JENS ERNSTBERGER

+49 170-781-7661 ◇ Munich, Germany ◇ jens.ernstberger@gmail.com

ACADEMIC INTEREST

I am a PhD student at Technical University of Munich under the supervision of Prof. Sebastian Steinhorst and co-supervision of Dr. Arthur Gervais from University College London. My research is focused on security and privacy in decentralized systems. Currently, my main research focus lies in systems for data sovereignty, with a particular focus on practical applications of secure computing and security of applied crypto systems. I am most excited about problems that require novel theoretical insights with real-world applications.

EDUCATION

Technical University of Munich 07/2021 – 04/2024
Research Assistant and PhD Candidate
- Professorship for Embedded Systems and IoT
- Advisor(s): Sebastian Steinhorst, Arthur Gervais

Technical University of Munich 09/2018 – 03/2021
Master of Science, Electrical Engineering and Information Technology
- Advisor: Sebastian Steinhorst
- Master Thesis: Zero Knowledge Proof of Authorization for DLT-based Identity Management

Technical University of Munich 08/2015 – 09/2018
Bachelor of Science, Electrical Engineering and Information Technology
- Bachelor Thesis: Teleoperated Control of a Humanoid Robot

Wilhems-Gymnasium, Stuttgart 09/2007 – 06/2015
High School Diploma

PROFESSIONAL EXPERIENCE

Simons Institute for Theory in Computing 06/2023 – 08/2023
Visiting Researcher - Zero Knowledge Proofs
- Developing a methodology for estimating the runtime of ZKP proof circuits from low-level arithmetic benchmarks.
- Research on ZK security vulnerabilties.

0xPARC 03/2023 – 04/2023
ZKP Spring Residency — Vietnam
- Developing a benchmarking framework for zk-SNARKs, Focus on Recursion, Composition, Aggregation
- Investigation, collection and systematization of bugs in ZKP circuits.

University of California, Berkeley 07/2022 – 09/2022
Visiting Researcher – Center for Responsible, Decentralized Intelligence
- Research Fields: Decentralized Identity, Decentralized Access Control, Decentralized Computation
- Collaboration with Imperial College London and Texas A&M University

FAS AG 10/2020 – 12/2020
Working Student – Digital Architects
- Support of the Managing Partner through preparation of meetings and project proposals
- Development of Business Intelligence solutions and platform-based data analytics applications

KPMG AG 06/2019 – 05/2020
Working Student – Automotive Institute
- Identification of trends in the automotive industry through extensive data analysis
- Content development & conception of a study on the future of the autmotive sector
- Led the Business Intelligence for the study by building more than 50 BI dashboards

Tsinghua – Daimler Joint Research Center 12/2018 – 05/2019
Research Associate – Digital Hub

- Research on new in-car applications through behavior prediction and customer interaction
- Created a location prediction application for automated destination prediction in China

Mercedes-Benz R&D North America 08/2017 – 11/2017
Intern – IoT & Wearables

- Programmed a skill for Amazon Alexa using the Amazon Alexa skills kit & Node.JS
- Implemented new and expanded already existing functions to interact with the vehicle

Daimler AG 03/2017 – 05/2017
Intern – Digital Vehicle & Mobility

PUBLICATIONS

2024 'Do You Need a Zero Knowledge Proof?'
Jens Ernstberger, Stefanos Chaliasos, Liyi Zhou, Phillip Jovanovic, Arthur Gervais
Crypto Finance Conference St. Moritz Academic Research Track (CFC, January 2024)

2023 'zk-Bench: A Toolset for Comparative Evaluation and Performance Benchmarking of SNARKs'
Jens Ernstberger, Stefanos Chaliasos, George Kadianakis,
Sebastian Steinhorst, Phillip Jovanovic, Arthur Gervais, Benjamin Livshits, Michele Orru
To be published

'Janus: Fast Privacy-Preserving Data Provenance For TLS 1.3'
Jan Lauinger, **Jens Ernstberger**, Andreas Finkenzeller, Sebastian Steinhorst
To be published

