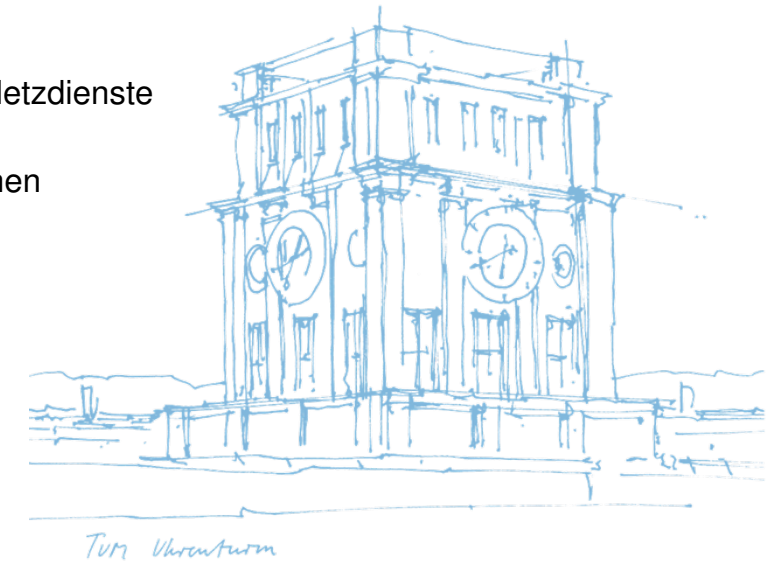
Lehrstuhl für Netzarchitekturen und Netzdienste
Fakultät für Informatik
Technische Universität München

Sichere und Privatheitsschützende Dienste auf Basis von Secure Multiparty Computation

Marcel von Maltitz

30. Juli 2019

Lehrstuhl für Netzarchitekturen und Netzdienste
Fakultät für Informatik
Technische Universität München



Motivation

Zielsetzung

Eigene Beiträge

- Empirische Analyse – Performance
- SMC as a Service

Zusammenfassung

Motivation

Sensordaten

Generierung und Verarbeitung von Sensordaten hat stark zugenommen

Beispiele:

- Smartphone, Wearables
- Smart Spaces, Intelligente Gebäude
- Industrie 4.0, Internet der Dinge

Motivation

Sensordaten

Generierung und Verarbeitung von Sensordaten hat stark zugenommen

Beispiele:

- Smartphone, Wearables
- Smart Spaces, Intelligente Gebäude
- Industrie 4.0, Internet der Dinge

Privatheit und Datenschutz

Bewusstsein für Privatheit und Datenschutz hat zugenommen

- Durch NSA-Leaks (2013), Datenschutzgrundverordnung (2018), . . .
- Forderung von Privacy und Datensparsamkeit in technischen Systemen

Zielsetzung

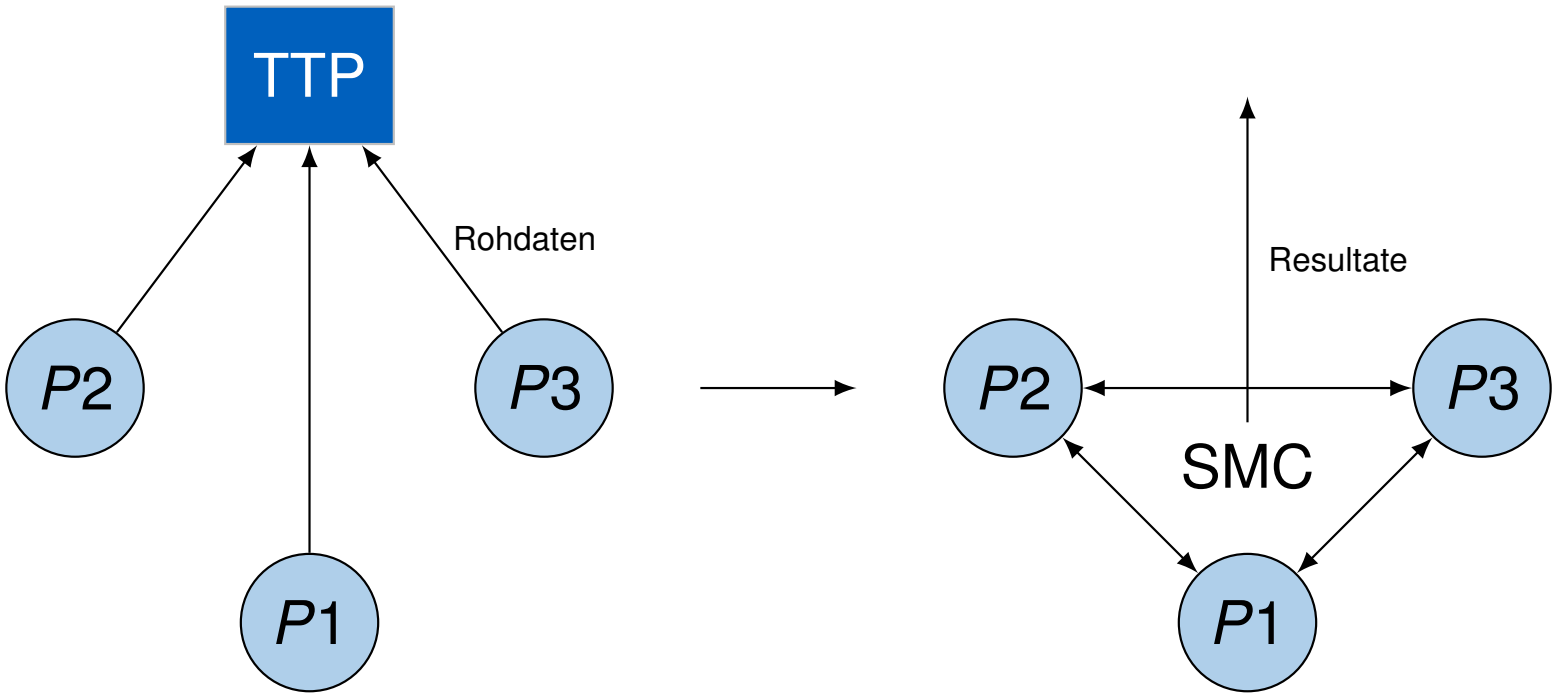
Wie ist privatheitsschützende Verarbeitung von Sensordaten möglich?

Zielsetzung

Wie ist privatheitsschützende Verarbeitung von Sensordaten möglich?

Kryptographischer Ansatz

Secure Multiparty Computation



Eigene Beiträge

Problem- und Lösungsdomäne

Empirische Analyse

Konstruktion
SMC as a Service

Eigene Beiträge

Problem- und Lösungsdomäne

- Privatheit
- SMC

Empirische Analyse

Konstruktion
SMC as a Service

Forschungsfrage

- Welches Verständnis von Privatheit kann zur Entwicklung privatheitsschützender Technologie herangezogen werden?

Beiträge

- Definitionsfindung für Privatheit
  - Historische Entwicklung des Begriffs
  - Unterschiedliche Definitionsversuche
  - Eignung für technische Fragestellungen
- Stand der Technik
  - Historische Entwicklung von SMC
  - Sicherheits- und Angreifermodelle
  - Mathematische Realisierungen

Eigene Beiträge

Problem- und Lösungsdomäne

- Privatheit
- SMC

Empirische Analyse

- Performance
- Infrastruktur
- Privatheit

Konstruktion
SMC as a Service

Forschungsfragen

- Was sind die Leistungseigenschaften von SMC und welche Einsatzumgebung legen sie nahe?
- Welche infrastrukturellen Anforderungen müssen beim Einsatz von SMC erfüllt werden?
- Welche Privatheitsanforderungen werden durch SMC bereits erfüllt?

Beiträge

- Quantitative Analyse
  - Einfluss von Host- und Netzwerkparametern
  - Zeitkosten und Ressourcenauslastung
- Qualitative Analyse
  - Fallstudie: Multizentrische Studien mit Patientendaten
  - Bewertung von SMC auf Basis von Privatheitsdefinition

Eigene Beiträge

Problem- und Lösungsdomäne

- Privatheit
- SMC

Empirische Analyse

- Performance
- Infrastruktur
- Privatheit

Konstruktion
SMC as a Service

- Anforderungsanalyse
- Orchestrierung & Self-Management
- Datenabfrage & Zugriffskontrolle

