How to Delegate Computations: The Power of No-Signaling Proofs

Ran Raz, Weizmann Institute and IAS

The Martians built an amazingly fast computer and they run it to answer the great question of life, the universe and everything. They claim that the answer is 42. Will they be able to convince us that 42 is the right answer, assuming that we do not have sufficient computational power to run the computation ourselves, and that we do not trust Martians?

I will talk about multi-prover interactive proofs that are sound against all no-signaling (cheating) strategies, a model that was studied in relation to multi-prover interactive proofs with provers that share entangled quantum states, and is motivated by Einstein's principle that information cannot travel faster than light.

We show that every language in EXP has polynomial-time multi-prover interactive proofs that are sound against no-signaling strategies. I will explain how this is relevant to the problem of computation delegation, a central problem in modern cryptography, and to building trust with the Martians.

Joint work with Yael Tauman Kalai and Ron Rothblum