A Privacy-Preserving Platform
for User-Centric Quantitative Benchmarking

Dominik Herrmann
Florian Scheuer
Philipp Feustel
Thomas Nowey
Hannes Federrath

University of Regensburg, Germany

AGENDA

MOTIVATION

PROPOSED SOLUTION

EVALUATION

Classical Offline Benchmarking

Complex methodology for identification of best practices within an industry by in-depth comparison of various players.

Participants give up some privacy for a greater good: specialised (trusted) consultants learn internal details.

Benchmarking projects are often expensive and cumbersome.

Objective: Develop an Online Platform for Quantitative Benchmarking of KPIs

Addresses only a sub-problem:

enable users to compare numeric metrics with their peers without disclosing their own values

Objective: Develop an Online Platform for Quantitative Benchmarking of KPIs

Addresses only a sub-problem:

enable users to compare numeric metrics with their peers without disclosing their own values

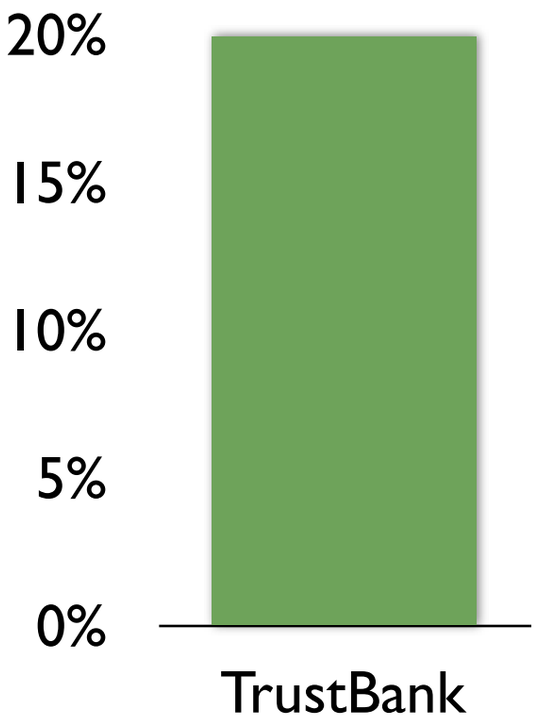
Main Contributions:

1) platform protects identity of participants
2) user-driven peer group formation
3) support for SMC protocols with differing communication models

We will only show how to **compute the sum** of KPI values.

Application Area: Financial Sector

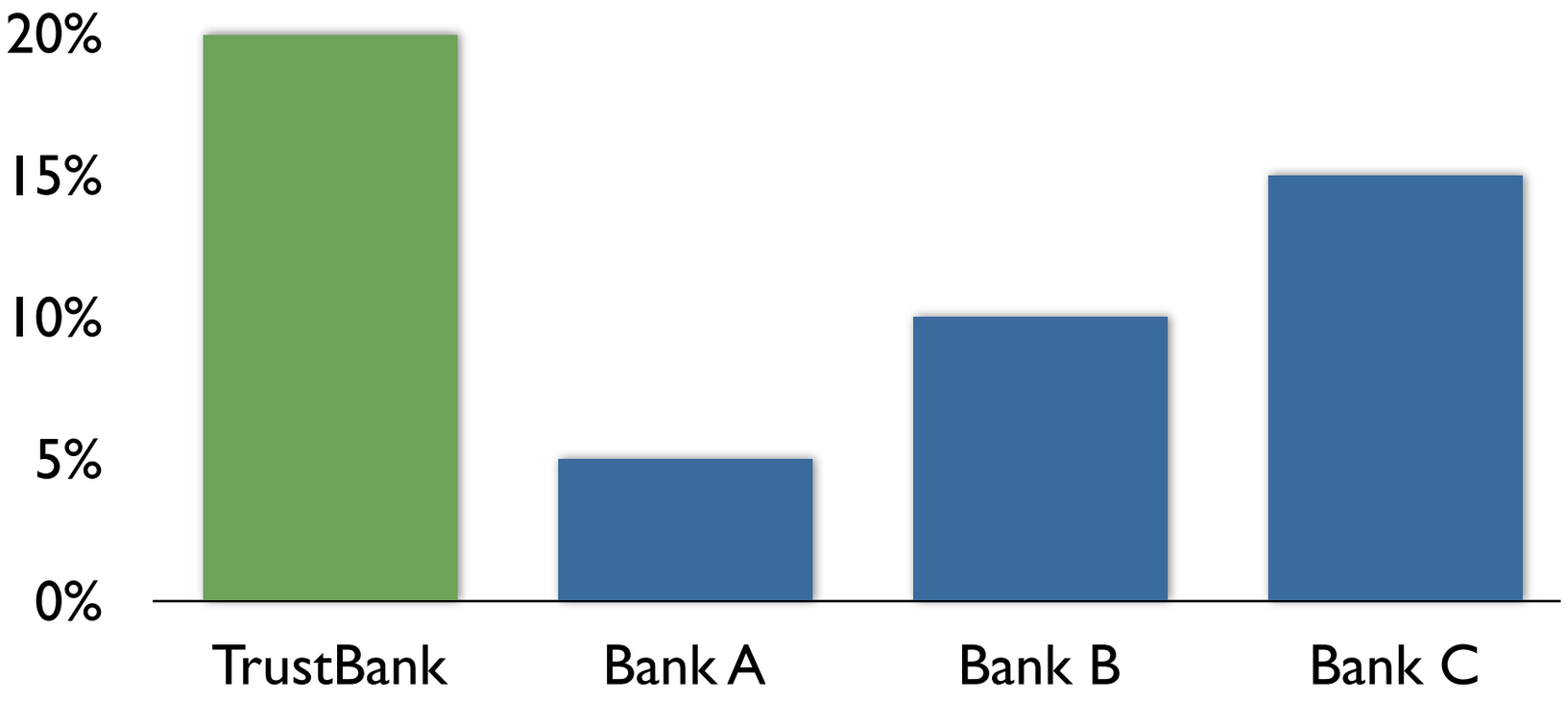
Compare business-critical metrics with competitors,
e. g. proportion of subprimes in credit portfolio



