Ziyu Wang

Homepage: ziyuwang11.github.io/ | Email: ziwa@umich.edu | Phone: 734-882-9092

Education

University of Michigan, Ann Arbor — Ann Arbor, MI, USA
PhD candidate in Electrical and Computer Engineering (GPA:3.94/4.0) — *Aug 2019 – Apr 2024*
Core Courses: Computer Architecture, VLSI Design I, Microarchitecture, A/D Interface Circuits, Machine Learning.

Tsinghua University — Beijing, China
Bachelor of Engineering in Material Science and Engineering — *Aug 2015 – July 2019*
Minor in Computer Technology and Applications — *Aug 2017 – July 2019*

Research Experience

Graduate Student Research Assistant — Ann Arbor, MI, USA
University of Michigan, Ann Arbor, Advisor: Wei D. Lu — *Aug 2019 – Present*
Research interests include vulnerability analysis of emerging non-volatile memory analog in-memory computing (IMC) accelerator for deep neural networks (DNNs), as well as designing secure and reliable IMC circuit and architecture.

- **Dynamic Power Simulator of IMC Systems**
  - Built a Python framework to simulate DNN inference specific dynamic power traces during runtime.
  - Simulated mixed-signal RRAM IMC circuits using Spectre and extracted power signature of each sub-block.
  - Implemented a CUDA framework with ports to PyTorch model for fast inference power feature simulation.
- **DNN Model Extraction Attack on IMC Architectures**
  - Developed algorithms for model extraction attack on IMC-based DNN accelerator by power and timing side-channel attack. The complete DNN architecture can be reconstructed from side-channel leakage.
  - Reconstructed DNN layer types and sequence, input/output feature sizes and filter sizes by side-channel analysis without prior knowledge to the model. Proposed countermeasures for securing IMC chips.
- **Reconstruction Private Input Data by Side-Channel Attack on IMC Systems**
  - Trained a UNet for MRI segmentation by PyTorch. Mapped the model to an RRAM IMC architecture.
  - Collated power feature dataset of each image processing step using a C/C++ CUDA framework.
  - Proposed an algorithm for reconstructing image from power feature using a conditional GAN.
- **Fingerprint Physical Unclonable Function (PUF) System**
  - Devised, fabricated and measured a PUF system based on fingerprint-like polymer self-assembly pattern.
  - PUF system achieves strong uniqueness, entropy and reliability, and is resilient to machine learning attacks.

Selected Publications

Z. Wang, F. Meng, Y. Park, J. K. Eshraghian, W. D. Lu, "Side-Channel Attack Analysis on In-Memory Computing Architectures," *arXiv preprint*, arXiv: 2209.02792.
Z. Wang, Z. Zhu, S. Jaloka, B. Cline, W. D. Lu, "Physical Unclonable Function Systems Based on Pattern Transfer of Fingerprint-Like Patterns," in *IEEE Electron Device Letters*, vol. 43, no. 4, pp. 655-658, April 2022.

Selected Course Projects

A 4-bit Compute-in-Memory 9T-SRAM Macro | VLSI Design I — 2021
- Implemented a 16-bit RISC processor with a 9T-SRAM IMC circuit to accelerate matrix multiplication.
- Designed analog circuits for 4-bit weighted sum and a 4-bit flash ADC for data conversion.
- Simulated the macro with HPICE, NC-Verilog, Spectre and Verilog-A. Integrated full physical layout.

A 2-Way Out-of-Order Superscaler Processor with R10k-Style Renaming | Computer Architecture — 2020
- Synthesized a 7-stage pipeline processor with reorder buffer and reservation station using SystemVerilog.
- Improved performance by adding branch predictor, load-store queue, instruction prefetcher, and write-back cache.

Skills

Programming Languages: Python, C/C++, CUDA, Verilog, SystemVerilog, Verilog-A, Matlab.
Tools: Cadence Virtuoso, Virtuoso-XL (physical layout), PyTorch, HSPICE, Spectre, Synopsis Synthesis, Git.
Key Strengths: Project Management, Engineering Design, Leadership, Presentation, Academic Writing.