Journal of Automata, Languages and Combinatorics **16** (2011) 2–4, 109–140

UNIFICATION OVER DISTRIBUTIVE EXPONENTIATION (SUB)THEORIES

SERDAR ERBATUR[1], ANDREW M. MARSHALL[1]
University at Albany – SUNY (USA)
e-mail: \tt\{se,marshall\}@cs.albany.edu

DEEPAK KAPUR[2]
University of New Mexico (USA)
e-mail: \ttkapur@cs.unm.edu

and

PALIATH NARENDRAN[1]
University at Albany – SUNY (USA)
e-mail: \ttdran@cs.albany.edu

ABSTRACT

Arithmetic operators are extensively used in cryptographic protocols. While a protocol using such operations may appear safe if semantic properties of these operations are not used by an intruder, the protocol can become vulnerable otherwise. Several such examples have been reported in the literature. The focus in this paper is on the modular exponentiation operator and its interaction with modular multiplication operators. Unification algorithms for theories involving exponentiation and multiplication operations play an important role in state exploration based approaches for finding attacks. This paper gives decidability results for unification problems for subtheories of exponentiation. The first property considered is the simplification of exponentiation when the exponent is an expression involving modular multiplication $\circledast$. The second property investigated is the simplification of exponentiation in which the base expression is expressed using yet another modular multiplication $*$. Extensions of these theories in which modular multiplication $\circledast$ is associative and/or commutative are investigated. The approach used for developing unification algorithms is novel and hierarchical, in the sense a unification algorithm for properties of the multiplication operator can be employed as a plug-in into the inference rules for unification derived from equational properties of exponentiation with multiplication operations. A table summarizing all known results about theories of exponentiation is included as well.

Keywords: Unification, Term Rewriting, Protocol Security

[1] Partially supported by the NSF grants CNS-0831209 and CNS-0905286
[2] Partially supported by the NSF grants CNS-0831462 and CNS-0905222