Faculdade de Ciências da Universidade de Lisboa
cmafcio@fc.ul.pt Tel. (+351) 21 750 00 27

SEMINÁRIO DE LÓGICA MATEMÁTICA

Dia 29 de Outubro (segunda-feira), sala 6.2.33 às 16:00

Individual approach to witness hiding protocols

André Souto
(Universidade de Lisboa)

Abstract:
In protocols like witness hiding and zero knowledge, the two parties Prover and Verifier interact in such a way that the Prover can convince the Verifier of the possession of a secret without revealing the secret. The classical definition of these protocols uses extractors or simulators of the interaction with the intuitive meaning that if the communication can be simulated then no information is leaked. Unfortunately, the criteria used does not prevent that the randomness used is poor in a round of the protocol, in the sense that the instance produced may have a lot of information about the proof. In those cases, the Prover's secret is compromised.

Recently, we proposed a new way of looking at witness hiding based on the information conveyed in each particular instance of the protocol. We have introduced the concept of "individual witness hiding" (IWH) and prove that zero-knowledge protocols for classical problems, like Hamiltonian cycles in graphs, are not IWH. We explore the individual approach showing that one can use this approach to show that some classical problems can be adapted to be IWH that still have zero-knowledge relative to an oracle. These notions capitalize on Kolmogorov complexity, a characterization of information of strings, and on some of our previous work on this direction (Kolmogorov on-way functions and time bounded incompressibility reversed).

Seminário financiado por Fundos Nacionais através da FCT – Fundação para a Ciência e a Tecnologia no âmbito do projeto UID/MAT/04561/2013

Local: FCUL, C6 - Piso 2, 6.2.33