Is this too much?

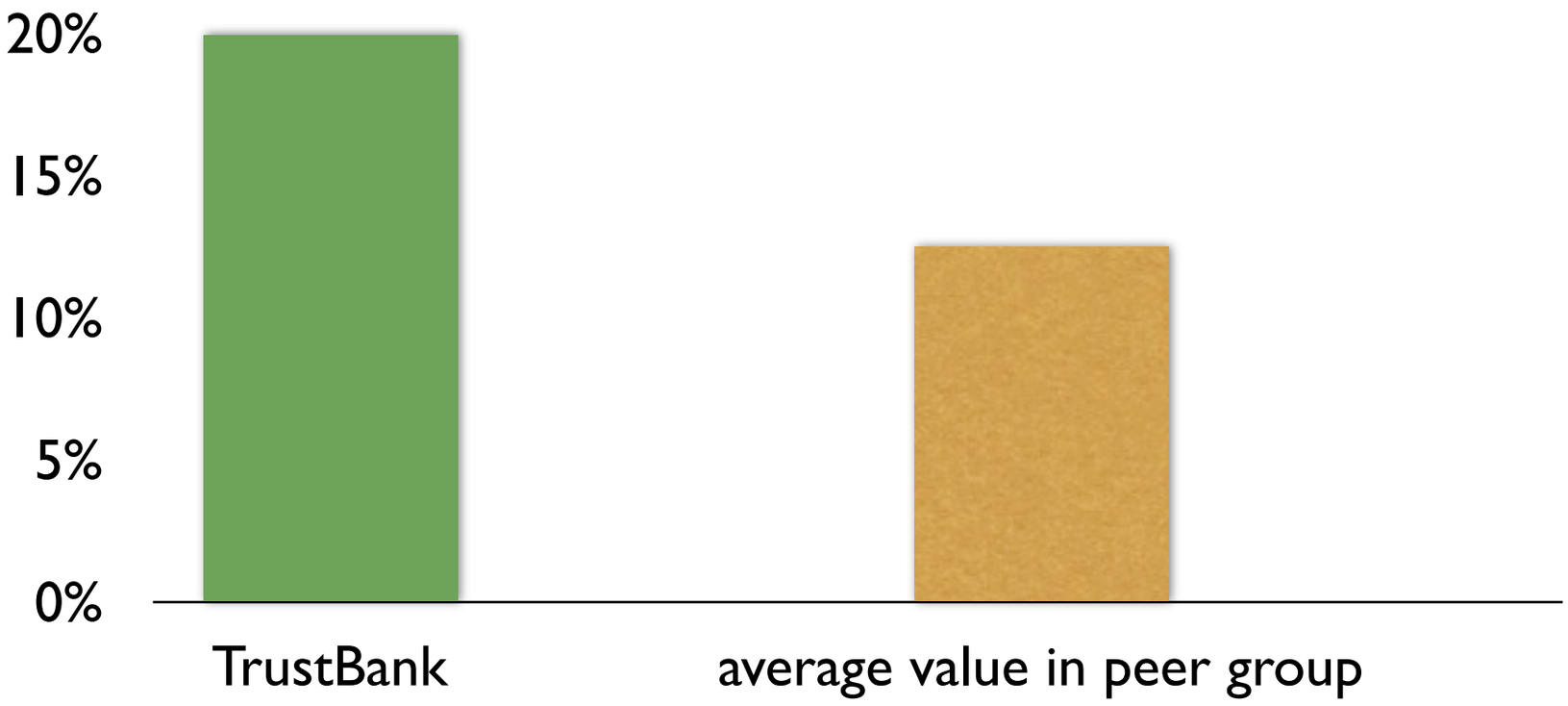
Application Area: Financial Sector

Compare business-critical metrics with competitors,
e. g. proportion of subprimes in credit portfolio



Application Area: Financial Sector

Compare business-critical metrics with competitors,
e. g. proportion of subprimes in credit portfolio



Comparison makes only sense for peer groups with a well-known profile!

