Deeksha Dangwal

deekshadangwal@gmail.com • deekshadangwal.com • Google Scholar • LinkedIn

Research Summary

I am a research scientist specializing in hardware-software co-design and on-device AI acceleration. My current work is focused on low-latency machine perception on ultra low-power wearables (AR/smart glasses). I have developed techniques for near- and on-sensor processing, model compression and partitioning (e.g. on device and cloud), and integration of custom accelerators. My broader research interests include privacy-preserving computing, hardware security, and sustainable computing.

Areas of Expertise: Computer Architecture, Hardware-Software Codesign, On-device AI, Privacy and Security

Highlights

- 4 years of experience with hardware-software codesign for ultra-low power sensing and machine perception systems
- Led innovation in privacy-preserving at the system-level, establishing novel threat models and mitigation strategies for application tuning and AR/MR systems
- Selected as a **Rising Star in EECS in 2020**
- Co-authored 12 publications in top-tier computer architecture venues, including ISCA, ASPLOS, PLDI, FPL and recognized in **IEEE Micro's Top Picks**.
- Program Committee member for top-tier architecture conferences (HPCA, ASPLOS, ISCA, and MICRO).

Education

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

Master of Science, Electrical and Computer Engineering - University of California, Santa Barbara 2016

Bachelor of Engineering, Electronics and Instrumentation - Ramaiah Institute of Technology 2014

Experience

Research Scientist - Reality Labs Research, Meta 01/2022 - Present

- Optimized latency, area, thermal, and battery life constraints for on-device computer vision
  - Invented a novel low-power always-on event-based wake up system on custom accelerators using hand gestures and demonstrated improved latency of smart glasses interactions
  - Used model compression to translate CNNs to **few hundred KBs** for optimized on-device inference
  - **Achieved latency improvements of 93% and power reduction by 74%**
  - Benchmarked novel and emerging technologies such as compute-in-memory, on-sensor compute using 3D stacking
- Built system-level power and performance modeling tool for data collection Aria wearable devices
  - Developed a process-based discrete-event simulation modeling tool. The tool considers idle and active states, and estimates latency and power of running machine learning workloads on prototypes and data collection devices such as Aria V2.
  - Implemented device components including sensors, accelerators/processors, and interfaces
  - Validated, measured, and benchmarked device performance against machine perception algorithms, e.g. hand tracking, visual-inertial odometry and SLAM
  - Enabled scenario modeling, i.e. asking "what if" questions for design of future systems/variations to improve power and performance of on-device ML models
- Developed security and privacy research program for mixed and augmented reality

- Established threat models in augmented and mixed reality, including safety of codec avatars, crowd-sourced data collection in public spaces, reverse engineering of user images from feature descriptors and diffusion model priors.

Graduate Student Researcher - University of California, Santa Barbara 06/2015 - 12/2021

- Trace wringing: Safer program behavior sharing for application tuning and hardware-software codesign
- PyRTL: Pythonic Agile Hardware Development and Instrumentation
- Evaluating architectures for cryptographic algorithms
- OpenTPU: An open-source TPU written in PyRTL
- Closed-form high-level architecture modeling with Charm

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

- Implemented a novel reverse engineering attack on local feature descriptors to reconstruct raw user images with accuracy that surpassed the state-of-the-art.
- Established, for the first time, a privacy threat model for such a computer vision task.
- Developed privacy-preserving mitigation techniques and studied the effect of privatized feature descriptors on the performance of the downstream vision system.

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

- Implemented parameterizable architecture-aware machine learning graph primitives for custom hardware instructions
- Wrote tools to automatically convert hardware instructions to high-level graph primitives for machine learning models that remain true-to-hardware
- Designed computational experiments to compare and verify accuracy of neural network models

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

- Testing and measurements of throughput for a network of RAPID Data Processing Unit (DPU), a bandwidth-optimized architecture for big data computation.

