Efficient Identification Schemes Using Two Prover Interactive Proofs

Michael Ben-Or
Shafi Goldwasser
Joe Kilian
Avi Wigderson

Abstract

We present two efficient identification schemes based on the difficulty of solving the subset sum problem and the circuit satisfiability problem. Both schemes use the two prover model introduced by [BGKW], where the verifier (e.g. the Bank) interacts with two untrusted provers (e.g. two bank identification cards) who have jointly agreed on a strategy to convince the verifier of their identity. To believe the validity of their identity proving procedure, the verifier must make sure that the two provers cannot communicate with each other during the course of the proof process. In addition to the simplicity and efficiency of the schemes, the resulting two prover interactive proofs can be shown to be perfect zero knowledge, making no intractability assumptions.