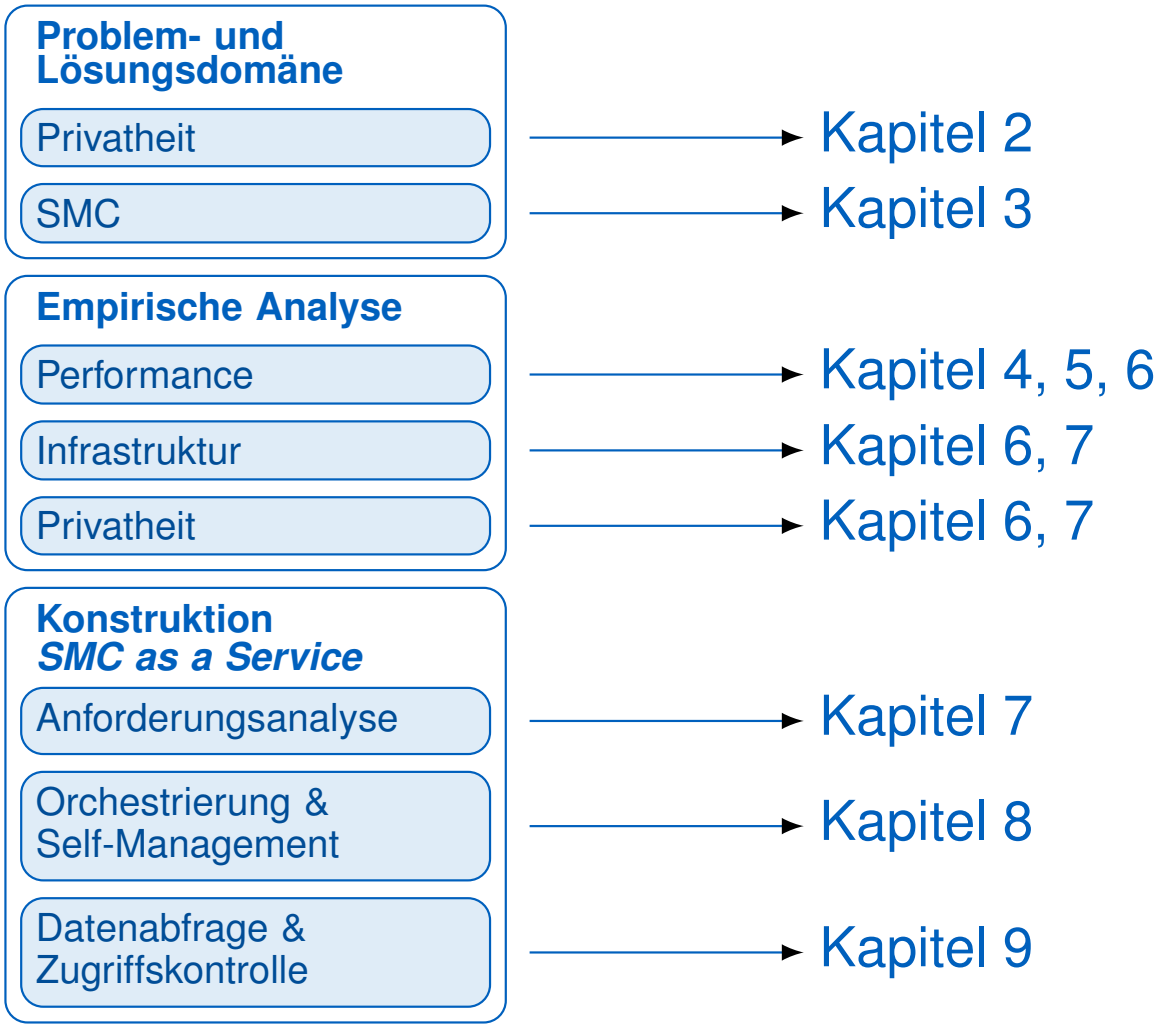
Forschungsfragen

- Wie kann SMC verlässlich in dynamischen Umgebungen genutzt werden?
- Wie kann ein vollständig privatheitsschützender Dienst auf Basis von SMC realisiert werden?

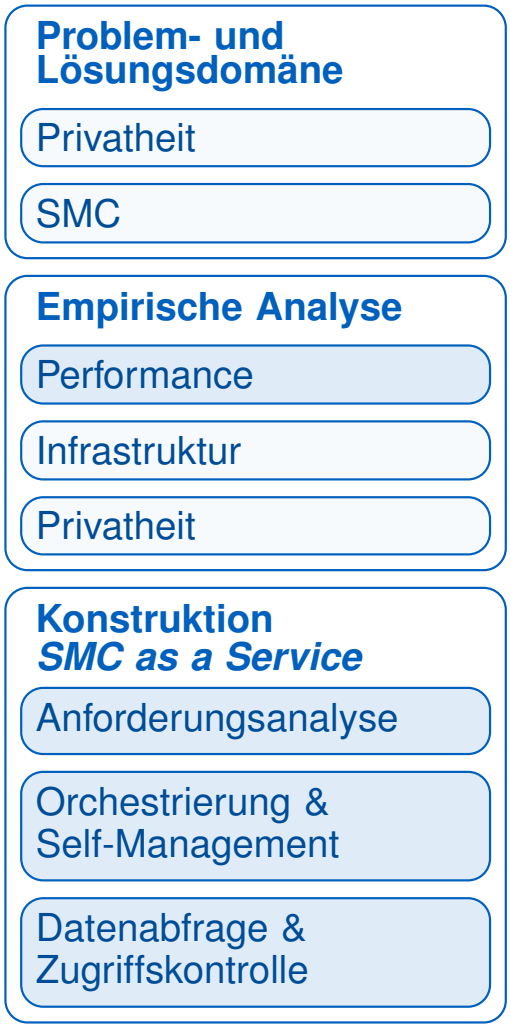
Beiträge

- Orchestrierungslösung für SMC
  - Selbst-Management, Robuste Ausführung, Sitzungsverwaltung
- Dienstabstraktion für SMC
  - Abfragesprache, Zugriffskontrolle
- Transparenz und Intervenierbarkeit für SMC

Eigene Beiträge



Eigene Beiträge



- M. von Maltitz and G. Carle. A Performance and Resource Consumption Assessment of Secret Sharing based Secure Multiparty Computation.
  In *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Springer, 2018
- M. von Maltitz and G. Carle. Leveraging Secure Multiparty Computation in the Internet of Things.
  In *Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services*. ACM Press, 2018
- M. von Maltitz, S. Smarzly, H. Kinkelin, and G. Carle. A Management Framework for Secure Multiparty Computation in Dynamic Environments.
  In *Proceedings of 30th IEEE/IFIP Network Operations and Management Symposium*. IEEE, 2018
- M. von Maltitz, D. Bitzer, and G. Carle. Data Querying and Access Control for Secure Multiparty Computation.
  In *Proceedings of the 16th IFIP/IEEE International Symposium on Integrated Network Management*. IEEE, 2019

Eigene Beiträge

Problem- und Lösungsdomäne

- Privatheit
- SMC

Empirische Analyse

- Performance
- Infrastruktur
- Privatheit

Konstruktion
SMC as a Service

- Anforderungsanalyse
- Orchestrierung & Self-Management
- Datenabfrage & Zugriffskontrolle

Empirische Analyse – Performance

Problem- und Lösungsdomäne
- Privatheit
- SMC

Empirische Analyse
- Performance
- Infrastruktur
- Privatheit

Konstruktion
SMC as a Service
- Anforderungsanalyse
- Orchestrierung & Self-Management
- Datenabfrage & Zugriffskontrolle

SMC-Implementierung FRESCO als technische Basis für Messungen

Baseline-Messungen

- Protokoll: Running Average
- Daten: GPS-Daten
- Infrastruktur: lokale Testsysteme
- Zielsetzung: Best-Case-Analyse

Real-World-Anwendungsfall

- Protokoll: Kaplan-Meier-Schätzer & Log-Rank-Test
- Daten: Patientendaten der LMU und Charité Berlin
- Infrastruktur: lokale Testsysteme und Server bei LMU/Charité
- Zielsetzung: Realistischer Anwendungsfall

Empirische Analyse – Performance

A Performance and Resource Consumption Assessment of Secret Sharing based Secure Multiparty Computation.

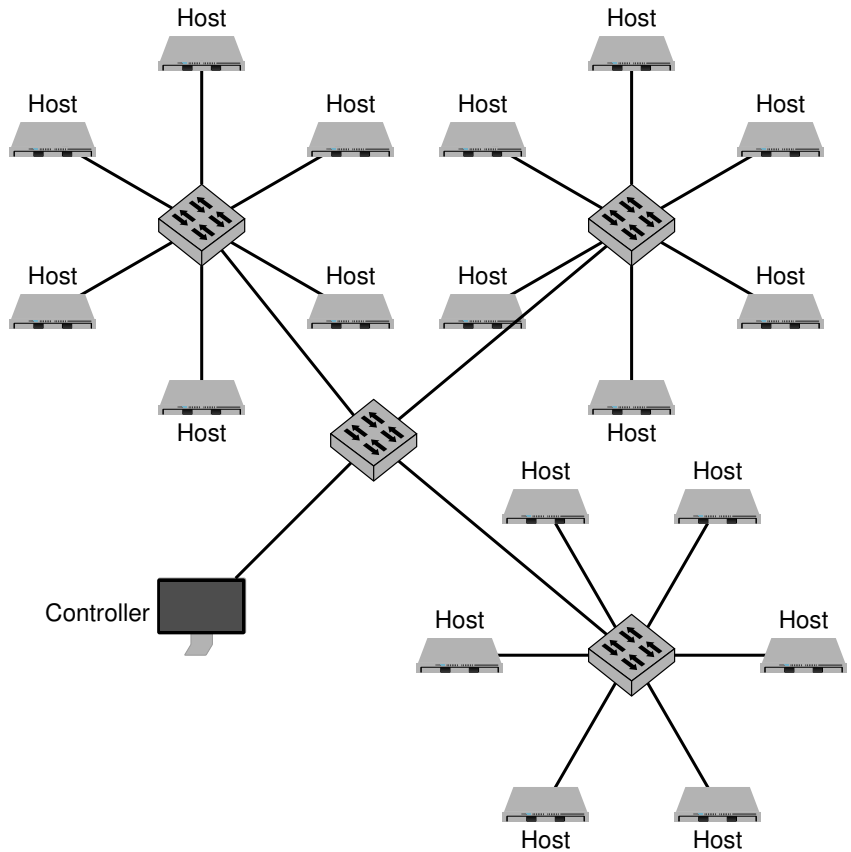
M. von Maltitz and Georg Carle. (2018, European Symposium on Research in Computer Security, DPM Workshop)

	Secret Sharing	$\lvert$Teilnehmer$\rvert > 2$	Ausführungszeit	Ausnutzung Hostressourcen	Ausnutzung Netzressource	Teilnehmer & Eingabemenge	Hostparameter	Netzparameter
Pinkas et al. [12]	nein	✗	✓	✗	✓	✓	✗	✗
Bogdanov et al. [2]	ja	○	✓	✗	✗	✓	✗	✗
Bogdanov et al. [3]	ja	○	✓	✗	✗	✓	✗	✗
Ben-David et al. [1]	nein	✓	✓	✗	✗	✓	○	✗
Henecka et al. [10]	nein	✗	✓	✗	✓	✓	✗	✗
Keller et al. [11]	ja	✓	✓	✗	✓	✓	✗	✓
Burkhart [7]	ja	✓	✓	✓	✓	✓	✗	✗
Diese Arbeit	ja	✓	✓	✓	✓	✓	✓	✓

