Mulong Luo

Website: http://mulongluo.me
Email: ml2558@cornell.edu
Mobile: +858-263-6752

Education

- **Cornell University** — Ithaca, NY
  Ph.D. candidate in Computer Engineering — *July 2017 - May 2023*
  - **Thesis Title**: AI methods for cyber-physical systems security and safety
  - **Thesis Committee**: Edward Suh (chair), 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*

Research Experience

- **Reinforcement Learning for Cache Side Channel Vulnerability Discovery** — Ithaca, NY
  Using reinforcement learning methodology to discover microarchitectural attack — *Sept 2021- now*
  - Built micro-architectural reinforcement learning environment.
  - Applied PPO and DQN agents to automatically discover prime+probe, flush+reload, attacks.
  - Discovered novel side channel attacks using RL.

- **Accelerating Motion Planning for AI-based Safe Autonomous Driving** — Ithaca, NY
  Algorithm design that performs path planning algorithm with dynamic obstacles — *August. 2020 - Sept 2021*
  - Modified gem5 simulator to incorporate content-addressable memory for path planning acceleration.
  - Implemented RRT path planning with dynamic obstacles and use CAM for acceleration

- **TEE Timestamp Integrity Attack in AI-based Vehicles** — Ithaca, NY
  An attack on autonomous driving software protected by Intel SGX — *Sept 2019-Sept 2020*
  - Measured how interrupt by an adversarial OS can affect the sensor timestamp used for sensor fusion.
  - Demonstrated and evaluated the impact of adversarial interrupt on vehicles ego and obstacle localization.

- **AI-based CPU Cache Side Channel Attack on x86 Processors** — Ithaca, NY
  AI method for analyze cache side channel attack to track autonomous vehicles — *Sept 2018 - August 2019*
  - Performed side channel attack to collect the memory access patterns of autonomous driving software.
  - Trained random forest and RUSBoost model to learn the locations of the vehicles via the memory access patterns.

- **Secure AI-based Autonomous Vehicles with Information Flow Control** — Ithaca, NY
  Implemented autonomous vehicle with software and hardware information flow control — *July 2017 - July 2018*
  - Ported a customized robot control software with information-flow control to a generic ROS-based system.
  - Deployed the system onto a RISCV-based information-flow processor.

- **Embedded System Time Synchronization and AI-workload offloading** — San Diego, CA
  Implement and evaluate computation workload on time-sensitive platform — *July 2016 - July 2017*
  - Implemented time series forecasting technology to predict task execution time.
  - Co-developed scheduling policy to reduce the server respond time in case of congestion.

- **Content-Aware Power Optimization** — San Diego, CA
  Internship at Qualcomm: architecture and algorithm co-optimize DRAM power for ML — *June 2021 - August 2021*
  - Developing new power-aware coding schemes for ML to minimize DRAM power.
  - Making architecture recommendations for incorporating low-power coding scheme in HW.

- **VLSI Interconnect crosstalk Optimization** San Diego, CA
  Use analytical method for solving complex DRAM design issues *Jan 2015 - Dec 2016*
  - Build a analytical model for crosstalk in DRAM and use mixed integer linear programming for interconnect crosstalk optimization using CPlex .
- **Machine Learning Modeling for VLSI Interconnect Coupling Delay** San Diego, CA
  A machine learning model for efficient circuit timing prediction *Jan 2015 - May 2015*
  - Use artificial neural network (ANN) and support vector machine (SVM) to predict the timing delay of VLSI.

Professional Services

- Technical Program Committee: ACM Symposium on Computer and Communications Security (CCS), 2023, Symposium on Vehicle Security and Privacy, 2023
- Artifiact Evluation Committee: Usenix Security Symposium 2022, Symposium on Operating System Design and Implementation (OSDI), 2022.

Selected Publications

- J. Cui, X. Yang, G. Lee, **M. Luo**, et al., "MACTA: A Multi-agent Reinforcement Learning Approach for Cache Timing Attacks and Detection", ***International Conference on Learning Representation (ICLR)*** , 2023.
- **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**, 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.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.
- **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.
- 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)*, 2018, pages 48-59 (**Best Paper Award**).
- 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 (ASP-DAC)**, pp.697-704.
- **M. Luo***, S. Nath*, "SI for Free: Machine Learning of Interconnect Coupling Delay and Transition Effects", in *System-Level Interconnect Prediction Workshop*, 2015 (* alphabetical order, co-primary author).