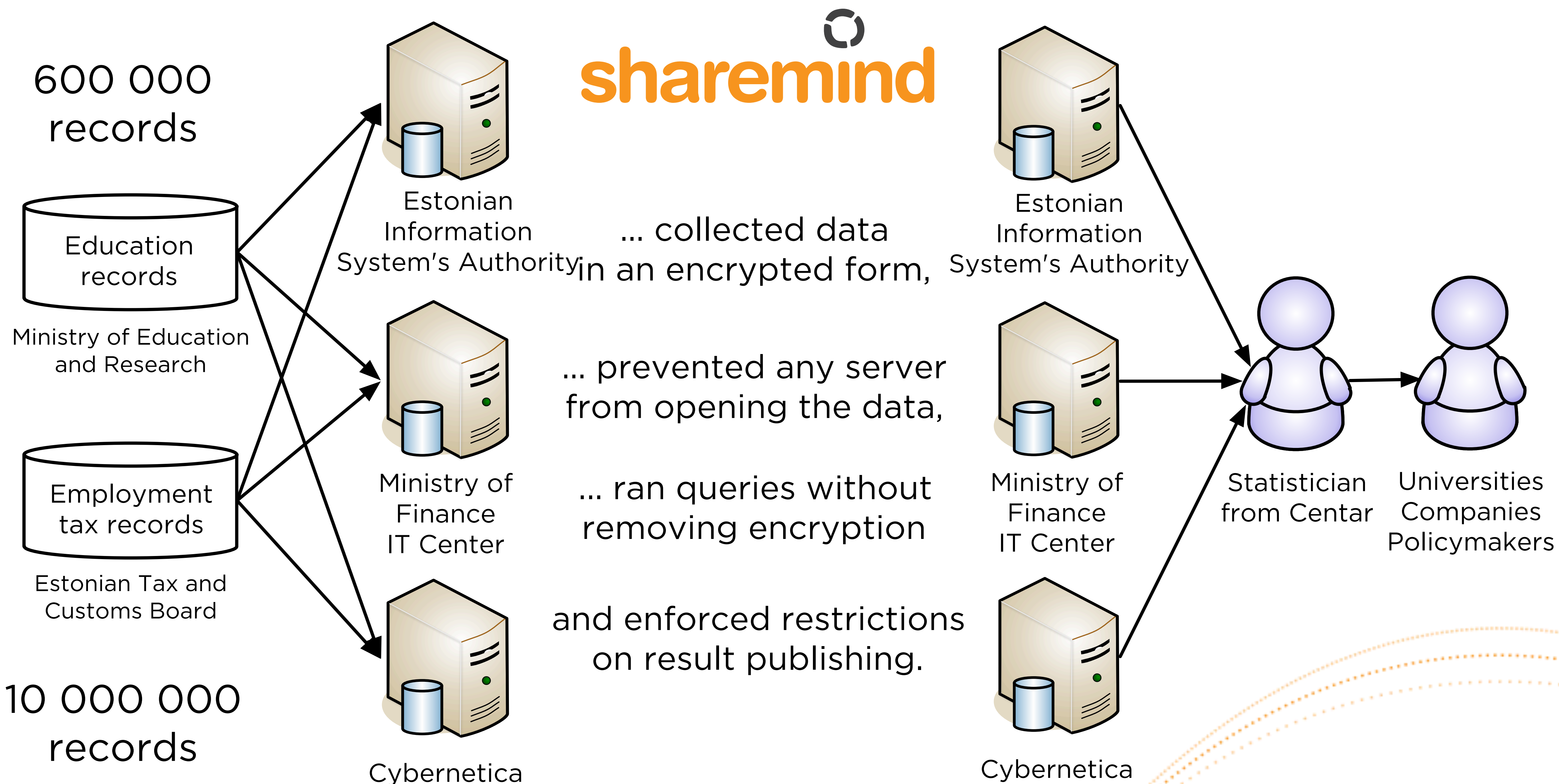
Education records



When did the student enrol?
When did he or she graduate?
In an IT curriculum?

