THE WEIZMANN INSTITUTE OF SCIENCE
FACULTY OF MATHEMATICS AND COMPUTER SCIENCE

Foundations of Computer Science Colloquium

Room 290C, Ziskind Building
on Monday, Apr 03, 2017
at 14:30

Udi Wieder
VMware Research

Circuit based PSI via Cuckoo Hashing

Abstract:

While there has been a lot of progress in designing efficient custom protocols for computing Private Set Intersection (PSI), there has been less research on using generic MPC protocols for this task. However, there are many variants of the set intersection functionality which seem hard to compute with existing custom protocols and are easy to compute with generic MPC based solutions (for example comparing the cardinality of the intersection with a threshold or measuring ad conversion rates). Generic protocols work over circuits which compute the intersection. For sets of size n the best known circuit constructions compute $O(n \log n)$ comparisons. In this work we propose new circuit-based protocols for computing variants of the intersection, with circuits computing only $O(n)$ comparisons. Our constructions are based on a new variant of Cuckoo hashing in two dimensions. We employ several optimizations and determine experimentally the required sizes of tables and circuits, and measure the runtime, showing that our protocol is more efficient in concrete terms than existing constructions. The proof technique is new and can be generalized to analyzing simple Cuckoo hashing as well as new variants.