Mulong Luo

Website: http://mulongluo.me
Email: mulong@utexas.edu
Phone: 858-2636752

Current Employment

- **The University of Texas at Austin** — Austin, TX
  Postdoctoral Research Fellow — *August 2023 - now*
  - **Faculty Host**: Prof. Mohit Tiwari
  - **Research Interests**: AI security, computer architecture security, hardware and cyber-physical system security.

Education

- **Cornell University** — Ithaca, NY
  Ph.D. in Computer Engineering — *July 2017 - December 2023*
  - **Thesis**: Hardware-level Vulnerabilities and Support for Secure and Safe Cyber-Physical Systems
  - **Thesis Committee**: Edward Suh (advisor/chairperson), Zhiru Zhang and Andrew Myers

- **University of California San Diego** — La Jolla, CA
  M.S. in Computer Science and Engineering — *Sept 2014 - June 2017*

- **Peking University** — Beijing, China
  B.S. in Microelectronics (highest honors) — *Sept 2010 - July 2014*

Conference Publications

- S. Banerjee, P. Sahu, **M. Luo**, et al., "SoK: Compound AI Attack and Defenses", submitted to IEEE Symposium on Security and Privacy (**IEEE SP**), 2025.
- J. Cui, X. Yang*, **M. Luo***, G. Lee*, et al., "MACTA: A Multi-agent Reinforcement Learning Approach for Cache Timing Attacks and Detection", International Conference on Learning Representation (**ICLR**) , 2023.(* Equal Contributions)
- **M. Luo**, et al., "AutoCAT: Reinforcement Learning for Automated Exploration of Cache Timing Attacks", Symposium on High Performance Computer Architecture **(HPCA)**, 2023.
- **M. Luo**, G. E. Suh, "Accelerating Path Planning for Autonomous Driving with Hardware-assisted Memorization", International Conference on Application-specific Systems, Architectures and Processors (**ASAP**) 2022.
- **M. Luo**, A. C. Myers, G. E. Suh, "Stealthy Tracking of Autonomous Vehicles with Cache Side Channels", in **29th USENIX Security Symposium**, 2020, pp.859-876.
- Z. Fang, **M. Luo**, et al., "Mitigating multi-tenant interference in continuous mobile offloading", International Conference on Cloud Computing (**CLOUD**) 2018, 20-36.
- Z. Fang, **M. Luo**, et al., "Exploiting Synchrony in Replicated State Machines", 2017 IEEE International Conference on Cloud Computing (**CLOUD**), pp. 155.
- X. Jiao, **M. Luo**, et al., "An assessment of vulnerability of hardware neural networks to dynamic voltage and temperature variations", International conference on computer-aieded design **(ICCAD)** 2017, pp.945-950.
- **M. Luo**, et al., "Delay uncertainty and signal criticality driven routing channel optimization for advanced DRAM products", 2016 IEEE Asia and South Pacific Design Automation Conference **(ASPDAC)**, pp.697-704.
- A. Kahng, **M. Luo**, et al., "Toward metrics of design automation research impact", International conference on computer-aieded design **(ICCAD)**, 2015, pp. 263-270.

Workshop Publications

- **M. Luo**, M. Tiwari, "Towards Reinforcement Learning for Eviction-Set Finding for Randomized Caches", SRC TECHCON, 2024.
- **M.Luo**, G. E. Suh, "Impact of Timestamp Integrity Attack in Cyber-Physical Systems", Workshop on Automotive and Autonomous Vehicle Security (AutoSec) collocated with Symposium on Networked and Distributed System Security (**NDSS**), 2022.
- J. Liu, J. C. Davies, A. Ferraiuolo, A. Ivanov, **M. Luo**, et al., "Secure Autonomous Cyber-Physical Systems Through Verifiable Information Flow Control", in *Workshop on Cyber-Physical Systems Security and PrivaCy (CPS-SPC) collocated with ACM Conference on Computer and Communication Security (***CCS***)*, 2018, pages 48-59 (**Best Paper Award**).
- **M. Luo**, G.E. Suh, "Stealing Zero-Thresholding Neural Network Data using Timing Channel", Technical Report, 2021.
- **M. Luo***, S. Nath*, A. B. Kahng, "SI for Free: Machine Learning of Interconnect Coupling Delay and Transition Effects", in *System-Level Interconnect Prediction Workshop*, 2015 (* alphabetical order, co-primary authors).

