

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

- 2019 - 2024 Doctor of Philosophy in Computer Science
National University of Singapore (NUS), Singapore
Thesis: *"Building Efficient and Secure Processors thorough Hardware/Software Co-design"*
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 (\$\$ 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 2nd 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 164th 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
<i>LEVIOSO: Efficient Compiler-Informed Secure Speculation.</i>
To appear in Proceedings of 61 st ACM/IEEE Design Automation Conference (DAC 2024), June 2024. Acceptance rate: 337/1465 = 23.0%
► <i>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.</i> |
| DAC'24 | Ali Hajiabadi , Trevor E. Carlson
<i>CONJURING: Leaking Control Flow via Speculative Fetch Attacks.</i>
To appear in Proceedings of 61 st ACM/IEEE Design Automation Conference (DAC 2024), June 2024. Acceptance rate: 337/1465 = 23.0%
► <i>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.</i> |
| HPCA'24 | Yun Chen*, Ali Hajiabadi* , Trevor E. Carlson
<i>GADGETSPINNER: A New Transient Execution Primitive using the Loop Stream Detector.</i>
Proceedings of 30 th IEEE International Symposium on High-Performance Computer Architecture (HPCA 2024), March 2024. Acceptance rate: 75/410 = 18.3%
*Joint first-authors with equal contribution.
► <i>Analyzing and discovering vulnerabilities of the Loop Stream Detector (LSD) in Intel CPUs that enables cross-core transient execution attacks without requiring branch mistraining/poisoning.</i>
Paper Artifact |
| HPCA'24 | Yun Chen, Ali Hajiabadi , Lingfeng Pei, Trevor E. Carlson
<i>PREFETCHX: Cross-Core Cache-Agnostic Prefetcher-Based Side-Channel Attacks.</i>
Proceedings of 30 th IEEE International Symposium on High-Performance Computer Architecture (HPCA 2024), March 2024. Acceptance rate: 75/410 = 18.3%
► <i>Extensive reverse-engineering of an undocumented Intel prefetcher, called XPT (an LLC miss predictor) that enables cross-core cache-agnostic side and covert channels.</i>
Paper Artifact |
| ICCAD'23 | Arash Pashrashid, Ali Hajiabadi , Trevor E. Carlson
<i>HIDFix: Efficient Mitigation of Cache-based Spectre Attacks through Hidden Rollbacks.</i>
Proceedings of 42 nd IEEE/ACM International Conference on Computer-Aided Design (ICCAD 2023), November 2023. Acceptance rate: 172/768 = 22.4%
► <i>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.</i>
Paper |
| ICCAD'22 | Arash Pashrashid, Ali Hajiabadi , Trevor E. Carlson
<i>Fast, Robust and Accurate Detection of Cache-based Spectre Attack Phases.</i>
Proceedings of 41 st IEEE/ACM International Conference on Computer-Aided Design (ICCAD 2022), November 2022. Acceptance rate: 132/586 = 22.5%
► <i>(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.</i>
Paper Github |
| ASPLOS'21 | Ali Hajiabadi , Andreas Diavastos, Trevor E. Carlson
<i>NOREBA: A Compiler-Informed Non-speculative Out-of-Order Commit Processor.</i>
Proceedings of 26 th ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS 2021). April 2021. Acceptance rate: 75/398 = 18.8%
► <i>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.</i>
Paper Extended Abstract Short Slides Short Talk Slides Full Talk |

TOCS'21	<p>Mohammad Sadrosadati, Amirhossein Mirhosseini, Ali Hajiabadi, Seyed Borna Ehsani, Hajar Fala-hati, Hamid Sarbazi-Azad, Mario Drumond, Babak Falsafi, Rachata Ausavarungnirun, Onur Mutlu <i>Highly Concurrent Latency-tolerant Register Files for GPUs</i>. In ACM Transactions on Computer Systems (TOCS), 2021. ► <i>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.</i> arXiv Paper</p>
CGO'21	<p>Harish Patil, Alexander Isaev, Wim Heirman, Alen Sabu, Ali Hajiabadi, Trevor E. Carlson <i>ELFies: Executable Region Checkpoints for Performance Analysis and Simulation</i>. Proceedings of 19th IEEE International Symposium on Code Generation and Optimization (CGO 2021), March 2021. Acceptance rate: 31/89 = 34.8% ► <i>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.</i> Paper Github</p>

TEACHING EXPERIENCE

► National University of Singapore, Singapore

SPRING 2020 and SPRING 2021	<p>Teaching Assistant, Tutorial Instructor Course: CS2106 Introduction to Operating Systems Instructor: Prof. Djordje Jevdjic</p>
--------------------------------	--

► Sharif University of Technology, Tehran, Iran

SPRING 2017	<p>Teaching Assistant, Assignments/Projects Assistant Course: CE323 Computer Architecture Instructor: Prof. Hamid Sarbazi-Azad</p>
FALL 2017 and FALL 2018	<p>Teaching Assistant, Tutorial Instructor, Assignments/Projects Assistant Course: CE453 Real-Time Systems Instructor: Prof. Amirhossein Jahangir</p>

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

2020 - 2024	Yun Chen, PhD Student at NUS Advised by Trevor E. Carlson
2021 - 2023	Arash Pashrashid, 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	<p>Will CPUs Be Free of Spectre? Dark Side and Light Side of the Battle ETH Zurich, COMSEC Group, Zurich, Switzerland.</p>
MAR. 2024	<p>GADGETSPINNER: A New Transient Execution Primitive using the Loop Stream Detector International Symposium on High-Performance Computer Architecture (HPCA 2024), Edinburgh, Scotland, UK.</p>
AUG. 2021	<p>NOREBA: A Compiler-Informed Non-speculative Out-of-Order Commit Processor Computing Research Week, School of Computing (NUS), Virtual.</p>
APR. 2021	<p>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.</p>
FEB. 2021	<p>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.</p>
MAR. 2020	<p>Speculation-Free Out-of-Order Commit 2nd Young Architect Workshop at the 25th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS 2020), Virtual.</p>

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