Speaker: Elette Boyle, Technion

Title: Large-Scale Secure Computation

We are interested in secure computation protocols in settings where the number of parties is huge and their data even larger. Assuming the existence of a single-use broadcast channel (per player), we demonstrate statistically secure computation protocols for computing (multiple) arbitrary dynamic RAM programs over parties' inputs, handling (1/3 - epsilon) fraction static corruptions, while preserving up to polylogarithmic factors the computation and memory complexities of the RAM program. Additionally, our protocol is load balanced and has polylogarithmic communication locality.

Joint work with Kai-Min Chung and Rafael Pass.