sharemind
CYBERNETICA

Sharemind Deployment

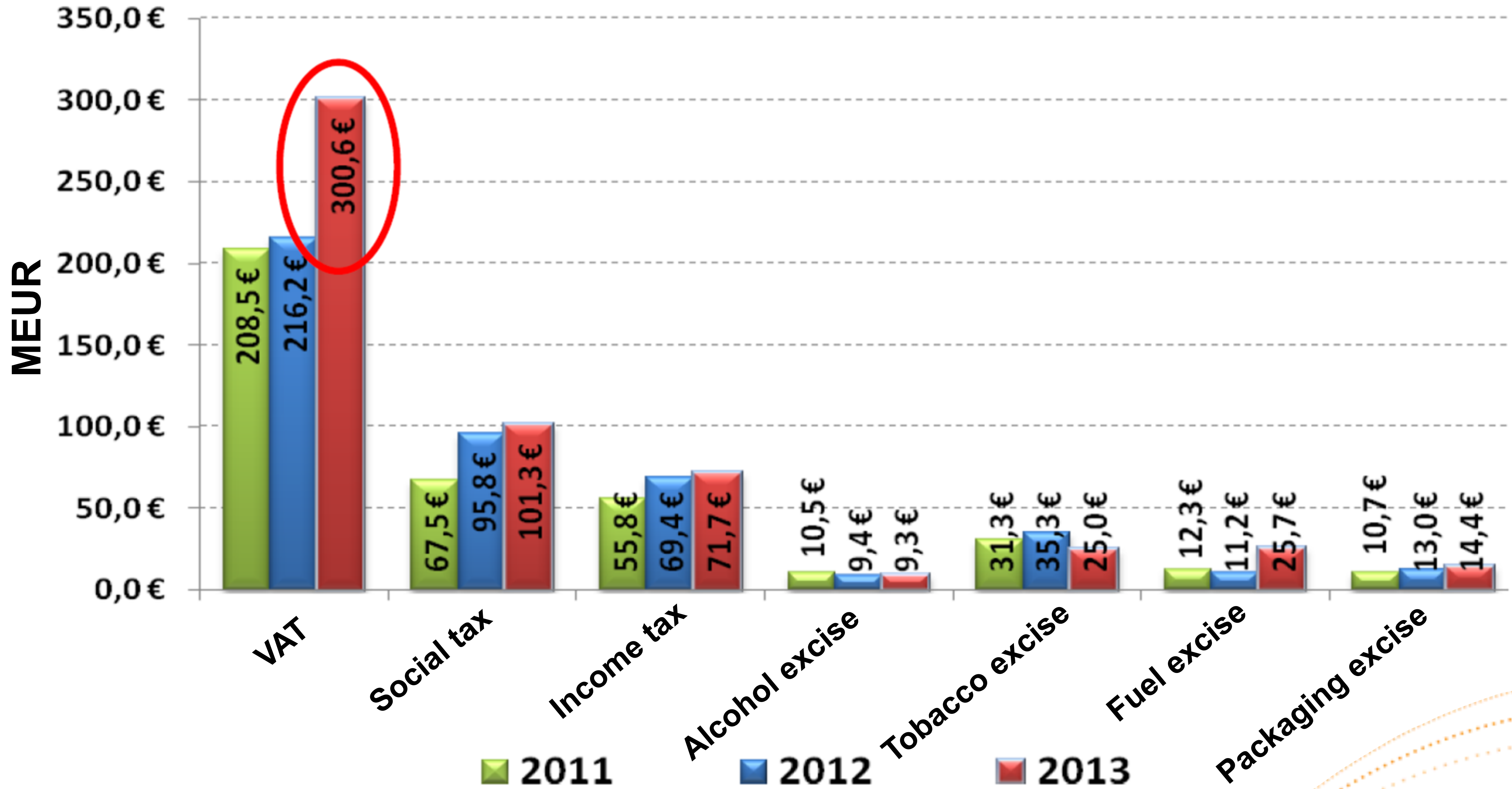


Dan Bogdanov, Liina Kamm, Baldur Kubo, Reimo Rebane, Ville Sokk, Riivo Talviste.
Students and Taxes: a Privacy-Preserving Social Study Using Secure Computation.
In Proceedings on Privacy Enhancing Technologies, PoPETs, 2016 (3), pp 117–135, 2016.

