J Autom Reasoning (2012) 48:263–292
DOI 10.1007/s10817-010-9199-5

Decidability of Equivalence of Symbolic Derivations

Yannick Chevalier · Michaël Rusinowitch

Received: 2 August 2010 / Accepted: 4 August 2010 / Published online: 21 August 2010

Abstract We give in this paper an alternative, and we believe simpler, proof of a deep result by Mathieu Baudet, namely that the equivalence of symbolic constraints is decidable for deduction systems on a finite signature modulo a subterm convergent equational theory.

Keywords Security protocol · Dolev–Yao model · Observational equivalence · Symbolic derivation · Subterm deduction system

1 Introduction

Context Security protocols are designed to provide communication means between several parties in a way that ensures that some information is protected. Well-known stories about flaw discoveries [18] have revealed that protocols may be subject to unexpected and undesirable behaviours under malevolent attackers actions. Formal analysis of protocols is therefore mandatory for gaining the level of confidence required in critical applications. Formal methods and related tools have proved to be successful to some extent for this task. But they are limited in expressiveness since in most cases authors were focused on the resolution of reachability problems, and as a consequence very few effective procedures consider the more general case of equivalence properties.

Y. Chevalier
IRIT, Université Paul Sabatier, 118 Route de Narbonne,
31062, Toulouse Cedex 9, France
e-mail: ychevali@irit.fr

M. Rusinowitch (✉)
Loria, Inria Nancy Grand Est, Campus Scientifique,
BP 239 54506, Vandœuvre-lès-Nancy, France
e-mail: rusi@loria.fr