Requirements

FUNCTIONALITY

- Users can request a new benchmarking at any time.
- Users can specify the peer group requirements for new benchmarkings.
- Users can view a listing of available benchmarking requests.
- Users can opt to (not) take part in announced benchmarkings.
- Support for various statistics

SECURITY

Requirements

CTIONALITY

SECURITY

- Users are anonymous against platform provider and other users.
- Benchmarked KPI values are not disclosed to provider and other users.
- Requested peer group formation is enforced by platform.

USABILIT

Requirements

TY

SECURITY

USABILITY

- Platform is built on off-the-shelf technologies.
- Communication protocol is client-driven (polling).
- Benchmarking results are available within short time.
- Platform offers satisfactory performance for reasonable loads.

Related Research

Bogetoft et al. (2002)	Internet Based Benchmarking
Crotts et al. (2006)	A Case Study on Developing an Internet-Based Competitive Analysis and Benchmarking Tool for Hospitality Industry
Kerschbaum et al. (2008)	Privacy-Preserving Benchmarking
Catrina et al. (2008)	Fostering the Uptake of Secure Multiparty Computation in E-Commerce

Identified important building blocks, but no platform available that meets our requirements.

Research Questions

1. How to combine existing building block technologies to address our requirements?

2. Will the performance of the benchmarking platform be acceptable?

AGENDA

MOTIVATION

PROPOSED SOLUTION

