Ali Hajiabadi

Computer Science PhD Candidate
National University of Singapore (NUS)

Contact Information

Address: 13 Computing Drive, Singapore, 117417, SoC @ NUS
Email: ali.hajiabadi@u.nus.edu
Homepage: hajiabadi.github.io

Research Interests

Systems Security, Hardware/Software Co-design, Computer Architecture, Optimizing Compilers, Formal Methods, Trusted Execution Environments, Confidential Computing for Heterogeneous Systems, Secure Architectures and Software, Microarchitectural Attacks and Side Channels, Machine Learning Security and Privacy

Education

Aug. 2019 - Present — Doctor of Philosophy in Computer Science
National University of Singapore (NUS), Singapore
Thesis: *"Non-speculative and Non-deterministic Processing for Efficient and Secure Modern CPUs"*
Advisor: Dr. Trevor E. Carlson

2014 - 2019 — Bachelor of Science in Computer Engineering
Sharif University of Technology, Tehran, Iran
Thesis: *"High Concurrency Latency Tolerant Register Files for GPUs"*
Advisor: Prof. Hamid Sarbazi-Azad

2009 - 2013 — Diploma in Physics and Mathematics Discipline
Shahid Beheshti High School, Birjand, Iran
Affiliated with the National Organization for the Development of Exceptional Talents (NODET)

Honors & Awards

Oct. 2023 — Recipient of SoC Research Incentive Award from School of Computing, NUS (S$ 2,500 award).
Jan. 2022 — Recipient of Student Travel Award from ASPLOS'22 conference.
Aug. 2021 — Recipient of Research Achievement Award from School of Computing, NUS.
Mar. 2020 — Invited talk and travel grant for the 2^{nd} Young Architect Workshop at ASPLOS'20, Switzerland.
Feb. 2019 — Recipient of President's Graduate Fellowship, the most prestigious doctoral fellowship at National University of Singapore (NUS).
Sep. 2014 — Ranked **164**th in Iranian National University Entrance Exam among more than 250,000 students.
2006/2009 — Recognized as talented student in entry exam of NODET for middle school and high school.

Research Experience

Aug. 2019 - Present — Graduate Research Assistant at National University of Singapore, Singapore
NUS Computer Architecture Group
Advisor: Prof. Trevor E. Carlson
My current research spans around HW/SW co-design to build secure and efficient general-purpose processors. My focus is on microarchitectural attacks, including speculation-based attacks and power analysis attacks.

Jul. 2016 - Jun. 2019 — Research Assistant at Sharif University of Technology, Tehran, Iran
High Performance Computer Architectures and Networks (HPCAN) Lab
Advisor: Prof. Hamid Sarbazi-Azad
Focus of my research has been on latency tolerant register files for GPUs through HW/SW cooperative register prefetching. I contributed to an ASPLOS'18 paper and an ACM TOCS paper. In collaboration with *Institute for Research in Fundamental Sciences (IPM)*, *EPFL*, and *ETH Zürich*.

Summer 2018 — Research Intern at National University of Singapore, Singapore
Advisor: Prof. Trevor E. Carlson
As a visiting research assistant, I investigated the potentials of out-of-order commit in modern processors and explored implementations (simulation+compiler) to enable efficient out-of-order commit.

In-Progress Work

Yun Chen*, **Ali Hajiabadi***, Romain Poussier, Andreas Diavastos, Shivam Bhasin, Trevor E. Carlson
Mitigating Power Attacks through Fine-Grained Instruction Reordering.
*Joint first-authors with equal contribution.
▶ *Proposing a novel criticality-aware and non-deterministic instruction scheduling for out-of-order processors to resist power analysis attacks.*
arXiv Paper

Peer-Reviewed Publications

DAC'24 | **Ali Hajiabadi**, Archit Agarwal, Andreas Diavastos, Trevor E. Carlson
LEVIOSO*: Efficient Compiler-Informed Secure Speculation.*
To appear in Proceedings of 61st ACM/IEEE Design Automation Conference (DAC 2024), June 2024.
Acceptance rate: 337/1465 = 23.0%
▶ *Efficient and comprehensive mitigation for speculative execution attacks through compiler-informed hints about true branch dependencies to restrict execution of speculative instructions only if necessary.*

