Nikhil Vanjani

Research Interests

Cryptography, Blockchains

Education

Carnegie Mellon University (CMU) Pittsburgh, PA, USA
Ph.D. Candidate, Electrical and Computer Engineering Jan 2022 - Present
- Advisor: Elaine Shi

M.S., Information Security Aug 2020 - Dec 2021
- Advisor: Elaine Shi
- Thesis: *Multi-Input Inner Product Encryption: Function-Hiding Instantiations without Random Oracles*

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

Publications

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

Conference Proceedings

[5] **New Constructions of Functional Adaptor Signatures : Broader Functions and Improved Efficiency**
Nikhil Vanjani (first author), Garrett Greiner (first author), Sri AravindaKrishnan Thyagarajan, Pratik Soni
IEEE Security and Privacy (Oakland) 2026

[4] **Fully Adaptive Decentralized MA-ABE: Simplified, Optimized, ASP Supported**
Pratish Datta, Junichi Tomida, Nikhil Vanjani
IACR Asiacrypt 2025 Paper

[3] **Functional Adaptor Signatures: Beyond All-or-Nothing Blockchain-based Payments**
Nikhil Vanjani (first author), Pratik Soni, Sri AravindaKrishnan Thyagarajan
ACM CCS 2024, TPMPC 2025 Code, Paper

[2] **Non-Interactive Anonymous Router with Quasi-Linear Router Computation**
Rex Fernando, Elaine Shi, Pratik Soni, Nikhil Vanjani, Brent Waters
IACR TCC 2023 Paper

[1] **Multi-Client Inner Product Encryption: Function-Hiding Instantiations Without Random Oracles**
Elaine Shi, Nikhil Vanjani
IACR PKC 2023 Paper

Maunscripts

[2] **Large-Universe (Multi-Authority) ABE from LWE**
Pratish Datta, Yannis Rouselakis, Junichi Tomida, Nikhil Vanjani
In Submission

[1] **Unbounded Large-Universe Decentralized MA-ABE from Static Assumptions**
Pratish Datta, Junichi Tomida, Nikhil Vanjani
In Submission

Patents

[1] **Multi-Authority Attribute-Based Encryption with Adaptive Security for Arithmetic Span Programs**
Pratish Datta, Junichi Tomida, Nikhil Vanjani
US Patent App. **63/875,152**, Filed Sep 3, 2025 (Pending)

Scholastic Achievements

- Research led by me on Functional Adaptor Signatures project formed the basis of a **$75000** grant from the Stellar Development Foundation (awarded to collaborators) 2024
- Awarded **Carnegie Institute of Technology Dean's Fellowship** for outstanding academic achievement 2022
- Awarded **Best Masters Thesis** for exemplary research by Information Networking Institute, CMU 2022
- Awarded **$9000 tuition scholarship** for 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 by 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

Professional Experience

NTT Research | Research Intern Jun - Aug 2025
Supervisor: Pratish Datta
Pioneered new attribute-based encryption schemes that expanded functionality and significantly improved efficiency, advancing the practicality of lattice-based cryptography

0xPARC Foundation | Research Intern Mar - May 2025
Supervisor: Brian Lawrence
Benchmarked modern zero-knowledge proof systems (Plonky2/Plonky3), providing performance insights to guide practical adoption of advanced cryptographic protocols

NTT Research | Research Intern Jun - Aug 2024
Supervisor: Pratish Datta
Developed foundational advances in multi-authority attribute-based encryption by proving full adaptive security for the classic Lewko–Waters scheme and designing the first scheme for Arithmetic Span Programs

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

IIT Madras | Research Assistant Aug 2019 - Jun 2020
Supervisor: Shweta Agrawal
Designed a blockchain-based voting system with support for vote verification

Cohesity | Member of Technical Staff Jun 2018 - Jul 2019
Built and integrated authentication, data deduplication, multistreaming features in distributed backup systems

Professional Service

- **Program Committee:**
  - Crypto Valley Conference 2025
- **External Reviewer:**
  - Crypto (2025, 2024); Eurocrypt (2024); Asiacrypt (2022); TCC (2023, 2024); Indocrypt (2024)
  - CCS (2024); FC (2024, 2025); TDSC (2023)
- **Co-organizer of CMU Cylab Crypto Seminar**

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
- **Blockchains, Association of Computing Activities, IITK** | *Student Instructor* Jan - Apr 2018
- **Cryptography, Association of Computing Activities, IITK** | *Student Instructor* Aug - Nov 2017
- **Cyber Security, Association of Computing Activities, IITK** | *Student Instructor* Jan - Apr 2017

Selected Talks

- **Fully Adaptive Decentralized MA-ABE: Simplified, Optimized, ASP Supported.**
  Stanford Security Seminar — Slides | Oct 2025
  NTT Research CIS Seminar — Slides | Oct 2025
  CMU Crypto Seminar — Slides | Sep 2025
- **Functional Adaptor Signatures: Beyond All-or-Nothing Blockchain-based Payments.**
  Invited Lecture, University of Utah — Slides | Oct 2024
  ACM CCS conference — Slides | Oct 2024
- **Non-Interactive Anonymous Router with Quasi-Linear Router Computation**
  IACR TCC conference — Slides | Dec 2023
  Ph.D. Qualifying Exam, CMU — Slides | Nov 2022
- **Multi-Client Inner Product Encryption: Function-Hiding Instantiations Without Random Oracles**
  IACR PKC conference — Slides | May 2023
  CMU Theory Lunch — Slides | Apr 2023
  MS thesis defense, CMU — Slides | Nov 2021
- **Attribute-based Signatures for Unbounded Circuits in the Random Oracle Model**
  Cryptography reading group talk, IITM — Slides | Jul 2020
- **Obfuscation of Probabilistic Circuits and Applications**
  Course project for Computing on Encrypted Data, IITM — Slides | Nov 2019
- **Two case studies on advances in Blockchains: Algorand, Zcash**
  Seminar talk for National Blockchain Project being undertaken by C3I Center, IITK — Slides | Apr 2018

Personal Information

- Phone: +1-412-626-9195
- Email: nikhilvanjani61@gmail.com
- Google Scholar: https://scholar.google.com/citations?user=TgFRe-YAAAAJ
- Github: https://github.com/nikhilvanjani
- LinkedIn: https://www.linkedin.com/in/nikhilvanjani/
- Website: https://nikhilvanjani.github.io