Kanav Gupta

Email : kanav@umd.edu
Webpage: https://cs.umd.edu/∼kanav
Google Scholar: QEFy_4wAAAAJ

Research Interests

Secure Multi-Party Computation, Privacy Enhancing Technologies, Privacy-Preserving Machine Learning

Education

- **University of Maryland, College Park** College Park, MD, USA
  PhD in Computer Science; Advisor: Prof. Jonathan Katz; GPA: 4.0 *Aug 2023 - Aug 2028 (Expected)*
- **Indian Institute of Technology Roorkee** Roorkee, India
  B.Tech in Computer Science and Engineering; CGPA: 9.04/10 *July 2017 - July 2021*

Publications

[1] Kanav Gupta, Nishanth Chandran, Divya Gupta, Jonathan Katz, and Rahul Sharma. "Shark: Actively Secure Inference using Function Secret Sharing". In: *IEEE S&P 2025*.

[2] Kanav Gupta, Neha Jawalkar, Ananta Mukherjee, Nishanth Chandran, Divya Gupta, Ashish Panwar, and Rahul Sharma. "SIGMA: Secure GPT Inference with Function Secret Sharing". In: *PETS 2024*. Accepted for a talk at RWC'24 and TPMPC'24.

[3] Neha Jawalkar, Kanav Gupta, Arkaprava Basu, Nishanth Chandran, Divya Gupta, and Rahul Sharma. "Orca: FSS-based Secure Training with GPUs". In: *IEEE S&P*. 2024.

[4] Kanav Gupta, Deepak Kumaraswamy, Nishanth Chandran, and Divya Gupta. "LLAMA: A Low Latency Math Library for Secure Inference". In: *PETS*. 2022.

Work Experience

- **Google** New York City, NY
  Software Engineering PhD Intern *May 2025 - Aug 2025*
  - Designed and implemented Garbled Circuits based protocol for secure multi-party differentially private training.
- **Microsoft Research India** Bengaluru, India
  Research Intern *May 2024 - August 2024*
  - Designed protocols for secure inference of transformer models, secure against a malicious adversary.
- **Microsoft Research India** Bengaluru, India
  Research Fellow *July 2021 - July 2023*
  - Worked on problems related to applications of secure multi-party computation to machine learning.
  - Published 3 research papers in secure inference and secure training.
  - Lead the development of *Sytorch*, a C++ framework that allows the developer to describe a machine learning model, similar to pytorch, and execute secure inference and training of the model using a variety of protocol options.
- **MaidSafe** Remote
  Intern *Feb 2021 - May 2021*
  - Contributed to open-source development of the *self-encryption* toolkit - a component of Safe Network which splits data into chunks and encrypts each of these chunks with a key derived from subsequent chunk.
- **Simula UiB** Bergen, Norway
  Research Assistant *Sep 2020 - Dec 2020*
  - Studied Shortest Vector Problem in Lattice-based Cryptography as a part of Bachelor's project.
  - Introduced the notion of Obtuse Basis and showed that it is exponentially faster to solve SVP on such a basis.

Review Experience

Journals. ACM TOPS 2024
External Reviewer. ACM CCS 2023; Eurocrypt 2024,2026; Asiacrypt 2024; USENIX Security 2025,2026; Crypto 2025

Honors and Awards

- Awarded RSAC Security Scholar 2026
- Awarded Kulkarni Summer Research Fellowship 2024 (declined)
- Awarded Dean's fellowship at UMD
- Bronze Medal in NSUCRYPTO Olympiad 2020.
- Rank 1 in Regional Mathematics Olympiad, KVS Region, 2015.

Programming Skills

- **Skills**: Reverse Engineering, Low-Latency Programming, Emulation, web3
- **Languages**: C++, C, Python, Rust, Golang, OCaml, Solidity
- **Tools**: IDA Pro, Ghidra, Docker, XCode

Teaching Experience (TA)

- Governing Algorithms and Algorithmic Governance (with Prof. Gabriel Kaptchuk), UMD, Fall 2024
- Introduction to Quantum Computing (with Prof. Gorjan Alagic), UMD, Spring 2024
- Discrete Structures, UMD, Fall 2023
- Data Structures, IIT Roorkee, Spring 2020
- Discrete Structures, IIT Roorkee, Spring 2019

Extra Curricular Activities

- Currently serving as the organizer for UMD Crypto Reading Group.
- Served as a Joint Secretary of the technical group *SDSLabs*. I was responsible for organizing several open institute lectures on fundamental topics of computer science. Led several projects like Backdoor, Beast and Watchdog.
- Participated in and won numerous CTFs as a part of the team *SDSLabs*.
- Actively participated in open-source development of *DifferentialEquations.jl* - a toolchain to solve ordinary differential equations using numerical methods.