Nikhil Vanjani

+1-412-626-9195 • nvanjani@cmu.edu • nikhilvanjani.github.io • linkedin.com/in/nikhilvanjani/

Research Interests

Cryptography, Blockchains, Theoretical Computer Science, Cyber Security

Education

Carnegie Mellon University (CMU) — Pittsburgh, PA, USA
Ph.D. Candidate in Electrical and Computer Engineering, Advisor: Elaine Shi — Jan 2022 - Present
M.S. in Information Security — Aug 2020 - Dec 2021

Indian Institute of Technology Kanpur (IITK) — Kanpur, UP, India
B.Tech. in Computer Science and Engineering — Jul 2014 - May 2018

Publications

Unless otherwise noted, the author order is either alphabetical or randomized.

Conference Proceedings

- **Non-Interactive Anonymous Router with Quasi-Linear Router Computation** — TCC 2023
  Rex Fernando, Elaine Shi, Pratik Soni, Nikhil Vanjani, Brent Waters — Paper link
- **Multi-Client Inner Product Encryption: Function-Hiding Instantiations Without Random Oracles** — PKC 2023
  Elaine Shi, Nikhil Vanjani — Paper link

Maunscripts

- **Functional Adaptor Signatures: Definitions, Constructions, and Applications** — 2023
  Pratik Soni, Sri AravindaKrishnan Thyagarajan, Nikhil Vanjani

Selected Talks

- **Non-Interactive Anonymous Router with Quasi-Linear Router Computation**
  Theory of Cryptography Conference (TCC) — Slides link | Dec 2023
  Ph.D. Qualifying Exam, CMU — Slides link | Nov 2022
- **Multi-Client Inner Product Encryption: Function-Hiding Instantiations Without Random Oracles**
  International Conference on Practice and Theory of Public-Key Cryptography (PKC) — Slides link | May 2023
  CMU Theory Lunch — Slides link | Apr 2023
  MS thesis defense, CMU — Slides link | Nov 2021
- **Attribute-based Signatures for Unbounded Circuits in the Random Oracle Model**
  Cryptography reading group talk, IITM — Slides link | Jul 2020
- **Obfuscation of Probabilistic Circuits and Applications**
  Course project for Computing on Encrypted Data, IITM — Slides link | Nov 2019
- **Two case studies on advances in Blockchains: Algorand, Zcash**
  Seminar talk for National Blockchain Project being undertaken by C3I Center, IITK — Slides link | Apr 2018

Research Experience

Algorand | Smart Contracts Research Intern — May - Aug 2021
Supervisor: Jing Chen
Designed, evaluated and implemented cryptographic primitives in the smart contract language AlgoClarity

- Implemented a Foreign Function Interface (FFI)-safe Rust library for performing ops on the BLS12-381 curve
- Used K framework to define syntax and semantics of AlgoClarity methods to perform the ops according to EIP-2537
- Built smart contracts for verification and aggregation of BLS signatures using the BLS12-381 curve ops

IIT Madras | Research Assistant — Aug 2019 - Jun 2020
Supervisor: Shweta Agrawal

- Studied state of the art E-Voting Protocols such as Pret A Voter, Scratch & Vote, Scantagreity, MarkPledge
- Designed a blockchain-based voting system with support for vote verification to enable 1 billion voters to vote from anywhere with the goal of increasing voter turnout (in collaboration with Election Commission of India)

Scholastic Achievements

- Awarded **$9000 tuition scholarship** for pursuing Masters degree by Information Networking Institute, CMU 2020
- **Red Hat Certified System Administrator (RHCSA)**, Certificate Number: 170-124-598 *2017*
- Secured 1^{st} position in **Blockchain Hackathon** organised at Techkriti, IIT Kanpur *2017*
- Secured Rank **461** in **Codechef Snackdown** Final Round among **8500** teams *2015*
- Secured **All India Rank 201** in **Joint Entrance Examination (JEE) Advanced** among **1 million** applicants *2014*

Technical Skills

- **Programming**: C++, C, Go, Rust, K framework, Clarity, Python, Octave, LaTeX, Bash, Assembly
- **Libraries/Softwares**: Git, Jenkins, SunRPC, gRPC, OpenSSL, Protobuf, GDB, Wireshark, TensorFlow, Numpy

Professional Service

- **External Reviewer:** Eurocrypt 2024, FC 2024, TCC 2023, TDSC 2023, Asiacrypt 2022
- **Co-organizer of CMU Cylab Crypto Seminar**

Graduate Coursework

- **Cryptography:** Intro to Cryptography, Computing on Encrypted Data, Modern Cryptology
- **Theory:** Randomness in Computation, CS Theory Toolkit, Advanced Approximation Algorithms, Quantum Computing
- **Security & Privacy:** Foundations of Privacy, Information Security, Computer Systems Security, Cyber Risk Modelling
- **Systems:** Distributed Systems, Computer Networks, Intro to Computer Systems

Teaching / Mentoring

- **Foundations of Blockchains (15435), CMU** | *Teaching Assistant* Sep - Dec 2022, Sep - Dec 2023
- **Intro to Information Security (14741), CMU** | *Teaching Assistant* Feb - May 2021
- **Theory of Blockchains, Association of Computing Activities, IITK** | *Mentor* Jan - Apr 2018
- **Cryptography, Association of Computing Activities, IITK** | *Mentor* Aug - Nov 2017
- **Blockchain-based medical record-keeping system, Programming Club, IITK** | *Mentor* May - Jul 2017
- **Cyber Security, Association of Computing Activities, IITK** | *Mentor* Jan - Apr 2017

Work Experience

Cohesity | *Member of Technical Staff* Jun 2018 - Jul 2019

- **Distributed File System Team**
  - Implemented CHAP Authentication protocol for iSCSI
  - Built a light weight client supporting source-side deduplication for the company's distributed filesystem for backups
- **Distributed Systems Team (Sub team: SAP)**
  - Led the design and integration of Authentication feature in SAP HANA Backint plugin
  - Implemented Multistream Backup and Restore feature support in Backint