'SoK: Data Sovereignty'
Jens Ernstberger, Jan Lauinger, Fatima Elsheimy, Liyi Zhou,
Sebastian Steinhorst, Arthur Gervais, Dawn Song
IEEE European Symposium on Security and Privacy (Euro S&P, July 2023)

'Blockchain Censorship'
Anton Wahrstätter, **Jens Ernstberger**, Aviv Yaish, Liyi Zhou, Kaihua Qin, Taro Tsuchiya,
Sebastian Steinhorst, Davor Svetinovic, Nicolas Christin, Mikolaj Barczentewicz, Arthur Gervais
To be published

'Mitigating Decentralized Finance Liquidations with Reversible Call Options'
Kaihua Qin, **Jens Ernstberger**, Liyi Zhou, Phillip Jovanovic, Arthur Gervais
Financial Cryptography (FC, May 2023)

'Anonymous Domain Ownership'
Jan Lauinger, **Jens Ernstberger**, Sebastian Steinhorst
International Conference on Blockchain and Cryptocurrency (ICBC, May 2023)

'SoK: Decentralized Finance (DeFi) Attacks'
Liyi Zhou, Xihan Xiong, **Jens Ernstberger**, Stefanos Chaliasos, Zhipeng Wang, Ye Wang,
Kaihua Qin, Roger Wattenhofer, Dawn Song, Arthur Gervais
IEEE Symposium on Security and Privacy (S&P, May 2023)

2021 'A-PoA - Anonymous Proof of Authorization for Decentralized Identity Management'
Jan Lauinger, **Jens Ernstberger**, Emanuel Regnath, Mohammad Hamad, Sebastian Steinhorst
IEEE International Conference on Blockchain and Cryptocurrency (ICBC, May 2021)

TALKS

2024 **Do You Need a Zero Knowledge Proof?**
Crypto Finance Conference (St. Moritz, January 2024)

2023 **TLS Oracles - Tradeoffs in Security and Performance**
with a perspective on application in Decentralized Credit Networks
Workshop on Decentralized Credit Networks (DCN) (Princeton, October 2023)
Benchmarking SNARKs
zkSummit 10 (London, September 2023)
Introduction to Blockchain Privacy
TUM Blockchain Conference (Munich, September 2023)
ZK Benchmarking
0xPARC Spring Residency (Ho-Chi Minh City, April 2023)
Data Provenance with Public Verifiability
Algorand ACE Conference 2023 (Barcelona, January 2023)

2022 **SoK: Data Sovereignty**
Crypto Economics Security Conference (CESC, September 2022)
SoK: Decentralized Finance (DeFi) Attacks
UC Berkeley Center for Responsible Decentralized Intelligence (RDI Lunch Seminar, September 2022)
An Empirical Study of DeFi Liquidations: Incentives, Risks, and Instabilities
The Science of Blockchain Conference, Stanford (August 2022)
Data Sovereignty and Decentralized Data Science
UC Berkeley Haas Institute for Business Innovation (IBI Brown Bag Seminar, July 2022)

SKILLS

Languages	German, English, French, Chinese
Programming	Advanced in Python, Go, Sufficient in Rust, Matlab, Javascript
Tools	Git, Docker, Tableau, Powerpoint

TEACHING EXPERIENCE

Teaching Assistant

Software Architecture for Distributed Embedded Systems
Technical University of Munich, Fall 2021, 2022, 2023

Advanced Seminar Embedded Systems IoT
Fall 2021, 2022; Summer 2022, 2023

FUNDING & SERVICES

Ethereum Foundation	FY23-1050: A toolset for benchmarking Zero Knowledge Proofs (2023, $60,000)
Ceramic Network	Builder Grant: A Data Provenance Architecture for Ceramic (2022, $16,000)

Co-Chair	2023: ZKP/Web3 Hackathon at UC Berkeley RDI
Reviewer	2023: CCS DeFi Workshop
External Reviewer	2021: FC, AFT
	2022: CESC, S&P (Oakland), NDSS, Usenix Security, CCS, AFT, ConsensusDay22
	2023: S&P (Oakland), NDSS, ConsensusDay23, CCS