CFEM & CTIC workshop:
Theory and Practice of Secure Multiparty Computation
May 30 to June 3, 2016
Aarhus University, Denmark

Title: Adaptive & Fully Succinct Garbled RAM

Ran Canetti, Tel Aviv University and Boston University

We show how to garble a large persistent database and then garble, one by one, a sequence of adaptively and adversarially chosen RAM programs that query and modify the database in arbitrary ways. The garbled database and programs are guaranteed to reveal only the outputs of the programs when run in sequence on the database. Still, the runtime, space requirements and description size of the garbled programs are proportional only to those of the plaintext programs and the security parameter. We assume indistinguishability obfuscation for circuits and poly-to-one collision-resistant hash functions.

As an immediate application, our scheme is the first to provide a way to outsource large databases to untrusted servers, and later query and update the database over time in a private and verifiable way, with complexity and description size proportional to those of the unprotected queries.

The talk will cover joint works with Justin Holmgren, Yilei Chen and Mariana Raykova.