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 - Information Networking Institute — Pittsburgh, PA, USA
Master of Science in Information Security, GPA: 4.0/4.0 — Expected Graduation: December 2021
Indian Institute of Technology Kanpur (IITK) — Kanpur, UP, India
Bachelor of Technology in Computer Science and Engineering, GPA: 7.8/10.0 — 2018

Research Experience

Multi-Client Functional Encryption | *Masters thesis advised by Dr. Elaine Shi, CMU* — Jan 2021 - Present
Worked on constructing functional encryption (FE) schemes in Multi-Client (MC) and Multi-Input (MI) settings satisfying function-hiding security from pairings-based standard assumptions — Thesis Proposal

- Constructed *selectively-secure function-hiding* **Ad Hoc MIFE for inner products from DLIN assumption**
- Working on extending the function-hiding construction obtained for Ad Hoc MIFE to Dynamic Decentralized MCFE
- Studying the difficulty in achieving *adaptive security* for *function-hiding* MCFE from standard assumptions

Theory Group, Algorand | *Smart Contracts Researcher under Dr. Jing Chen* — May - Aug 2021
Investigated about cryptographic tools needed to enable building complex and powerful Layer 2 Smart Contracts in AlgoClarity (Algorand's version of the Clarity Smart Contract Language)

- **BLS12-381 elliptic curve ops for Layer 2 Smart Contracts**
  - Designed and integrated the support for **EIP-2537** (precompile for BLS12-381 curve ops) into AlgoClarity
    - Wrote *pairing-plus-binding* - a **FFI-safe Rust library** for performing ops on the BLS12-381 curve
    - Using K framework, defined syntax and semantics of AlgoClarity functions for performing BLS12-381 curve ops
  - Added functional tests for BLS12-381 curve ops in AlgoClarity
  - Built smart contracts for verification and aggregation of **BLS signatures** using the BLS12-381 curve ops
- **Privacy-preserving auctions**
  - Initiated and led the review of existing literature on privacy-preserving auctions on smart contracts
  - Explored cryptographic and game-theoretic security definitions of sealed bid auctions

Cryptography Group, IIT Madras | *Research Assistant under Dr. Shweta Agrawal* — Aug 2019 - Jun 2020

- **Blockchain-based Voting Systems**
  - Studied State of the Art E-Voting Protocols - **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**)
- **Homomorphic Signatures for uniform models of computation**
  - Studied the relations between Homomorphic Signatures (**HS**) and Attribute-Based Signatures (**ABS**) and investigated the gap between their constructions based on lattices and pairings.
  - Constructed a **lattice-based HS scheme for NFA from standard assumptions** by using Verifiable Functional Encryption, Non-Interactive Zero-Knowedge proofs and Commitment scheme

Blockchain Technology — Aug - Nov 2017
Under-Graduate Project advised by Dr. Arnab Bhattacharya, IITK; Dr. Piyush Kurur, IITK — Report

- Explored challenges in blockchains such as - consensus, scalability, privacy
- Studied a paper by Micali et. al. -**Algorand** for Scaling Byzantine Agreements for Cryptocurrencies
- Studied about **zk-SNARKs**, the Zero-Knowledge Proofs based protocol behind Zcash

Monitoring Darknets for detecting Malicious Activities — May 2016 - Apr 2017
Under-Graduate Project advised by Dr. Sandeep Shukla, IITK; Dr. Nasir Memon, New York University — Report

- Studied about trap-based monitoring systems, operation of darknet, taxonomy of darknet data, extraction of insights on suspicious activities and threats on the Internet
- Performed **darknet profiling** and **visualized geographical distribution** of attack attempts and port scans
- Detected **Mirai botnet** on the various ports it operated on in accordance with the global observations of zero days
- Leveraged Collective Intelligence Framework on a **honeypot-like network** to gain **cyber threat intelligence**

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

Lucideus Inc. | *Summer Intern* May - July 2017

- Articulated **security configuration controls** for **hardening** of Servers (HP - UX), Switches (Juniper, HP, 3COM), Firewalls & VPN (Fortigate), Databases (MySQL, MSSQL) to automate the company's enterprise product

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*

Relevant Coursework

- **Cryptography:** Foundations of Privacy, Intro to Cryptography, Computing on Encrypted Data, Modern Cryptology
- **Theory:** Advanced Approximation Algorithms, Advanced Algorithms, Data Structures & Algorithms, Quantum Computing, Linear Algebra Tools for Theoretical CS, Abstract Algebra, Discrete Mathematics, Probability & Statistics
- **Security:** Information Security, Computer Systems Security, Cyber Risk Modelling
- **Systems:** Distributed Systems, Computer Networks, Intro to Computer Systems

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

Teaching / Mentoring

Teaching Assistant for 14-741/18-631 - Intro to Information Security, CMU Feb - May 2021
Course instructor: Dr. Hanan Hibshi

- Taught recitation lectures to a class of **35 students** on padding oracle attacks, access control lists, wireshark, cryptographic protocols, security considerations in writing smart contracts
- Answered students' questions via office hours, created new assignment problems and graded assignments

Mentor at Association of Computing Activities, IITK

- **Taught 40 students** across 3 semesters about blockchains, cyber security, cryptography Jan 2017 - Apr 2018

Mentor at Programming Club, IITK

- **Guided 8 students** to build a blockchain-based medical record-keeping system May - Jul 2017

Selected Talks

- **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