Rohit Chatterjee

Research Fellow
School of Computer Science
National University of Singapore
Singapore - 117417

rohitchatterjee94@gmail.com
rochat@nus.edu.sg
+65 8166 7354

POSITIONS

Postdoctoral Research Fellow — Supervisor: Prashant Nalini Vasudevan
National University of Singapore — *November 2023 - Ongoing*

EDUCATION

PhD — Advisor: Omkant Pandey
Computer Science & Engineering Department
Stony Brook University — *August 2017 - September 2023*
Thesis: Efficient Approaches to Emerging Cryptography against Quantum Threats

Master of Science (Research) — Advisors: Bhavana Kanukurthi &
Bachelor of Science (Research), First Class — Himanshu Tyagi
Major: Mathematics
Undergraduate Department
Indian Institute of Science — *August 2012 - May 2017*
Undergraduate Thesis: Information Theoretic Secure Computation

MANUSCRIPTS

Public Key Encryption from the MinRank Problem
In Submission
With Changrui Mu & Prashant Nalini Vasudevan

Decoding Balanced Linear Codes With Preprocessing
In Submission
With Andrej Bogdanov, Yunqi Li & Prashant Nalini Vasudevan

PUBLICATIONS

The Round Complexity of Black-Box Post-Quantum Secure Computation
CRYPTO 2025
With Xiao Liang, Omkant Pandey & Takashi Yamakawa

On the Necessity of Uncloneable Proof and Advice States
STOC 2025
With Supartha Podder & Srijita Kundu

Building Unclonable Cryptography: A Tale of Two No-cloning Paradigms
SECRYPT 2023
With Ghada Almashaqbeh

A Note on the Post-Quantum Security of (Ring) Signatures
PKC 2022
With Kai-Min Chung, Xiao Liang, & Giulio Malavolta

Compact Ring Signatures from Learning With Errors
CRYPTO 2021
With Sanjam Garg, Mohammad Hajiabadi, Dakshita Khurana, Xiao Liang, Giulio Malavolta, Omkant Pandey & Sina Shiehian

Improved Black-Box Constructions of Composable Secure Computation
ICALP 2020
With Xiao Liang & Omkant Pandey

TALKS

On the Necessity of Uncloneable Proof and Advice States
Invited Talk at SoC AlgoTheory Seminar at **NUS**, October 2025.
Invited Talk at CS Departmental Seminar at **CUHK**, August 2025.
Invited Long Talk at **AQIS 2025**, August 2025

Post-Quantum Black-Box Secure Computation from Minimal Assumptions
Invited Talk at SoC AlgoTheory Seminar at **NUS**, February 2024

SERVICE

Invited Reviewer for **Journal of Cryptology** [2023], **EUROCRYPT** [2023-2026], **CRYPTO** [2023-2025], **ASIACRYPT** [2022,2024,2025], **TCC** [2021-2025], **PKC** [2019,2024,2025], **TQC** [2024,2025], **ITC** [2023], **SCN** [2022], **QCRYPT** [2023], **WWW S&P** [2026]

Organizer of the **AlgoTheory Seminar** at School of Computing at NUS, since January 2024

AWARDS

Recipient of the prestigious **Kishore Vaigyanik Protsahan Yojana (KVPY) fellowship** in 2012, a National Fellowship in Basic Sciences, funded by the Department of Science and Technology (DST), Government of India for showing promise in research in basic science (All India Rank: 159)

EXPERIENCE

Mentorship:
Co-supervised 3 undergraduates as part of the **Odyssey Summer Research** program at NUS School of Computing for advanced undergraduates
Co-supervising an undergraduate **Final Year Project** at NUS School of Computing (as part of the FYP program)

Teaching & Assistantship:
Modern Cryptography, Analysis of Algorithms, Foundations of Computer Science(UG)

Programming Languages known:
Python, Java, C, R