Using the PIR Heuristic to Enhance Secrecy

Abstract:

The use of a computational PIR scheme has been instrumental in reducing interaction from interactive proofs, and in converting multi-prover interactive proofs to (single prover) 2-message computationally sound proofs (also known as arguments).

In this talk we will focus on the secrecy guarantees of this transformation. We show that if we start with an interactive proof which is only *honest-verifier* zero-knowledge, and we use a quasi-poly secure *symmetric* PIR scheme (or a 2-message OT scheme) to reduce interaction, then the resulting 2-message argument is witness indistinguishable, and in the delayed-input setting it is distributional weak zero-knowledge (which implies strong witness indistinguishable and witness hiding in the delayed input setting). Moreover, under the same assumption (which can be instantiated from quasi-poly DDH/QR/N'th residuosity assumption), we construct a two-message argument with (similar) *statistical* secrecy guarantees. For the latter, we apply the PIR heuristic on a computationally sound proof, which is honest-verifier statistical zero-knowledge.

This is based on joint works with Abhishek Jain, Dakshita Khurana, Ron Rothblum and Amit Sahai.