Empirische Analyse – Performance

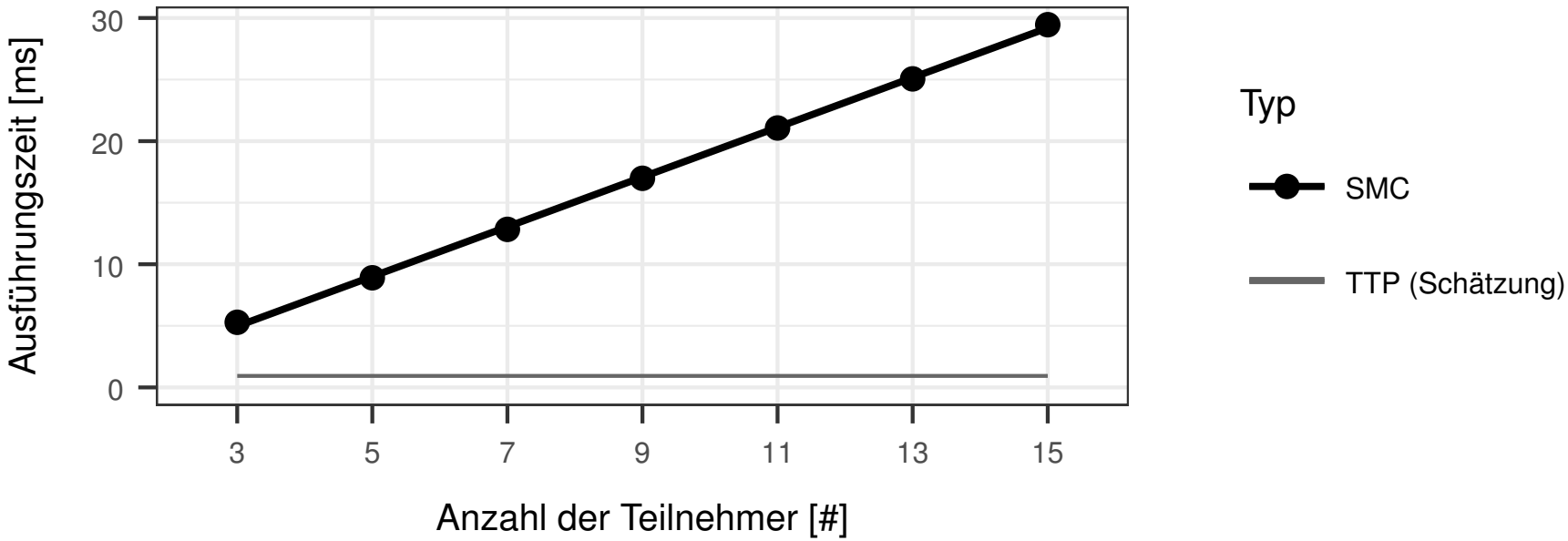
Testinfrastruktur

- Intel Xeon E3-1265L V2 CPU, 8 Kerne, 2.50GHz, Cache 8192 KB
- 16 GB RAM
- 1Gbit Netzwerkschnittstelle



Empirische Analyse – Performance

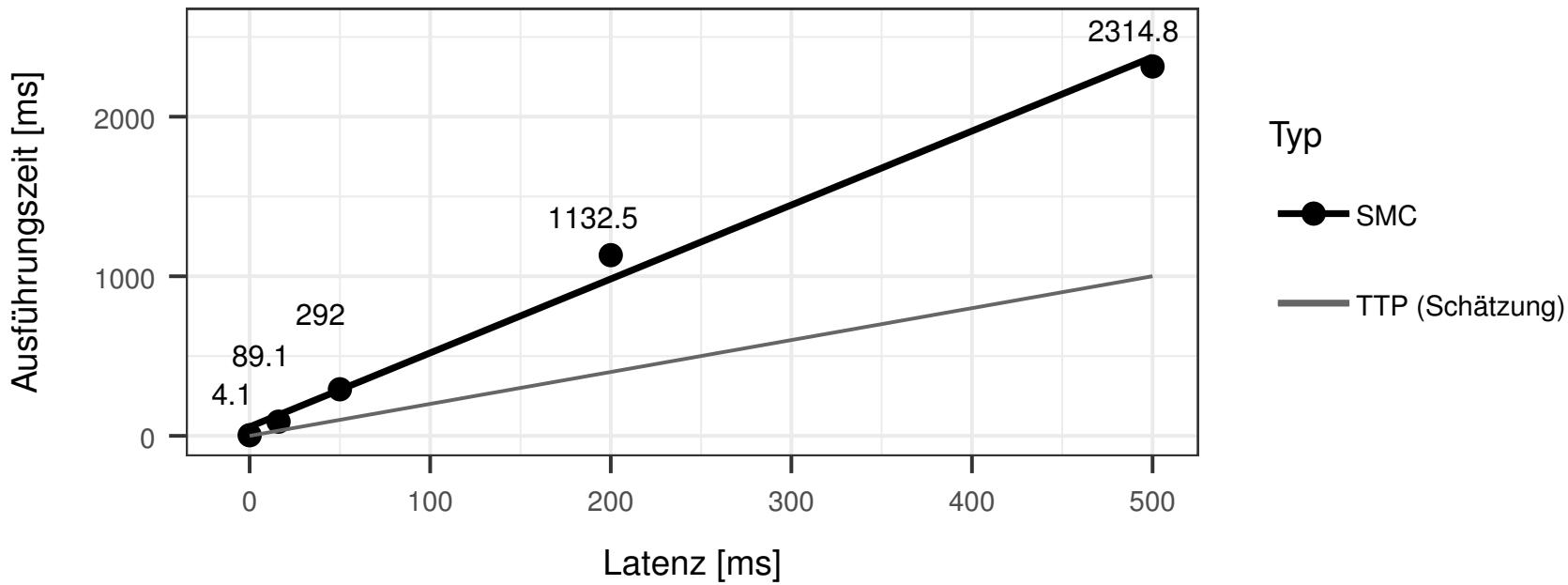
Anzahl der Teilnehmer



Verzögerung pro Teilnehmer und Berechnung: ~ 2 – 3 ms

Empirische Analyse – Performance

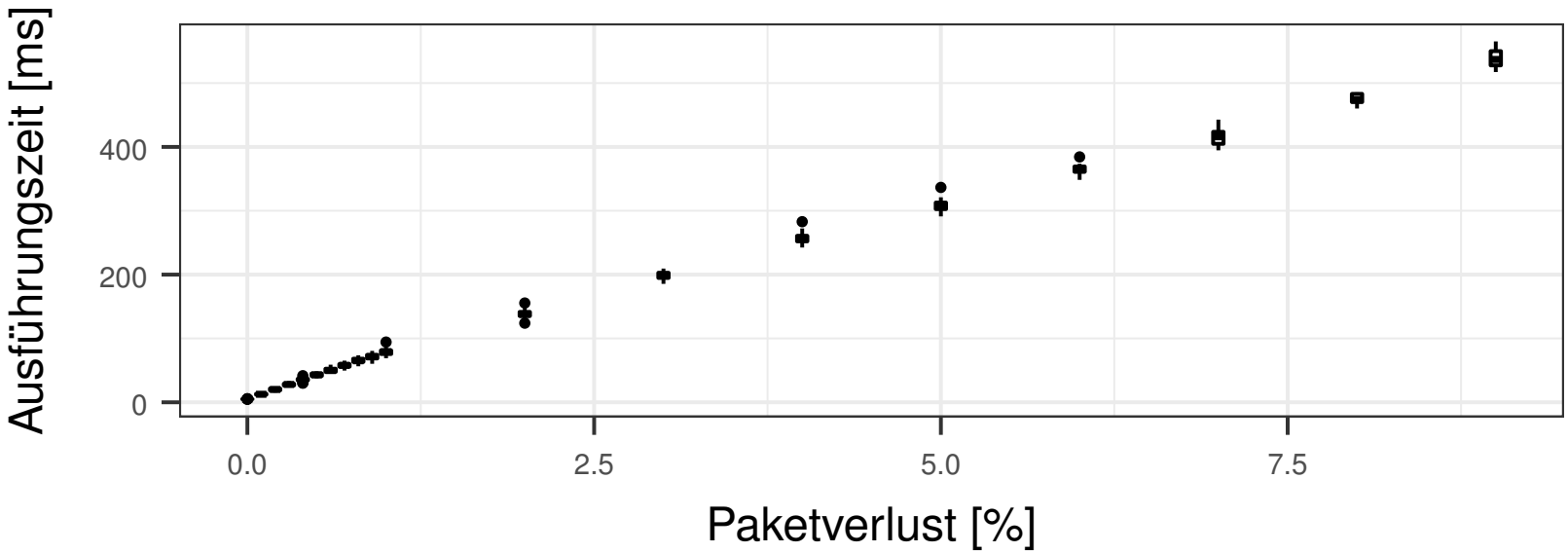
Netzlatenz



- Hoher Kommunikationsaufwand
- Starker Einfluss aufgrund hoher Paketanzahl
- 1 – 2 Sekunden pro Berechnung via Internet (200-400ms Latenz)

