Deeksha Dangwal

deekshadangwal@gmail.com | GScholar | deekshadangwal.com

Research Interests

Computer Systems Research, Security and Privacy, MLSys

I am a computer architect working at the intersection of hardware-software co-design, privacy, and AI systems. As AI systems grow more complex and pervasive, privacy and safety cannot be an afterthought, it demands the same rigor as performance. My work spans formal privacy models, secure and homomorphic computation, architecture modeling and agile hardware tooling, and privacy-preserving computer vision for augmented reality, with publications in top venues including **ISCA, ASPLOS, PLDI, FPL, and TMLR**.

My SoK on hardware-software-security codesign was cited in the **US National Strategy on Microelectronics Research**. I am a **Rising Stars in EECS** alumna, and trace wringing was recognized as an **IEEE Micro Top Pick**.

Education

Doctor of Philosophy, Computer Science **03/2022**
University of California, Santa Barbara
Thesis: **"A System-level Framework for Privacy"**
Advised by **Prof. Timothy Sherwood**

Master of Science, Electrical and Computer Engineering **09/2016**
University of California, Santa Barbara

Bachelor of Engineering, Instrumentation and Electronics **05/2014**
Ramaiah Institute of Technology, Bangalore, India

Awards and Honors

Our paper, "SoK: Opportunities for Software-Hardware-Security Codesign for Next-Generation Secure Computing" (HASP'20) appears in the *United States National Strategy on Microelectronics Research* **2024**

Runner-up, UCSB Grad Slam Competition **2021**

Rising Stars in EECS, UC Berkeley **2020**

IEEE Micro Top Pick, Trace Wringing for Program Trace Privacy **2020**

Fiona and Michael Goodchild Graduate Mentoring Award, UCSB Graduate Division **2020**

Outstanding Graduate Student Award, Department of Computer Science, UCSB **2020**

Second Place, NXP Embedded Design Challenge **2015**

Experience

Consultant, *Office of the CTO, The Allen Institute, Seattle, WA* **07/2025 - 09/2025**

- Neural tracing: Co-developed neural tracing for mechanistic interpretability of LLMs and bio-foundation models. Submitted patent application *"Model Optimization and Data Analysis Using Neural Traces"* (P2)

Research Scientist, *Reality Labs Research, Meta* **01/2022 - 04/2025**

- Distributed Intelligence and On-device AI: Prototyped gesture interaction for smart glasses (data collection, model training, compression, and demo) on SoC with custom and off-the-shelf accelerators. Through HW/SW codesign and energy-aware scheduling, my pipeline improved latency and power (by 93% & 74%)
- Performance and Power Modeling: Built Python-based system-level power and performance modeling tool for Project Aria and other wearable devices using discrete-event simulation. The system latency and power was calibrated against measurments on prototype devices running machine perception pipelines: eye tracking, hand and gesture tracking, localization and mapping.
- Hardware-Software-Security Codesign in Extended Reality : Developed security and privacy research program for mixed and augmented reality, establishing threat models for codec avatars, privately crowdsourced data collection for world modeling, and other extended reality applications; published in HASP 2020 (W3), PLDI 2020 (C5), BMVC 2021 (C4), TMLR 2025 (J4, A1)

Graduate Student Researcher, *ArchLab, UC Santa Barbara* **06/2015 - 12/2021**

- Trace Wringing : Developed trace wringing for safer program behavior sharing, achieving privacy through lossy compression and information flow tracking with verifiable leakage bounds; published in ASPLOS 2019, SEED 2020 (C3, C6) and recognized as IEEE Micro Top Pick (J2)
- Agile Hardware Development with PyRTL Co-developed PyRTL, a Pythonic hardware development toolkit enabling rapid prototyping and agile hardware design; published in FPL 2017 (C1) and IEEE Micro 2020 (J3)
- Architecture Modeling with Charm: Worked on Charm, a domain-specific language for high-level architecture modeling; published in ISCA 2018, JETC 2019 (C2, J1)
- OpenTPU: Led development in PyRTL, creating open-source tensor processing unit implementation

Research Scientist Intern, *Reality Labs Research, Meta* **06/2020 - 01/2021**

- Implemented novel reverse engineering attack on local feature descriptors, surpassing state-of-the-art reconstruction accuracy for user image recovery
- Established first privacy threat model for computer vision feature descriptor sharing in AR systems
- Developed privacy-preserving mitigation techniques and studied effects on downstream vision system performance; published in BMVC 2021 (C3)

