

Speaker: Elaine Shi, University of Maryland

Title: Binary Tree Oblivious RAM Framework and Applications in MPC

First, I will describe the binary-tree Oblivious RAM framework. Then, I will describe our recent efforts that bring together programming language techniques and cryptography, in making secure computation usable for non-expert programmers, and scalable for big data.