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 2022 (Expected)*
  - **Thesis Title:**: 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*
  - **Related Courses**: Compiler Construction, Digital circuit implementation, VLSI design
- **Peking University** Beijing, China
  B.S. in Microelectronics (highest honors) *Sept 2010 - July 2014*

Research Experience

Computer Architecture, Security and Embedded Systems

- **Machine Learning for Microarchitectural Side Channel Discovery** Ithaca, NY
  Using ML/RL to automatically learn how to perform attack *Sept. 2021 - now*
  - Working on leveraging machine/reinforcement learning to learn and discover new side channel attacks.
- **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.
  - Validating low-power coding scheme in software on existing SoC.
  - Making architecture recommendations for incorporating low-power coding scheme in HW.
- **Accelerating Motion Planning for Autonomous Driving** Ithaca, NY
  Algorithm design that performs path planning algorithm with dynamic obstacles *August. 2020 - now*
  - Working on performance improvement of an path planning algorithm using SW/HW codesign techniques.
- **Trusted Execution Environment Timestamp Integrity Attack** Ithaca, NY
  An attack on autonomous driving software protected by trusted execution environment *Sept 2019-Sept. 2020.*
  - Measured how interrupt by an adversarial OS can affect the sensor timestamp.
  - Demonstrated and evaluated the impact of adversarial interrupt on vehicles ego and obstacle localization.
- **CPU Cache Side Channel Attack on x86 processors** Ithaca, NY
  An adversarial 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 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.
  - The paper wins best paper award at CPS-SPC 2018.
- **Embedded System time synchronization and Mobile offloading** San Diego, CA
  Implement and evaluate computation workload on time-sensitive platform *July 2016 - July. 2017*
  - Implemented machine learning and time series forecasting technology to predict task execution time.
  - Co-developed scheduling policy to reduce the server respond time in case of congestion.
  - Deployed the system on Raspberry PI and Android with Docker, demonstrated with face detection and simultaneous localization and mapping applications.

Electronic Design Automation

- **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 interconnect routing channel.
  - Formulate 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*
  - Study the different circuit parameters on the crosstalk level.
  - Use artificial neural network (ANN) and support vector machine (SVM) to predict the timing delay of VLSI.

Professional Skills

- Programming Languages: C/C++, Python, MATLAB
- Systems: Linux, ROS, Trusted Execution Environment, ARM TrustZone
- Miscellaneous: machine learning, compiler construction, robotics.

Selected Publications

- **M.Luo**, G. E. Suh, "Software-Hardware Co-optimization of Path Planning with Dynamic Obstacles for autonomous driving", in preparation.
- **M.Luo**, G. E. Suh, "Impact of Timestamp Integrity Attack in Cyber-Physical Systems", manuscript in submission.
- 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.
- Z. Fang, **M. Luo**, et al., "Mitigating multi-tenant interference in continuous mobile offloading", International Conference on Cloud Computing 2018, 20-36.
- S. Guo, R. Wang, P. Ren, C. Liu, **M. Luo**, et al., "Investigation on NBTI-induced dynamic variability in nanoscale CMOS devices: Modeling, experimental evidence, and impact on circuits", Microelectronics Reliability 81, pp. 101- 111.
- 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**).
- 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.
- 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.
- Z. Fang, **M. Luo**, et al., "Exploiting Synchrony in Replicated State Machines", 2017 IEEE CLOUD, pp. 155.
- **M. Luo**, et al., "Delay uncertainty and signal criticality driven routing channel optimization for advanced dram products", 2016 IEEE Asia and Sout Pacific Design Automation Conference (ASP-DAC), 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.
- **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).