Journal Publications

- E. Lai, **M. Luo**, M. Tiwari, et al., "SpecRL: Reinforcement Learning for Speculative Execution Vulnerabiltiy Exploration", submitted to IEEE Computer Architecture Letters.
- J.H. Lin, X. Jiao, **M. Luo**, et al., "Vulnerability of Hardware Neural Networks to Dynamic Operation Point Variations", IEEE Design and Test 2020, 37(5), 75-84. (IF=1.527.)
- Z. Fang, **M. Luo**, et al., "Go-realtime: a lightweight framework for multiprocessor real-time system in user space ", ACM SIGBED Review 14(4), pp. 46-52. (IF=0.9)
- **M. Luo**, et al., "Impacts of Random Telegraph Noise (RTN) on Digital Circuits" in IEEE Transactions on Electron Devices, 2015. (IF=2.9).

Tutorials

- LDMA: Learning-based Detection of Microarchitectural Attacks Tutorial, colocated with **ASPLOS**, 2024.
- Reinforcement Learning for Computer Architecture and Systems (RL4CAS) Tutorial, colocated with **ISCA** and **FCRC**, 2023.

Professional Services

- Program Committee, IEEE Symposium on Security and Privacy (**IEEE SP**), 2025
- Program Committee, Symposium on International Symposium Computer Architecture (**ISCA**), 2024
- Program Committee, Symposium on High-Performance Computer Architecture (**HPCA**), 2024
- Program Committee, **Usenix Security Symposium**, 2024.
- Program Committee, ACM Symposium on Computer and Communications Security (**CCS**), 2023.
- Program Committee, International Symposium on Research in Attacks, Intrusions and Defenses (**RAID** 2023).
- Program Committee, ISOC Symposium on Vehicle Security and Privacy, 2023 - 2025.
- Program Committee, Workshop on Hardware and Architectural Support for Security and Privacy, 2023, 2024.
- Program Committee, Workshop on Attacks and Solutions in Hardware Security (ASHES), 2023.

- Program Committee, EAI International Conference on Security and Privacy in Cyber-Physical Systems and Smart Vehicles (SmartSP), 2024.
- External Reviewer, Conference on Cryptographic Hardwareand Embedded Systems (CHES), 2023.
- Reviewer, IEEE Transactions on Computer (TC), 2023.
- Reviewer, IEEE Computer Architecture Letters (CAL), 2023.
- Artifact Evaluation Committee, Usenix Security Symposium 2022.
- Artifact Evaluation Committee, Usenix Annual Technical Conference (ATC), 2022.
- Artifact Evaluation Committee, Symposium on Operating System Design and Implementation (OSDI), 2022.
- Publication Chair, ISOC Symposium on Vehicle Security and Privacy (**VehicleSec**, colocated with NDSS, 2024, 2025.)
- Session Chairs, Usenix Security Symposium, 2024.
- Judge for Master of Engineering Porject, Cornell ECE Department, 2023.

Awards

- Best Reviewer Award, VehicleSec, 2024.
- Best Reviewer Award, RAID, 2023.
- CPS Rising Stars, 2023.
- Student Travel Grant, IEEE Symposium on High-Performance Computer Architecture (HPCA), 2023.
- Top Picks in Hardware and Embedded Security 2022 Shortlist.
- Student Travel Grant, ACM Conference on Computer and Communication Security (CCS), 2021.
- Student Travel Grant, Network and Distributed System Security Symposium (NDSS), 2020.
- Best Paper Award, CPS-SPC, 2018.
- Jacobs Fellowship, Cornell University, 2017.
- Powell Fellowship, UCSD, 2014.
- Oustanding Graduate, Beijing Municipality, 2014.
- Outstanding Graduate in Class of 2014, Peking University, 2014.
- The May Fourth Festival Scholarship, Peking University, 2012.
- Okamatsu Scholarship, Peking University, 2011.
- First Price, Physics Olympics for College Students, 2011.