DAC'24 | **Ali Hajiabadi**, Trevor E. Carlson
CONJURING*: Leaking Control Flow via Speculative Fetch Attacks.*
To appear in Proceedings of 61st ACM/IEEE Design Automation Conference (DAC 2024), June 2024.
Acceptance rate: 337/1465 = 23.0%
▶ *Proposing a new and practical variant of speculative fetch attacks that enables unprivileged attackers to leak control flow information of victims, without requiring priming a side channel.*

HPCA'24 | Yun Chen*, **Ali Hajiabadi***, Trevor E. Carlson
GADGETSPINNER*: A New Transient Execution Primitive using the Loop Stream Detector.*
Proceedings of 30th IEEE International Symposium on High-Performance Computer Architecture (HPCA 2024), March 2024. Acceptance rate: 75/410 = 18.3%
*Joint first-authors with equal contribution.
▶ *Analyzing and discovering vulnerabilities of the Loop Stream Detector (LSD) in Intel CPUs that enables cross-core transient execution attacks without requiring branch mistraning/poisoning.*
Paper | Artifact

HPCA'24 | Yun Chen, **Ali Hajiabadi**, Lingfeng Pei, Trevor E. Carlson
PREFETCHX*: Cross-Core Cache-Agnostic Prefetcher-Based Side-Channel Attacks.*
Proceedings of 30th IEEE International Symposium on High-Performance Computer Architecture (HPCA 2024), March 2024. Acceptance rate: 75/410 = 18.3%
▶ *Extensive reverse-engineering of an undocumented Intel prefetcher, called XPT (an LLC miss predictor) that enables cross-core cache-agnostic side and covert channels.*
Paper | Artifact

ICCAD'23 | Arash Pashrashid, **Ali Hajiabadi**, Trevor E. Carlson
HIDFIX*: Efficient Mitigation of Cache-based Spectre Attacks through Hidden Rollbacks.*
Proceedings of 42nd IEEE/ACM International Conference on Computer-Aided Design (ICCAD 2023), November 2023. Acceptance rate: 172/768 = 22.4%
▶ *Co-designing detection and mitigation to defend cache-based Spectre with no performance overhead; extensive study of existing detection/mitigation combinations and proposing attacks to bypass them.*
Paper

ICCAD'22 | Arash Pashrashid, **Ali Hajiabadi**, Trevor E. Carlson
Fast, Robust and Accurate Detection of Cache-based Spectre Attack Phases.
Proceedings of 41st IEEE/ACM International Conference on Computer-Aided Design (ICCAD 2022), November 2022. Acceptance rate: 132/586 = 22.5%
▶ *(1) Demonstrating different attacks bypassing ML-based detectors for Spectre attacks; (2) proposing an efficient, accurate, robust, and timely mechanism to detect cache-based Spectre attack phases.*
Paper | Github

ASPLOS'21 | **Ali Hajiabadi**, Andreas Diavastos, Trevor E. Carlson
NOREBA*: A Compiler-Informed Non-speculative Out-of-Order Commit Processor.*
Proceedings of 26th ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS 2021). April 2021. Acceptance rate: 75/398 = 18.8%
▶ *A hardware/software co-design that compiler informs the hardware about true branch dependencies enabling safe and non-speculative out-of-order commit of instructions improving efficiency.*
Paper | Extended Abstract | Short Slides | Short Talk | Slides | Full Talk

TOCS'21 | Mohammad Sadrosadati, Amirhossein Mirhosseini, **Ali Hajiabadi**, Seyed Borna Ehsani, Hajar Falahati, Hamid Sarbazi-Azad, Mario Drumond, Babak Falsafi, Rachata Ausavarungnirun, Onur Mutlu
Highly Concurrent Latency-tolerant Register Files for GPUs.
In ACM Transactions on Computer Systems (TOCS), 2021.
▶ *A hardware/software co-operative design for register prefetching in GPUs. The compiler constructs the prefetch sets and ensures minimal register bank conflicts via register renumbering.*
arXiv Paper

