RUYI DING

Email: ding.ruy@northeastern.edu Phone1: (+1) 404-271-7158 Phone2: (+86) 178-168-78071
Personal website: rollinding.github.io

EDUCATION

Northeastern University, Boston, USA *Jul. 2020 - Present*
Ph.D. candidate in Computer Engineering
Advisor: Prof. Yunsi Fei GPA: 4.0/4.0

Georgia Institute of Technology, Atlanta, USA *Aug. 2018 - May 2020*
M.S. in Electrical and Computer Engineering
Advisor: Prof. Yao Xie GPA: 3.86/4.0

Zhejiang University, China *Sept. 2014 - Jul.2018*
B.S. in Information Science & Electronic Engineering
Advisor: Prof. Fan Zhang GPA: 3.80/4.0

RESEARCH INTERESTS

My research lies at the intersection of hardware and AI security, with a specific focus on ***side-channel analysis*** and ***AI security–encompassing robustness, privacy, and intellectual property (IP) protection of machine learning models***. The core objective of my work is to develop machine learning systems that prioritize both security and privacy. This involves identifying and mitigating hardware side-channel attacks and micro-architectural vulnerabilities, while also exploring machine learning-hardware co-design for enhanced security applications. Through this, I aim to make significant contributions to the advancement of **Responsible AI** and **Reliable Computing Systems**. .

PUBLICATIONS

The authors are ordered by contribution and (*) indicates that authors are equally contributed

- **Ruyi Ding**, Tong Zhou, Lili Su, Aidong Adam Ding, Xiaolin Xu, Yunsi Fei, *Probe-Me-Not: Protecting Pre-trained Encoders from Malicious Probing.* The Network and Distributed System Security Symposium 2025 (NDSS 2025) *Accepted/In Press.*
- Shijin Duan*, **Ruyi Ding***, Jiaxin He, Aidong Adam Ding, Yunsi Fei, Xiaolin Xu, *GraphCroc: Cross-Correlation Autoencoder for Graph Structural Reconstruction.* The Thirty-Eighth Annual Conference on Neural Information Processing Systems (NeurIPS 2024) *Accepted/In Press.*
- **Ruyi Ding**, Lili Su, Aidong Adam Ding, Yunsi Fei, *Non-transferable Pruning.* In European Conference on Computer Vision (pp. 375-393). Springer, Cham.
- **Ruyi Ding***, Shijin Duan*, Xiaolin Xu, Yunsi Fei *VertexSerum: Poisoning Graph Neural Networks for Link Inference.* In Proceedings of the IEEE/CVF International Conference on Computer Vision (pp. 4532-4541).
- **Ruyi Ding**, Cheng Gongye, Siyue Wang, Aidong Adam Ding, Yunsi Fei, *EMShepherd: Detecting Adversarial Samples via Side-channel Leakage.* In Proceedings of the 2023 ACM Asia Conference on Computer and Communications Security (pp. 300-313). (**Distinguished Paper Award.** (One of four recipients))
- **Ruyi Ding**, Ziyue Zhang, Xiang Zhang, Cheng Gongye, Yunsi Fei, Aidong Adam Ding *A cross-platform cache timing attack framework via deep learning.* In 2022 Design, Automation & Test in Europe Conference & Exhibition (DATE) (pp. 676-681). IEEE. (**Best Paper Award Nomination.** (One of five in T Track))

- Yize Li, Pu Zhao, **Ruyi Ding**, Tong Zhou, Yunsi Fei, Xiaolin Xu, Xue Lin. *Neural architecture search for adversarial robustness via learnable pruning.* Frontiers in High Performance Computing, 2: 1301384.
- Xiang Zhang, Ziyue Zhang, **Ruyi Ding**, Cheng Gongye, Aidong Adam Ding, Yunsi Fei. *Ran $ Net: An Anti-Ransomware Methodology based on Cache Monitoring and Deep Learning.* In Proceedings of the Great Lakes Symposium on VLSI 2022, pp. 487-492. 2022.
- Shixiang Zhu, **Ruyi Ding**, Minghe Zhang, Pascal Van Hentenryck, Yao Xie *Spatio-temporal point processes with attention for traffic congestion event modeling.* IEEE Transactions on Intelligent Transportation Systems 23.7 (2021): 7298-7309.
- Shixiang Zhu, Minghe Zhang, **Ruyi Ding**, Yao Xie *Deep Fourier Kernel for Self-Attentive Point Processes.* In International conference on artificial intelligence and statistics, pp. 856-864. PMLR, 2021.
- Fan Zhang, Xiaoxuan Lou, Xinjie Zhao, Shivam Bhasin, Wei He, **Ruyi Ding**, Samiya Qureshi, Kui Ren. *Persistent fault analysis on block ciphers.* IACR Transactions on Cryptographic Hardware and Embedded Systems (2018): 150-172.