Empirische Analyse – Performance

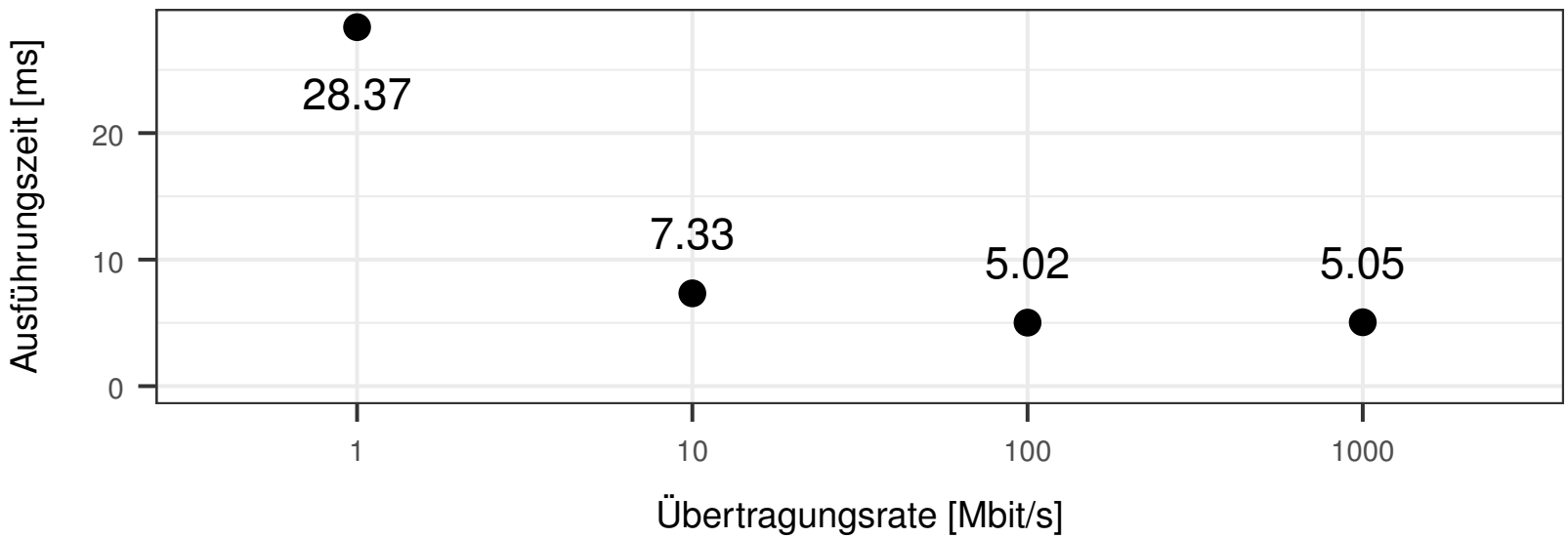
Paketverlust



- > 10 % keine erfolgreiche Ausführung mehr möglich

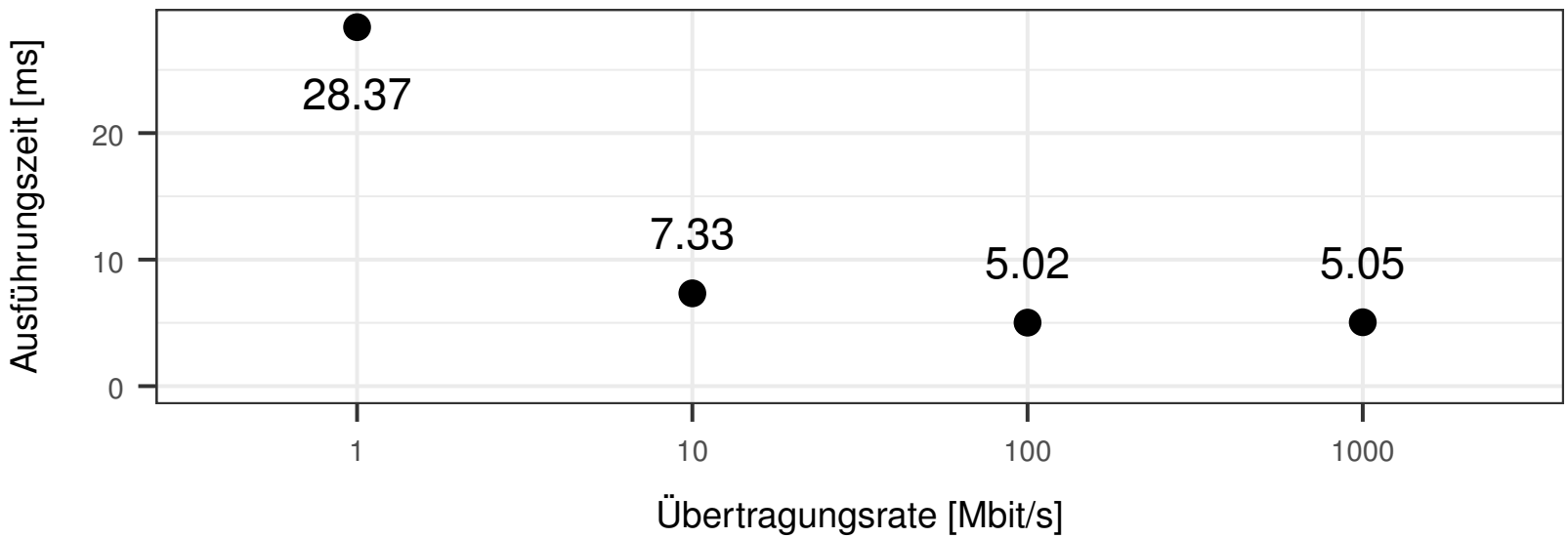
Empirische Analyse – Performance

Übertragungsrate



Empirische Analyse – Performance

Übertragungsrate



- Kontinuierlicher Strom von 2 Mbit/s mit vereinzelten Spitzen
- Übertragungsrate typischerweise kein Flaschenhals

Empirische Analyse – Performance

Problem- und Lösungsdomäne
- Privatheit
- SMC

Empirische Analyse
- Performance
- Infrastruktur
- Privatheit

Konstruktion
SMC as a Service
- Anforderungsanalyse
- Orchestrierung & Self-Management
- Datenabfrage & Zugriffskontrolle

SMC-Implementierung FRESCO als technische Basis für Messungen

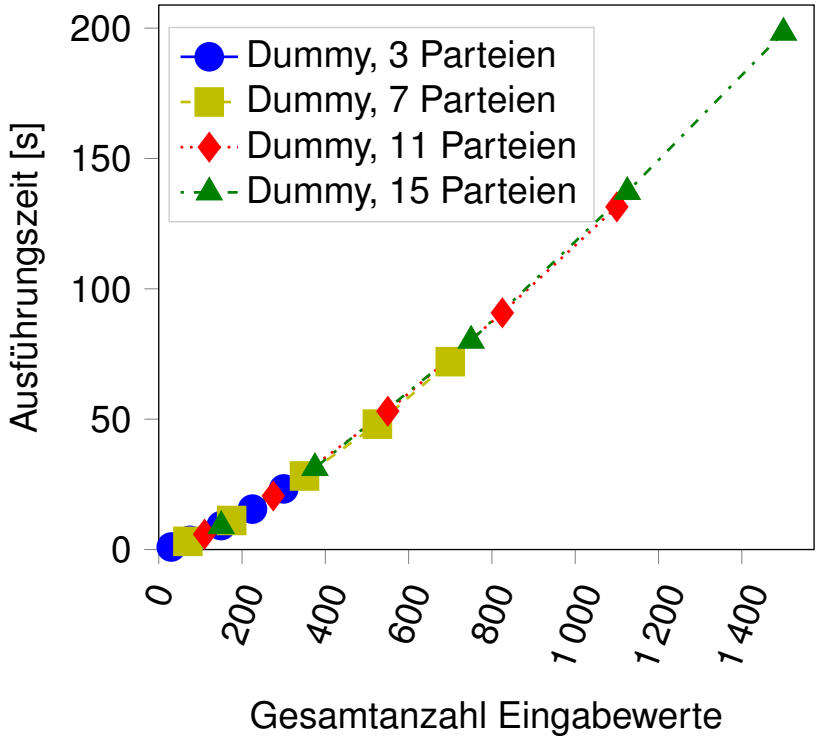
Baseline-Messungen

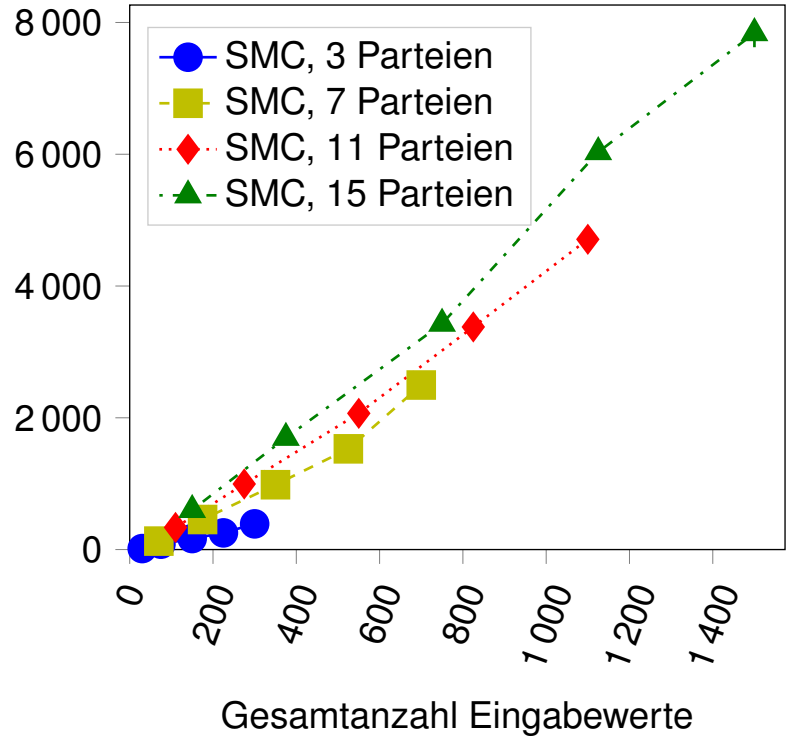
- Protokoll: Running Average
- Daten: GPS-Daten
- Infrastruktur: lokale Testsysteme
- Zielsetzung: Best-Case-Analyse

Real-World-Anwendungsfall

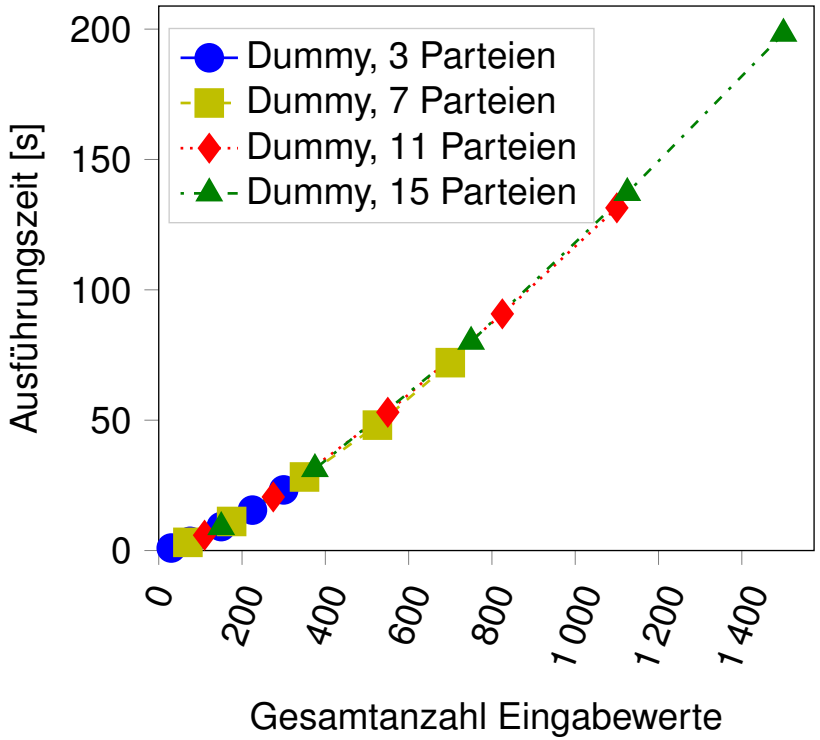
- Protokoll: Kaplan-Meier-Schätzer & Log-Rank-Test
- Daten: Patientendaten der LMU und Charité Berlin
- Infrastruktur: lokale Testsysteme und Server bei LMU/Charité
- Zielsetzung: Realistischer Anwendungsfall

