Nikhil Pappu

Basic Info

: nikpappu@pdx.edu WWW: http://nikhilpappu.info

Fifth year computer science PhD student at Portland State University working on quantum cryptography.

Institutions

2021- | **PhD in Computer Science**
Portland State University, USA

2016-2021 | **Integrated M.Tech (B.Tech + M.Tech) in Computer Science and Engineering**
IIIT Bangalore, India

Experience

Summer 2025- | **Research Internship - Unclonable Puncturable Obfuscation**
Portland State University Advisors: Fuyuki Kitagawa, Ryo Nishimaki
Currently working on collusion-resistant constructions and compilers for unclonable puncture obfuscation and single-decryptor encryption. Also studying the notion of non-interactive zero-knowledge proofs with certified everlasting zero-knowledge guarantees.

Winter 2025 | **Research Assistant - Secure Key Leasing from Traitor Tracing**
Portland State University Collaborators: Fuyuki Kitagawa, Ryo Nishimaki
Worked on a traitor-tracing based approach to collusion-resistant secure key leasing (SKL). Constructed collusion-resistant SKL for PRFs from LWE, among other results. In submission to the Eurocrypt 2026 conference.

Summer 2024 | **Research Internship - Collusion-Resistant Secure Key Leasing**
NTT Research, Tokyo Advisors: Fuyuki Kitagawa, Ryo Nishimaki
Worked on unbounded collusion-resistant secure key leasing for public-key encryption, achieving it based on LWE among other results. Appears in the Crypto 2025 conference.

Winter 2024 | **Research Assistant - Unclonable Cryptography**
Portland State University Advisor Fang Song
Worked on attacks that succeed with 3/4 probability for an XOR variant of the BB84-based quantum money game.

Spring 2022-23 | **Research Assistant - Quantum Black-Box Reductions**
Portland State University Advisor Fang Song
Proved that quantum black- box reductions are insufficient to prove the security of statistical non-interactive zero-knowledge arguments (S-NIZKs) based on standard assumptions. Reinterpreted this result by constructing a unified framework for studying reductions in a quantum world.

Winter 2022 | **Teaching Assistant - Introduction to Cryptography**
Portland State University Instructor: Fang Song

Spring 2021 | **Master's Thesis - Research on Secure Multi-Party Computation**
IIIT Bangalore Advisor: Ashish Choudhury
Studied information-theoretic secure multi-party computation tolerating a generalized non-threshold adversary in the asynchronous communication model.

Spring 2021 | **Teaching Assistant - Foundations of Cryptography**
IIIT Bangalore Instructors: Ashish Choudhury, Srinivas Vivek

Summer 2018 | **Open Source Developer - Google Summer of Code 2018**
SymPy: a Python library for symbolic mathematics. Mentors: Jason Moore, Ondřej Čertík
Implemented a parser that translates Autolev (a proprietary symbolic dynamics language, now superseded by MotionGenesis) code to SymPy code using the ANTLR parser generator. More details here, and here.

Manuscripts

2025 | **Collusion-Resistant Quantum Secure Key Leasing Beyond Decryption**
Fuyuki Kitagawa, Ryo Nishimaki, Nikhil Pappu
In Submission.

2024 | **Notions of Quantum Reductions and Impossibility of Statistical NIZK**
Chuhan Lu, Nikhil Pappu
ePrint: https://eprint.iacr.org/2024/1847

Publications

2025 | **PKE and ABE with Collusion-Resistant Secure Key Leasing**
Fuyuki Kitagawa, Ryo Nishimaki, Nikhil Pappu
CRYPTO 2025. ePrint: https://eprint.iacr.org/2025/262

2020 | **Perfectly-Secure Asynchronous MPC for General Adversaries (Extended Abstract)**
Ashish Choudhury, Nikhil Pappu
INDOCRYPT 2020

Programming Skills

Skills | Python, C/C++, Java, HTML5, Javascript, Git, Jenkins, MySQL, Android, bash/shell