

Nikhil Pappu

Basic Info

: nikpappu@pdx.edu

: <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 <i>Portland State University</i> 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 <i>Portland State University</i> 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 <i>NTT Research, Tokyo</i> 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 and TQC 2025 conferences.
WINTER 2024	Research Assistant - Unclonable Cryptography <i>Portland State University</i> 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 <i>Portland State University</i> 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 <i>Portland State University</i> Instructor: Fang Song
SPRING 2021	Master's Thesis - Research on Secure Multi-Party Computation <i>IIIT Bangalore</i> 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 <i>IIIT Bangalore</i> 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. TQC 2025 (Talk). 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
--------	--