Speaker: Yuval Ishai, Technion

Title: Share Conversion and Private Information Retrieval

Private Information Retrieval (PIR) protocols allow a client to access a remote database without revealing what it is after. In the so-called "information-theoretic" setting for PIR, the client interacts with several servers which hold copies of the database, and the client's choices remain unconditionally hidden from each individual server.

We introduce a new framework for the construction of information-theoretic PIR protocols which relies on a generalized notion of "share conversion" in secret sharing schemes. Our framework unifies previous results in the area and gives rise to protocols that improve the concrete complexity of PIR even for feasible real-life parameters.

Joint work with Amos Beimel, Eyal Kushilevitz, and Ilan Orlov.