Rohit Chatterjee

Graduate Student
Computer Science & Engineering
Stony Brook University
Stony Brook, New York - 11794

rohitchatterjee94@gmail.com
rochatterjee@cs.stonybrook.edu
+1 (631) 579 5142

EDUCATION

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

Stony Brook University, Stony Brook, New York, USA
PhD Program, Computer Science & Engineering Department.
Advisor: Prof. Omkant Pandey
GPA (current): 3.9/4 *(Ongoing - 5th year)*

PUBLICATIONS & MANUSCRIPTS

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

We construct a $\max(R_{\mathsf{OT}}, \widetilde{O}(\log n))$-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 $\mathsf{NP} \cap \mathsf{coNP}$, 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
In Submission

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.

Round-Optimal Concurrent 2PC from Polynomial Hardness Assumptions
With Xiao Liang & Omkant Pandey

In Submission

We consider 2PC protocols in the *super-polynomial simulation in the universally composable model* (UC-SPS). On the negative side, we show that assuming the existence of non-interactive witness-indistinguishable proofs, 4 rounds are necessary for *asymmetric* (i.e., only one party receiving output) UC-SPS 2PC protocols that are based on black-box security reductions to *polynomial hardness assumptions*. Our techniques also extend to ruling out existence of *witness pseudo-random functions* (Zhandry, TCC'16) that can be proven secure via black-box reduction to *polynomial hardness assumptions*.

To complement our 2PC lower bound, we present a 4-round asymmetric *concurrent* UC-SPS 2PC protocol with black-box security proof, and based solely on polynomial hardness assumptions. Previous constructions of this primitive had the same round complexity but used super-polynomial hardness assumptions, while others were based on polynomial hardness but required additional rounds.

RELEVANT COURSEWORK

Mathematics: Linear Algebra, Algebra, Real Analysis, Probability Theory, Combinatorics, Measure Theory, Ordinary Differential Equations, Complex Analysis, Commutative Algebra & Galois Theory, Partial Differential Equations, Functional Analysis

Computer Science: Algorithms and Programming, Automata Theory And Computability, Computational Complexity Theory, Theoretical Foundations of Cryptography, Discrete Mathematics, Design and Analysis of Algorithms, Approximation Algorithms, Randomness in Cryptography, Fundamentals of Computer Networks, Data Science Fundamentals

Miscellaneous: Foundations of Data Sciences, Information Theory, Concentration Inequalities, Information & Communication Complexity

AWARDS AND ACHIEVEMENTS

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 QUALIFICATIONS

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