Seyed Mani Sadati

B.Sc. student in Computer Engineering

✉ sadati.man@outlook.com
🖥 ManiSadati.netlify.app
in Seyed-Mani-Sadati
⊛ ManiSadati

Summary

Education

2018–Present **B.Sc. in Computer Engineering**, Shahid Bahonar University of Kerman, **19.0/20**.

Selected Honors & Awards

2020 **First Place**, CAD Contest at ICCAD 2020
Winner team of problem C: GPU Accelerated Logic Re-simulation.

2018/19 **Bronze Medal**, ICPC Asia Tehran Regional Contest
Rank 4 in the 2018 ICPC Asia Tehran Regional Contest. Rank 1 in Asia Tehran Internet Online Programming Contest.

2018–Present **Ranked Second GPA**, Shahid Bahonar University
Among 120 computer engineering students.

Papers

○ **Seyed Mani Sadati**, Behnam Ghavami, Zhenman Fang, and Lesley Shannon. FitAct: Error Resilient Deep Neural Networks via Fine-Grained Post-Trainable Activation Functions. In *Proceedings of the 2022 Design, Automation & Test in Europe Conference & Exhibition (DATE)*.

○ **Seyed Mani Sadati**, Mohammad Shahidzade , Behnam Ghavami, Zhenman Fang, and Lesley Shannon. BDFA: A Blind Data-Free Attack on Deep Neural Networks.

Selected Projects

○ **GPU Acclerated Logic re-simulation**
I designed and implemented a new method to optimally parallelize the verilog design of various circuits.

○ **Fault injection on Deep learning models**
I studied the robustness of multiple DNN architectures, and designed a new activation function to increase the robustness and reliability of DNNs.

○ **Blind Data-Free Attack**
I developed various methods to do an optimal bit-flip attack on DNN's parameters without using any data.

International Research Collaborations

Reconfigurable Computing LAB, *Simon Fraser University*, BC, Canada
Collaboration on reliability and security of Deep Learning models against fault injection and bit-flip attacks.
http://www2.ensc.sfu.ca/ lshannon/rcl/

Education

2018–Present	**B.Sc. in Computer Engineering**, *Department of Computer Engineering, Shahid Bahonar University of Kerman, Iran.* 🎓**19.0/20**,

Supervisor: Professor Behnam Ghavami

Selected Courses and GPAs:

- Algorithm Design: 20/20
- Operating Systems: 19.5/20
- Probabilistic and statistics: 20/20
- Automated Design of Digital Circuits: 20/20
- Artificial Intelligence: 18/20
- Compiler Design: 20/20
- Electronic Digital: 20/20

Selected Online Courses:

- Machine Learning Offered By Stanford University
- Reinforcement Learning Offered By University of Alberta

Honors & Awards

2021 **Ranked Second GPA**, Shahid Bahonar University
Among 120 computer engineering students.

2020 **First Place**, CAD Contest at ICCAD 2020
Winner team of problem C: GPU Accelerated Logic Re-simulation.

2020 **Rank 6**, ICPC Asia Tehran Regional Contest
Rank 6 in the 2020/21 ICPC Asia Tehran Regional Contest. Rank 12 in Asia Tehran Internet Online Programming Contest.

2018 **Bronze Medal, Rank 4**, ICPC Asia Tehran Regional Contest
Rank 4 in the 2018/19 ICPC Asia Tehran Regional Contest. Rank 1 in Asia Tehran Internet Online Programming Contest.

2018 **Received full Scholarship**, for Bachelors degree (Tuition waiver), Shahid Bahonar University of Kerman.

2016, 2017 **Top 70**, National Olympiad in Informatics
Among 10000 high school students, passed first and second exam.

