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: Dr. 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

- Rex Fernando, Elaine Shi, Pratik Soni, **Nikhil Vanjani** (2023). Non-Interactive Anonymous Router with Quasi-Linear Router Computation. *In Submission.* ePrint
- Elaine Shi, **Nikhil Vanjani** (2023). Multi-Client Inner Product Encryption: Function-Hiding Instantiations Without Random Oracles. *PKC 2023 (to appear).*
- **Nikhil Vanjani** (2021). Multi-Input Inner Product Encryption: Function-Hiding Instantiations without Random Oracles. *Masters thesis.* Thesis Report

Research Experience

Non-Interactive Anonymous Router with Quasi-Linear Router Computation
Advisor: Dr. Elaine Shi, CMU — Jun - Oct 2022

- Employed a novel approach of indistinguishabily obfuscating (iO) a network of circuits to show feasability results for non-interactive anonymous routing with sub-quadratic router computation
- Developed a new iO-compatible technique for authentication called Somewhere Statistically Unforgeable (SSU) signatures and constructed it from the sub-exponential hardness of iO and one way permutations

Follow-up research on Non-Interactive Anonymous Routing
Advisor: Dr. Elaine Shi, CMU — Nov 2022 - Present

- Investigating how to instantiate SSU signatures from polynomial stretch assumptions
- Investigating new notions of security for anonymous routing

Multi-Client Inner Product Encryption: Function-Hiding Instantiations Without Random Oracles
Advisor: Dr. Elaine Shi, CMU — Jan 2021 - Feb 2022
Investigated functional encryption (FE) schemes in Multi-Client (MC) setting satisfying function-hiding security

- Constructed the first function-hiding MCFE scheme for inner products, relying on standard bilinear group assumptions
- Proposed a new upgrade from single-input FE for inner-products to a multi-client one that preserves function privacy
- Proved adaptive function-hiding security in static corruption setting without the use of a random oracle

Follow-up research on Multi-Client Functional Encryption
Advisor: Dr. Elaine Shi, CMU — Mar 2022 - Present

- Investigating the challenges with improving the above MCFE results to handle adaptive corruptions
- Investigating the challenges with constructing MCFE for quadratic functions

BLS12-381 elliptic curve ops for Layer 2 Smart Contracts
Advisor: Dr. Jing Chen, Theory Group, Algorand Inc. — May - Aug 2021
Designed, evaluated and implemented cryptographic primitives in the smart contract language AlgoClarity

- Implemented a 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

Blockchain-based Voting Systems
Advisor: Dr. Shweta Agrawal, IIT Madras — Aug 2019 - Jun 2020

- 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)

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

Selected Talks

- **Non-Interactive Anonymous Router with Quasi-Linear Router Computation** Nov 2022
  Ph.D. Qualifying Exam, CMU Slides
- **Multi-Input Functional Encryption: Function-Hiding Instantiations Without Random Oracles** Nov 2021
  MS thesis defense, CMU Slides
- **Attribute-based Signatures for Unbounded Circuits in the Random Oracle Model** Jul 2020
  Cryptography reading group talk, IITM Slides
- **Obfuscation of Probabilistic Circuits and Applications** Nov 2019
  Course project for Computing on Encrypted Data, IITM Slides
- **Two case studies on advances in Blockchains: Algorand, Zcash** Apr 2018
  Seminar talk for National Blockchain Project being undertaken by C3I Center, IITK Slides
- **Fully Homomorphic Encryption** Apr 2018
  Course project for Linear Algebra Tools for Theoretical CS, IITK Slides
- **Post Quantum Cryptography** Oct 2017
  Course project for Quantum Computing, IITK Slides 1, Slides 2

Scholastic Achievements

- Awarded **$9000 tuition scholarship** for pursuing Masters degree by Information Networking Institute 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** total teams *2015*
- Secured **All India Rank 201** in **Joint Entrance Examination (JEE) Advanced** among **150,000** 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

Relevant 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
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

Service

External Reviewer: Asiacrypt 2022