Elisaweta (Lisa) Masserova

✉ *elisawem@andrew.cmu.edu*
masserova.github.io
orcid.org/0009-0002-8970-9624

Education

Aug 2018–Sep 2024 **Ph.D. in Computer Science**, *Carnegie Mellon University*, Pittsburgh, USA
Thesis: Distributed Cryptography as a Service
Advisors: Prof. Bryan Parno, Prof. Vipul Goyal

May 2016–Mar 2019 **M.Sc. in Computer Science**, *Karlsruhe Institute of Technology (KIT)*, Germany
Focus: Cryptography and algorithms
Master's thesis: Rerandomizing Oblivious Transfer for Online Oblivious Bingo Voting
Advisors: Prof. Jörn Müller-Quade, Dr. Rebecca Schwerdt

Oct 2013–Aug 2018 **B.Sc. in Mathematics**, *KIT*, Karlsruhe, Germany

Oct 2011–May 2016 **B.Sc. in Computer Science**, *KIT*, Karlsruhe, Germany
Undergraduate thesis (conducted at Carnegie Mellon University): Evaluation of Publishable Humanly Usable Secure Password Creation Schemas
Advisors: Prof. Manuel Blum, Prof. Jörn Müller-Quade

Work, Teaching, and Research Experience

Sep 2024–present **Carnegie Bosch Postdoctoral Fellow**, *Carnegie Mellon University*, USA
Host: Prof. Elaine Shi

Jun 2024–Aug 2024 **Summer Research Associate**, *JP Morgan Chase*, NYC, USA
Project: Non-Interactive and Publicly Verifiable Zero Knowledge for Fair Decision Trees

Jun 2023–Aug 2023 **Summer Research Associate**, *JP Morgan Chase*, NYC, USA
Project: Towards Scalable YOSO MPC via Packed Secret-Sharing

Aug 2020–Dec 2020 **Teaching Assistant**, *Carnegie Mellon University*, Pittsburgh, USA
Course: Introduction to Cryptography

Aug 2019–Dec 2019 **Teaching Assistant**, *Carnegie Mellon University*, Pittsburgh, USA
Course: Introduction to Cryptography

Dec 2014–Aug 2018 **Freelancing in Software- and Web-Development**, Karlsruhe, Germany

Sep 2014–Aug 2018 **Student Research Assistant**, *Karlsruhe Institute of Technology*, Germany
Projects: Visualisation of zero-knowledge principles, CCA-secure commitments

Sep 2013–Aug 2014 **Student Software Developer**, *bluehands GmbH & Co.mmunication KG*, Germany
Project: Augmented reality city guide app

Apr 2013–Dec 2013 **Student Research Assistant**, *FZI Research Center for Information Technology*, Karlsruhe, Germany
Project: App for the recovery of stroke patients

Honors, Grants and Awards

2024 **Carnegie Bosch Postdoctoral Fellowship**, Pittsburgh, USA
Two-year award for postdoctoral researchers conducting high-potential research supported by the CBI institute (collaboration of Bosch and CMU)

2022 **Protocol Labs Research Gift**, *35.000 USD*, Pittsburgh, USA
Project: Stateless Distributed Randomness Generation

2015 **InterAct scholarship**, Karlsruhe, Germany
Scholarship awarded to conduct undergraduate thesis research in the USA

2014 **Winner of HackZurich**, Zurich, Switzerland
Winner of Europe's largest hackathon, team "Immersive"

2014 **Microsoft Imagine Cup**, Berlin, Germany
Winner of the national final, Innovation category
Team: “Krowd”
Project: System to monitor crowd movement by tracking signals of WiFi enabled devices to ensure security at large-scale events

2014-2015 **Femtec Careerbuilding Program**, Karlsruhe, Germany
Stipend for outstanding females in engineering and applied sciences, in cooperation with Germany’s top universities and employers

2012-2014 **ACM ICPC**, Netherlands and Germany
German Collegiate Programming Contest (GCPC) participation,
Northwestern European Regional Contest (NWERC) participation

2005–2010 **Mathematics and physics olympiads**, Zaporizhzhya, Ukraine
Multiple awards at the ukrainian mathematics and physics olympiads

2009 **Ukrainian Young Historian Tournament**, Luhansk, Ukraine
Winner of the national historian debate contest

2009 **International Competition for Mathematical and Logical Games**, Vinnytsia, Ukraine
8th place in the national final

Publications

The author ordering is alphabetical.

EUROCRYPT ’25, TPMPC ’25 Efficient Distributed Randomness Generation from Minimal Assumptions where PArties Speak Sequentially Once. Chen-Da Liu-Zhang, Elisaweta Masserova, João Ribeiro, Pratik Soni, Sri AravindaKrishnan Thyagarajan. *Annual International Conference on the Theory and Applications of Cryptology and Information Security (EUROCRYPT)* 2025. *Further accepted as talk at the Theory and Practice of Multi-Party Computation Workshop (TPMPC)* 2025.

