NJIT

# Department of Computer Science

## DPFs to the rescue: Applications of Distributed Point Functions to Secure Multiparty Computations

**Adithya Vadapalli**
University of Waterloo

**Hosted by Reza Curtmola**

**Date:** Monday, January 24, 2022

**Seminar:** 2:30 PM – 3:30 PM

**WebEx Link:** https://njit.webex.com/njit/j.php?MTID=mc12e8fd393179fa0868abf4a8b04f9ea

**https://cs.njit.edu/seminars**

**Abstract:**

This talk will describe a cryptographic primitive called Distributed Point Functions (DPFs). The primary focus will be on the relationship of DPFs with three fundamental cryptographic primitives; namely, private information retrieval (PIR), secure multi-party computation (secure MPC), and zero-knowledge proofs of knowledge (ZKP). The talk will constitute the presentation of two DPF-based secure systems, namely, a secure recommendations system and an anonymous messaging system establishing the relationship of DPFs with PIR, MPC and, ZKPs

**Bio:**

Adithya is a Postdoc at University of Waterloo with Ian Goldberg. Prior to that, he completed his PhD from Indiana University, Bloomington in 2021 under the supervision of Ryan Henry. His PhD dissertation was on Distributed Point Functions and their applications to secure Multi-party computation. His primary research interests lie in Privacy Enhancing Technologies. He works on both coming up with cryptographic protocols and building secure systems.