Awards

UCSB Grad Slam Runner-up: "Privacy through Wringing" 03/2021
Grad Slam is an award-winning UC-wide competition for the best three-minute talk by a graduate student

Rising Stars in EECS, UC Berkeley 11/2020
Participants are selected based on academic excellence and interest in a faculty career in the EECS discipline

IEEE Micro Top Pick: "Trace Wringing for Program Trace Privacy" 06/2020
IEEE Micro's Top Picks from Computer Architecture Conferences, May-June 2020

UCSB Graduate Division's Fiona and Michael Goodchild Graduate Mentoring Award 06/2020
To recognize graduate students who have distinguished themselves as mentors of undergraduates

Department of Computer Science Outstanding Graduate Student Award 06/2020
To recognize academic achievement and contributions to the community and campus

Second Place Winner, NXP Embedded Design Challenge 08/2015

Selected Publications

(Full list available here)

"Unlocking Visual Secrets: Inverting Features with Diffusion Priors for Image Reconstruction" Sai Qian Zhang, Ziyun Li, Chuan Guo, Saeed Mahloujifar, **Deeksha Dangwal**, Edward Suh, Barbara De Salvo, Chiao Liu **[ArXiv Pre-print, 2024]**

"Context-aware privacy-optimizing address tracing" **Deeksha Dangwal**, Zhizhou Zhang, Jedidiah R Crandall, Timothy Sherwood **[Secure and Private Execution Environment Design (SEED), 2021]**

"Porcupine: A synthesizing compiler for vectorized homomorphic encryption" Meghan Cowan, **Deeksha Dangwal**, Armin Alaghi, Caroline Trippel, Vincent T Lee, Brandon Reagen **[Programming Language Design and Implementation (PLDI) 2021]**

"Mitigating Reverse Engineering Attacks on Local Feature Descriptors" **Deeksha Dangwal**, Vincent T Lee, Hyo Jin Kim, Tianwei Shen, Meghan Cowan, Rajvi Shah, Caroline Trippel, Brandon Reagen, Timothy Sherwood, Vasileios Balntas, Armin Alaghi, Eddy Ilg **[British Machine Vision Conference (BMVC) 2021]**

"Sok: Opportunities for software-hardware-security codesign for next generation secure computing" **Deeksha Dangwal**, Meghan Cowan, Armin Alaghi, Vincent T Lee, Brandon Reagen, Caronline Trippel **[Hardware and Architectural Support for Security and Privacy (HASP) 2020]**

"Agile hardware development and instrumentation with PyRTL" **Deeksha Dangwal**, Georgios Tzimpragos, Timothy Sherwood **[IEEE Micro Special Issue, 2020]**

"Trace wringing for program trace privacy" **Deeksha Dangwal**, Weilong Cui, Joseph McMahan, Timothy Sherwood **[IEEE Micro Top Picks, 2020]**

"Safer program behavior sharing through trace wringing" **Deeksha Dangwal**, Weilong Cui, Joseph McMahan, Timothy Sherwood **[Architectural Support for Programming Languages and Operating Systems (ASPLOS) 2019]**

"Charm: a language for closed-form high-level architecture modeling" Weilong Cui, Yongshan Ding, **Deeksha Dangwal**, Adam Holmes, Joseph McMahan, Ali Javadi-Abhari, Georgios Tzimpragos, Frederic Chong, Timothy Sherwood **[International Symposium on Computer Architecture (ISCA) 2018]**

"A pythonic approach for rapid hardware prototyping and instrumentation" John Clow, Georgios Tzimpragos, **Deeksha Dangwal**, Sammy Guo, Joseph McMahan, Timothy Sherwood **[Field Programmable Logic and Applications (FPL) 2017]**

Patents

"Deriving a concordant software neural network layer from a quantized firmware neural network layer" Jeremy Fowers, Daniel Lo, **Deeksha Dangwal [US Patent 11556764, 2023]**

Professional Service

- **uArch Workshop Organizer** (ISCA '25, ISCA '24, Micro '24, ISCA '23),
- **Program Committee Member**: ASPLOS '25, HPCA '25, YArch '25, ISCA '24, SEED '24, YArch '23, HASP '23, ISCA '22, SEED '21, ASPLOS '20 (Artifact Evaluation)
- Invited to contribute to **CCC's Mechanism Design for Improving Hardware Security Workshop** (2022)
- Graduate Representative for Faculty Recruitment, Department of Computer Science, UCSB (2019-2020)
- Co-President, Women in Computer Science (WiCS), Department of Computer Science, UCSB (2018-2020)
- Graduate Representative for Diversity, Department of Computer Science, UCSB (2018-2019)