135 Yellowstone Drive
Apt. 301
Charlottesville, VA 22903
+1 (757) 279 4582
cedar.ren@gmail.com
linkedin.com/in/renxida/
github.com/renxida

Xida Ren

Research Interests

Responsible AI.

- Verifiable claims about AI projects
- Hardware mechanisms for supporting auditing / monitoring machine learning projects for safety
- Formal verification of neural networks
- Interpretable Machine Learning

Hardware Performance and Security.

- Privacy and Security
- Side-channel attacks
- Automated Hardware/Software Co-Optimization
- MLIR and other ML compilers
- Formal Verification
- Co-optimization for efficient machine learning

Education

2019- **PhD Computer Architecture**, *University of Virginia*.

2016-2019 **B.A. Computer Science / Mathematics**, *College of William and Mary*, *3.81*.

Publications

ISCA 2021 **I see dead μops: Leaking Secrets via Intel/AMD Micro-Op Caches**, *Xida Ren, Logan Moody, Mohammadkazem Taram, Matthew Jordan, Dean M Tullsen, Ashish Venkat*, 2021 ACM/IEEE 48th Annual International Symposium on Computer Architecture (ISCA).

USENIX 2022 **SecSMT: Securing SMT Processors against Contention-Based Covert Channels**, *Mohammadkazem Taram, Xida Ren, Ashish Venkat, Dean Tullsen*, 2022 31st USENIX Security Symposium.

Research Projects

Fall 2022- **Project VeriQuant**, University of Virginia.

- Deisgn quantized + full-precision ML inference accelerator to exploit efficiency of quantization inference while maintaining safety and reliability of full-precision computation.
- Ensure functional correctness and adversarial safety of deep learning models by applying formal verification to quantized deep neural networks.
- Handle input items in un-veried portions of the input space by escalating to full precision inference.

Spring 2021- **Project "Proxy VM"**, Venkat Lab, University of Virginia.

Project lead. Uses MLIR to transform machine learning workloads into proxy benchmarks for no-hassle accelerator design.

- Capture MLaaS workload performance characteristics for tailored hardware optimization
- Removes sensitive information from proxy workload to relieve hardware designer of the burden to handle workloads that contain proprietary model and confidential user data

2020- **Project"SecSMT"**, Collaboration with Mohammadkazam M. Tarem & Dean Tullsen at UCSD.
Project explores side channel safety of Simultaneous Multi-Threading (SMT) and develops defenses for key channels of cross-thread information leakage

2019-2021 **Project "I See Dead Micro-Ops"**, Computer Architecture Lab, University of Virginia.
Microarchitectural side channel attack published in ISCA 2021 paper "I See Dead μ-Ops: Leaking Secret via Intel / AMD Micro-Op Caches"
- Microbenchmarks to reverse engineer streaming RISC micro-op cache in Intel processors
- New Spectre variant that uses this micro-op cache
- LFENCE-bypassing transient execution attack that also bypasses major transient execution attack

2017-2019 **Data Science Research Assistant**, Equity AI Lab, William & Mary.
- Timeseries forecast using DNN and convolutional NN
- Distributed computing (for hyperparameter search)

Employment

2022-Current **Research Intern**, Computer Architecture Design Tools , Intel Labs.
- Build compiler/profiler toolchain for software-hardware codesign by extracting architectuure

May - August 2022 **ML Performance & Security Research Intern**, Microcontrollers Group, NXP Semiconductors.
- Benchmark/test machine learning models on MCU/MPU devices.
- Implement and integrate machine learning software modules.

2022-Current **Research Scholar**, SRC Research Scholars Program, Semiconductor Research Company.
Task 3105.001 ProxyVM: A Scalable and Retargetable Compiler Framework for Privacy-Aware Proxy Workload Generation

2019-Current **Research Assistant**, Venkat Lab, University of virginia.
Computer Architecture Research

Fall 2020 **Research Intern**, Lawrence Berkeley National Lab, PARADISE++ Simulator Project.
Worked on improving speed and memory usage of Memory Hierarchy Simulator
- Architecture: Parallel Discrete Event simulation
- Optimistically Synchronized using Global Virtual Time
- Valgrind, C++

Summer 2019 **Summer Quantitative Analyst**, Citigroup Global Markets, PB Quant Desk.
Machine Learning and fullstack web development to inform trading in Prime Brokerage
- Python, SkLearn, Flask, Javascript, React.js
- Made dashboard for forecasting equity lending fees; used across multiple trading desks

2018-2019 **Research Assistant**, Equity AI Group, William and Mary.
Research on Machine Learning in Equity Market
- Linux environment, Python & BASH scripting
- Tensorflow

Volunteering

2021-2022 **Chair**, Computer Science Grad Student Group, University of Virginia.
- Increased grad student social event participation 300% by hosting events with food and promoting outdoor activities

2017-2018 **Career Prep Chair**, ACM@WM.
- Increased participation by 100% by hosting learn-to-code sessions & career outreach events

Summer 2017 **Math Modeling Lead**, *William and Mary* team for the *International Genetic Engineered Machines* contest.

- Developed tools for synthesizing genetic engineered organisms
- Did math, wrote code, won prizes:
  - 2nd place worldwide
  - Best Math Model (ODE-based)
  - Best Measurement (Markov-chain Montecarlo model validated in wet-lab)
- Did web development w/ **Bootstrap** & **JQuery** to present results

Teaching

2021 **TA**, Undergraduate Computer Architecture, University of Virginia.

2021 **TA**, Graduate Computer Architecture, University of Virginia.

2020 **TA**, Computer Hardware Security, University of Virginia.

2019 **TA**, Graduate Computer Architecture, University of Virginia.

2018 **Undergraduate Graph Theory**, William & Mary.
Grade homework and host help sessions

Recent Coursework Highlights

Spring 2022 **Deep Neural Network Verification**, *Matt Dwyer*, University of Virginia.
The "VeriQuant" project began in this course.

Spring 2022 **Operating Systems**, *Felix Xiaozhu Lin*, University of Virginia.
Used ARM TEE confidential computing enclaves to secure machine learning workloads.

Fall 2021 **Mobile and IoT Security**, *Yuan Tian*, University of Virginia.

Spring 2021 **Graph Mining**, *Jundong Li*, University of Virginia.
Graph Neural Networks and methods for processing graph data.

Spring 2020 **Software Analysis and Applications**, *Marylou Sofa*, University of Virginia.
A deep dive into securing and optimizing software using algorithms on Control Flow Graphs and Data Flow Graphs.

Fall 2019 **Software Security via Program Analysis**, *Yonghwi Kwon*, University of Virginia.
Combine static and dynamic program analysis to detect malware and patch software vulnerabilities.

Fall 2019 **Computer Architecture**, *Ashish Venkat*, University of Virginia.
Architecture of pipelined, parallelized, and heterogeneous computers. Bottleneck analysis, out-of-order execution, and other techniques to increase instructions-per-cycle.

Foreign Languages

Mandarin **Business Fluent**

Japanese **JLPT Level N2** *Fluent*