AWARDS

- **Distinguished Paper Award** for Paper *EMShepherd: Detecting Adversarial Samples via Side-channel Leakage.* List of awardees: `https://asiaccs2023.org/program/awards/` ASIACCS, July 2023
- **Best Paper Awards Nomination** for Paper *A cross-platform cache timing attack framework via deep learning.* List of awardees: `https://past.date-conference.com/proceedings-archive/2022/html/bestpaper.html` DATE, March 2022
- **Graduate Student External Award.** NEU College of Engineering, June 2024

TEACHING

- Teaching Assistant at Northeastern *Summer 2022*
  EECE 5699: Computer Hardware and System Security
- Graduate Teaching Assistant at Georgia Tech *Fall & Spring 2020*
  ISyE 6740: Computational Data Analysis / Machine Learning

RESEARCH PROJECTS

RINGS: Internet of Things Resilience through Spectrum-Agile Circuits, Learning-Based Communications and Thermal Hardware Security *Northeastern University* *Dec, 2023 -*

- Leverage sensors to detect the small temperature swift when the circuit has a hardware Trojan.
- Utilize graph neural network to find and localize the Trojan on SOC.

Poisoning Graph Neural Networks for Link Inference
Northeastern University *Nov. 2022 - Mar 2023*
Advisor: Prof. Yunsi Fei

- Investigated edge privacy vulnerabilities in graph neural networks.
- Employed poisoning techniques to exacerbate link inference leaks using adversarial samples.
- Developed 'Intra-AUC', an innovative metric to more accurately assess link leakage within classes.

ONR: Security DNN on Edge *Northeastern University* *Jun, 2022 - Jun, 2023*

- Investigate SOTA adversarial pruning method on edge DNN models.
- Propose learnable pruning for adversarial robustness.

Protecting Confidentiality and Integrity of Deep Neural Networks against Side-Channel and Fault Attacks
Northeastern University *May 2021 - Nov. 2022*
Advisor: Prof. Yunsi Fei

- Pioneered the use of Side-channel Information for malicious behavior detection.
- Analyzed Xilinx DPU execution using EM emanation to detect anomalies.
- Developed a detector for adversarial samples based on EM abnormalities.

EAGER: Side Channels Go Deep - Leveraging Deep Learning for Side-channel Analysis and Protection
Northeastern University *July 2020 - Sept. 2021*
Advisor: Prof. Yunsi Fei, Prof. Aidong Ding

- Investigated CPU microarchitecture side channels (cache timing) in Intel, AMD, and ARM.
- Applied deep neural networks for learning-based cache timing analysis.
- Enhanced cross-platform side channel analysis using transfer learning.

Anomaly Detection on Traffic Event Data
Georgia Institute of Technology *Nov. 2018 - Oct. 2019*
Advisor: Prof. Yao Xie

- Conducted statistical analysis and visualization of Sacramento traffic data.
- Implemented machine learning models for holiday detection using time series analysis.
- Utilized Spatio-temporal analysis for traffic incident detection on distributed sensors.

Cyber Security Research Internship
National University of Singapore *Jul. 2017 - Oct. 2017*
Advisor: Prof. Zhenkai Liang (NUS) & Prof. Fan Zhang (ZJU)

- Researched page fault attacks on Intel Security Guard Extensions (SGX).
- Analyzed FPGA faults in Advanced Encryption Standard (AES) implementations.