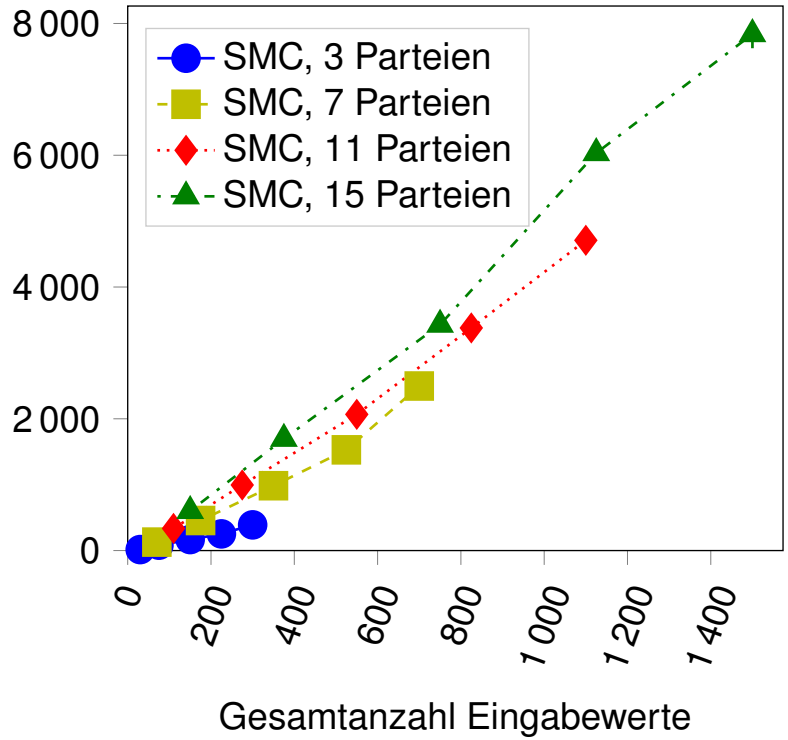
Empirische Analyse – Performance





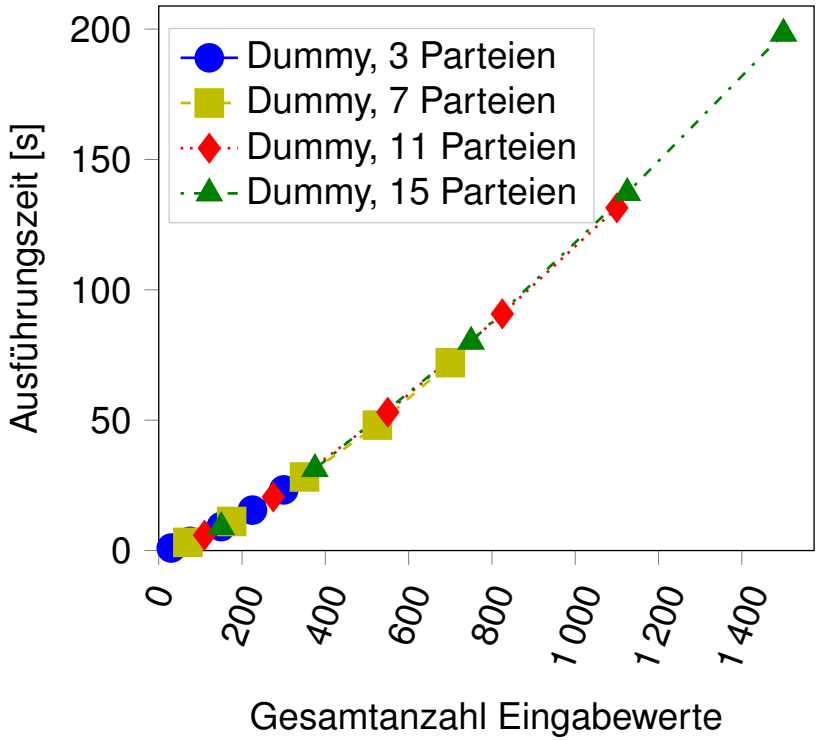
Empirische Analyse – Performance

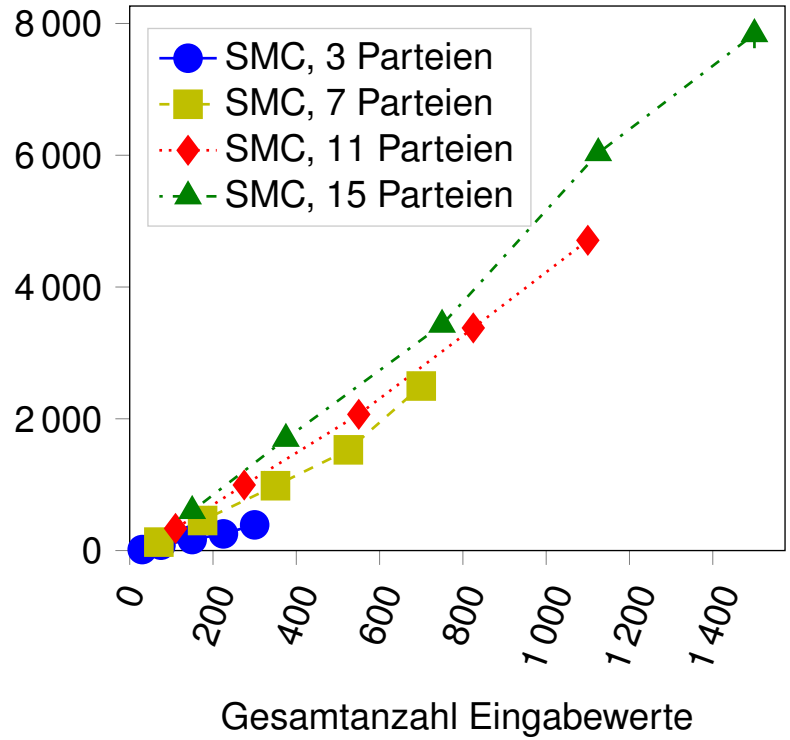




- Differenzierung Schaltkreisdarstellung vs. Kommunikationsaufwand

Empirische Analyse – Performance

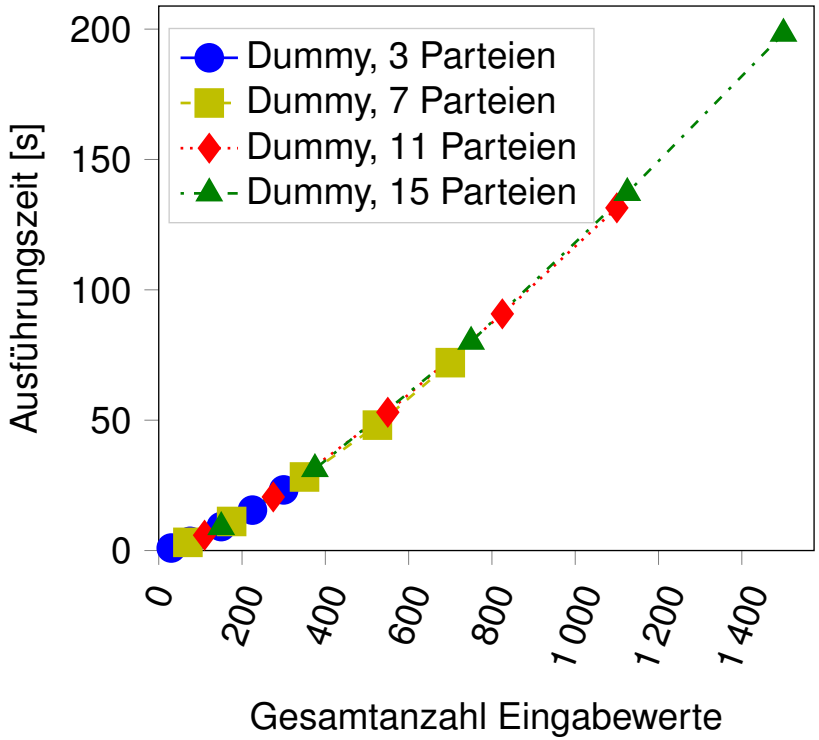


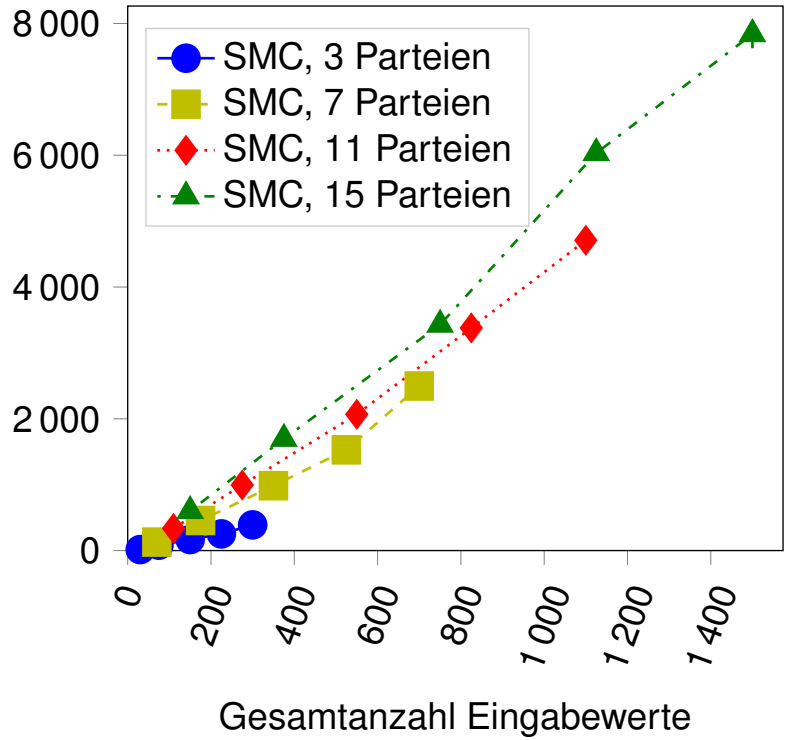


- Differenzierung Schaltkreisdarstellung vs. Kommunikationsaufwand

$$0.52s + 0.28s * |\text{Teilnehmer}| = \frac{\text{Ausführungszeit}}{|\text{Eingabewerte}|}$$

Empirische Analyse – Performance



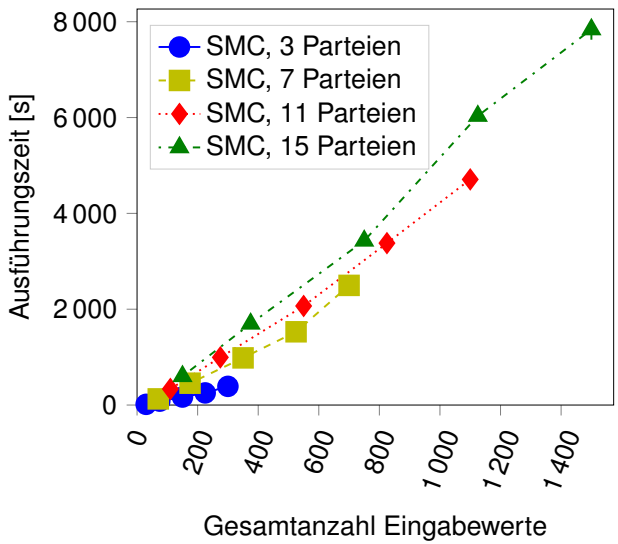


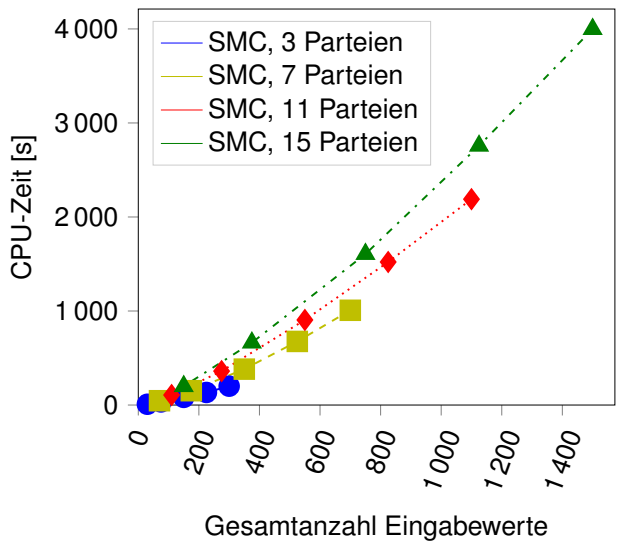
- Differenzierung Schaltkreisdarstellung vs. Kommunikationsaufwand

