Abstract:
We prove that finding a Nash equilibrium of a game is hard, assuming the existence of indistinguishability obfuscation and injective one-way functions with sub-exponential hardness. We do so by showing how these cryptographic primitives give rise to a hard computational problem that lies in the complexity class PPAD, for which finding Nash equilibrium is known to be complete. Previous proposals for basing PPAD-hardness on program obfuscation considered a strong "virtual black-box" notion that is subject to severe limitations and is unlikely to be realizable for the programs in question. In contrast, for indistinguishability obfuscation no such limitations are known, and recently, several candidate constructions of indistinguishability obfuscation were suggested based on different hardness assumptions on multilinear maps. Our result provides further evidence of the intractability of finding a Nash equilibrium, one that is extrinsic to the evidence presented so far. Joint work with Omer Paneth and Alon Rosen (http://eccc.hpi-web.de/report/2015/001/)