Department of Computer Science

Foundations of Advanced Cryptography

Pratik Soni
Carnegie Mellon University

Hosted by Reza Curtmola

Date: Monday, November 14, 2022
Coffee: 2:15 PM – 2:30 PM
Seminar: 2:30 PM – 3:30 PM
Location: GITC 4402 (4th Floor Seminar Lecture Hall)
WeEx Link: https://njit.webex.com/njit/j.php?MTID=m5284f6402997a2c8aa3a34721bbcb3e9

https://cs.njit.edu/seminars

Abstract:
Today, cryptography has transcended beyond protecting data in transit. Many advanced cryptographic techniques are gaining traction due to their significance in emerging systems like blockchains, privacy-preserving computation, and cloud computing. However, designing cryptography for these systems is challenging as they require underlying cryptographic algorithms to provide strong security and privacy guarantees and admit very efficient implementations.

In the first part of this talk, I will present my work that explores fundamental connections between cryptography and blockchains. Blockchains rely on advanced cryptography like Zero-Knowledge Proofs, and despite amazing advances in building efficient cryptographic tools, scalability is a major challenge plaguing blockchain-based applications like cryptocurrencies. I will discuss my work on improving prover's time and memory overheads in Zero-Knowledge Proofs, which is currently a primary bottleneck towards building more efficient Zero-Knowledge Proofs. Then, I will discuss my work where I use blockchains to build new and useful cryptography.

Finally, I will discuss my work on designing cryptographic commitments, digital analogs of sealed envelopes, secure against man-in-the-middle attacks. While heuristic constructions are known, my work introduces new fundamental techniques to circumvent strong barriers established for achieving provably secure protocols with minimal interaction. Specifically, I build provably secure protocols that require minimal (to no) interaction between the sender and the receiver.

Bio:
Pratik Soni is a Postdoctoral Research Fellow in the School of Computer Science at Carnegie Mellon University. He received his Ph.D. from UC Santa Barbara in 2015. His research interests span a wide range of topics across cryptography, including zero-knowledge proofs, non-malleable cryptography, secure multi-party computation, and its connections with blockchain technology. His work at FOCS 2017 was invited to SIAM Journal of Computing's special issue, and he is currently serving as a Program Committee Member at ACM CCS 2022 and ASIACRYPT 2022.