Nikhil Pappu

Basic Info

✉ : nkhlpappu@gmail.com WWW : http://nikhilpappu.info

5th year Integrated M.Tech (B.Tech + M.Tech) student of Computer Science and Engineering at the International Institute of Information Technology Bangalore (IIIT-B), India.

Interests

- Secure Multi-Party Computation (MPC)
- Cryptography and Privacy
- Secure Distributed Computing

Institutions

2016-
Integrated M.Tech in Computer Science and Engineering
International Institute of Information Technology Bangalore, India
CGPA: 3.34/4 (after 8/10 semesters)

2014-2016
Grade XI & XII
FIITJEE Junior College, Narayanguda, Hyderabad, India
Studied Math, Physics and Chemistry; 97.7%; JEE Main Rank: 5995

2014
Grade X
Meridian School, Banjara Hills, Hyderabad, India
CGPA: 10

Experience

Fall 2020
Research in Secure Multi-Party Computation - Capstone Project
International Institute of Information Technology 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.

Fall 2020
Teaching Assistant - Discrete Mathematics
International Institute of Information Technology Bangalore Instructor: Ashish Choudhury
Prepared and evaluated graded assignments and conducted tutorial sessions for a class of 100 sophomores.

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Implemented a parser that translates Autolev (a proprietary symbolic dynamics language, now superseded by MotionGenesis) code to SymPy code using the ANTLR parser generator.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

Coursework in Cryptography

Spring 2019

Foundations of Cryptography
International Institute of Information Technology Bangalore Shannon's Theory, CPA & CCA Security, PRFs, Block Ciphers, MACs, Authenticated Encryption, Hash Functions, DES & AES, Diffie-Hellman key exchange, ElGamal Encryption, RSA Encryption, Digital Signatures

Fall 2019

Computing on Private Data
International Institute of Information Technology Bangalore Shamir Sharing, Verifiable Secret Sharing, BGW Protocol, Preprocessing Model, Simulation Proofs, Zero Knowledge Proofs, Byzantine Broadcast & Agreement, Asynchronous Protocols. Presented BCP18 as part of paper presentations.

Spring 2020

Privacy-Preserving Machine Learning
International Institute of Information Technology Bangalore Yao's Garbled Circuits, Oblivious Transfer, GMW Protocol, ABY Mixed Framework, Efficient 2, 3, 4 PC Protocols, Computing Linear & Logistic Regressions, Somewhat & Fully Homomorphic Encryption. Presented BJPR18 and JKLS18 as part of paper presentations.

Programming Skills

General	Python, C, C++, Java, OCaml
Web Dev	HTML5, CSS, Javascript, Node.js, React
DevOps	Git, Jenkins, Docker, ELK stack
Misc.	MySQL, Android, LaTeX/XeLaTeX, R Markdown, bash/shell, SciPy, scikit-learn, cryptoTools