Research Intern, *Microsoft Research* **06/2018 - 09/2018**

- Implemented parameterizable architecture-aware machine learning graph primitives for custom hardware instructions on Brainwave Neural Processing Unit
- Built tools for automatic lifting of hardware instructions to high-level graph primitives while maintaining hardware fidelity
- Designed computational pipeline for NPU model decompilation with accuracy verification; resulted in patent (P1)

Research Assistant, *Oracle Labs* **06/2016 - 09/2016**

- Established testing environment for measuring throughput of RAPID Data Processing Unit (DPU) network, a bandwidth-optimized big data computation architecture
- Implemented network congestion tests for best/worst case traffic using hardware RPC acceleration mechanisms

Publications

[C]=Conference, [J]=Journal or Magazine, [W]=Workshop

W4 **The Need for Computational Pluralism**
D. Dangwal, A. Rajagopal. *Workshop on Ethical Systems and Architecture Design **(HotEthics)**, 2026*

J4 **Unlocking Visual Secrets: Inverting Features with Diffusion Priors for Image Reconstruction**
S. Q. Zhang, Z. Li, C. Guo, S. Mahloujifar, D. Dangwal, E. Suh, B. D. Salvo, C. Liu. *Transactions on Machine Learning Research **(TMLR)**, 2025*

C6 **Context-Aware Privacy-Optimizing Address Tracing**
D. Dangwal, Z. Zhang, J. Crandall, T. Sherwood. *IEEE International Symposium on Secure and Private Execution Environment Design **(SEED)**, 2021*

C5 **Porcupine: A Synthesizing Compiler for Vectorized Homomorphic Encryption**
M. Cowan, D. Dangwal, A. Alaghi, C. Trippel, V. T. Lee, B. Reagen. *Programming Language Design and Implementation **(PLDI)**, 2021*

C4 **Mitigating Reverse Engineering Attacks on Local Feature Descriptors**
D. Dangwal, V. T. Lee, H. J. Kim, T. Shen, M. Cowan, R. Shah, C. Trippel, B. Reagen, T. Sherwood, V. Balntas, A. Alaghi, E. Ilg. *British Machine Vision Conference **(BMVC)**, 2021*

W3 **SoK: Opportunities for Software-Hardware-Security Codesign for Next Generation Secure Computing**
D. Dangwal, M. Cowan, A. Alaghi, V. Lee, B. Reagen, C. Trippel. *Hardware and Architectural Support for Security and Privacy **(HASP)**, 2020*

J3 **Agile Hardware Development and Instrumentation with PyRTL**
D. Dangwal, G. Tzimpragos, T. Sherwood. *IEEE Micro Special Topics on Agile & Open Source Hardware, 2020*

J2 **Trace Wringing for Program Trace Privacy**
D. Dangwal, W. Cui, J. McMahan, T. Sherwood. *IEEE Micro's Top Picks from Computer Architecture Conferences, 2020 **(IEEE Micro Top Pick)***

C3 **Safer Program Behavior Sharing through Trace Wringing**
D. Dangwal, W. Cui, J. McMahan, T. Sherwood. *Architectural Support for Programming Languages and Operating Systems **(ASPLOS)**, 2019*

J1 **Language Support for Navigating Architecture Design in Closed Form**
W. Cui, G. Tzimpragos, Y. Tao, J. McMahan, D. Dangwal, N. Tsiskaridze, G. Michelogiannakis, D. Vasudevan, T. Sherwood. *ACM Journal on Emerging Technologies in Computing Systems **(JETC)**, 2019*

W2 **PyRTLMatrix: an Object-Oriented Hardware Design Pattern for Prototyping ML Accelerators**
D. Aboye, D. Kupsh, M. Lim, J. Mai, D. Dangwal, D. Mirza, T. Sherwood. *Workshop on Energy Efficient Machine Learning and Cognitive Computing for Embedded Applications **(EMC2)**, 2019*

W1 **PyRTL in Early Undergraduate Research**
D. Mirza, D. Dangwal, T. Sherwood. *Workshop on Computer Architecture Education **(WCAE)**, 2019*

C2 **Charm: A Language for Closed-form High-level Architecture Modeling**
W. Cui, Y. Ding, D. Dangwal, A. Holmes, J. McMahan, A. JavadiAbhari, G. Tzimpragos, F. Chong, T. Sherwood. *International Symposium on Computer Architecture **(ISCA)**, 2018*

