Ashish Venkat

Office: Rice 312, Dept. of Computer Science
University Virginia
PO Box 400740
Charlottesville, VA – 22904
Phone: (434) 243-5219
Fax: (434) 982-2214
venkat@virginia.edu
http://www.cs.virginia.edu/venkat

Professional Appointments

University of Virginia **Aug 2018-Present**
Assistant Professor, Department of Computer Science

University of California, San Diego **Apr 2011-Aug 2018**
Research Assistant, Department of Computer Science

IBM Research Labs, Haifa, Israel **Aug 2016-Dec 2016**
Research Intern, Cloud Platforms Division

Microsoft Research, Redmond, WA **Mar 2015-Jun 2015**
Research Intern, MSR Technologies Lab

Intel Corporation, Santa Clara, CA **Jun 2012-Sep 2012**
Graduate Technical Intern, Processor Binary Translation Group

Amazon.com, Inc., Seattle, WA **Jun 2011-Sep 2011**
Software Development Intern, Retail Systems Group

Brocade Communications, Bangalore, India **May 2009-Aug 2010**
Software Engineer, Storage Encryption Group

Freescale Semiconductor, Bangalore, India **Jul 2008-May 2009**
Software Engineer, Symbian Middleware Group

Education

PhD., Computer Science **Spring 2018**
Thesis: Breaking the ISA Barrier in Modern Computing.
Advisor: Prof. Dean Tullsen
University of California, San Diego

M.S., Computer Science **Spring 2014**
University of California, San Diego

B.Eng., Computer Science **Spring 2008**
National Institute of Engineering, Mysore, India

Honors and Awards Received

NSF CAREER Award
The Faculty Early Career Development (CAREER) Program is a Foundation-wide activity that offers the National Science Foundation's most prestigious awards in support of early-career faculty who have the potential to serve as academic role models in research and education and to lead advances in the mission of their department or organization.

ISCA Prolific Author of the Decade 2013-2022
List of prolific authors at ISCA for the decade 2013-2022, put together as part of the retrospective on Fifty Years of ISCA!

DATE 2023 Best Paper Award Nomination
Best Paper Nomination at a top VLSI Design conference with an acceptance rate of 25%.

IEEE TCAD Hardware and Embedded Security Top Pick 2021
ISCA 2020 paper on a transparent memory safety defense selected across all top architecture, security, and VLSI design conferences (DAC, DATE, ICCAD, HOST, VLSI Design, CHES, ETS, VTS, ITC, IEEE S&P, Euro S&P, USENIX Security, ASIA CCS, NDSS, ISCA, HASP, MICRO, ASPLOS, HPCA, ACSAC, and ACM CCS) held in the six years between the years 2015-2020, for publication in a Special Issue of IEEE TCAD.

IEEE TCAD Hardware and Embedded Security Top Pick 2020
ASPLOS 2019 paper on Spectre mitigation selected across all top architecture, security, and VLSI design conferences (DAC, DATE, ICCAD, HOST, VLSI Design, CHES, ETS, VTS, ITC, IEEE S&P, Euro S&P, USENIX Security, ASIA CCS, NDSS, ISCA, HASP, MICRO, ASPLOS, HPCA, ACSAC, and ACM CCS) held in the six years between the years 2014-2019, for publication in a Special Issue of IEEE TCAD.

IEEE Micro Top Pick 2019
ISCA 2018 paper on on-demand microcode customization selected across all top architecture conferences (ISCA, ASPLOS, MICRO, HPCA) held in 2018, for publication in a Special Issue of IEEE Micro.

HPCA 2019 Best Paper Award Runner-Up
Best Paper Runner-Up at a top Computer Architecture conference with an acceptance rate of 21%.

ACM SIGARCH Student Scholarship
One of the seven SIGARCH student scholars to attend the *ACM Turing Centenary Celebrations.*

TEQIP Best Undergraduate Student Project
Awarded by the Technical Education Quality Improvement Programme (TEQIP) foundation, Government of India.

Significant Press and Coverage

Research on micro-op cache vulnerability published at ISCA 2021 was covered widely by multiple international technology news and mainstream media outlets in **May 2021**.

Research on Composite-ISA Cores published at HPCA 2019 was covered on Coreteks, in the **Aug 2020** article "AMD Master Plan Pt. 2 -- Heterogeneous Revolution".

Research on the Packet Chasing Attack that exploits a new vulnerability in Intel processors was listed by NIST in **Sep 2019** as a medium severity vulnerability under CVE-2019-11184.

