Department of Computer Science

Foundations and Advancements in Cryptographic Proofs

Arka Rai Choudhuri
Nexus

Hosted by: Zephyr Yao

Date: Wednesday, March 12, 2025
Coffee: 2:15 PM – 2:30 PM
Time: 2:30 PM – 3:30 PM (Eastern Time (US and Canada)
Location: GITC 4402 (4th floor Seminar Lecture Hall)
Zoom Link: https://njit-edu.zoom.us/j/99214620014?pwd=uQEU7eZXEe0m6kd4z66wi0tS0SbwSq.1

Meeting ID: 992 1462 0014
Passcode: 570479

Abstract:

Cryptographic proofs - an enhancement of mathematical proofs - allow one to assert complex mathematical claims with proofs that are both compact and efficiently verifiable. The remarkable efficiency guarantees of cryptographic proofs have driven applications in both cryptography and theoretical computer science. In practice, they have enabled the rapid verification of millions of blockchain transactions. Despite their usefulness, constructing cryptographic proofs from widely believed assumptions - a cornerstone of cryptographic rigor - has remained elusive, forcing practical systems to rely on heuristics that offer solutions in the absence of fully rigorous constructions.

In this talk, we will cover a series of recent results that, for the first time, establish the feasibility of constructing cryptographic proofs from a variety of well-studied cryptographic problems, enabling the verification of assertions about a large class of computations. In particular, we will discuss the central idea of these results - a novel approach to batching proofs - that has already become central to the construction of many cryptographic primitives.

The talk will also briefly discuss recent research on scaling cryptographic proofs for wider adoption, concluding with a discussion on privacy in computation and a look ahead at future research directions.

Bio:

Arka Rai Choudhuri is a research scientist at Nexus, where he works on leveraging theoretical advancements to realize scalable cryptographic proofs in practice. Prior to this, he was most recently a postdoctoral researcher at NTT Research and UC Berkeley, hosted by Prof. Sanjam Garg. He received his Ph.D. in computer science from Johns Hopkins University, advised by Prof. Abhishek Jain. His research focuses on cryptographic proofs and privacy aspects of computing, as well as their interplay with theoretical computer science. His work has been published in top conferences such as the Symposium on Theory of Computing (STOC), the Symposium on Foundations of Computer Science (FOCS), CRYPTO, EUROCRYPT, the Conference on Computer and Communications Security (CCS), and other leading venues. He has also served on the program committees for CRYPTO and ASIACRYPT.