Available online at www.sciencedirect.com
SCIENCE DIRECT®
Electronic Notes in Theoretical Computer Science
ELSEVIER
Electronic Notes in Theoretical Computer Science
www.elsevier.com/locate/entcs

Data independent verification of crypto-protocols

A.W. Roscoe, Philippa Broadfoot and Gavin Lowe

Abstract

It is only possible to model check very small implementations of cryptographic protocols (when measured by numbers of agents, nonces, etc.). It is highly desirable to have results which permit us to infer the security of much larger implementations from carefully-chosen small ones, and the specialised use of data independence provides one route to this type of result. I will report on the methods we use and some recent results and conjectures which provide generalisations.

10.1016/S1571-0661(05)80062-3