sharemind
CYBERNETICA

Secure Computing for Tax Fraud Prevention

VAT Evasion is a Problem



sharemind
CYBERNETICA

The Story of the 1000 € Law

- In 2013, the Estonian parliament ratified the Value-Added Tax Act and the Accounting Act Amendment Act that would force enterprises to report all invoices above 1000 € to the Tax and Customs Board (MTA).
- MTA then matches outgoing invoices to the incoming invoices reported by others and find companies trying to get refunds for fraudulently declared input VAT.
- President Ilves refused to proclaim the law, as "…creating a database containing almost all of Estonia's business secrets cannot be justified with a hypothetical, unproven conjecture that the tax hole would diminish."

http://news.err.ee/v/politics/5b358dbd-8836-43ca-992c-973d206a3ec6

sharemind

CYBERNETICA

Prototype with SMC

Benefits

Analyze, combine and build reports without decrypting data.

Confidentiality is guaranteed against all servers and against malicious hackers.

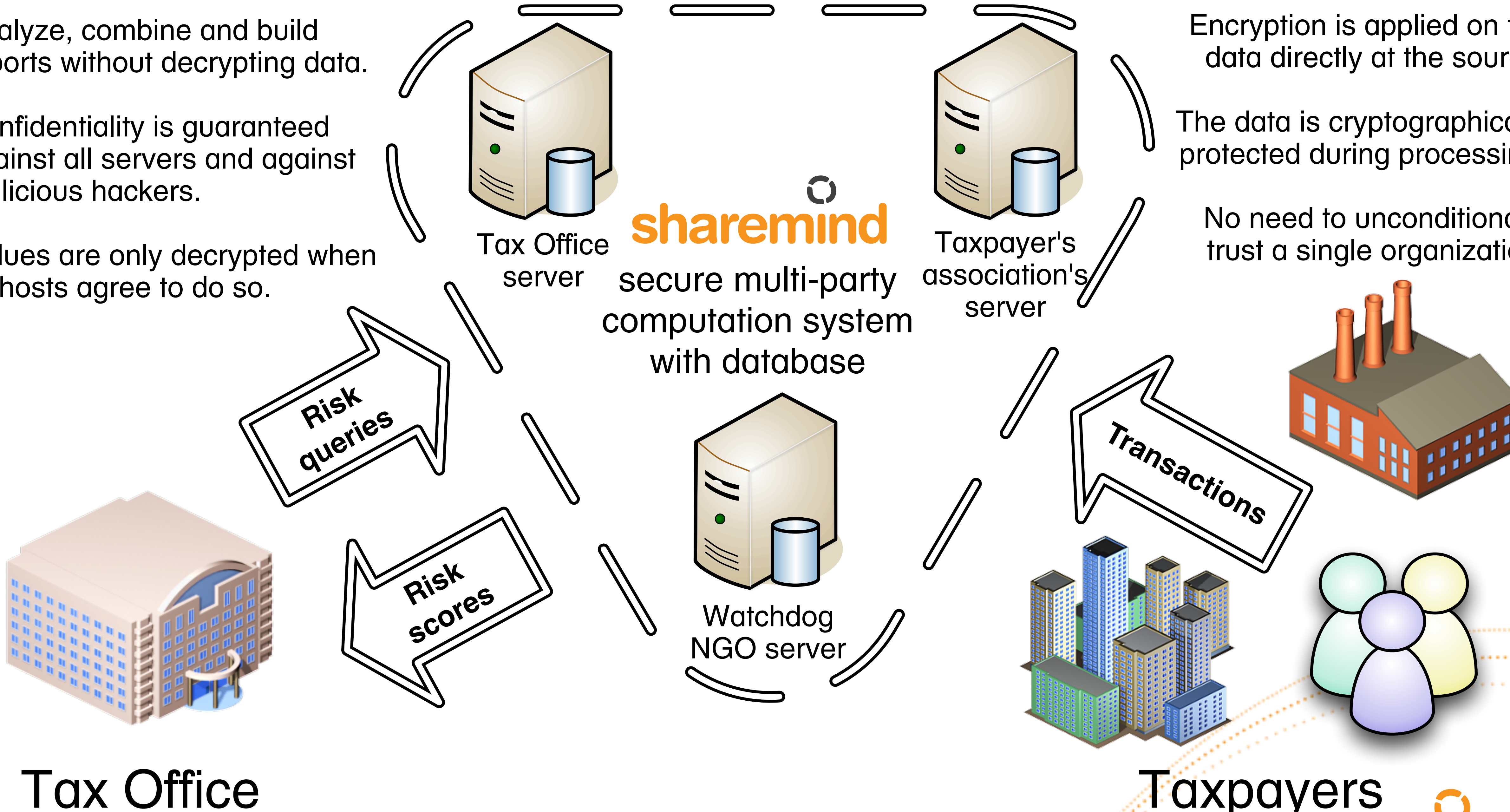
Values are only decrypted when all hosts agree to do so.