Talks

- Reinforcement learning for microarchitectural security: cache timing channel, speculative execution, and defense
  - Keynote talk at The l Workshop on Hardware and Architectural Support for Security and Privacy (HASP), 2024.
  - ACE Center for Evolvabel Computing Liason Meeting, 2024.
- ConfusedPilot: Data Corruption and Leakage by Misusing Copilot for Microsoft 365
  - DEF CON 32 AI Village 2024.
- Reinforcement Learning for Eviction-Set Finding for Randomized Caches
  - Semiconductor Research Corporation Technical Conference (SRC TechCON), 2024.
- AutoCAT: Reinforcement Learning for Automated Exploration of Cache Timing-Channel Attacks
  - International Symposium on High Performance Computer Architecture, 2023.
  - International Workshop on Design Automation for CPS and IoT (DACPS), 2023.
  - ACE Center for Evolvable Computing Liason Meeting, 2023.
  - Cornell Computer Systems Laboratory Seminar, 2022.
- Accelerating Path Planning for Autonomous Driving with Hardware-assisted Memorization
  - International conference on Application-specific Systems, Architectures and Processors (ASAP).
- Machine Learning-based Hardware and Cyber-Physical Systems Security
  - SPARK Lab, the University of Texas at Austin, 2023.
  - Department of Microelectronics, Peking University, 2022.
  - Secure Systems Group, University of Waterloo, 2022.
- Interrupt Attack on TEE for Robotic Vehicles
  - Automobile and Autonomous Vehicle Security Workshop (AutoSec), 2022
- Stealthy Tracking of Autonomous Vehicles with Cache Side Channels
  - Top Picks in Hardware and Embedded Security Workshop, 2022.
  - USENIX Security Symposium, 2020.
  - Cornell Computer Systems Laboratory Seminar, 2019.
- Exploiting Synchrony in Replicated State Machines
  - IEEE International Conference on Cloud Computing (CLOUD), 2017.

Teaching

- **Embedded Systems (UT Austin)** — Guest Lecturer
  Instructor: Prof. Mohit Tiwari — *Spring 2024.*
- **Enterprise Security (UT Austin)** — Guest Lecturer
  Instructor: Prof. Mohit Tiwari — *Fall 2023.*
- **Digital Logic and Computer Organization (Cornell Univeristy)** — Lead Teaching Assistant
  Instructor: Prof. David Albonesi — *Fall 2020.*
- **Resilient Computer Systems (Cornell University)** — Lead Teaching Assistant
  Instructor: Prof. Edward Suh — *Fall 2019 and Fall 2018.*
- **Digital System Design (UC San Diego)** — Lead Teaching Assistant
  Instructor: Prof. Chung-Kuan Cheng — *Spring 2017.*
- **Digital Circuits Laboratory (UC San Diego)** — Lead Teaching Assistant
  Instructor: Prof. Rajesh Gupta and Visiting Prof. Arvind from MIT — *Winter 2017.*

Research Mentoring

- **Ayush RoyChowdhury**: Master of Science student at UT Austin. (first-author paper submitted to MLSys and presented at DEFCON AI Village 2024.)
- **Evan Lai**: undergraduate at UT Austin. (first-author paper submitted to IEEE CAL 2024.)
- **Kellen Watts**: undergraduate at UT Austin.
- **Shayan Chatiwala**: high school student at Wayne Hills High School, New Jersey. (co-authored paper submitted to ISCA 2025.)
- **Geunbae Lee**: master student at Virginia Tech with Prof. Wenjie Xiong. (co-authored papers at HPCA 2023 and ICLR 2023.)
- **Erfan Iravani**: Ph.D. student at Virginia Tech with Prof. Wenjie Xiong.
- **Yueying Li**: Ph.D. student at Cornell University with Prof. Edward Suh. (co-authored paper at HPCA 2023.)
- **Yan Zhang**: Master of Engineering at Cornell University with Prof. Edward Suh.
- **Yifan Yang**: Master of Engineering at Cornell University with Prof. Edward Suh.

Industry Experience

- **Qualcomm Inc.** — San Diego, CA
  Research and Development Intern, System-on-Chip Architecture Team. — *May-August, 2021.*
- **Synopsys Inc.** — Sunnyvale, CA
  Software Research and Development Intern, Place-and-Route (IC Compiler) Team. — *June-September, 2016.*