Nikhil Pappu

Basic Info

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

Third year computer science PhD student at Portland State University. Interested in cryptography, quantum computing, and more broadly in theoretical computer science.

Institutions

2021-

PhD in Computer Science
Portland State University, USA
Conducting research focusing on quantum cryptography.

2016-2021

Integrated M.Tech in Computer Science and Engineering
IIIT Bangalore, India
CGPA: 3.39/4.00

Experience

Fall 2023

Research Assistant: Quantum NIZKs
Portland State University Advisor Fang Song
Conducting research on constructing Non-interactive Zero-Knowledge Proofs (NIZKs) satisfying the properties of unclonability and certified deletion under different setup assumptions. This involves the use of quantum information, as these properties are impossible to achieve classically.

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). Reinterpreted this result by constructing a unified framework for studying reductions in a quantum world. Submitted our results to Eurocrypt 2024.

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. Submitted some of our results in a paper titled *Perfectly-Secure Asynchronous MPC for General Adversaries (Extended Abstract)*, which has been published in INDOCRYPT 2020.

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Implemented a parser that translates Autolev (a proprietary symbolic dynamics language, now superseded by MotionGenesis) code to SymPy code using the ANTLR parser generator.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.

Publications

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, LaTeX, bash/shell