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**: computer architecture security, AI for security, AI 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*

Awards

- CPS Rising Stars, 2023.
- Eric and Wendy Schmidt AI in Science Postdoctoral Fellowship, University of Michigan, 2023.
- Top Picks in Hardware and Embedded Security Finalist, 2022.
- Best Paper Award, CPS-SPC, 2018.
- Irwin and Joan Jacobs Fellowship, Cornell University, 2017.
- Kunzel Powell Fellowship, UC San Diego, 2014.
- Outstanding 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.

Conference Publications and Manuscripts

- A. Cathis, **M. Luo**, M. Tiwari, A. Geurstlauer. "LAPD: Lifecycle-aware Power-based Malware Detection", in submission.
- S. Banerjee*, P. Sahu*, **M. Luo**, A. Valhdiek-Oberwager, N. J. Yadwadkar, M. Tiwari. "SoK: A Systems Perspective on Compound AI Threats and Countermeasures", in submission.
- A. RoyChowdhury, **M. Luo***, P. Sahu, S. Banerjee, M. Tiwari*. "ConfusedPilot: Confused Deputy Risks in RAG-based LLMs", in submission.
- **M. Luo**, M. Kaya, W. Xiong, G. E. Suh, M. Tiwari. "AlphaEvict: Reinforcement Learning for Eviction-Set Finding", in preparation for submission to a security venue, 2025.

- **M. Luo**, M. Tiwari. "Towards Reinforcement Learning for Eviction-Set Finding for Randomized Caches", SRC TECHCON, 2024.
- **M. Luo***, W. Xiong*, G. Lee, Y. Li, X. Yang, A. Zhang, H. H. S. Lee, Y. Tian, G. E. Suh. "AutoCAT: Reinforcement Learning for Automated Exploration of Cache Timing Attacks", Symposium on High Performance Computer Architecture (**HPCA**), 2023 (* Equal contributions).
- J. Cui, X. Yang*, **M. Luo***, G. Lee*, B. C. Lee, H. H. S. Lee, G. E. Suh, W. Xiong$^{\$}$, Y. Tian$^{\$}$, "MACTA: A Multi-agent Reinforcement Learning Approach for Cache Timing Attacks and Detection", International Conference on Learning Representation (**ICLR**) , 2023 (* Equal contributions, $ Equal supervisions).
- **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**, G. E. Suh. "Impact of Timestamp Integrity Attack in Cyber-Physical Systems", Workshop on Automotive and Autonomous Vehicle Security (**VehicleSec**) collocated with Symposium on Networked and Distributed System Security (NDSS), 2022.
- **M. Luo**, A. C. Myers, G. E. Suh. "Stealthy Tracking of Autonomous Vehicles with Cache Side Channels", in **Usenix Security Symposium**, 2020. (Shortlisted for Top Picks in Hardware and Embedded Security 2022).
- **M. Luo**, G. E. Suh. "Stealing Zero-Thresholding Neural Network Data using Timing Channel", Technical Report, 2021.
- Z. Fang, **M. Luo**, T. Yu, O. Mengshoel, M. Srivastava, R. K. Gupta. "Mitigating Multi-tenant Interference in Continuous Mobile Offloading", International Conference on Cloud Computing (**CLOUD**), 2018.
- J. Liu, J. C. Davies, A. Ferraiuolo, A. Ivanov, **M. Luo**, A. C. Myers, G. E. Suh, M. Campbell. "Secure Autonomous Cyber-Physical Systems Through Verifiable Information Flow Control", in Workshop on Cyber-Physical Systems Security and PrivaCy (**CPS-SPC**) co-located with ACM Conference on Computer and Communication Security (CCS), 2018, (**Best Paper Award**).
- Z. Fang, **M. Luo**, R. K. Gupta. "Exploiting Synchrony in Replicated State Machines", IEEE International Conference on Cloud Computing (**CLOUD**), 2017.
- X. Jiao, **M. Luo**, J. H. Lin, R. K. Gupta. "An Assessment of Vulnerability of Hardware Neural Networks to Dynamic Voltage and Temperature Variations", International Conference on Computer-Aided Design **(ICCAD)**, 2017.
- S. Bang, A. B. Kahng, K. Han, **M. Luo***. "Delay Uncertainty and Signal Criticality Driven Routing Channel Optimization for Advanced DRAM Products", IEEE Asia and South Pacific Design Automation Conference (**ASPDAC**), 2016 (*Alphabetical order, leading author).
- A. B. Kahng, **M. Luo***, S. Nath. "SI for Free: Machine Learning of Interconnect Coupling Delay and Transition Effects", System-Level Interconnect Prediction Workshop (**SLIP**), 2015 (* Alphabetical order, co-primary authors).