Projects

- **GPU Acclerated Logic re-simulation**
Timing-aware gate-level simulation usually runs much slower than RTL simulation, from a few cycles per second on smaller unit-level designs to many seconds per cycle on today's largest full-chip SoC designs. In this project, I developed several methods to parallelize the computations in the two dimensions of gate-parallelism and stimuli-parallelism and a new method for memory management of the stored signal waveforms. I did most of the project using C++ and the CUDA library and used several parallelization techniques. In addition, I developed a parser for Verilog as well as a Verilog to C++ translator. Our project managed to speed up the simulation up to 40x compared to a CPU simulator.

- **Fault injection on Deep learning models**
  With the rise of Deep Neural Networks (DNNs), many safety-critical applications, such as self-driving cars and healthcare devices, are using them to improve their performance. In these systems, error resilience is a top priority since faults in DNN inference could lead to mispredictions and safety hazards. In this work, I developed a new method to improve the error resiliency of DNNs called FitAct. The idea is to bound the activation function with a post-trained, neuron-wise activation function. I tested this method on several DNN architectures and datasets. For this project, I used PyTorch, a deep learning framework based on Python, to implement and test FitAct.

- **Blind Data-Free Attack**
  Adversarial parameter attacks are well-known bit-flip attacks that try to flip a few bits of DNNs parameters to crush their functionality. However, these attacks are not always performable since the attacker may not have access to data for many applications containing sensitive or proprietary data. For example, medical and biometric datasets are not available for everyone due to privacy and security concerns. In this project, I deployed several approaches to attack DNN parameters without having access to any training/test data. One of the methods is the Blind Data-Free attack which produces synthetic data samples using the model information and with the help of knowledge distillation. This method was able to decrease the accuracy of ResNet50 to 12% on the CIFAR100 dataset.

- **Full Facial Recognition System**
  Most of the Deep learning methods are not practical for real-world applications because they are too large and computationally expensive. One of the most popular applications that suffer from this problem is Face Recognition. I deployed a Full Facial Recognition system that consumes negligible power and memory compared to other big DNNs. that first detects people's faces in the picture. After properly aligning the faces, I used a face recognition model to recognize the identity of the faces. YOLOV5 was used for face detection and SphereFace for face recognition. I implemented the project using Pytorch and OpenCV frameworks.

- **Reliability of Bayesian Neural Networks**
  In this project, I studied the Reliability of Bayesian DNNs against fault injections. Furthermore, I proposed a new way to improve their robustness by using statistical information of Bayesian networks and uncertainty estimation.

- **Saba Programming Contest**
  In this project, I designed two problems and prepared several problem statements for the Saba Programming Contest. In addition, I implemented the solutions and did validation checks and testing for several problems using C++.

Experiences

2021–Present **Research Assistant**, Shahid Bahonar University of Kerman
Reliable Embedded System Design Laboratory

- **Supervisor:** Professor Behnam Ghavami

- **Description:** I contributed to 6 projects related to Deep Learning, efficient and low-cost Deep learning systems, Safety and reliability of DNNs, and logic simulations.

2019 **Teacher**, Allame Helli High School
I prepared students for the Iranian National Olympiad in Informatics. I taught Algorithms, Programming, and Graph theories.

2019 **Scientific Team Member**, Saba Programming Contest
An onsite and online programming contest. I prepared students for the Iranian National Olympiad in Informatics. I taught Algorithms, Programming, and Graph theories. I designed several problems for the competition, prepared the problem statements, and tested the solutions. The Online contest was held at HackerEarth.

Skills

- **Programming Languages:**
  C/C++, Python, C#, Octave (MATLAB), CUDA
- **Deep Learning Frameworks:**
  Pytorch, Tensorflow, Keras
- **Hardware Desing Languages:**
  VHDL, Verilog
- **Simulators:**
  Hspice, ModelSim, Proteus, Xilinx ISE Design Suite

References

- **Associate Professor Behnam Ghavami**
  Department of Computer Engineering
  Shahid Bahonr University of Kerman
  ghavami@uk.ac.ir