RUYI DING

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

EDUCATION

Northeastern University, Boston, USA *Jul. 2020 - Present*
Ph.D. candidate in Computer Engineering
Advisors: 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
Advisors: Prof. Yao Xie GPA: 3.86/4.0

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

RESEARCH INTERESTS

My research covers the intersection of AI security and hardware security. I am particularly focused on neural network model robustness, privacy, and IP protection and side-channel analysis. The primary objective of my work is building machine-learning systems that are both secure and privacy-preserving; identifying and mitigating hardware side channels and micro-architectural vulnerabilities; employing machine learning-hardware co-design for security applications. My efforts aim to contribute significantly to **Responsible AI** and **Reliable Computer Systems**.

PUBLICATIONS

- **Ding, R.**, Su, L., Ding, A. A., Fei, Y., *Non-transferable Pruning.* The 18th European Conference on Computer Vision (ECCV 2024).
- **Ding, R.***, Duan, S.*, Xu X., Fei, Y. *VertexSerum: Poisoning Graph Neural Networks for Link Inference.* International Conference on Computer Vision (ICCV 2023).
- **Ding, R.**, Gongye, C., Wang, S., Ding, A. A., Fei, Y., *EMShepherd: Detecting Adversarial Samples via Side-channel Leakage.* ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2023). **Distinguished Paper Award.**
- **Ding, R.**, Zhang, Z., Zhang, X., Gongye, C., Fei, Y., & Ding, A. A. *A cross-platform cache timing attack framework via deep learning.* In 2022 Design, Automation & Test in Europe Conference & Exhibition (DATE 2022). **Best Paper Awards Nomination.**
- Zhang, X., Zhang, Z., **Ding, R.**, Gongye, C., Ding, A. A., & Fei, Y. (2022, June). Ran $ Net: An Anti-Ransomware Methodology based on Cache Monitoring and Deep Learning. In Proceedings of the Great Lakes Symposium on VLSI (GLSVLSI 2022).
- Zhu, S., **Ding, R.**, Zhang, M., Van Hentenryck, P., & Xie, Y. *Spatio-temporal point processes with attention for traffic congestion event modeling.* IEEE Transactions on Intelligent Transportation Systems. (2021)
- Zhu, S., Zhang, M., **Ding, R.**, & Xie, Y. *Deep Fourier Kernel for Self-Attentive Point Processes.* In International Conference on Artificial Intelligence and Statistics (AISTATS 2021).

SELECTED AWARDS

- **Distinguished Paper Award** ASIACCS, July 2023

- **Best Paper Awards Nomination** DATE, March 2022

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 EXPERIENCE

VertexSerum: 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.

EMShepherd: Detecting Adversarial Samples via Side-channel Leakage
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.

Leveraging Deep Learning for Side-channel Analysis and Protection
Northeastern University *July 2020 - Sept. 2021*
Advisor: Prof. Yunsi Fei

- 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
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.