Peer-Reviewed Journal Publications

- E. Lai, **M. Luo***, W. Xiong, G. E. Suh, M. Tiwari*. "SpecRL: Reinforcement Learning for Speculative Execution Vulnerability Exploration", in preparation for IEEE Computer Architecture Letters (* Corresponding authors).
- J. H. Lin, X. Jiao, **M. Luo**, Z. Tu, R. K. Gupta. "Vulnerability of Hardware Neural Networks to Dynamic Operation Point Variations", IEEE Design and Test, 2020.

- Z. Fang, **M. Luo**, R. K. Gupta. "Go-realtime: a Lightweight Framework for Multiprocessor Real-time System in User Space ", ACM SIGBED Review, 2016.
- **M. Luo**, R. Wang, J. Wang, S. Guo, J. Zou, R. Huang. "Impacts of Random Telegraph Noise (RTN) on Digital Circuits" IEEE Transactions on Electron Devices, 2015.

Tutorials

- **M. Luo**, A. RoyChowdhury, M. Tiwari. "LDMA: Learning-based Detection of Microarchitectural Attacks Tutorial", co-located with **ASPLOS**, 2024. https://ut-ldma.github.io.
- **M. Luo**, W. Xiong, Y. Tian. H. H. S. Lee, G. E. Suh. "Reinforcement Learning for Computer Architecture and Systems (RL4CAS) Tutorial", co-located with **ISCA**, 2023. https://rl4cas.github.io

Talks

- Reinforcement learning for microarchitectural security: cache timing channel, speculative execution, and defense
  - Keynote talk at The Workshop on Hardware and Architectural Support for Security and Privacy (HASP), 2024.
  - ACE Center for Evolvable Computing Liaison 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 Liaison 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), 2022.
- 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.

Professional Services

- Proposal Reviewer, NSF Secure and Trustworthy Cyberspace (SaTC) 2.0 Program.
- Program Committee, ACM Symposium on Computer and Communications Security (**CCS**), 2023, 2025.
- Program Committee, IEEE Symposium on Security and Privacy (**IEEE S&P**), 2025.
- Program Committee, **Usenix Security Symposium**, 2024.
- External Review Committee, Symposium on International Symposium Computer Architecture (**ISCA**), 2024.
- Light Program Committee, Symposium on High-Performance Computer Architecture (**HPCA**), 2024.
- Program Committee, International Symposium on Research in Attacks, Intrusions and Defenses (**RAID**), 2023.
- Program Committee, Usenix Symposium on Vehicle Security and Privacy (**VehicleSec**), 2023, 2024, 2025.
- Program Committee, Workshop on Hardware and Architectural Support for Security and Privacy (**HASP**), 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 Hardware and 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, Usenix Symposium on Vehicle Security and Privacy (**VehicleSec**), co-located with NDSS, 2024, 2025.
- Local Arrangement Chair, Workshop on Hardware and Architectural Support for Security and Privacy (**HASP**), 2024.
- Session Chairs, Usenix Security Symposium, 2024.
- Judge for Master of Engineering Project, Cornell ECE Department, 2023.
- Session Chair, Hardware and Archiecture Support for Security and Privacy Workshop, 2024.

Teaching

- **Embedded Systems (UT Austin)** Guest Lecturer
  Instructor: Prof. Mohit Tiwari *Spring 2024.*
- **Enterprise Network Security (UT Austin)** Guest Lecturer
  Instructor: Prof. Mohit Tiwari *Fall 2023, Fall 2024.*
- **Digital Logic and Computer Organization (Cornell University)** 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 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 in preparation for IEEE CAL.)
- **Mahir Kaya**: undergraduate at UT Austin.
- **Kellen Watts**: undergraduate at UT Austin.
- **Shayan Chatiwala**: high school student at Wayne Hills High School, New Jersey.
- **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.*

References

- **Dr. G. Edward Suh** esuh@nvidia.edu
  Senior Director of Research, Nvidia Inc and Adjunct Professor, Cornell University
- **Dr. Mohit Tiwari** tiwari@austin.utexas.edu
  Associate Professor, UT Austin and CEO, Symmetry Systems Inc
- **Dr. Hsien-Hsin Sean Lee** sean.lee@intel.com
  Intel Fellow, Office of the CTO, Intel Corporation
- **Dr. Wenjie Xiong** wenjiex@vt.edu
  Assistant Professor, Virginia Tech