The Ada Lovelace Bicentenary Lectures on Computability, December 2015 – January 2016

Michael Rabin (Harvard University)

Zero Knowledge Proofs and Applications

Tuesday, 19 January, 11:00-12:30

We shall present the surprising concept of Zero Knowledge Proofs. A Prover knows a solution to a problem. He proves the existence of a solution and his knowledge of it to a Verifier. This is done in a Zero Knowledge fashion. Namely, the Verifier is convinced of the truth of the above two statements but learns nothing about the solution or anything else. We shall explain in an easily understood way. We shall also present a simple novel method for ZKPs and give important practical applications. The lecture is self-contained and widely accessible.

Watch the video