On information-theoretic definitions of protocol security

Jeroen van de Graaf
CENAPAD-MG/CO
Universidade Federal de Minas Gerais - UFMG
Av. Antônio Carlos, 6627, Prédio do ICEx, sala 2040
31270-010 Belo Horizonte (MG)
BRASIL

Abstract

In Chapter 2 of the author's thesis, various existing definitions of protocol security using information theory are reviewed, and an attempt is made to extend these definitions to protocols for general Two-Party Computation. However, this attemp fails for technical reasons, and the definition is dropped in favor of another approach, essentially Beaver's based on simulatability. However, the same thesis shows that if one uses quantum computing as the model of computation, then any definition of protocol security based in simulatability is doomed to fail, basically because the copying of quantum states is impossible. In this presentation, which is work in progress, we return to the issue of information theoretic or *black box* definitions of protocol security. Partly inspired by Jaynes interpretation of probability theory (who treats probability theory as an extension of logic), and also by Goldwasser and Micali's notion of sematical security, we give a new definition, and try to show its properties and merits.