J Autom Reasoning (2012) 48:219–262
DOI 10.1007/s10817-010-9197-7

Computing Knowledge in Security Protocols Under Convergent Equational Theories

Ştefan Ciobâcă · Stéphanie Delaune · Steve Kremer

Received: 28 July 2010 / Accepted: 29 July 2010 / Published online: 1 September 2010

Abstract The analysis of security protocols requires reasoning about the knowledge an attacker acquires by eavesdropping on network traffic. In formal approaches, the messages exchanged over the network are modelled by a term algebra equipped with an equational theory axiomatising the properties of the cryptographic primitives (e.g. encryption, signature). In this context, two classical notions of knowledge, deducibility and indistinguishability, yield corresponding decision problems. We propose a procedure for both problems under arbitrary convergent equational theories. Since the underlying problems are undecidable we cannot guarantee termination. Nevertheless, our procedure terminates on a wide range of equational theories. In particular, we obtain a new decidability result for a theory we encountered when studying electronic voting protocols. We also provide a prototype implementation.

Keywords Formal methods · Security protocols · Static equivalence

1 Introduction

Cryptographic protocols are small distributed programs that use cryptographic primitives such as encryption and digital signatures to communicate securely over a network. It is essential to gain as much confidence as possible in their correctness.

This work has been partly supported by the ANR SeSur project AVOTÉ. A preliminary version of this work was presented in [17].

Ş. Ciobâcă · S. Delaune (✉) · S. Kremer
LSV, ENS Cachan & CNRS & INRIA Saclay Île-de-France,
61, avenue du Président Wilson,
94230 Cachan, France
e-mail: delaune@lsv.ens-cachan.fr