Benefits

Encryption is applied on the data directly at the source.

The data is cryptographically protected during processing.

No need to unconditionally trust a single organization.



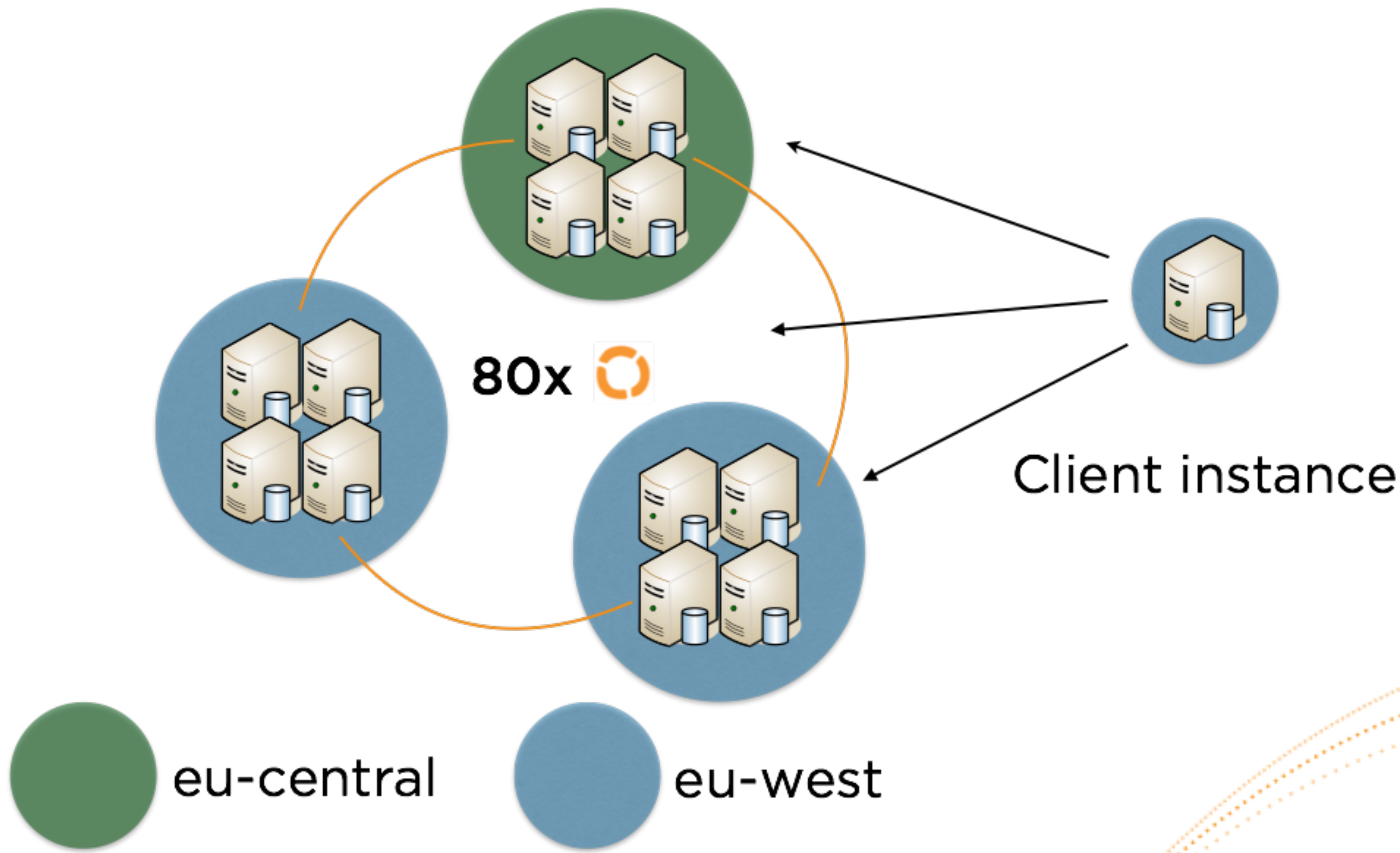
Dan Bogdanov, Marko Jõemets, Sander Siim, Meril Vaht. **How the Estonian Tax and Customs Board Evaluated a Tax Fraud Detection System Based on Secure Multi-party Computation.** Financial Cryptography and Data Security - 19th International Conference. 2015.

