How to Play Any Mental Game

Oded Goldreich
Silvio Micali
Avi Wigderson

Abstract

We present a polynomial-time algorithm that, gives as an input the description of a game with incomplete information and any number of players, produces a protocol for playing the game that leaks no partial information, provided the majority of the players are honest.

Our algorithm automatically solves all the multi-party protocol problems addressed in complexity-based cryptography during the last 10 years. It actually is a *completeness theorem* for the class of distributed protocols with honest majority. Such completeness theorems are optimal in the sense that, if the majority of the players are not honest, some protocol problems have not efficient solution[C].