C1 **A Pythonic Approach for Rapid Hardware Prototyping and Instrumentation**
J. Clow, G. Tzimpragos, D. Dangwal, S. Guo, J. McMahan, T. Sherwood. *International Conference on Field-Programmable Logic and Applications **(FPL)**, 2017*

Pre-Prints, Reports, Articles

A2 **Mechanism Design for Improving Hardware Security Workshop Report** *CCC Workshop Report, August 2022*

A1 **Analysis and Mitigations of Reverse Engineering Attacks on Local Feature Descriptors**
D. Dangwal, V. T. Lee, H. J. Kim, T. Shen, M. Cowan, R. Shah, C. Trippel, B. Reagen, T. Sherwood, V. Balntas, A. Alaghi, E. Ilg. *arXiv preprint, May 2021*

Patents

P2 **Model Optimization and Data Analysis Using Neural Traces**
A. Rajagopal, G. H. Huynh, D. Dangwal *Provisional Patent Filed September 2025*

P1 **Deriving a concordant software neural network layer from a quantized firmware neural network layer**
J. Fowers, D. Lo, D. Dangwal *US Patent 11556764B2, Microsoft Technology Licensing LLC, 2023*

Invited Talks and Seminars

T8 **Performance, Power, and Privacy: Codesign Strategies for Always-On Wearables**
Washington State University, Pullman 06/2025

T7 **Privacy and Security in the age of Metaverse: A case for data minimization and on-device AI**
Washington State University, Everett 05/2025

T6 **A System-Level Framework for Privacy: Applications of Wringing in AR/VR**
Meta, Reality Labs Research 03/2021

T5 **A System-Level Framework for Privacy**
Arizona State University, Phoenix 03/2021

T4 **A System-Level Framework for Privacy**
Pennsylvania State University, State College 03/2021

T3 **Privacy through Wringing**
UCSB Grad Slam Final 03/2021

T2 **Agile hardware development and instrumentation with PyRTL**
Agile-RTL Workshop, UC Santa Barbara, CA 09/2019

T1 **OpenTPU: Prototyping ML Accelerators with PyRTL**
IEEE Space Computing Conference, Caltech, Pasadena, CA 09/2019

Teaching and Mentorship

Teaching Assistant, CS 154: Computer Architecture, UCSB — Spring 2021

Teaching Assistant, Research Mentorship Program (RMP), UCSB — Summer 2019

NSF ERSP Mentor, Department of Computer Science, UCSB — 2018 - 2019

- Students published "PyRTLMatrix: an Object-Oriented Hardware Design Pattern for Prototyping ML Accelerators" at EMC2 workshop (W2)
- Awarded university-wide Fiona and Michael Goodchild Graduate Mentoring Award for excellence in mentorship

Women in STEM Mentorship Program, UCSB — 10/2016 - 03/2018

Teaching Assistant, Department of Physics, UCSB — 01/2015 - 06/2015

EUREKA Mentorship Program, California NanoSystems Institute, UCSB — 06/2015 - 08/2015

Students Mentored

- Joann Chen (Research Intern, Meta, 2022), Manu Kondapaneni (2020), Junayed Naushad (2019), Dawit Aboye (2018-2019), Dylan Kupsh (2018-2019), Maggi Lim (2018-2019), Jacqueline Mai (2018-2019), Angela Yung (2016-2017), Saurabh Gupta (2015)

Professional Service and Activities

CRA Congressional Visit Day, Washington State Contingent — 09/2025

- Represented CRA and Washington State in Washington, D.C., and joined meetings with Members of Congress to make the case for federal support of computing research

Invited Participant, CCC Future of AI Research in Industry — 07/2025

Invited Participant, CCC Computing Futures Symposium — 05/2025

Invited Participant, CCC Mechanism Design for Improving Hardware Security — 08/2022

Organizer, Undergrad Architecture Mentoring Workshop (uArch) — 2022 - 2025

Program Committee Member

- MICRO '26, ISPASS '26, HPCA ('26, '25, '24), ASPLOS '25, ISCA '24, SEED '24, HASP '23

External Review Committee

- MICRO '24, YArch ('25, '23), ISCA '22, SEED '21, ASPLOS '20 (Artifact Evaluation)

Co-President, Women in Computer Science (WiCS), UCSB — 2018 - 2020

Graduate Representative for Faculty Recruitment, Department of Computer Science, UCSB — 2019 - 2020

Graduate Representative for Diversity, Department of Computer Science, UCSB — 2018 - 2019

Grace Hopper Celebration of Women — 2017, 2018, 2019

CRA-W Grad Cohort — 2017, 2018

(Updated March 2026)