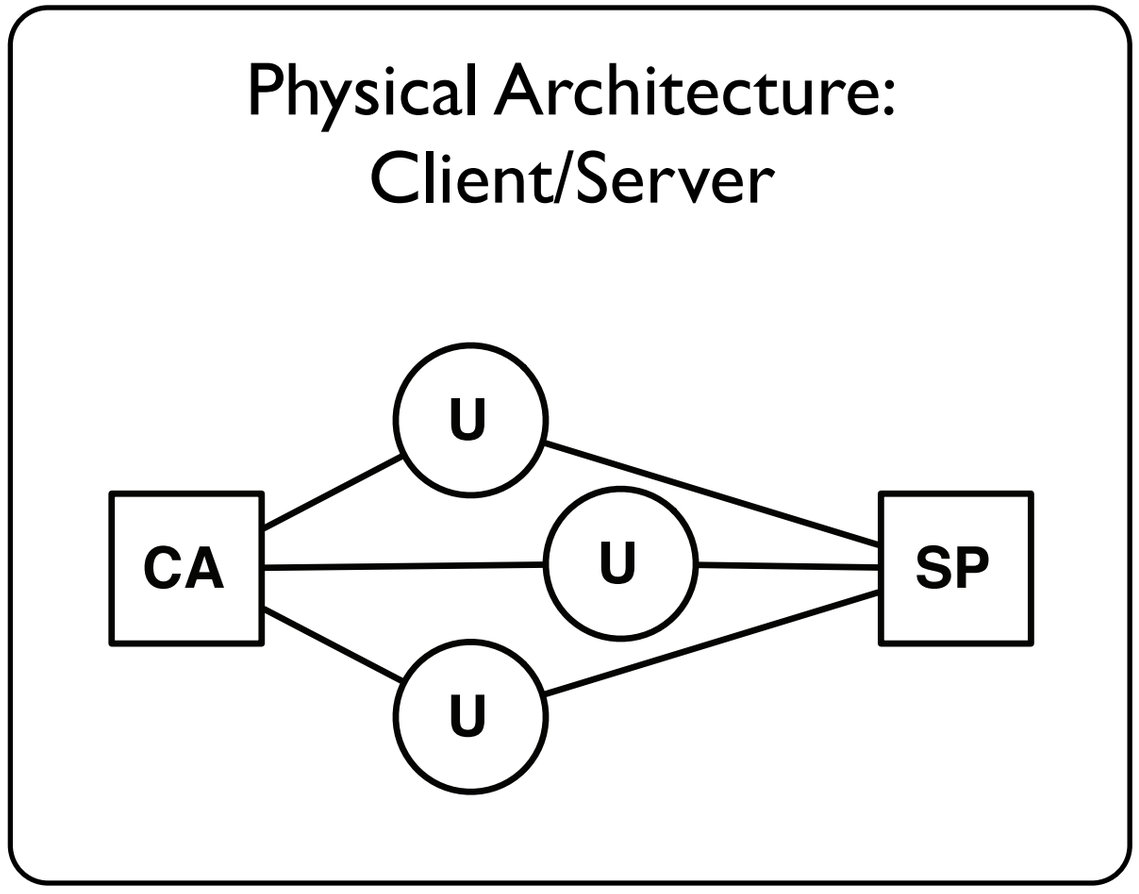
EVALUATION

Have to Address Three Main Issues

1. Protect benchmarked KPI values
2. Protect privacy of users
3. Allow for user-driven peer group formation

Architecture

U Users
SP Platform Service Provider
CA Certification Authority

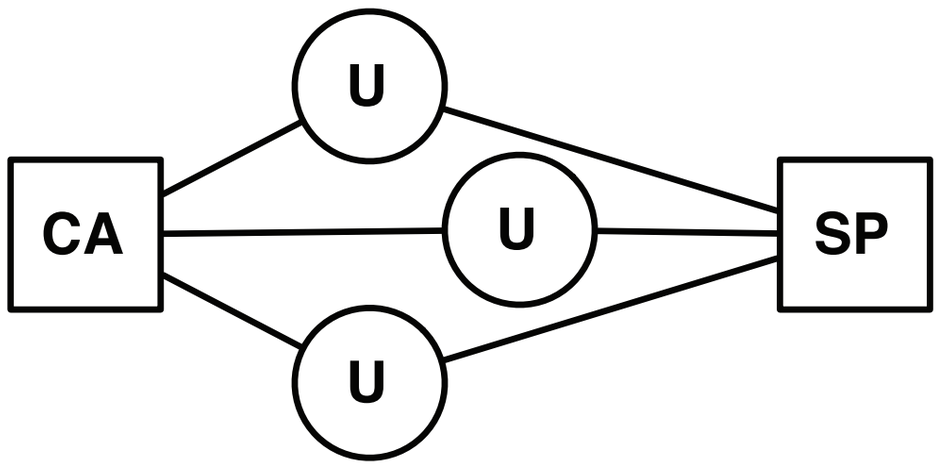


Architecture

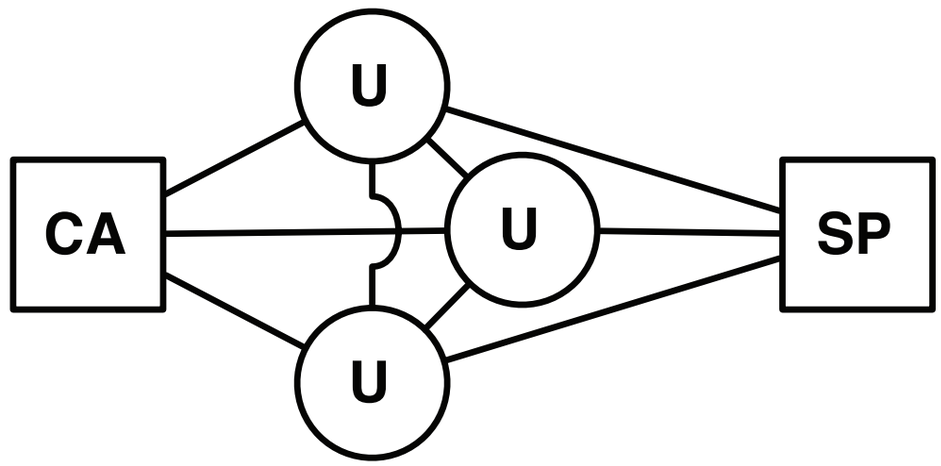
U Users
SP Platform Service Provider
CA Certification Authority

Some SMC protocols assume P2P architecture!

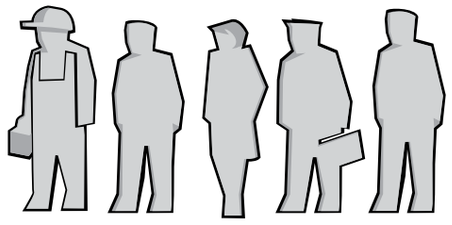
Physical Architecture:
Client/Server



end-to-end encryption
allows for P2P messages



Activities of Involved Parties

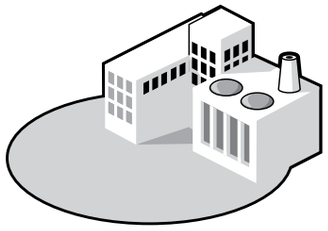


Users

register at platform

request a new benchmarking

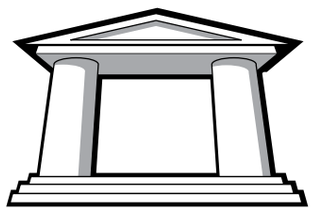
participate in published benchmarkings



SP

publishes benchmarkings and results on a bulletin

relays messages for users

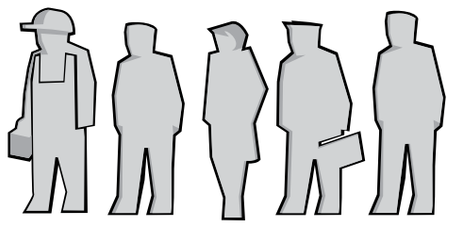


CA

checks users' identity and selection attributes

issues certificates for users

Attacker Model

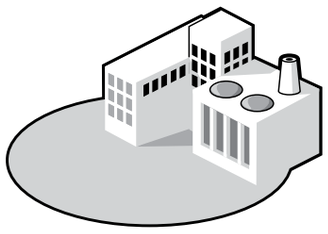


Users

honest but curious

may collude or cooperate with SP

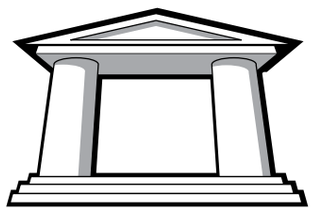
try to learn KPI values and identity of other users



SP

honest but curious

tries to learn KPI values and identity of other users



CA

trusted, does not attack

does not cooperate with SP and users

Possible extensions: truth-telling, free-riding, active attacks, ...

