Proofs that Yield Nothing but Their Validity or All Languages in NP have Zero-Knowledge

Oded Goldreich
Silvio Micali
Avi Wigderson

Abstract

In this paper the generality and wide applicability of Zero-knowledge proofs, a notion introduced by Goldwasser, Micali, and Rackoff is demonstrated. These are probabilistic and interactive proofs that, for the members of a language, efficiently demonstrate membership in the language without conveying any additional knowledge. All previously known zero-knowledge proofs were only for number-theoretic languages in $NP fl CONP$.

Under the assumption that secure encryption functions exist or by using “physical means for hiding information, ‘‘ it is shown that all languages in NP have zero-knowledge proofs. Loosely speaking, it is possible to demonstrate that a CNF formula is satisfiable without revealing any other property of the formula, in particular, without yielding neither a satisfying assignment nor properties such as whether there is a satisfying assignment in which $xl = X3$ etc.

It is also demonstrated that zero-knowledge proofs exist “outside the domain of cryptography and number theory. ” Using no assumptions. it is shown that both graph isomorphism and graph nonisomorphism have zero-knowledge interactive proofs. The mere existence of an interactive proof for graph nonisomorphism is interesting, since graph nonisomorphism is not known to be in NP and hence no efficient proofs were known before for demonstrating that two graphs are not isomorphic.