Omid Aramoon

Linkedin account | github.com/oaramoon | +1 (443) 968-1638 | oaramoon@umd.edu

I am a researcher at the Maryland Cybersecurity Center at the University of Maryland. I started my Ph.D. working on security problems in hardware design including IP watermarking, fingerprinting, and logic locking schemes, which led to several publications at prestigious EDA conferences. Later on, I became interested in the security, and privacy aspects of Machine Learning (ML) and Deep Learning (DL) systems, and I studied techniques for protecting ML/DL systems against adversarial attacks such as IP infringements, backdooring attempts as well as model tampering attacks, which led to several publications at top ML conferences. I am confident in my research skills, knowledge of deep learning and machine learning concepts, and ability to build complex ML/DL algorithms using Python and TensorFlow. **I am expected to graduate in August 2022.**

Education

In Progress	PhD in Electrical and Computer Engineering | **University of Maryland**
2022	MSc in Electrical and Computer Engineering | **University of Maryland**
2016	BSc in Computer Engineering | **Sharif University of Technology**

Professional Experience

Present – August 2016 — **Graduate Research Assistant | University of Maryland , College Park, MD**

- **[ongoing]** Utilizing power side-channel analysis to detect training and test time adversarial attacks against FPGA implementations of deep learning systems.
- In collaboration with *IBM Research*, developed a novel federated learning framework with improved privacy and security guarantees.
- In collaboration with *IBM Research*, developed an attestation framework for deep neural networks capable of detecting any trivial breaches to the integrity of models deployed on edge devices.
- In collaboration with *IBM Research*, developed a watermarking framework for deep neural networks which out-performed the state-of-the-art in terms of robustness and embedding capacity.
- Developed a fault detection method for deep neural networks with provable performance guarantees.
- Performed Independent Verification & Validation (IV&V) of side-channel countermeasures for DARPA's Automatic Implementation of Secure Silicon (AISS) platform.
- Developed a genetic algorithm approach to design polymorphic gates.
- Developed new applications for polymorphic gates in watermarking and fingerprinting ICs.
- Designed a robust authentication framework for embedded systems built upon their scan chains.

Python | C/C++ | Keras | TensorFlow | Verilog | Linux | Synopsys Design Compiler | Synopsys PrimePower | Xilinx Vivado

September 2021 – June 2021 — **R&D Technical Intern | Synopsys Inc , Mountain View, CA**

- Developed a framework to evaluate the security of hardware designs against voltage glitching attacks.
- Developed a framework to simulate laser fault injection attacks on hardware design using Synopsys Z01X Fault Simulator.

Python | Synopsys Z01X Fault Simulator | Synopsys Design Compiler | Linux

September 2018 – May 2018 — **Research Intern | National Tsing Hua University , Hsinchu City, Taiwan**

- Developed a machine learning-based attack to break logic locking schemes for ICs.

Python | Keras | TensorFlow | Verilog

February 2016 – August 2015 — **Undergraduate Researcher | Sharif University of Technology, Tehran, Iran**

- Developed a file-based database, graphical user interface, and communication APIs with fingerprint and RFID sensors for an authentication system.

C/C++

August 2015 – May 2015 — **Software Developer Intern | HPDS (High Performance Distributed Systems), Tehran, Iran**

- Developed hardware health monitoring software for Linux operating system.

C/C++ | Shell Script

Publications

Omid Aramoon, Pin-Yu Chen, Yuan Tian and Gang Qu, **"Meta Federated Learning"** published on DPML workshop in International Conference on Learning Representations (ICLR-21)

Omid Aramoon, and Gang Qu, **"Provably Accurate Memory Fault Detection Method for Deep Neural Networks."** published on proceedings of the 2021 on Great Lakes Symposium on VLSI (GLSVLSI-21)

Omid Aramoon, Pin-Yu Chen and Gang Qu, **"AID: Attesting the Integrity of Deep Neural Networks"** published on 2021 58th ACM/IEEE Design Automation Conference (DAC-21)

Omid Aramoon, Pin-Yu Chen and Gang Qu, **"Don't Forget to Sign the Gradients!"** published on Proceedings of Machine Learning and Systems 3 (MLSys-21)

