Journal of Automata, Languages and Combinatorics **16** (2011) 2–4, 75–90

STRING REWRITING AND SECURITY ANALYSIS: AN EXTENSION OF A RESULT OF BOOK AND OTTO

Siva Anantharaman
LIFO – Université d'Orléans (France)
e-mail: \ttsiva@univ-orleans.fr

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

and

Michael Rusinowitch
Loria – INRIA Nancy Grand Est (France)
e-mail: \ttrusi@loria.fr

ABSTRACT

In their seminal work Dolev and Yao used string rewriting to check protocol security against an active intruder. The main technical result and algorithm were improved by Book and Otto who formulated the security check in terms of an *extended word problem* for cancellation rules. We extend their main decidability result to a larger class of string rewrite systems called *opt-monadic* systems.

Keywords: String Rewriting, Regular Languages, Pushdown Automata, Protocol Security

1. Introduction

Cryptographic protocols define rules for exchanging in a secure way messages between agents called principals. They employ in general secret or public key cryptography techniques in order to protect network communications, and they can ensure for instance message secrecy (unauthorized principals cannot read it) or integrity (unauthorized principals cannot modify it). Alternative security properties such as authentication, non-repudiation, anonymity, have also been targeted by some cryptographic protocols. The difficulty of designing these protocols properly is well-understood: such systems should prevent intruders from exploiting passive eavesdropping but also user impersonation, message interception and modifications.

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