J Autom Reasoning (2012) 48:133–134
DOI 10.1007/s10817-011-9242-1

Special Issue on Security and Rewriting Foreword

Hubert Comon-Lundh · Catherine Meadows

Received: 11 November 2011 / Accepted: 11 November 2011 / Published online: 30 November 2011

Rewriting theory is becoming of increasing interest to security researchers. Rewriting logic is a form of logic which has the advantage of being straightforward to automate, thus making it useful not only for specifying security properties of systems, but verifying that these properties hold.

One particular application in which rewriting is making important contributions is the verification of security protocols that are used to protect communication in networks. Security protocols are used now in more and more applications as the extent of our networked environment grows. Since the early 1980s, a growing effort has been put into the automated verification of such protocols. Following Dolev and Yao (1983), the most popular model of protocols relies on a representation of messages as terms: each cryptographic primitive is a function symbol. Variables usually represent parts of the messages that cannot be analysed, hence that could be replaced by an attacker who intercepts and forges new messages. That is why, since this area of research started, term unification plays an important role in the automated verification of security protocols.

Until ten years ago, only a few security primitives were considered. More recently, several other primitives were introduced, for instance exclusive or. For most examples, the free term algebra is too rough for a faithful abstraction of the cryptographic primitives. Thus it is necessary to require that the function symbols used in specifying the cryptosystems satisfy some algebraic properties: the messages are now member of a quotient term algebra. This quotient structure is specified by a set of equations. Many of these equations can be specified as rewrite rules, which allows us to bring rewriting theory to bear on the problem.

H. Comon-Lundh (✉)
LSV Ecole Normale Supérieure de Cachan, 61 Avenue du président Wilson,
94235, Cachan cedex, France
e-mail: comon@lsv.ens-cachan.fr

C. Meadows
Naval Research Laboratory, Washington, DC 20375, USA
e-mail: catherine.meadows@nrl.navy.mil

This is only one of the places where rewriting plays a central role. Rewriting can also be used to specify the actions which can take place in a secure system or protocol. Techniques from rewriting theory, such as narrowing, can then be used to verify security via symbolic execution.

This issue is dedicated to new results in term rewriting and unification, and their application to the automated verification of security protocols. In particular:

- S. Anantharaman et al. consider homomorphic encryption, which is used in several contexts (for instance some E-voting protocols). This primitive satisfies a distributive law, requiring a non-trivial rewriting system and reasoning modulo this rewriting theory.
- Security properties are often more complex than simple (non)-reachability properties. *Fair exchange* properties are considered by J. Guttman, who proposes an automated proof technique relying on a multiset rewriting computation model of the protocols.

Other important properties rely on the indistinguishability between two experiments: for instance anonymity can be stated as the indistinguishability between two instances of a protocol in which the identities have been switched. In this issue, there are three contributions to the automation of indistinguishability proofs:

- S. Kremer et al. propose some techniques for splitting the static equivalence problem (indinstinguishability in presence of a passive attacker) into simpler problems.
- S. Ciobaca et al. propose a technique for the computation of knowledge (that includes the static equivalence), for abitrary primitives. The technique is proven to be complete, although not always terminating.
- Y. Chevalier and M. Rusinowitch propose a decision procedure for the indistinguishability of bounded processes, for a class of subterm-convergent equational theories and an active attacker.

These contributions show that term rewriting techniques can be useful in automating the verification of security and, conversely that security raise new challenges in rewriting theory.

We believe that rewriting and security is emerging as an active area of research, with applications in the automated verification of protocols. This issue witnesses this claim.