Publications

Core Fuzzing - A Versatile Platform for Security Verification
Alenkruth Krishnan Murali, **Ashish Venkat**,
In *Semiconductor Research Corporation's Annual Technical Conference **(SRC TECHCON)***, September, 2023.
Industry Conference – Acceptance Rate not available.

Hardware Trojan Threats in eNVM Neuromorphic Devices
Lingxi Wu, Rahul Sreekumar, Rasool Sharifi, Kevin Skadron, Mircea Stan, **Ashish Venkat**,
In *Proceedings of the 26th Design, Automation and Test in Europe Conference* **(DATE),** April, 2023.
Acceptance rate: 25%
Nominated for Best Paper Award!

Speculative Code Compaction: Eliminating Dead Code via Speculative Microcode Transformations
Logan Moody, Wei Qi, Abdolrasoul Sharifi, Layne Berry, Joey Rudek, Jayesh Gaur, Jeff Parkhurst, Sreenivas Subramoney, Kevin Skadron, **Ashish Venkat**,
In *Proceedings of the 55th ACM/IEEE International Symposium on Microarchitecture **(MICRO)***, October, 2022.
Acceptance Rate: 23%

ProxyVM: A Scalable and Retargetable Compiler Framework for Privacy-Aware Proxy Workload Generation
Xida Ren, Alif Ahmed, Yizhou Wei, Kevin Skadron, **Ashish Venkat**,
In *Semiconductor Research Corporation's Annual Technical Conference **(SRC TECHCON)***, September, 2022.
Industry Conference – Acceptance Rate not available.

DRAM-CAM: General-Purpose Bit-Serial Exact Pattern Matching
Lingxi Wu, Rasool Sharifi, **Ashish Venkat**, Kevin Skadron,
In *IEEE Computer Architecture Letters **(IEEE CAL)***, Issue 2, Jul-Dec, 2022.
Impact Factor: 2.118

SecSMT: Securing SMT Processors against Contention-Based Covert Channels
Mohammadkazem Taram, Xida Ren, **Ashish Venkat**, Dean M. Tullsen,
In *Proceedings of the 31st USENIX Security Symposium **(USENIX Security)***, Aug, 2022.
Acceptance Rate: 17%

I See Dead µops: Leaking Secrets via Intel/AMD µop Caches
Xida Ren, Logan Moody, Mohammadkazem Taram, Matthew Jordan, Dean M. Tullsen, **Ashish Venkat**.
In *Proceedings of the 48th International Symposium on Computer Architecture **(ISCA)***, June 2021.
Acceptance Rate: 18%

Sieve: A Scalable In-Situ DRAM-based Accelerator for Massively Parallel K-mer Matching
Lingxi Wu, Rasool Sharifi, Marzieh Lenjani, Kevin Skadron, and **Ashish Venkat**.
In *Proceedings of the 48th International Symposium on Computer Architecture **(ISCA)***, June 2021.
Acceptance Rate: 18%

CHEx86: Context-Sensitive Enforcement of Memory Safety via Microcode-Enabled Capabilities.
Rasool Sharifi and **Ashish Venkat**.
In *Proceedings of the 47th International Symposium on Computer Architecture **(ISCA)***, June 2020.
Acceptance Rate: 18%
Selected for IEEE TCAD Hardware and Embedded Security Top Picks, 2021!

Mitigating Speculative Execution Attacks via Context-Sensitive Fencing
Mohammadkazem Taram, **Ashish Venkat**, Dean M. Tullsen,
In HW-Security TopPicks issue of IEEE Design & Test, February 2021
Impact Factor: 1.77

Agon: A Scalable Competitive Scheduler for Large Heterogeneous Systems.
Andreas Prodromou, **Ashish Venkat**, Dean M. Tullsen.
arXiV preprint, 2021

Packet Chasing: Observing Network Packets over a Cache Side-Channel.
Mohammadkazem Taram, **Ashish Venkat**, and Dean M. Tullsen.
In *Proceedings of the 47th International Symposium on Computer Architecture* ***(ISCA)***, June 2020.
Acceptance Rate: 18%

Platform-Agnostic Learning-Based Scheduling
Andreas Prodromou, **Ashish Venkat**, and Dean M. Tullsen.
In *Proceedings of the 19th International Conference on Embedded Computer Systems: Architectures, Modeling, and Simulation (SAMOS),* July, 2019.
Acceptance Rate: 38%

Context-Sensitive Decoding: On-Demand Microcode Customization for Security and Energy Management
Mohammadkazem Taram, **Ashish Venkat**, Dean M. Tullsen.
In ***IEEE Micro***, *Special Issue on the Top Picks from the Computer Architecture Conferences,* May 2019.
Impact Factor: 2.57
Special Issue Acceptance Rate: 9%,
Theme Article!