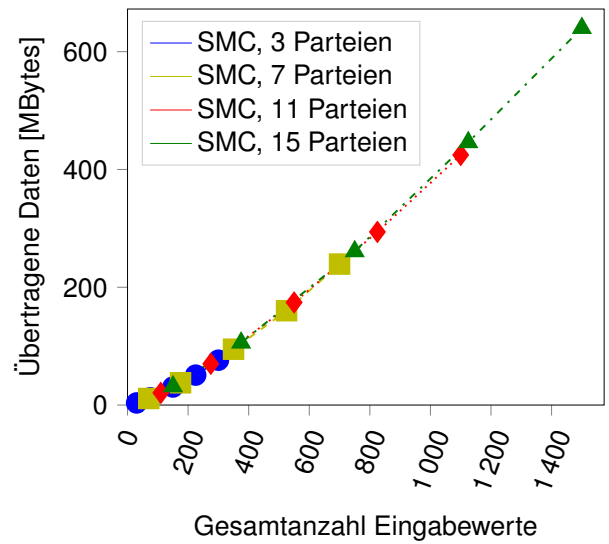
$$0.52s + 0.28s * |\text{Teilnehmer}| = \frac{\text{Ausführungszeit}}{|\text{Eingabewerte}|}$$

- Erfolgreiche Parallelisierung

Empirische Analyse – Performance







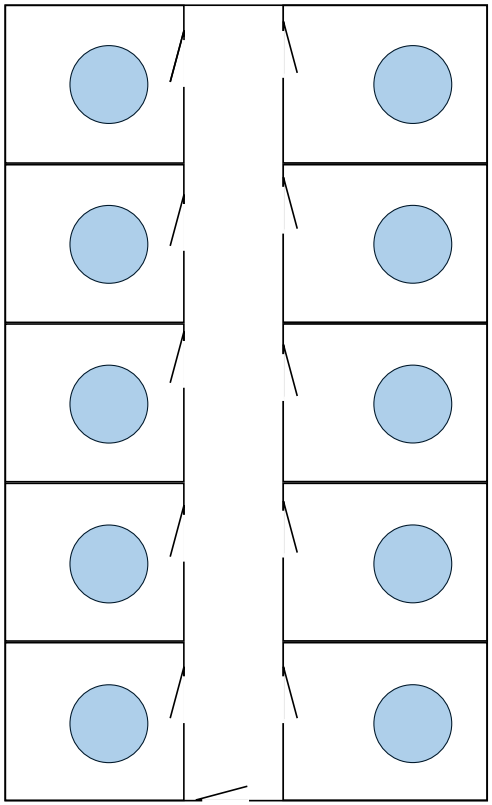
Anwendungsfall
Einsatz von SMC bei Sensordaten in dynamischen Umgebungen

Gründe

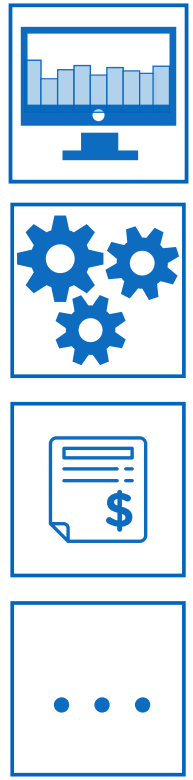
- Hohe Relevanz und Kritikalität von Sensordaten
- Dynamische Umgebungen als Abstraktion von Smart Homes und Smart Buildings
- Praktische Einsetzbarkeit von SMC, insbesondere im Intranet

SMC as a Service

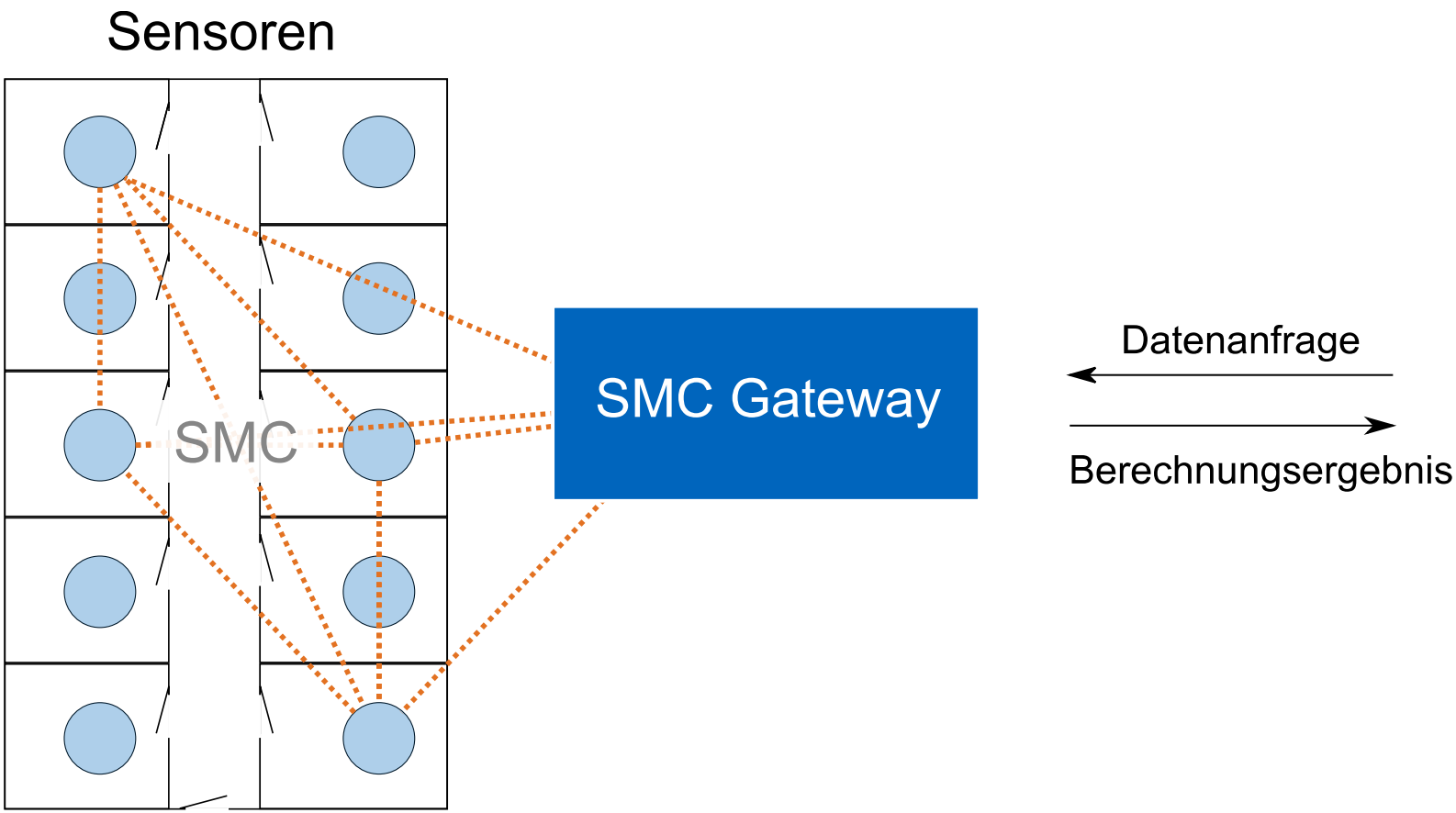
Sensoren



Clients



SMC as a Service



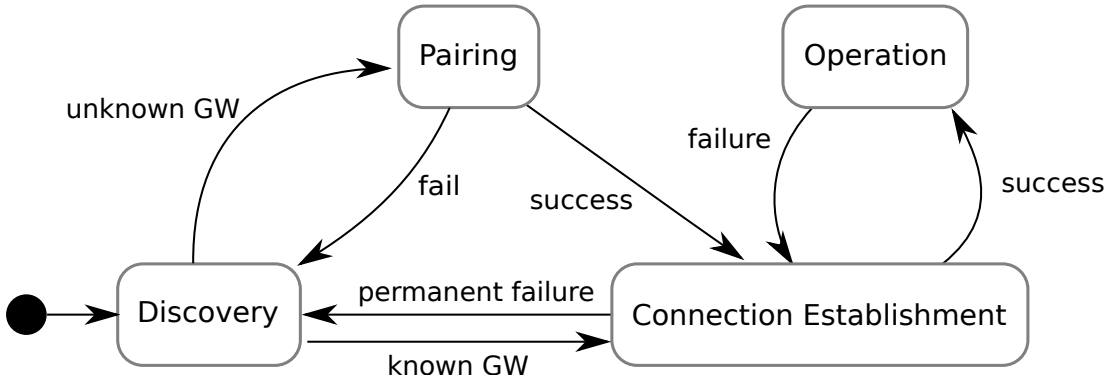
SMC as a Service

A Management Framework for Secure Multiparty Computation in Dynamic Environments.

