Zero Knowledge Proofs for Exact Cover and 0-1 Knapsack

Li Feng/Du

ABSTRACT
Zero Knowledge Proofs (ZKPs) are interactive protocols in which one party, named the prover, can convince the other party, named the verifier, that some assertion is true without revealing anything other than the fact that the assertion being proven is true. The remarkable property of being both convincing and yielding nothing except the assertion is indeed valid makes ZKPs very powerful tools for the design of secure cryptographic protocols and play an important role in complexity theory. Goldreich, Micali and Wigderson gave a ZKP for an NP-complete problem: Graph Three-colorability. One of fascinating aspects of complexity theory is that if any one of the problems in the class could been constructed an efficient solution, it could automatically obtain efficient solutions for the entire class. According to Karp's reduction, chromatic number, which is also known as the k coloring problem, can reduce to exact cover and exact cover can reduce to knapsack, which ensures that those two languages in NP have associated with ZKP systems correspondingly. In this paper, we design ZKPs for those two NP problems: exact cover and 0-1 knapsack.