Omid Aramoon, **"Trust in Machine Learning as a Service"** published on System on Chip Conference (SOCC-20)

Omid Aramoon, Pin-Yu Chen and Gang Qu, **"Do You Sign Your Model?"** published on DMMLSys workshop in International Conference on Machine Learning (ICML-20)

Omid Aramoon, and Gang Qu, **"Impacts of Machine Learning on Counterfeit IC Detection and Avoidance Techniques"** published on 21st International Symposium on Quality Electronic Design (ISQED-20)

Qian Wang, **Omid Aramoon**, and Gang Qu, **"Efficient Transfer Learning Attack for Modeling Physical Unclonable Functions"** published on 21st International Symposium on Quality Electronic Design (ISQED-20)

Gang Qu, **Omid Aramoon**, Qian Xu, et al. , **"Independent Verification and Validation of Security-Aware CAD Tools"** published on 2021 58th ACM/IEEE Design Automation Conference (DAC-21)

Xi Chen, **Omid Aramoon**, Gang Qu and Aijiao Cui, **"Balancing Testability and Security by Configurable Partial Scan Design"** published on 2018 IEEE International Test Conference in Asia (ITC-Asia-18)

Omid Aramoon, Xi Chen and Gang Qu,**"A Reconfigurable Scan Network based IC Identification for Embedded Devices"** published on 2018 Design, Automation Test in Europe Conference Exhibition (DATE-18)

Timothy Dunlap, **Omid Aramoon**, Gang Qu, Tian Wang, Xiaxin Cui and Dunshan Yu, **"A Novel Circuit Authentication Scheme based on Partial Polymorphic Gates"** published on Asian Hardware Oriented Security and Trust Symposium (AsianHOST-21)

Tian Wang, **Omid Aramoon**, Xiaoxin Cui, Dunshan Yu, Gang Qu and Xiaole Cui, **"A Novel Polymorphic Gate based Circuit Fingerprinting Technique"** published on 2018 IEEE International Symposium on Circuits and Systems (ISCAS-18)

Tian Wang, Xiaoxin Cui, Dunshan Yu, **Omid Aramoon**, Timothy Dunlap, Gang Qu and Xiaole Cui, **"Polymorphic Gate based IC Watermarking Techniques"** published on Asia and South Pacific Design Automation Conference (ASP-DAC-18)

Personal Projects

Reservoir Computing based Generative Adversarial Network (RC-GAN) 2018

Implemented a reservoir computing (RC)-based generative adversarial network, where the generator consists of only a large reservoir network. Showed that the synthetic images generated by the RC generator were comparable in quality to those from more complicated generators comprising convolutional-transpose layers. Furthermore, showed that the RC-GAN was easier to train and was less likely to suffer from vanishing gradients.

Python | Verilog | PyTorch

Identifying Fake News using Social Media Analytic 2017

Decided to take action against fake news publishers. Investigated the information available on Twitter to find discerning patterns in propagation of the fake news and the users who are extensively involved. Then, used this information to train a ML-based classifier to detect tweets containing fake news.

Python | Twitter API | Scikit-learn

Temperature Aware floor planner 2017

Developed a simulated annealing-based floor planner for soft blocks under C++ that utilized HotSpot temperature modeling tool for estimating temperature of the chip.

C++ | HotSpot

Skills

Programming	Python (Numpy, scikit-learn, pandas, matplotlib, OpenCV), C/C++, Verilog, Bash
Machine Learning Frameworks	TensorFlow/Keras (Expert), PyTorch
EDA tools	Design Compiler, PrimePower, Z01X Fault Simulator, Vivado
Development Tools	git, Docker, vscode
Work Authorization	I am a U.S. Citizen and do not need work authorization or visa support.

Open Source Code

MLSys'21 Paper: Codes for reproducing the MLSyS'21 paper "Don't Forget to Sign the Gradients!"

DAC'21 Paper: Codes for reproducing the DAC'21 paper "AID: Attesting the Integrity of Deep Neural Networks"

AsianHOST'21, ISCAS'18, ASPDAC'18 Papers: Codes for generating polymorphic gates designed via a genetic algorithm

Meta Federated Learning Paper: Codes for reproducing the paper "Meta Federated Learning"