User-Driven Peer Group Formation

Users provide *Selection Attributes* during registration at CA:

REGISTRATION

Identity:
TrustBank & Company

Selection Attributes:
Location: Germany
No. of employees: 200
Business area: *financial services*

User specifies required *Selection Criteria* for benchmark initiation:

BENCHMARKING REQUEST

Benchmarked KPI:
proportion of subprimes

Selection Criteria:
Location = Germany
No. of employees < 500
Business area=*financial services*

Platform will allow only users with matching attributes to participate.

Protecting Privacy of Users

Only (trusted) CA knows real identity of users, SP does not.

Users are addressed with pseudonyms (public-key certificates) that do not contain any identifying information.

Selection Attributes may reveal identity, thus must not be disclosed to platform provider or other users.

Anonymity of users still at risk:
users must hide their IP address from SP!

Protection Against Intersection Attacks

Cannot use **static pseudonyms** due to intersection attacks!

INTERSECTION ATTACK RECIPE

1. Set up a benchmarking and record the set of participating pseudonyms
2. Vary selection criteria slightly
3. Go back to step 1

Intersect and compare sets to deduce actual selection attribute values of various pseudonyms.

Protection Against Intersection Attacks

Cannot use **static pseudonyms** due to intersection attacks!

INTERSECTION ATTACK RECIPE

1. Set up a benchmarking and record the set of participating pseudonyms
2. Vary selection criteria slightly
3. Go back to step 1

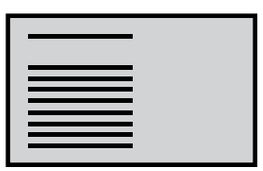
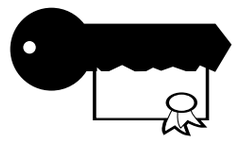
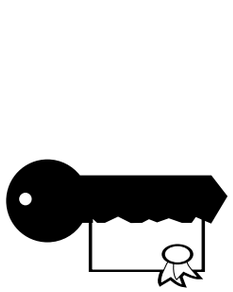
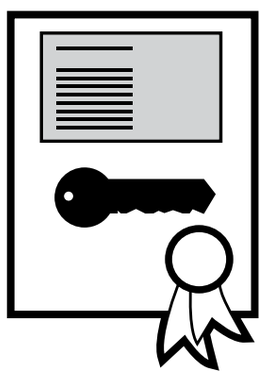
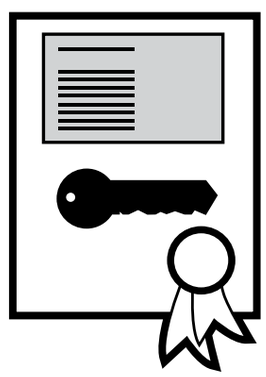
Intersect and compare sets to deduce actual selection attribute values of various pseudonyms.

Solution:
Never re-use a pseudonym!

Clients create *ephemeral key-pairs* for each new benchmarking and for each participation.

Peer Group Formation

Phase I
Register at CA

User		CA
create *permanent* key pair 	→	verify identity and correctness of *Selection Attributes*
Selection Attributes 	→	sign Permanent Public Key 
 	←	create *Attribute Certificate* 
	←	

Pebus GUIClient

File Options Help

Register | Setup benchmarking | Participate

Your identity: Pebuc Inc.

Register

Selection attribute: Location of your company

Value: Bavaria

Add Remove

Attribute Identifier	Value
numberOfEmployees	1
LocationRegion	Bavaria

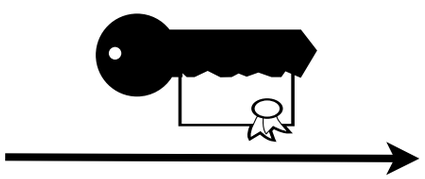
Set selection attributes

Peer Group Formation

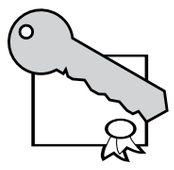
Phase 2
New Benchmarking

User

create *ephemeral*
key pair



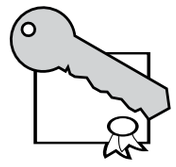
authenticate with
Permanent Key Pair



CA

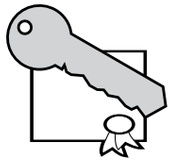
authenticate user

sign Ephemeral Public Key



Peer Group Formation

Phase 2 (cont.)
New Benchmarking

User		SP
send *Benchmarking Request*	→	
	→	
KPI (proportion of subprimes)	→	
deadline (60 minutes)	→	
Selection Criteria (Germany, financial services, 1000-10.000 employees) 	→	check signature
		publish benchmarking
		wait for participants to join

