J Autom Reasoning (2012) 48:441–487
DOI 10.1007/s10817-010-9208-8

Decidability and Combination Results for Two Notions of Knowledge in Security Protocols

Véronique Cortier · Stéphanie Delaune

Received: 11 January 2009 / Accepted: 11 October 2010 / Published online: 28 October 2010

Abstract In formal approaches, messages sent over a network are usually modeled by terms together with an equational theory, axiomatizing the properties of the cryptographic functions (encryption, exclusive or, ...). The analysis of cryptographic protocols requires a precise understanding of the attacker knowledge. Two standard notions are usually considered: deducibility and indistinguishability. Those notions are well-studied and several decidability results already exist to deal with a variety of equational theories. Most of the existing results are dedicated to specific equational theories and only few results, especially in the case of indistinguishability, have been obtained for equational theories with associative and commutative properties (AC). In this paper, we show that existing decidability results can be easily combined for any disjoint equational theories: if the deducibility and indistinguishability relations are decidable for two disjoint theories, they are also decidable for their union. We also propose a general setting for solving deducibility and indistinguishability for an important class (called *monoidal*) of equational theories involving AC operators. As a consequence of these two results, new decidability and complexity results can be obtained for many relevant equational theories.

Keywords Formal methods · Security protocols · Equational theories

This work has been partly supported by the ANR-07-SESU-002 project AVOTÉ.

V. Cortier
LORIA, CNRS, Nancy, France
e-mail: cortier@loria.fr

S. Delaune (✉)
LSV, ENS de Cachan & CNRS & INRIA, 61 avenue du Président Wilson,
94235 Cachan Cedex, France
e-mail: delaune@lsv.ens-cachan.fr