M. von Maltitz et al. (2018, IEEE/IFIP Network Operations and Management Symposium, DOMINOS Workshop)

Teilnehmer-Orchestrierung

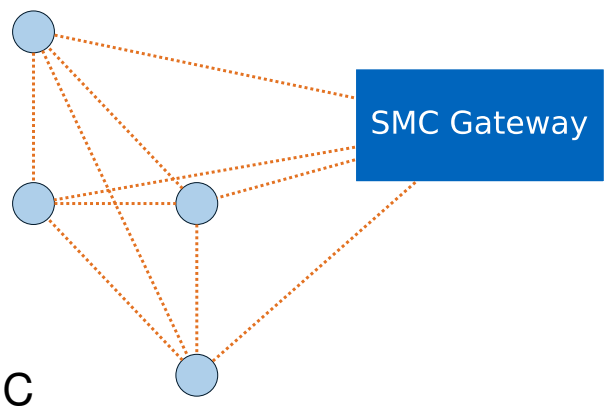
- Automatisierte Discovery
- Pairing mit Metadatenaustausch
- Fehlerbehandlung



⇒ Selbst-Management von SMC-Verbünden

SMC-Sitzungsverwaltung

- Sitzungsgenerierung
- Teilnehmerauswahl
- Monitoring und Fehlerbehandlung



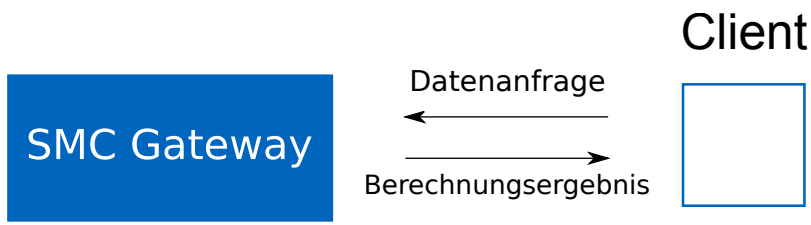
⇒ Automatisierte und robuste Ausführung von SMC

Data Querying and Access Control for Secure Multiparty Computation.

M. von Maltitz, D. Bitzer, and G. Carle. (2019, IFIP/IEEE International Symposium on Integrated Network Management)

Client-Interaktion

- Abfragesprache für SMC-Resultate und Sitzungsübersetzung
- Abfragebasierte Zugriffskontrolle und Autorisierung



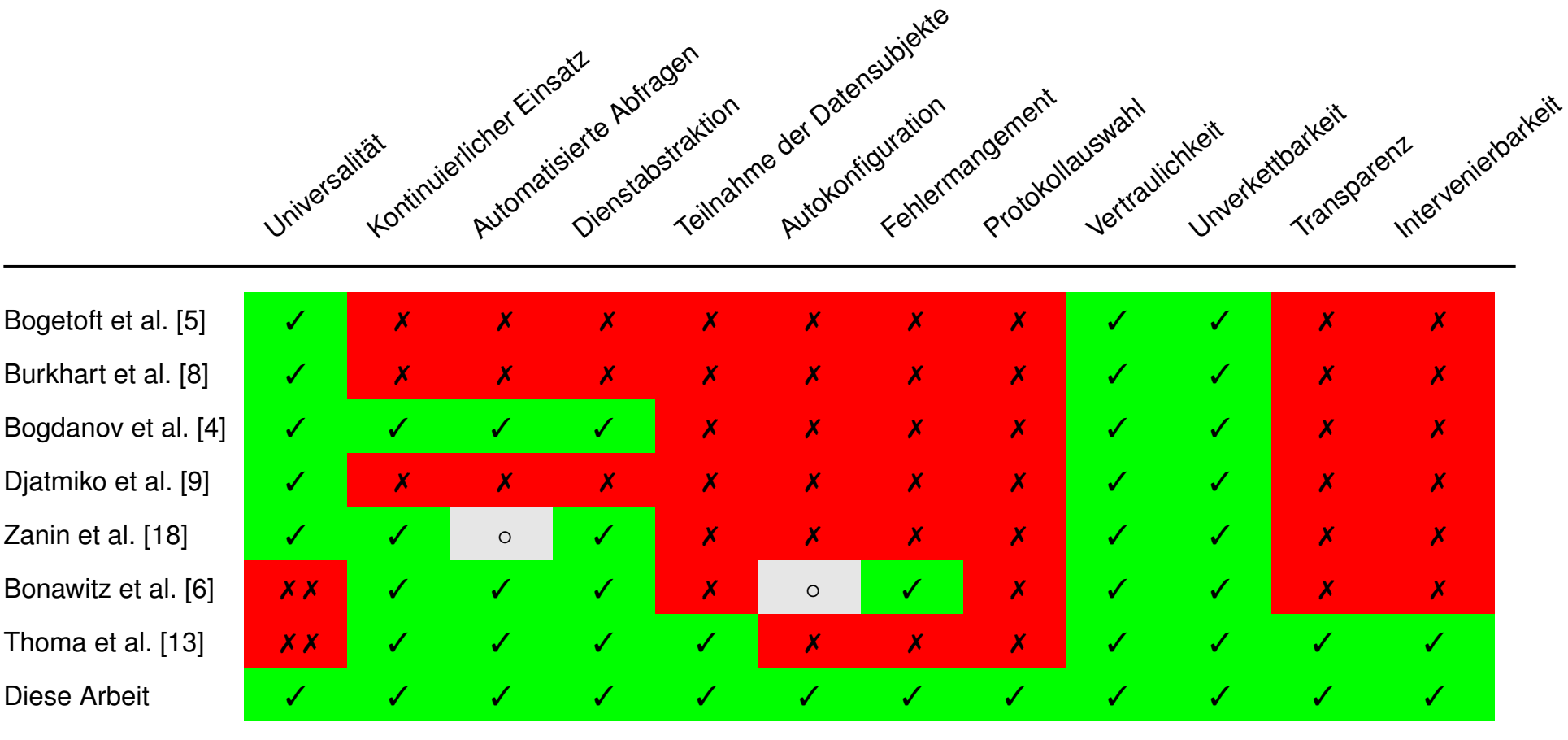
⇒ Dienstabstraktion

Ergänzte Schutzziele

- Transparenz von Anfragen
- Intervenierbarkeit der Teilnehmer bei jeder Berechnung
- Nachvollziehbarkeit aller erfolgter Anfragen und Berechnungen

⇒ Vollständig privatheitsschützender Dienst

SMC as a Service



Eigene Beiträge

Problem- und Lösungsdomäne

- Privatheit
- SMC

Empirische Analyse

- Performance
- Infrastruktur
- Privatheit

Konstruktion
SMC as a Service

- Anforderungsanalyse
- Orchestrierung & Self-Management
- Datenabfrage & Zugriffskontrolle

Zusammenfassung

- Evaluation von SMC als Technologie für Privatheit
- Leistungsbewertung von SMC
- Entwicklung von SMC als Dienst für dynamische Umgebungen
- Ergänzung bisher fehlender Schutzziele

Backup

peers	algorithm input lines	protocol invocations original	protocol invocations replaced	batches original	batches replaced	duration original	duration replaced
3	10	541802	9681	14026	362	7.452	0.131
	25	1334650	23856	14039	365	40.902	0.271
	50	2655997	47481	14043	369	41.251	0.283
	75	3977628	71106	14082	374	57.002	0.580
	100	5298722	94731	14068	375	117.215	0.611
7	10	542080	10001	14026	366	19.297	0.488
	25	1335500	24656	14038	369	45.040	0.513
	50	2657644	49081	14063	373	76.974	0.639
	75	3979801	73506	14074	378	120.186	0.854
	100	5302291	97931	14063	379	191.506	1.285

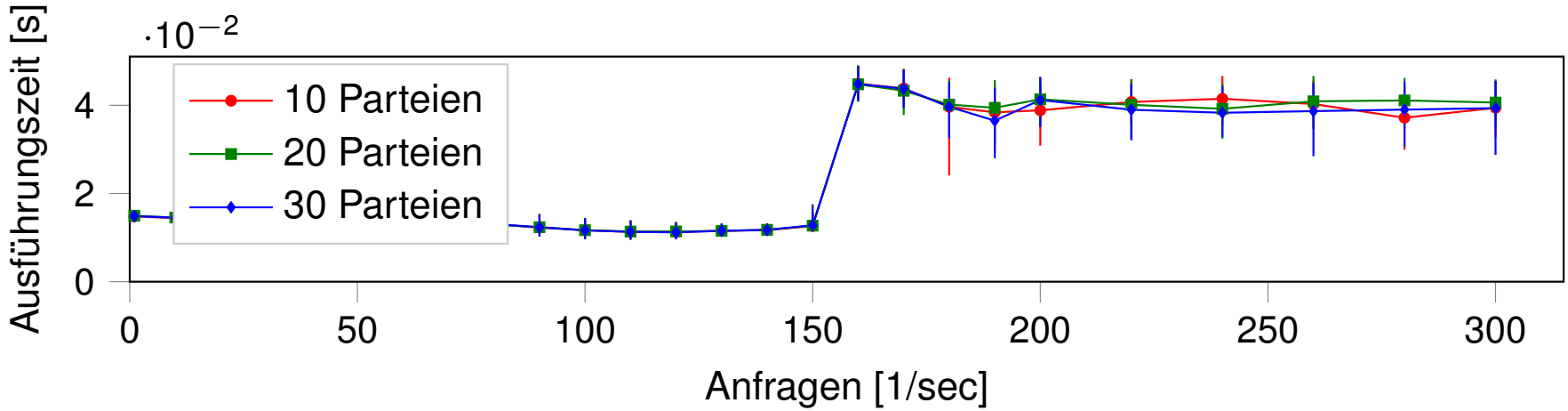
Tabelle 1: Comparison of the original log-rank algorithm with a variant where all division operations have been replaced by multiplication operations.