Pebus GUIClient

File Options Help

Register | Setup benchmarking | Participate

KPI: Proportion of subprimes in the asset portfolio

SMC-Profile: SumSecretSharing

Selection criteria: Location of your company = Bavaria [Add] [Remove]

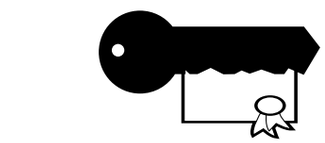
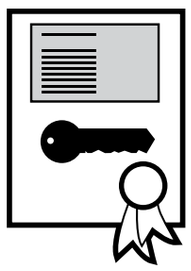
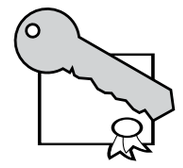
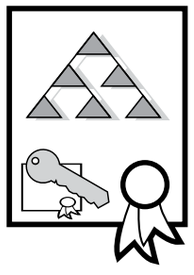
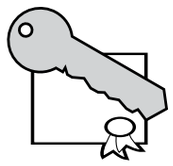
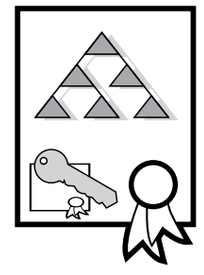
numberOfEmployees < 10
LocationRegion = Bavaria

Deadline in seconds 50

[Announce]

Peer Group Formation

Phase 3
Participation

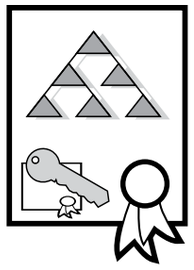
User		CA
create *ephemeral* key pair 		
	authenticate	
Selection Criteria 		iff presented *Attribute Certificate* matches *Selection Criteria*:
Attribute Certificate 		sign Ephemeral Public Key 
 		issue *Participation Certificate* 

Peer Group Formation

Phase 3 (cont.)
Participation

User

send
Participation Certificate



SP

iff presented *Selection Critera* match the ones of the benchmarking *and* certificate is valid:

accept client and add Ephemeral Public Key to *List of Participants*

once deadline is reached: publish *List of Participants*

Pebus GUIClient

File Options Help

Register | Setup benchmarking | Participate

Get announced benchmarkings

Identifier	KPI	Operator	Deadline	Selection Criteria fullfilled
1745050956	ProportionOfSubPrime...	SumSecretSharing	59 Seconds	yes

Specify your KPI for: ProportionOfSubPrimesInAssetPortfolio 23

Participate

☐ Enough participants? # 0

☐ Deadline expired? in: 0

Result: -

☐ SMC-Server started

Protection of Benchmarked KPI Values

SumSecureSplit

Robust Summation (Atallah, 2004)

P2P communication topology

O(n^2) message exchanges

Low computational complexity

SumHomomorphic

Paillier cryptosystem (1999)
with additive homomorphic
property: $E(x) \cdot E(y) = E(x + y)$

Client/server topology

O(n) message exchanges

High computational complexity

More SMC algorithms to be integrated in future work.

Pebus GUIClient

File Options Help

Register | Setup benchmarking | Participate

Get announced benchmarkings

Identifier	KPI	Operator	Deadline	Selection Criteria fullfilled
1745050956	ProportionOfSubPrime...	SumSecretSharing	59 Seconds	yes

