NJIT

Department of Computer Science

Perfectly/Statistically Secure MPC over Layered Graphs with Optimal Corruption Thresholds

Varun Narayanan
UCLA

Hosted by: Shantanu Sharma

Date: Friday, March 28, 2025
Coffee: 11:15 AM – 11:30 AM
Time: 11:30 AM – 12:30 PM (Eastern Time (US and Canada)
Location: GITC 4402 (4th floor Seminar Lecture Hall)

Zoom Link: https://njit-edu.zoom.us/j/95903616720?pwd=UrsFtzLWaZFP0ePgVmqLxAOES8ECNn.1

Abstract:
Secure Multiparty computation (MPC) is a fundamental primitive in cryptography that enables mutually distrusting parties to collaborate using their private data through a communication protocol, eliminating the need for a trusted third party. Secure MPC among n parties can achieve perfect security if up to $t<n/3$ parties are corrupted, and statistical security if up to $t < n/2$ parties are corrupted. These guarantees hold against malicious adversaries in the standard MPC model, where a fixed set of parties are corrupt throughout the protocol.

Ostrovsky and Yung (PODC 1991) introduced a more dynamic setting where an adversary can periodically move through the network—uncorrupting parties and corrupting new ones—emulating real-world network attacks.

In the extreme case, an adversary may be maximally mobile, corrupting a fresh set of parties in every round of the protocol. A related challenge arises in the You Only Speak Once (YOSO) model (Gentry et al. Crypto 2021), where not only is the adversary mobile, but each round is executed by a new set of parties. Previous positive results in these settings fall short of achieving full security, either assuming probabilistic corruption, relying on nonstandard communication models, or providing only security-with-abort. Whether full security with perfect/statistical guarantees can be achieved remained an open question.

In this talk, I will present our results addressing both challenges. We introduce a layered MPC model, a simplified variant of fluid MPC (Choudhuri et al., Crypto 2021), which abstracts both mobile-adversary and YOSO settings. This model structures computation over a layered graph of width n, where parties communicate privately and broadcast messages to the next layer. We achieve perfect/statistical security with optimal corruption thresholds: $t<n/3$ for perfect security and $t<n/2$ for statistical security.

This talk is based on joint works with Bernardo David, Yuval Ishai, Anders Konring, Eyal Kushilevitz (Crypto 2023), and with Anders Konring, Chen-Da Liu-Zhang, Giovanni Deligios (TCC 2024).

Bio:
Varun Narayanan is a postdoctoral researcher in the Computer Science department at UCLA, hosted by Prof. Rafail Ostrovsky. He previously held a postdoctoral position at Technion, working with Prof. Yuval Ishai and Prof. Eyal Kushilevitz. He earned his PhD from TIFR, Mumbai, advised by Dr. Vinod Prabhakaran.

Varun's research focuses on theoretical and practical aspects of cryptography, with an emphasis on secure multiparty computation.