Context-Sensitive Fencing: Securing Speculative Execution via Microcode Customization.
Mohammadkazem Taram, **Ashish Venkat**, and Dean M. Tullsen.
In *Proceedings of the 24th International Conference on Architectural Support for Programming Languages and Operating Systems* ***(ASPLOS)***, April 2019.
Acceptance Rate: 21%.
Selected for IEEE TCAD Hardware and Embedded Security Top Picks, 2020!

Fast and Efficient Deployment of Security Defenses Via Context Sensitive Decoding
Mohammadkazem Taram, Dean M. Tullsen, **Ashish Venkat**, Houman Homayoun, and Sai Manoj PD.
In *Proceedings of the 44th Government Microcircuit Applications and Critical Technology Conference (GOMACTech),* March 2019.
Government Conference – Acceptance Rate not available.

Composite-ISA Cores: Enabling Multi-ISA Heterogeneity using a Single ISA.
Ashish Venkat, Harsha Basavaraj, and Dean M. Tullsen.
In *Proceedings of the 25th International Symposium High Performance Computer Architecture* ***(HPCA)***, February 2019
Acceptance Rate: 21%.
Best Paper Award Runner-Up!

Deciphering Predictive Schedulers for Heterogeneous-ISA Architectures
Andreas Prodromou, **Ashish Venkat**, Dean M. Tullsen.
In *Proceedings of the 10th International Workshop on Programming Models and Applications for Multicores and Manycores (PMAM),* February, 2019.
Acceptance Rate: 53%

Breaking the ISA Barrier in Modern Computing
Ashish Venkat
Ph.D. Dissertation, UC San Diego, August 2018

Mobilizing the Micro-Ops: Exploiting Context-Sensitive Decoding for Security and Energy Efficiency.
Mohammadkazem Taram, **Ashish Venkat**, and Dean M. Tullsen.
In *Proceedings of the 45th International Symposium on Computer Architecture **(ISCA)***, June 2018.
Acceptance Rate: 17%.
Selected for IEEE Micro Top Picks, 2019!

Reliability-Aware Data Placement for Heterogeneous Memory Architecture.
Manish Gupta, Vilas Sridharan, David Roberts, Andreas Prodromou, **Ashish Venkat**, Dean M. Tullsen, and Rajesh Gupta.
In *Proceedings of the 24th International Symposium on High Performance Computer Architecture **(HPCA)***, February 2018.
Acceptance Rate: 21%

HIPStR: Heterogeneous-ISA Program State Relocation.
Ashish Venkat, Sriskanda Shamasunder, Hovav Shacham, and Dean M. Tullsen.
In *Proceedings of the 21st International Conference on Architectural Support for Programming Languages and Operating Systems **(ASPLOS)***, April 2016.
Acceptance Rate: 22%

Harnessing ISA Diversity: Design of a Heterogeneous-ISA Chip Multiprocessor.
Ashish Venkat and Dean M. Tullsen.
In *Proceedings of the 41st International Symposium on Computer Architecture **(ISCA)***, June 2014.
Acceptance Rate: 18%

Execution Migration in a Heterogeneous-ISA Chip Multiprocessor.
Matthew DeVuyst, **Ashish Venkat**, and Dean M. Tullsen.
In *Proceesings of the 17th International Conference on Architectural Support for Programming Languages and Operating Systems **(ASPLOS)***, March, 2012.
Acceptance Rate: 21%

Grants and Contracts

NSF CAREER *Oct 2023 – Sep 2028*
Enabling Robust and Adaptive Architectures through a Decoupled Security-Centric Hardware/Software Stack
Role: Principal Investigator.
Funding Amount (total): $509,500

NSF PPoSS *Oct 2022 – Sep 2027*
Co-designing Hardware, Software, and Algorithms to Enable Extreme-Scale Machine Learning Systems
Role: Co-Principal Investigator.
Funding Amount (total): $3,000,000

NSF CCRI *Oct 2022 – Sep 2025*
A Scalable Hardware and Software Environment Enabling Secure Multi-party Learning
Role: Co-Principal Investigator.
Funding Amount (total): $1,120,000

SRC CADT *Jan 2022 – Dec 2024*
A Scalable and Re-Targetable Compiler Framework for Privacy-Preserving Machine Learning
Role: Principal Investigator.
Funding Amount: $297,000

NSF/Intel Foundational Microarchitecture Research (FoMR) *Oct 2019 – Sep 2023*
Speculative Super-optimization: Boosting Performance via Speculation-Driven Dynamic Binary Optimization
Role: Principal Investigator.
Funding Amount: $416,000

