

Rohit Chatterjee

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

rohitchatterjee94@gmail.com
rochat@nus.edu.sg
+65 8261 4693

POSITIONS Postdoctoral Research Fellow, **National University of Singapore**, Singapore
Associated Faculty: Prashant N. Vasudevan
November 2023 - Ongoing

EDUCATION **Stony Brook University**, Stony Brook, New York, USA
PhD Program, Computer Science & Engineering Department, September 2023
Advisor: Prof. Omkant Pandey
Thesis: Efficient Approaches to Emerging Cryptography against Quantum Threats

Indian Institute of Science, Bangalore, Karnataka, India
Master of Science (Research), Undergraduate Department, 2017 (Math major)
GPA: 5.8/8
Bachelor of Science (Research), Undergraduate Department, 2016 (Math major)
GPA: 6.1/8

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

We construct a $\max(R_{\text{OT}}, \tilde{O}(\log n))$ -round MPC protocol secure in the *angel-based* security model, by way of a constant-round black-box 1-1 CCA commitment scheme. The construction works under the modest assumption of semi-honest oblivious transfer. This closes the gap in round complexity between black-box and non-black-box MPC constructions in this model.

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

We present the first compact ring signature scheme (i.e., where the size of the signature grows logarithmically with the size of the ring) from the (plain) learning with errors (LWE) problem. The construction is in the standard model and it does not rely on a trusted setup or on the random oracle heuristic. At the heart of our scheme is a new construction of compact and statistically witness-indistinguishable ZAP arguments for $\text{NP} \cap \text{coNP}$, that we show to be sound based on the plain LWE assumption. Prior to our work, statistical ZAPs (for all of NP) were known to exist only assuming sub-exponential hardness of LWE.

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

We consider signatures satisfying blind-unforgeability as recently proposed by Alagic et al. (Eurocrypt'20). We present two short signature schemes achieving this notion: one is in the quantum random oracle model, assuming quantum hardness of SIS; and the other is in the plain model, assuming quantum hardness of LWE with super-polynomial modulus. We further propose an analog of blind-unforgeability in the ring signature setting. Moreover, assuming the quantum hardness of LWE, we construct a compiler

converting any blind-unforgeable (ordinary) signatures to a ring signature satisfying our definition.

**Building Unclonable Cryptography:
A Tale of Two No-cloning Paradigms**

With Ghada Almashaqbeh

SECRYPT 2023

Unclonable cryptography builds primitives that enjoy some form of unclonability, which are impossible in the classical model as classical data is inherently clonable. Quantum computing, with its no-cloning principle, offers a solution. Very recently, an alternative no-cloning technology has been introduced [Eurocrypt'22], showing that unclonable polymers—proteins—can also be used to build bounded-query memory devices and unclonable cryptographic applications. In this work, we investigate the relation between these two technologies; whether one can replace the other, or complement each other such that combining them brings the best of both worlds. Towards this goal, we review the quantum and unclonable polymer models, discuss whether these primitives can be built using the other technology, and show alternative constructions and notions when possible. We also offer insights and remarks for the road ahead.

**AWARDS AND
ACHIEVE-
MENTS**

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

**OTHER QUALI-
FICATIONS**

Programming Languages known: Python, Java, C, R
Courses TA'ed: Modern Cryptography, Analysis of Algorithms, Foundations of Computer Science(UG)