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

Title: Mercury Delay Lines to Magnetic Core Memories: Progress in Oblivious Memories

David Evans, University of Virginia, USA

Hiding memory access patterns is required for secure computation, but remains prohibitively expensive for many interesting applications. Prior work has either developed custom algorithms that minimize the need for data-dependant memory access, or proposed the use of Oblivious RAM (ORAM) to provide a general-purpose solution. However, most ORAMs are designed for client-server scenarios, and although they provide asymptotic performance benefits, because of their high initialization and concrete costs they remain worse than linear scan for most actual uses.

In this talk, I will present work on a new ORAM approach for secure computation that revisits the classical square-root ORAM design of Goldreich and Ostrovsky. Our design replaces the expensive pseudo-random function needed in traditional hierarchical ORAM designs with inexpensive permutations and a recursive position map, and achieves orders of magnitude performance improvements over the best previous ORAM designs for use in secure computation applications. By combining the ORAM design with custom data structures, we are able to implement previously infeasible algorithms, including secure stable matching using both the Gale-Shapley and Roth-Peranson algorithms, as secure computations.

[This talk covers joint work with Samee Zahur, Xiao Wang, Mariana Raykova, Adrià Gascón, Jack Doerner, Jonathan Katz, and abhi shelat.]