Specify your KPI for: ProportionOfSubPrimesInAssetPortfolio 23

Participate

☑ Enough participants? # 27

☑ Deadline expired? in: 0 Seconds

☑ SMC-Server started

Result: 760

AGENDA

MOTIVATION

PROPOSED SOLUTION

EVALUATION

Prototypical Implementation

Implementation in Java SE 5

All connections encrypted with TLS

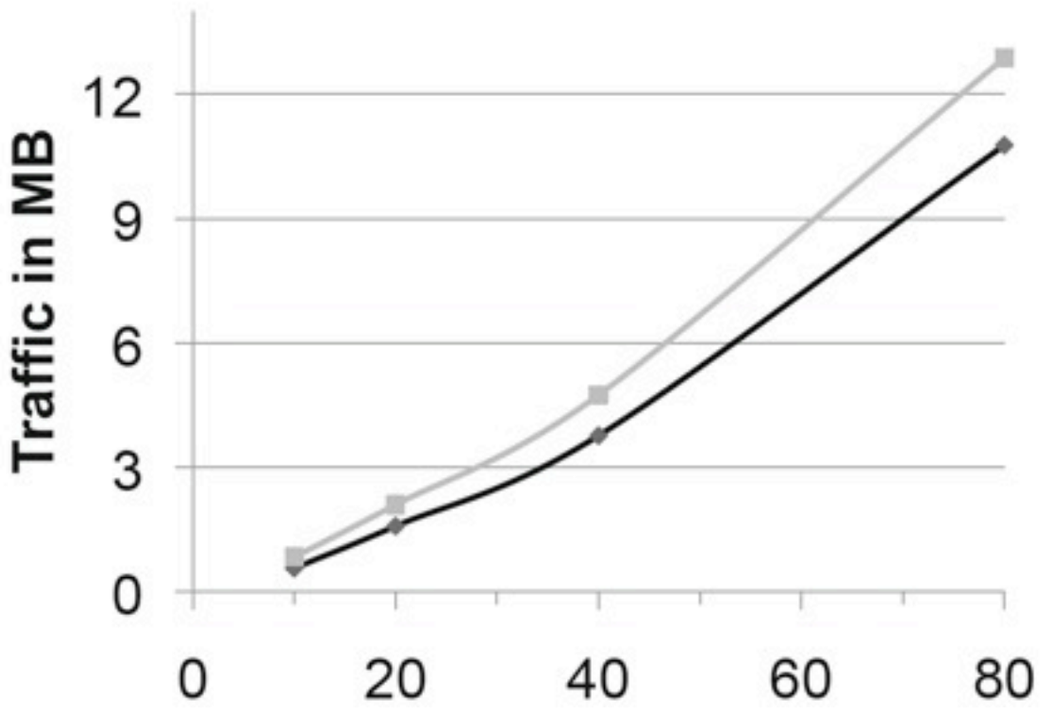
Hybrid encryption of P2P messages

Proprietary XML message format

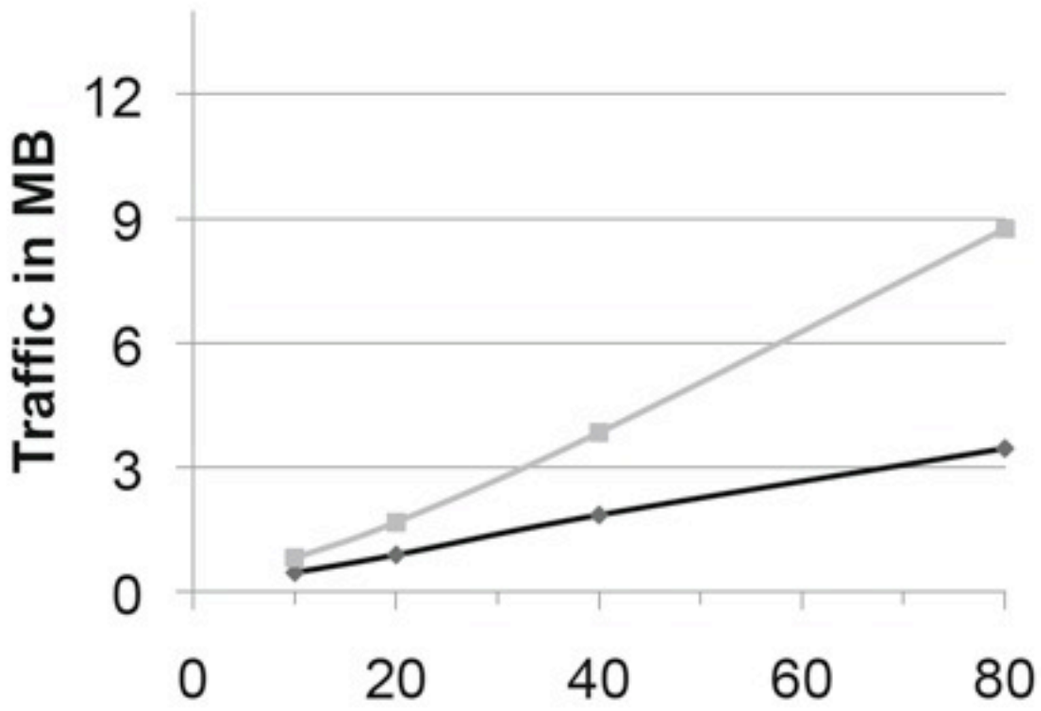
Client can be automated for evaluation

SumHomomorphic induces less traffic

Total server-side traffic of one benchmarking
for varying number of participants



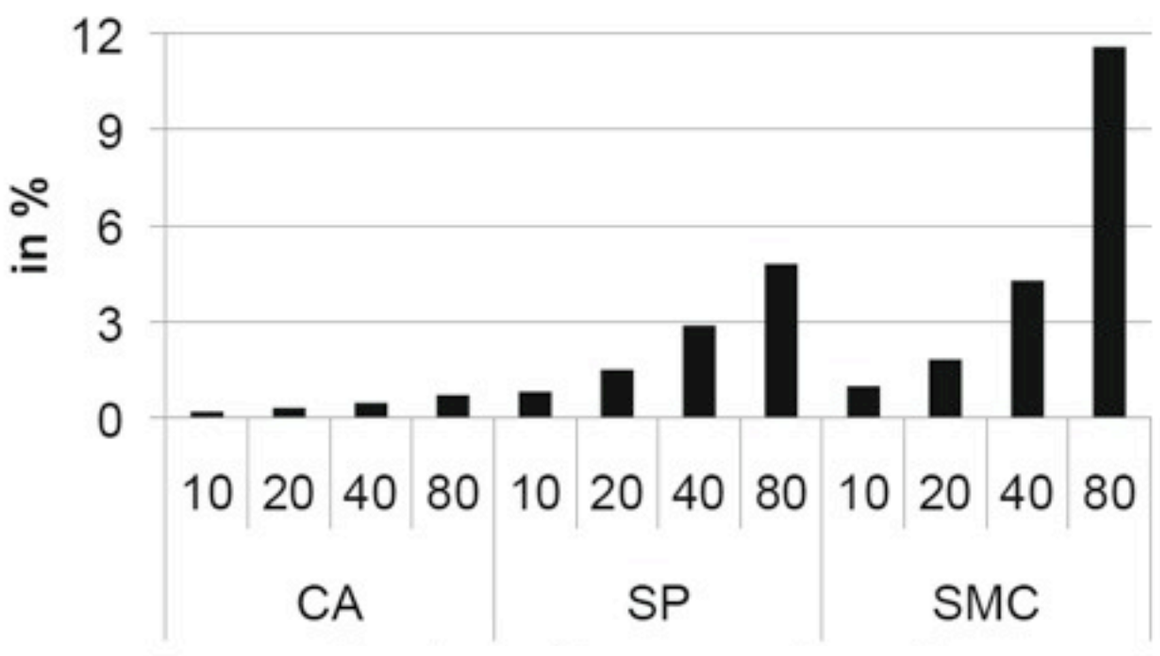