sharemind

CYBERNETICA

Large-scale Benchmarks

12 computing nodes running
a total of 80 Sharemind processes



PRACTICE

sharemind
CYBERNETICA

Even Larger Data Size

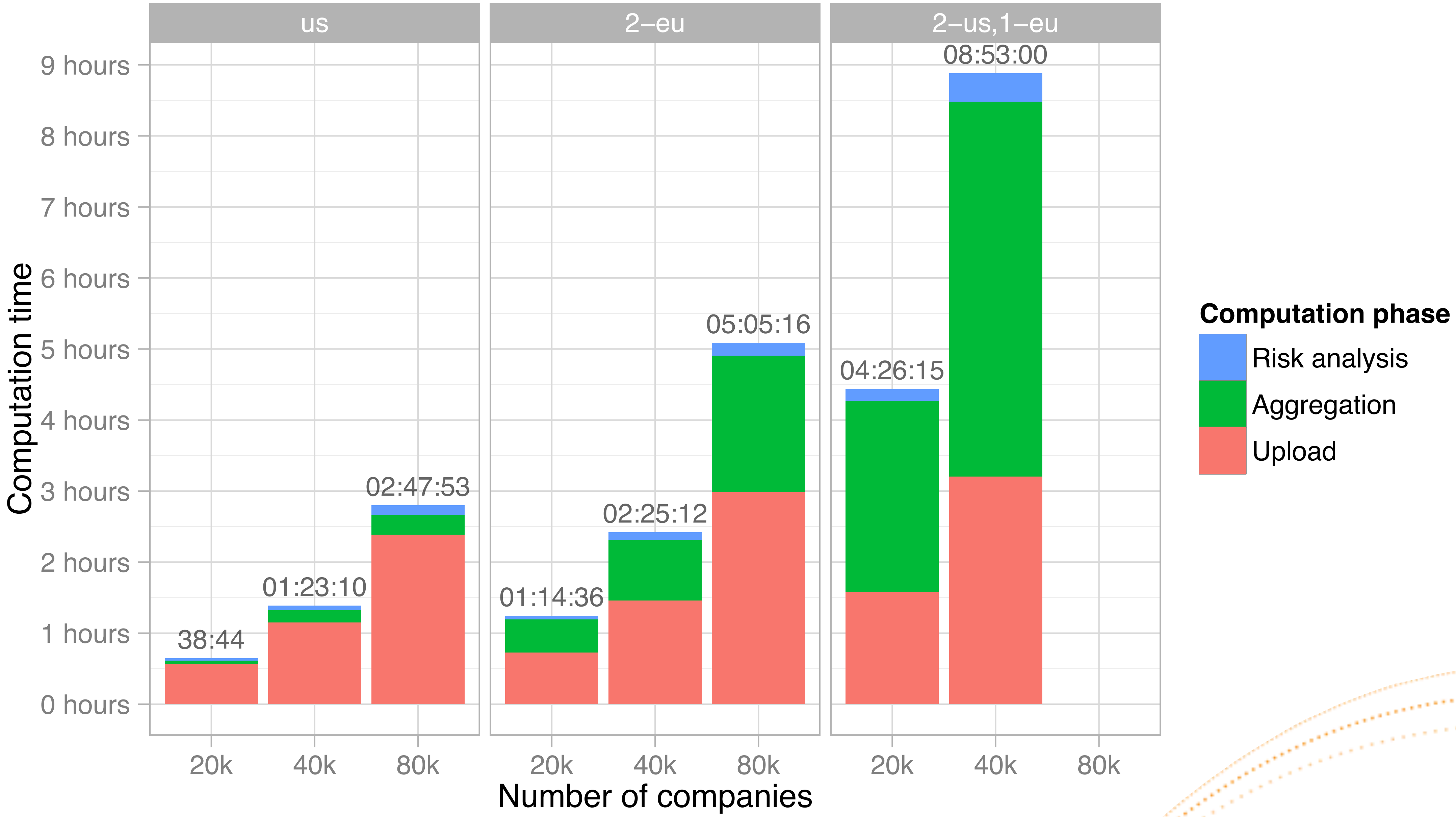
No. of companies	No. of transaction partner pairs	Total no. of transactions
20 000	200 000	25 000 000
40 000	400 000	50 000 000
80 000	800 000	100 000 000

The source data for 100 000 000 transactions had a total size of 35 GB in XML format (about 1 GB in the secret-shared database).

Computing Environment

Setup	Client	Computing parties	Latency (round-trip)
1	us-east – c3.8xlarge	us-east – 12x c3.8xlarge	< 0.1ms between all nodes
2	eu-west – c3.8xlarge	eu-west – 8x c3.8xlarge eu-central – 4x c3.8xlarge	< 0.1ms inside eu-west 19ms (eu-west/eu-central)
3	us-east – c3.8xlarge	us-east – 4x c3.8xlarge us-west – 4x c3.8xlarge eu-west – 4x c3.8xlarge	77ms (us-east/us-west) 133ms (us-west/eu-west) 76ms (us-east/eu-west)

