

Speaker: Abhi Shelat, University of Virginia

Title: Billion Gate Malicious Yao

We report results on our very large scale Yao garbled-circuits implementation. We describe what we consider to be the frontier of performance for this approach to secure computation in the malicious model.

Joint work with Chih-hao Shen and Ben Kreuter.