Speaker: Daniel Wichs, Northeastern University

Title: Outsourcing Private RAM Computation

We construct the first schemes that allow a client to privately outsource arbitrary program executions to a remote server while ensuring that: (I) the client's work is small and essentially independent of the complexity of the computation being outsourced, and (II) the server's work is only proportional to the run-time of the computation on a random access machine (RAM), rather than its potentially much larger circuit size. Furthermore, our solutions are non-interactive and have the structure of "reusable garbled RAM programs", where the client creates a garbled program which it gives to the server and later can outsource arbitrary executions of this program by providing fresh garbled inputs. We also construct schemes for an augmented variant of the above scenario, where the client can initially outsource a large private and persistent database to the server, and later outsource arbitrary program executions with read/write access to this database.

Our solutions are built from non-reusable garbled RAM in conjunction with new types of reusable garbled circuits that are more efficient than prior solutions but only satisfy weaker security. For the basic setting without a persistent database, we can instantiate the required reusable garbled circuits using indistinguishability obfuscation. For the more complex setting with a persistent database we need stronger notions of obfuscation. Our basic solution also requires the client to perform a one-time preprocessing step to garble a program at the cost of its RAM run-time, and we can avoid this cost using stronger notions of obfuscation. It remains an open problem to instantiate these new types of reusable garbled circuits under weaker assumptions, possibly avoiding obfuscation altogether.

Joint work with Craig Gentry, Shai Halevi and Mariana Raykova