Zero-Knowledge from MPC-in-the-Head: Constructions and Applications

Abstract:

MPC-in-the-head is a novel paradigm introduced in the work of Ishai et al. [IshaiKOS09] and, roughly speaking, allows the design of a zero-knowledge proof system for any NP-relation by relying on any multiparty computation (MPC) protocol in a modular way. On a high-level, in this transformation, the prover emulates "in-its-head" an execution of an MPC protocol that securely evaluates the NP-relation on the witness and commits to the views of the parties induced by this run. The verifier then tests the veracity of the computation by challenging the prover to open (decommit) the views of a subset of the parties. The key insight in the compilation is that the soundness and zero-knowledge property directly reduces to the robustness and simulation guarantees of the underlying MPC protocol.