# Multi-Prover Interactive Proofs: How to Remove Intractability Assumptions

Michael Ben-Or
Shafi Goldwasser
Joe Kilian
Avi Wigderson

**Abstract**

Quite complex cryptographic machinery has been developed based on the assumption that one-way functions exist; yet we know of only a few possible such candidates. It is important at this time to find alternative foundations to the design of secure cryptography. We introduce a new model of generalized interactive proofs as a step in this direction. We prove that all $NP$ languages have perfect zero-knowledge proof-systems in this model, without making any intractability assumptions.

The generalized interactive-proof model consists of two computationally unbounded and untrusted provers, rather than one, who jointly agree on a strategy to convince the verifier of the truth of an assertion and then engage in a polynomial number of message exchanges with the verifier in their attempt to do so. To believe the validity of the assertion, the verifier must make sure that the two provers cannot communicate with each other during the course of the proof process. Thus, the complexity assumptions made in previous work, have been traded for a physical separation between the two provers.

We call this new model the multi-prover interactive-proof model, and examine its properties and applicability to cryptography.