J Autom Reasoning (2012) 48:135–158
DOI 10.1007/s10817-010-9205-y

Unification Modulo Homomorphic Encryption

Siva Anantharaman · Hai Lin · Christopher Lynch · Paliath Narendran · Michael Rusinowitch

Received: 25 August 2010 / Accepted: 31 August 2010 / Published online: 15 September 2010

Abstract Encryption 'distributing over pairs' is a technique employed in several cryptographic protocols. We show that unification is decidable for an equational theory HE specifying such an encryption. The method consists in transforming any given problem in such a way, that the resulting problem can be solved by combining a graph-based reasoning on its equations involving the homomorphisms, with a syntactic reasoning on its pairings. We show HE-unification to be NP-hard and in EXPTIME. We also indicate, briefly, how to extend HE-unification to Cap unification modulo HE, that can be used as a tool for modeling and analyzing cryptographic protocols where encryption follows the ECB mode, i.e., is done block-wise on messages.

Keywords Rewriting · Unification · Protocol analysis

Work supported by NSF Grants CNS-0831305 and CNS-0831209,
and partially supported by the FP7-ICT-2007-1 Project no. 216471, AVANTSSAR.

S. Anantharaman (✉)
LIFO, University of Orléans, Orléans, France
e-mail: siva@univ-orleans.fr

H. Lin · C. Lynch
Clarkson University, Potsdam, NY, USA

H. Lin
e-mail: linh@clarkson.edu

C. Lynch
e-mail: clynch@clarkson.edu

P. Narendran
University at Albany-SUNY, Albany, NY, USA
e-mail: dran@cs.albany.edu

M. Rusinowitch
Loria-INRIA Lorraine, Nancy, France
e-mail: rusi@loria.fr