Nikhil Pappu

Basic Info

: nikpappu@pdx.edu WWW: nikhilpappu.info

I am a fifth year computer science PhD student at Portland State University working on quantum cryptography. My research statement can be found here.

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

Manuscripts

2025 | **Certified-Everlasting Quantum NIZK Proofs**
Nikhil Pappu
arXiv: https://arxiv.org/abs/2512.13628
Demonstrates a barrier to obtaining certified-everlasting NIZK proofs in the CRS model via natural approaches, followed by a unique construction that bypasses the barrier, establishing its feasibility from LWE. Also observes that the barrier does not apply to the shared EPR model, in which a more efficient protocol (in regards to the quantum computation involved) is constructed based on LWE.

2025 | **Collusion-Resistant Quantum Secure Key Leasing Beyond Decryption**
Fuyuki Kitagawa, Ryo Nishimaki, Nikhil Pappu
arXiv: https://arxiv.org/abs/2510.04754
Demonstrates a traitor-tracing based compiler for collusion-resistant secure key leasing (SKL). The compiler is leveraged to obtain collusion-resistant SKL for PRFs from LWE, among other results.

2024 | **Notions of Quantum Reductions and Impossibility of Statistical NIZK**
Chuhan Lu, Nikhil Pappu
ePrint: https://eprint.iacr.org/2024/1847
Proves that quantum black- box reductions are insufficient to prove the security of statistical non-interactive zero-knowledge arguments (S-NIZKs) based on standard assumptions. This result is re-interpreted using a unified framework for studying reductions in a quantum world.

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
Achieves unbounded collusion-resistant secure key leasing for public-key encryption based on LWE, among other results. Prior works either satisfy only bounded collusion-resistance, or rely on iO.

2020 | **Perfectly-Secure Asynchronous MPC for General Adversaries (Extended Abstract)**
Ashish Choudhury, Nikhil Pappu
INDOCRYPT 2020
Constructs an information-theoretic secure multi-party computation protocol that tolerates a generalized non-threshold adversary in the asynchronous communication model.

Experience

Fall 2025	**Research Assistant - Certified-Everlasting Quantum NIZK Proofs** *Portland State University* Advisors: Fang Song
Summer 2025	**Research Internship - Unclonable Puncturable Obfuscation** *NTT Research, Tokyo* Advisors: Fuyuki Kitagawa, Ryo Nishimaki Exploring collusion-resistant constructions and compilers for unclonable puncture obfuscation and copy protection, as part of ongoing work.
Winter 2025	**Research Assistant - Secure Key Leasing from Traitor Tracing** *Portland State University* Collaborators: Fuyuki Kitagawa, Ryo Nishimaki
Summer 2024	**Research Internship - Collusion-Resistant Secure Key Leasing** *NTT Research, Tokyo* Advisors: Fuyuki Kitagawa, Ryo Nishimaki
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
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
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.

Programming Skills

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

References (ranked list)

Fang Song	fang.song@pdx.edu
Fuyuki Kitagawa	fuyuki.kitagawa@ntt.com
Ryo Nishimaki	ryo.nishimaki@ntt.com