PODC ’25 Towards Scalable YOSO MPC via Packed Secret-Sharing. Brief announcement. Elisaweta Masserova, Antigoni Polychroniadou, Daniel Escudero. *44th ACM Symposium on Principles of Distributed Computing (PODC)* 2025.

FC ’25, SBC ’24 Rapidash: Atomic Swaps Secure under User-Miner Collusion. Hao Chung, Elisaweta Masserova, Elaine Shi, Sri AravindaKrishnan Thyagarajan. *International Conference on Financial Cryptography and Data Security (FC)* 2025. *Further accepted as talk at the Science of Blockchain Conference (SBC)* 2024.

RegML @NeurIPS ’24 Non-Interactive and Publicly Verifiable Zero-Knowledge Proof for Fair Decision Trees. Elisaweta Masserova, Antigoni Polychroniadou, Akira Takahashi. *RegML Workshop at Annual Conference on Neural Information Processing Systems (NeurIPS)* 2024. Selected for oral presentation.

FC ’24, CTB ’24 Improved YOSO Randomness Generation with Worst-Case Corruptions. Chen-Da Liu-Zhang, Elisaweta Masserova, João Ribeiro, Pratik Soni, and Sri AravindaKrishnan Thyagarajan. *International Conference on Financial Cryptography and Data Security (FC)* 2024. *Further accepted as talk at Eurocrypt’s Workshop on Cryptographic Tools for Blockchains (CTB)* 2024.

CESC ’22 Ponyta: Foundations of Side-Contract-Resilient Fair Exchange. Hao Chung, Elisaweta Masserova, Elaine Shi, Sri AravindaKrishnan Thyagaraja. *Crypto Economics Security Conference (CESC)*, 2022.

PKC ’22 Storing and Retrieving Secrets on a Blockchain (Fast Batched DPSS and its Applications). Vipul Goyal, Abhiram Kothapalli, Elisaweta Masserova, Bryan Parno, Yifan Song. *International Conference on Practice and Theory in Public Key Cryptography (PKC)*, 2022.

TCC ’21 Blockchains Enable Non-Interactive MPC. Vipul Goyal, Elisaweta Masserova, Bryan Parno, Yifan Song. *Theory of Cryptography Conference (TCC)*, 2021.

ACSAC '20 Talek: Private Group Messaging with Hidden Access Patterns. Raymond Cheng, William Scott, Elisaweta Masserova, Irene Zhang, Vipul Goyal, Thomas Anderson, Arvind Krishnamurthy, Bryan Parno. *Annual Computer Security Applications Conference (ACSAC)*, 2020.

Informatik '14 sGrid: Centralized Management of BOINC-based Research Projects – Summary. Emanuel Jöbstl, Jerome Urhausen, Elisaweta Masserova, Ainara Askar. *44. Jahrestagung der Gesellschaft für Informatik*, 2014.

Manuscripts

The author ordering is alphabetical.

2025 Fairness in the Wild: Secure Atomic Swap with External Incentives. Hao Chung, Elisaweta Masserova, Elaine Shi, Sri AravindaKrishnan Thyagarajan.

2022 Logic Locking via Universal Circuits On a Grid Topology. Deepali Garg, Vipul Goyal, Ken Mai, Elisaweta Masserova, Bryan Parno, and Lawrence Pileggi.

2020 Poppins: A Direct Construction for Asymptotically Optimal zkSNARKs. Abhiram Kothapalli, Elisaweta Masserova, Bryan Parno.

Selected Invited Talks

Apr 2025 Introduction to Cryptography (invited lecture). *Polkadot Blockchain Academy, PBA-X*, online course, over 300 participants.

Apr 2025 MEV and its Countermeasures. *Workshop on Recent Advances in Fairness in Distributed Applications*, Miyakojima, Japan.

March 2025 Maximal Extractable Value. *Polkadot Blockchain Academy, PBA Campus*, Lucerne, Switzerland.

Oct 2024 Efficient Distributed Randomness Generation from Minimal Assumptions where PArties Speak Sequentially Once. *Security and Privacy seminar at UPenn*, Philadelphia, USA.

Sep 2024 Rapidash: Atomic Swaps Secure under User-Miner Collusion. *Cryptographic Tools for Blockchains*, Zurich, Switzerland.

May 2023 Storing and Retrieving Secrets on a Blockchain. *Secure Blockchain Summit at CMU*, Pittsburgh, USA.

Academic Service

Organizer Roles

2025	Committee Member of CMU's Secure Blockchain Summit
2021-2024	Organizer of The CMU CyLab Crypto Seminar

Program Committee

2026	IEEE S&P
2025	USENIX, ACM CCS, WWW, FC, LATINCRYPT, CVC
2024	ACM CCS, FC

External Conference Reviewer

Cryptography	EUROCRYPT, CRYPTO, ASIACRYPT, TCC, PKC, ITC
Security	IEEE S&P, SCN