NSF CRII: SaTC *Mar 2019 – Feb 2022*
Mitigating Software-Based Microarchitectural Attacks via Secure Microcode Customization
Role: Principal Investigator
Funding Amount: $174,996

DARPA MTO: SSITH *Dec 2018 – Mar 2021*
Mobilizing the Micro-Ops: Securing Processor Architectures via Context-Sensitive Decoding
Role: Principal Investigator (Sub).
Funding Amount: $1,101,217

NSF CCF: SHF *Feb 2020 – Jan 2021*
Student Travel Grant for the 26th IEEE International Symposium on High Performance Computer Architecture (HPCA 2020)
Role: Principal Investigator
Funding Amount: $20,000

Patents

Binary Translation-Driven Program State Relocation.
Ashish Venkat, Arvind Krishnaswamy, Yamada Koichi, and Rajan Palanivel.
In *United States Patent Grant US009135435 B2*, September, 2015.

Graduate Students Research Advising

Lingxi Wu (Spring 2020-Present, co-advised by Kevin Skadron)
Milestones: Qualifying Exam Defense Completed.

Xida Ren (Fall 2019-Present)
Milestones: Qualifying Exam Defense Completed.

Logan Moody (Fall 2020-Present)
Milestones: Qualifying Exam Proposal Completed.

Arnabjyoti Kalita (Fall 2022-Present)

Alenkruth Krishnan Murali (Fall 2022-Present)
Milestones: Qualifying Exam Completed.

Saket Upadhyay (Fall 2022-Present)

Yilong Yang (Fall 2022-Present)

Uday Kiran (Fall 2022-Present, Master's student)

Undergraduate Students Research Advising

Edward Lue (Fall 2022-Present)

Dhruv Pandya (Fall 2022-Present)

Research Advisees Graduated

Virginia Layne Berry (Summer 2019-Fall 2020)
Placement: Ph.D. at University of Texas, Austin
Significant Achievements: **CRA Outstanding Undergraduate Researcher Award Honorable Mention**

Joey Rudek (Summer 2020-Spring 2021)
Placement: Ph.D. at University of California, San Diego

Muhammad Abdullah (Fall 2021-Spring 2022)
Placement: Capital One

AmirMohammad Deilami (Remote mentorship, Fall 2020-Spring 2022)
Placement: MS at Simon Fraser University

Wei Qi (Master's student, Fall 2021-Spring 2022)
Placement: Ph.D. at Università Bocconi

Conner Ward (Master's student, Fall 2021-Fall 2022)

Invited Talks

Speculative Code Compaction: Eliminating Dead Code via Speculative Microcode Transformations — *Sep 2022*
Intel Labs Worldwide (Virtual Tech Talk)

Mechanism Design for Improving Hardware Security — *Aug 2022*
Invited Participant at the CCC Visioning Workshop

Speculative Super-optimization: Boosting Performance via Speculation-Driven Dynamic Binary Optimization — *Oct 2021*
Intel Labs Worldwide (Virtual Tech Talk)

I See Dead µops: Leaking Secrets via Intel/AMD µop Caches — *Apr 2021*
Intel Labs Worldwide (Virtual Tech Talk)

Speculative Super-optimization: Boosting Performance via Speculation-Driven Dynamic Binary Optimization — *Jun 2020*
Intel Labs Worldwide (Virtual Tech Talk)

Fast and Efficient Deployment of Security Defenses via Microcode Customization. — *Nov 2019*
University of Cambridge, UK.

Breaking the ISA Barrier in Modern Computing. — *Mar 2019*
North Carolina State University, Raleigh.

Composite-ISA Cores: Enabling Multi-ISA Heterogeneity using a Single ISA. — *Feb 2019*
HPCA 2019, Best Paper Session.

Mobilizing the Micro-Ops: Exploiting Context-Sensitive Decoding for Performance and Security. — *Aug 2018*
Intel Labs, Santa Clara.

Breaking the ISA Barrier in Modern Computing. *May 2018*
Northeastern University, Boston.

Exploiting Multi-ISA Architectures for Security and Efficiency. *April 2017*
Qualcomm, San Diego.

Breaking the ISA Barrier in Modern Computing. *Nov 2016*
Intel Research Lab, Haifa, Israel.

Breaking the ISA Barrier in Modern Computing. *Nov 2016*
Technion, Israel.

HIPStR: Smashing ROP Gadgets via Cross-ISA Process Migration. *Oct 2016*
IBM Haifa Research Lab, Israel.

