One-Way Functions are Essential for Non-Trivial Zero-Knowledge

Rafail Ostrovsky
Avi Wigderson

July 15, 2000

Abstract

It was known that if one-way functions exist, then there are zero-knowledge proofs for every language in $*PSPACE$*. We prove that unless very *weak* one-way functions exist, Zero-Knowledge proofs can be given only for languages in $*BPP$*. For average-case definitions of *BPP* we prove an analogue result under the assumption that *uniform* one-way functions do not exist.