SumSecureSplit



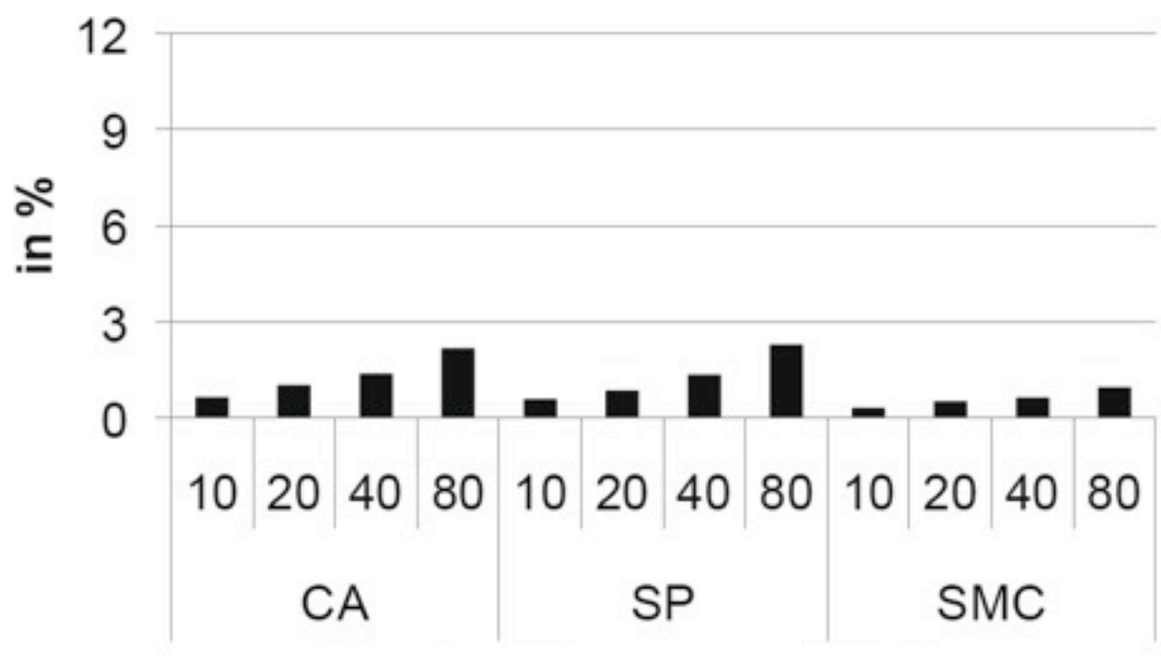
SumHomomorphic

SumHomomorphic induces less load

Average CPU load of server components
for varying number of participants



SumSecureSplit



SumHomomorphic

In Conclusion

Our platform facilitates quantitative benchmarking with user-controlled peer group formation.

It offers practical anonymity and unlinkability to its users.

Performance of implemented secure multi-party computation protocols is sufficient for our purpose.

Summation with Paillier crypto system is more efficient than Robust Summation.

Dominik Herrmann

dominik.herrmann@wiwi.uni-r.de http://www-sec.uni-regensburg.de/herrmann/