Kanav Gupta

Email : kanav@umd.edu

Research Interests

Secure Multi-Party Computation, Zero-Knowledge Proofs, Interactive Proofs, Theoretical Computer Science

Education

- **University of Maryland, College Park** College Park, MD
  PhD in Computer Science; Advisor: Prof. Jonathan Katz *Aug 2023 - Present*
- **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, Neha Jawalkar, Ananta Mukherjee, Nishanth Chandran, Divya Gupta, Ashish Panwar, and Rahul Sharma. *SIGMA: Secure GPT Inference with Function Secret Sharing*. Cryptology ePrint Archive, Paper 2023/1269. https://eprint.iacr.org/2023/1269. 2023. URL: https://eprint.iacr.org/2023/1269.

[2] 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.

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

Experience

- **Microsoft Research India** Bengaluru, India
  Research Fellow *July 2021 - July 2023*
  - Working on problems related to applications of secure multi-party computation to real-world scenarios.
  - Currently working on Secure Inference, Secure Training and Secure Aggregation.
  - Developed LLAMA - an FSS-based toolchain for Secure Inference and added it as a backend to EzPC environment.
  - Developed Sytorch - a crypto-agnostic way of writing machine learning model in C++ to securely train and perform secure inference over it.
  - Advised by Dr Divya Gupta, Dr Nishanth Chandran and Dr Rahul Sharma.
- **MaidSafe** Remote
  Intern *Feb 2021 - May 2021*
  - Worked on Safe Network - a fully autonomous data and communications network
  - Contributed to open-source development of the *self-encryption* toolkit - a component of Safe Network which splits some data into chunks and encrypts each of these chunks with a key derived from another 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.
  - Advised by Prof. Sugata Gangopadhyay and Dr Håvard Raddum.
- **Major League Hacking** Remote
  MLH Fellow *May 2020 - Aug 2020*
  - As part of the inaugural class of MLH Fellows, I contributed to Open Source projects with a team of Fellows under the educational mentorship of a professional software engineer.
  - Worked with the SciML organization on developing a software suite in Julia which solves non-linear equations using numerical methods.
  - Advised by Dr Christopher Rackauckas and Yingbo Ma.
- **The Julia Language** Remote
  GSoC Student *May 2019 - Aug 2019*
  - Participated in GSoC 2019 with JuliaDiffEq, an organization devoted towards developing the package DifferentialEquations.jl. This package solves most forms of the differential equations in the most optimal way.
  - Worked on project "Performance and General Fixes" to develop a toolkit to support the inclusion of different kinds of algorithms in a very optimal way.

- Advised by Dr Christopher Rackauckas and Yingbo Ma.

- **JoSAA, IIT Roorkee** Roorkee, India
  Student Developer *Jan 2018 - April 2019*
  - Part of the student team employed by IIT Roorkee (organizing institute of JEE Advanced 2019) to develop the allocation and validation software for the allocation of seats to more than 800,000 students.
  - Developed an individual implementation of Deferred Acceptance Algorithm for seat allocation.
  - Worked closely with NICSI, New Delhi to cross-verify and release results.
  - Advised by Prof. Sugata Gangopadhyay.

Honors and Awards

- Second place at Warpspeed web3 hackathon organized by Lightspeed Venture Partners.
- Bronze Medal in NSUCRYPTO Olympiad 2020.
- Winner of CSAW Embedded Security Challenge 2020 in India region as a part of team SDSLabs.
- Winner of GitHub Java CTF 2020.
- Winner of CSAW CTF 2019 in India region as a part of team InfoSecIITR.
- Winner of SecCon CTF 2019 hosted by Cisco India.
- Second Place in Warpspeed Hackathon 2022.
- Winner of UST Global d3code Hackathon 2019.
- Recipient of KVPY scholarship 2017 with All-India Rank 161.
- Secured All-India Rank 430 in JEE Advanced 2017 and All-India Rank 113 in JEE Main 2017.
- Rank 1 in Regional Mathematics Olympiad, KVS Region, 2015.

Programming Skills

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

Extra Curricular Activities

- 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*.
- Served as a TA for the courses *Data Structures* (Spring 2020) and *Discrete Structures* (Spring 2019) at IIT Roorkee.
- Actively participated in open-source development of *DifferentialEquations.jl* - a toolchain to solve ordinary differential equations using numerical methods.