Breaking the ISA Barrier in Modern Computing. *Aug 2016*
IBM Haifa Research Lab, Israel.

HIPStR: Heterogeneous-ISA Program State Relocation. *Apr 2016*
ASPLOS 2016, Atlanta.

Heterogeneous-ISA Chip Multiprocessors. *Oct 2014*
AMD Research, Sunnyvale.

Harnessing ISA Diversity: Design of a Heterogeneous-ISA Chip Multiprocessor. *Jun 2014*
ISCA 2014, Minneapolis.

Execution Migration in a Heterogeneous-ISA Chip Multiprocessor. *Mar 2012*
ASPLOS 2012, London, UK.

Teaching Experience

Assistant Professor, University of Virginia
CS 6354, Graduate Computer Architecture (Fall 2019, Fall 2021, Fall 2022)
CS 3330, Undergraduate Computer Architecture (Spring 2019, Spring 2020, Spring 2021, Spring 2022)
CS 6501/4501, Graduate/Undergraduate Hardware Security (Fall 2018, Fall 2020, Spring 2023)

Guest Lecturer
CS 6190, Computer Science Perspectives (Fall 2018, Fall 2019, Fall 2020)
CS 6354, Graduate Computer Architecture (Fall 2018)
CSE 141, Introduction to Computer Architecture at UC San Diego (Winter 2015, Winter 2017).

Internal Departmental/University Service

SEAS Computer Engineering Strategic Committee (2022-2023)

CS Faculty Search Committee, Systems Area Coordinator (2021-2022)

SEAS Computer Engineering Qualification Exam Committee, Chair (2020-2021)

SEAS Computer Engineering Graduate Program Committee, Member (2020-2021)

CS Faculty Search Committee, Member (2018-2019)

Computing Systems Committee, Member (2019-2023)

Thesis Defense Committees
Alif Ahmed, Spring 2023
Vaibhav Verma, Spring 2022
Marzieh Lenjani, Fall 2020
Reza Rahimi, Fall 2020
Chunkun Bo, Fall 2019
Elaheh Sadredini, Spring 2019 (Chair)

Ph.D. Qualifying Examination Committees
Akhil Shekar, Spring 2023
Alif Ahmed, Spring 2021
Alan Wang, Summer 2020
Yipei Song, Summer 2020
Jerry Xing, Summer 2020
Aaron Kinfe, Summer 2020
Qi Liu, Summer 2020
Yujia Mu, Summer 2020
Alif Ahmed, Summer 2020
Lingxi Wu, Spring 2020 (Chair)
Marzieh Lenjani, Fall 2019

External Professional Service

Organizing Committee
Student Travel Chair, IEEE/ACM International Symposium on Microarchitecture (MICRO), 2020, 2021, 2022
Student Travel Chair, IEEE International Symposium on High Performance Computer Architecture (HPCA), 2020

Program Committee
IEEE Micro Top Picks, 2021
ACM/IEEE International Symposium on Computer Architecture (ISCA), 2019, 2020, 2021, 2022, 2023
IEEE/ACM International Symposium on Microarchitecture (MICRO), 2022, 2023
ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS), 2023, 2024
IEEE International Parallel & Distributed Processing Symposium (IPDPS), 2021
IEEE International Symposium on High Performance Computer Architecture (HPCA), 2020, 2024
IEEE International Conference on Computer Design (ICCD), 2019, 2021, 2022
ACM International Workshop on Hardware and Architectural Support for Security and Privacy, 2020, 2021, 2022
IEEE International Symposium on Secure and Private Execution Environment Design (SEED), 2021, 2022
ACM Student Research Competition (SRC) in conjunction with ASPLOS, 2019
Young Architect Workshop (YArch) in conjunction with HPCA/ASPLOS, 2019, 2020

NSF Panel
Spring 2020, Spring 2022, Spring 2023

External Review Committee
IEEE/ACM International Symposium on Microarchitecture (MICRO), 2020, 2021
ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS), 2020
IEEE International Symposium on Quality Electronic Design (ISQED), 2012

Journal Peer Review
ACM Transactions on Architecture and Code Optimization, 2021
IEEE Transactions on Computers, 2020, 2022
IEEE Micro, Jul-Aug 2015, Jul-Aug 2019, Sep-Oct 2019
IEEE Computer Architecture Letters, 2015, 2019, 2021, 2022
IEEE Transactions on Parallel and Distributed Systems (TPDS), 2017, 2018
IEEE Concurrency and Computation, Practice and Experience (CCPE), 2019
Journal of Systems and Software (JSS), 2015

References

Made available upon request.