Backup

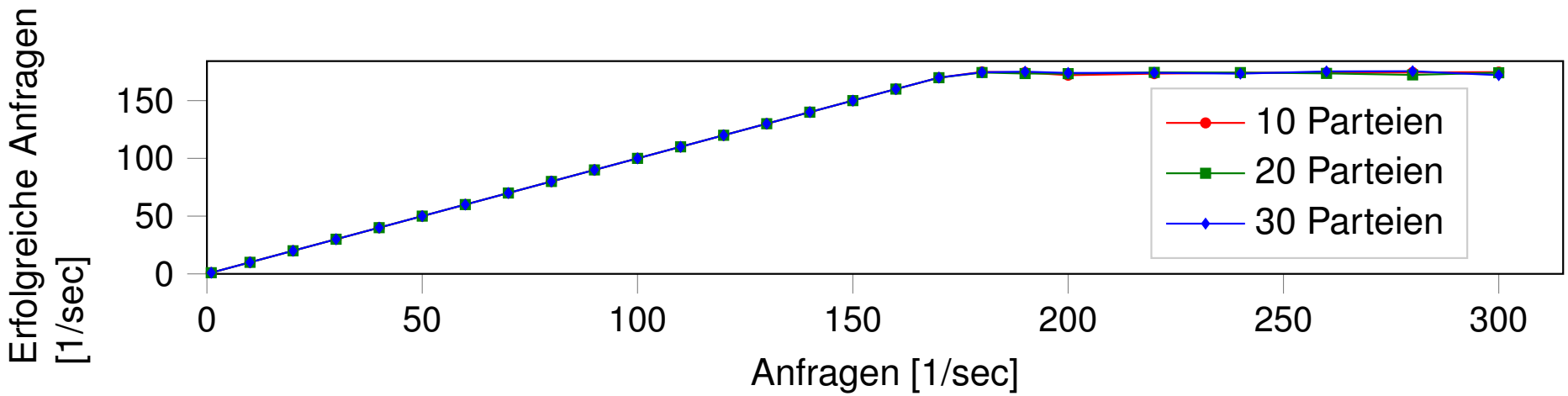
Kategorie	*Klassische Architekturen*		*Unser Ansatz*	
	Sensorplattformen	*Zentrale Komponente*	*Sensorplattformen*	*Zentrale Komponente*
Infrastruktur				
Komponenten	○	○	○	○
Netzwerk	✓	○	✗	○
Sicherheit				
Vertrauen	○	✗✗	✓✓✓	○
Vertraulichkeit	✗	✗	✓	✓✓
Integrität	✗	✗	✓	✓✓
Verfügbarkeit	✓	✓✓	✗	✓✓✓
Privatheit				
Datenminimierung	✗✗	✗	✓	✓✓
Unverkettbarkeit	○	✗	✓✓	✓✓
Transparenz	✗✗	✓	✓✓✓	✓
Intervenierbarkeit	✗	✓	✓✓	✓
Leistung				
Ressourcenkonsum	✓✓✓	✓	✗✗	✓
Ausführungszeit	✓	✓	✗✗	✗

Backup

Grant-Request-Protokoll: Bearbeitungsdauer einer einzelnen Anfrage durch das Gateway

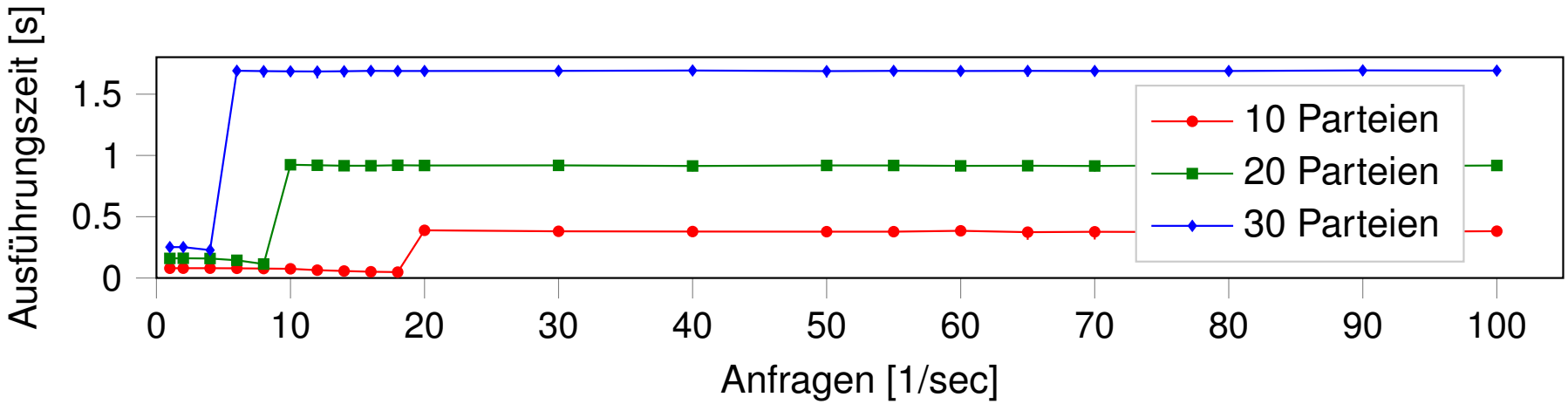


Grant-Request-Protokoll: Erfolgreich beantwortete Anfragen unter Last

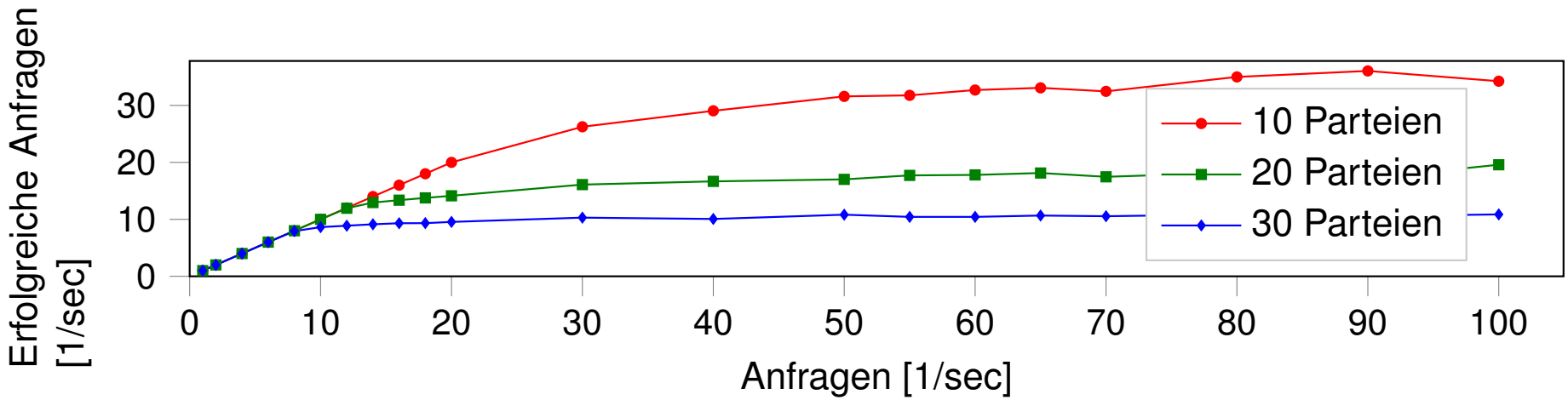


Backup

Computation-Request-Protokoll: Bearbeitungsdauer einer einzelnen Anfrage durch das Gateway inkl. Weiterleitung an Teilnehmer und ihrer Bearbeitungsdauer



Computation-Request-Protokoll: Erfolgreich beantwortete Anfragen unter Last



Bibliography

[1] A. Ben-David, N. Nisan, and B. Pinkas.
FairplayMP: A System for Secure Multi-Party Computation.
Proceedings of the 15th ACM Conference on Computer and Communications Security, pages 257–266, 2008.

[2] D. Bogdanov, S. Laur, and J. Willemson.
Sharemind: A Framework for Fast Privacy-Preserving Computations.
In S. Jajodia and J. Lopez, editors, *Proceedings of the 13th European Symposium on Research in Computer Security*, pages 192–206, Málaga, Spain, 2008. Springer Berlin Heidelberg.

[3] D. Bogdanov, M. Niitsoo, T. Toft, and J. Willemson.
High-performance secure multi-party computation for data mining applications.
International Journal of Information Security, 11(6):403–418, 2012.

[4] D. Bogdanov, R. Talviste, and J. Willemson.
Deploying Secure Multi-Party Computation for Financial Data Analysis.
In A. D. Keromytis, editor, *Financial Cryptography and Data Security*, pages 57–64. Springer Berlin Heidelberg, 2012.

[5] P. Bogetoft, D. L. Christensen, I. Damgård, M. Geisler, T. Jakobsen, M. Krøigaard, J. D. Nielsen, J. B. Nielsen, K. Nielsen, J. Pagter, M. Schwartzbach, and T. Toft.
Secure Multiparty Computation Goes Live.
In *Financial Cryptography and Data Security*, pages 325–343. Springer Berlin Heidelberg, 2009.

[6] K. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, H. B. McMahan, S. Patel, D. Ramage, A. Segal, and K. Seth.
Practical Secure Aggregation for Privacy Preserving Machine Learning.
In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 1175–1191, 2017.

[7] M. Burkhart.
Enabling Collaborative Network Security with Privacy-Preserving Data Aggregation.
PhD thesis, ETH Zürich, 2011.

Bibliography

[8] M. Burkhart, M. Strasser, D. Many, and X. Dimitropoulos.
SEPIA: Privacy-preserving Aggregation of Multi-domain Network Events and Statistics.
In *Proceedings of the 19th USENIX Conference on Security*, Berkeley, CA, USA, 2010. ACM Press.

[9] M. Djatmiko, D. Schatzmann, X. Dimitropoulos, A. Friedman, and R. Boreli.
Collaborative Network Outage Troubleshooting with Secure Multiparty Computation.
IEEE Communications Magazine, (November):78–84, 2013.

[10] W. Henecka, S. Kögl, A.-R. Sadeghi, T. Schneider, and I. Wehrenberg.
TASTY: Tool for Automating Secure Two-Party Computations.
Proceedings of the 17th ACM Conference on Computer and Communications Security, pages 451–462, 2010.

[11] M. Keller, E. Orsini, and P. Scholl.
MASCOT: Faster Malicious Arithmetic Secure Computation with Oblivious Transfer.
In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 830–842, 2016.

[12] B. Pinkas, T. Schneider, N. P. Smart, and S. C. Williams.
Secure Two-Party Computation Is Practical.
Advances in Cryptology, 5912:250–267, 2009.

[13] C. Thoma, T. Cui, and F. Franchetti.
Secure Multiparty Computation Based Privacy Preserving Smart Metering System.
In *Proceedings of the 44th North American Power Symposium*, 2012.

[14] M. von Maltitz, D. Bitzer, and G. Carle.
Data Querying and Access Control for Secure Multiparty Computation.
In *Proceedings of the 16th IFIP/IEEE International Symposium on Integrated Network Management*. IEEE, 2019.

[15] M. von Maltitz and G. Carle.
A Performance and Resource Consumption Assessment of Secret Sharing based Secure Multiparty Computation.
In *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Springer, 2018.

Bibliography

[16] M. von Maltitz and G. Carle.
Leveraging Secure Multiparty Computation in the Internet of Things.
In *Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services*. ACM Press, 2018.

[17] M. von Maltitz, S. Smarzly, H. Kinkelin, and G. Carle.
A Management Framework for Secure Multiparty Computation in Dynamic Environments.
In *Proceedings of 30th IEEE/IFIP Network Operations and Management Symposium*. IEEE, 2018.

[18] M. Zanin, T. T. Delibasi, J. C. Triana, V. Mirchandani, E. Álvarez Pereira, A. Enrich, D. Perez, C. Paşaoğlu, M. Fidanoglu, E. Koyuncu, G. Guner, I. Ozkol, and G. Inalhan.
Towards a secure trading of aviation CO2 allowance.
Journal of Air Transport Management, 56:3–11, 2016.