CGO'21 | Harish Patil, Alexander Isaev, Wim Heirman, Alen Sabu, **Ali Hajiabadi**, Trevor E. Carlson
ELFies: Executable Region Checkpoints for Performance Analysis and Simulation.
Proceedings of 19^{th} IEEE International Symposium on Code Generation and Optimization (CGO 2021), March 2021. Acceptance rate: 31/89 = 34.8%
▶ *Proposing a set of tools to generate checkpoint executables of the regions of interest of applications, called ELFies. ELFies run natively and can be used for detailed analysis in other tools and simulators.*
Paper | Github

Teaching Experience

▶ **National University of Singapore, Singapore**

Spring 2020 and Spring 2021 — **Teaching Assistant**, Tutorial Instructor
Course: CS2106 Introduction to Operating Systems
Instructor: Prof. Djordje Jevdjic

▶ **Sharif University of Technology, Tehran, Iran**

Spring 2017 — **Teaching Assistant**, Assignments/Projects Assistant
Course: CE323 Computer Architecture
Instructor: Prof. Hamid Sarbazi-Azad

Fall 2017 and Fall 2018 — **Teaching Assistant**, Tutorial Instructor, Assignments/Projects Assistant
Course: CE453 Real-Time Systems
Instructor: Prof. Amirhossein Jahangir

Services

Nov. 2023 — **Heavy Shadow PC member** at 19^{th} European Conference on Computer Systems (EuroSys 2024).
Oct. 2022 — **Shadow PC member** at 18^{th} European Conference on Computer Systems (EuroSys 2023).
Mar. 2022 — **Mentor in the Meet-a-Senior-Student program** at 27^{th} International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS 2022), Lausanne.
Jun. 2021 — **Student Volunteer** at 42^{nd} International Conference on Programming Language Design and Implementation (PLDI 2021), Virtual.

Research Mentoring

2021 - Present — Arash Pashrashid, PhD Student at NUS Advised by Trevor E. Carlson
2020 - 2024 — Yun Chen, PhD Student at NUS Advised by Trevor E. Carlson
2021 - 2023 — Archit Agarwal, Research Assistant at NUS
2020 - 2021 — Vernon Pang, Undergraduate Student at NUS

Talks

Mar. 2024 — **Will CPUs Be Free of Spectre? Dark Side and Light Side of the Battle**
ETH Zurich, COMSEC Group, Zurich, Switzerland.

Mar. 2024 — GadgetSpinner: **A New Transient Execution Primitive using the Loop Stream Detector**
International Symposium on High-Performance Computer Architecture (HPCA 2024), Edinburgh, Scotland, UK.

Aug. 2021 — Noreba: **A Compiler-Informed Non-speculative Out-of-Order Commit Processor**
Computing Research Week, School of Computing (NUS), Virtual.

Apr. 2021 — Noreba: **A Compiler-Informed Non-speculative Out-of-Order Commit Processor**
International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS 2021), Virtual.

Feb. 2021 — **Accelerating HPC applications with Out-of-Order Commit Processors**
Free and Open source Software Developers' European Meeting (FOSDEM 2021), HPC, Big Data, and Data Science track, Virtual.

Mar. 2020 — **Speculation-Free Out-of-Order Commit**
2^{nd} Young Architect Workshop at the 25^{th} International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS 2020), Virtual.

Skills

Programming Languages:	C, C++, Python, bash, and familiar with Java, Matlab, Scala
Instruction Set Architectures:	x86, Arm, RISC-V
Scientific Tools:	LLVM Compiler Infrastructure, gem5 Simulator, Sniper Simulator, Intel Pin, DynamoRIO
Typesetting:	LaTeX, Microsoft Word