Cross-ocean SMC Runtime



PRACTICE

sharemind

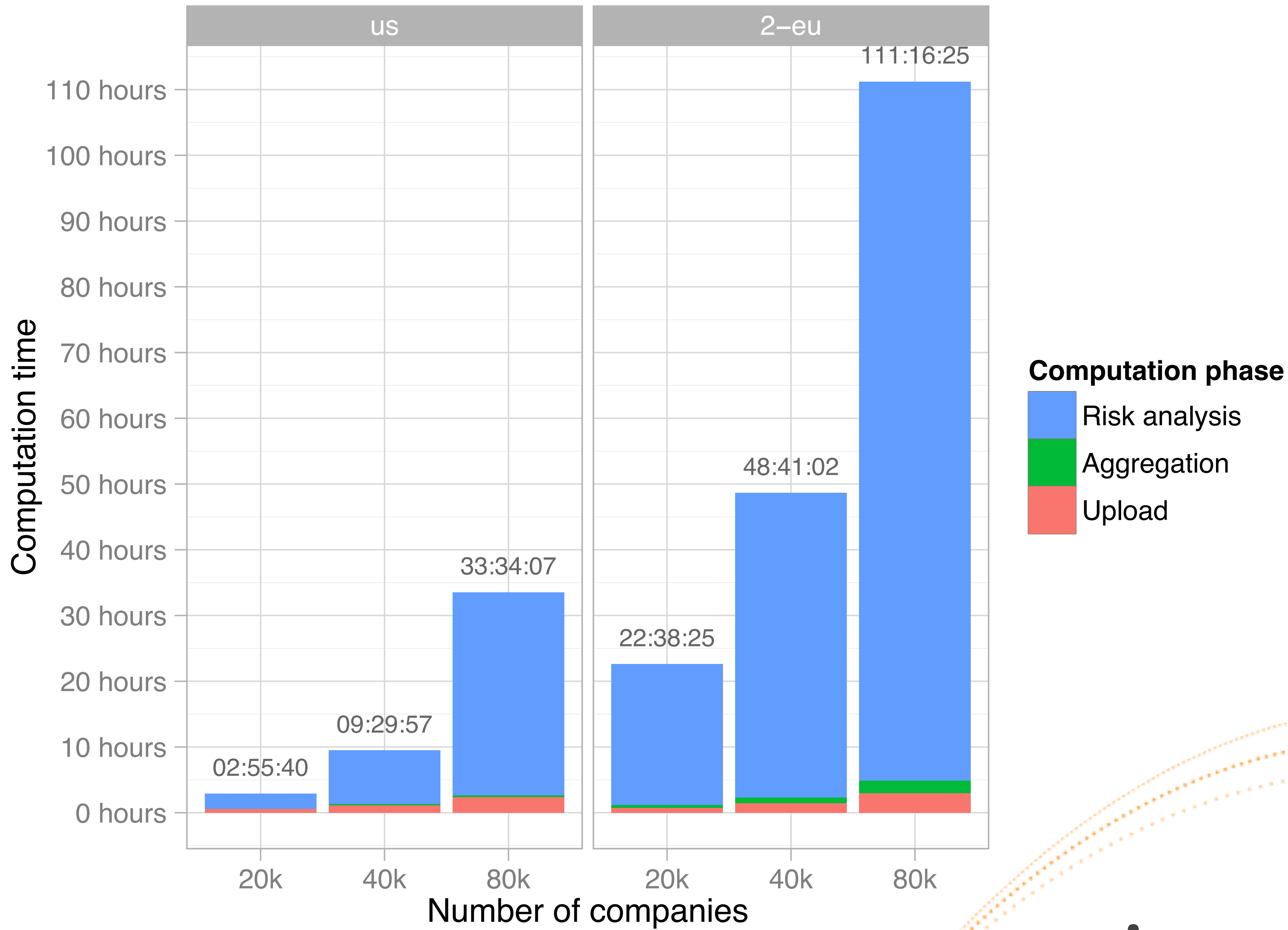
CYBERNETICA

Rather Acceptable Costs

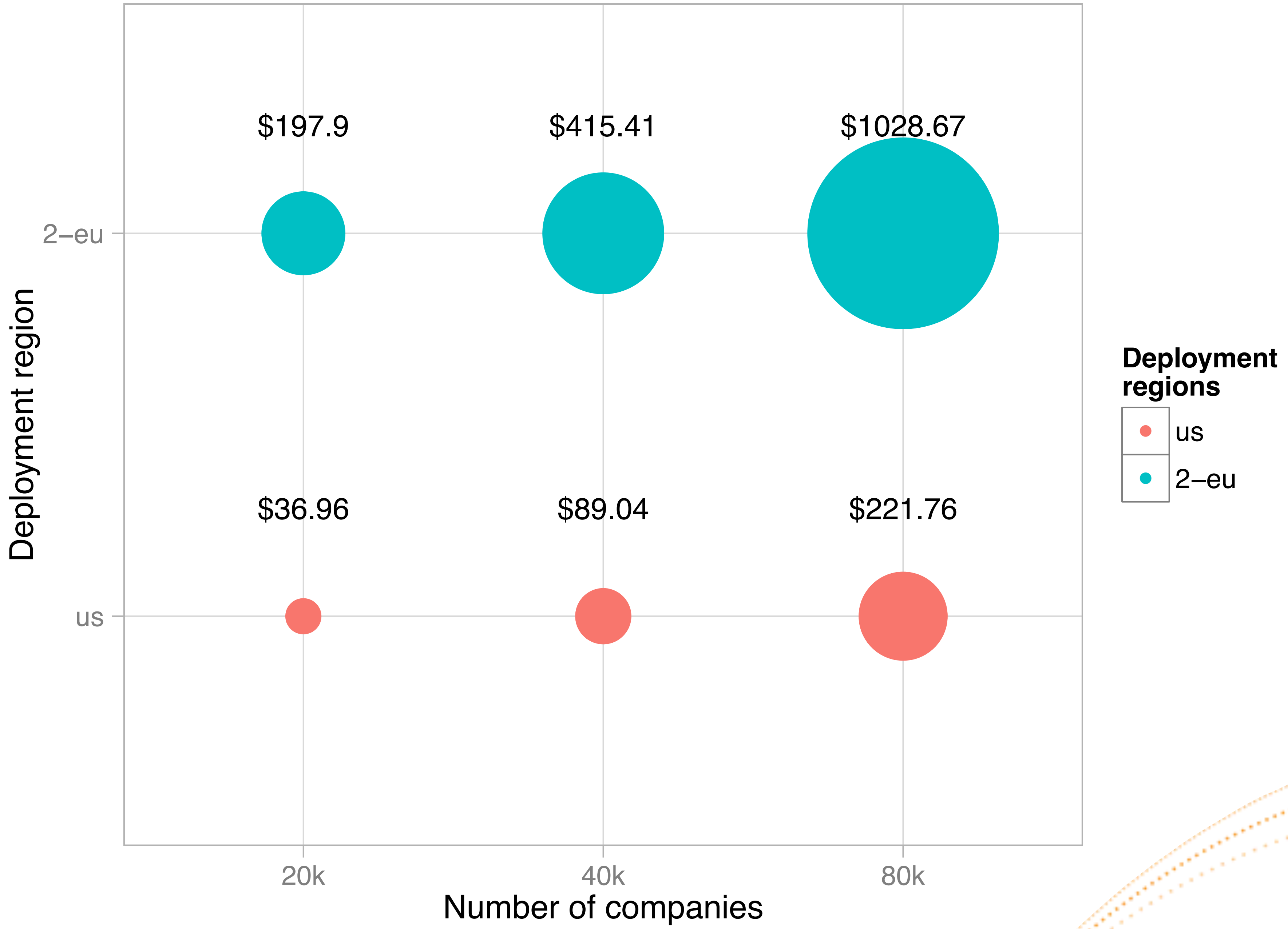
Dan Bogdanov, Marko Jõemets, Sander Siim, Meril Vaht. **Privacy-preserving tax fraud detection in the cloud with realistic data volumes.** Real World Crypto 2016 Lightning Talk. https://drive.google.com/file/d/0Bzm_4XrWnl5zVnRTRF9wT0EtUW8/view?pref=2&pli=1

sharemind CYBERNETICA

Brute force risk analysis



Cost of using brute force



PRACTICE

sharemind

CYBERNETICA

Take-home Messages

- Sharemind is designed to be a privacy platform that use secure computing as component.
  - It used to focus on three-party secure computing, but this less the case as time goes on.
- Sharemind also includes other privacy techniques like side-channel-safe statistics and audit features.
- Cybernetica is continuously developing privacy technologies for use in real-world applications.

We Build Applications

Learn about Sharemind

http://sharemind.cyber.ee/

Open source prototyping tools (under development)

http://sharemind-sdk.github.io/

Contact us for more information and collaborations

E-mail: sharemind@cyber.ee

Twitter: @sharemind

sharemind

CYBERNETICA