Abstract

The area of formal analysis of cryptographic protocols has been an active one since the mid 80's. The idea is to verify communication protocols that use encryption to guarantee secrecy and that use authentication of data to ensure security. Formal methods are used in protocol analysis to provide formal proofs of security, and to uncover bugs and security flaws that in some cases had remained unknown long after the original protocol publication, such as the case of the well known Needham-Schroeder Public Key (NSPK) protocol. In this thesis we tackle problems regarding the three main pillars of protocol verification: modelling capabilities, verifiable properties, and efficiency.

This thesis is devoted to investigate advanced features in the analysis of cryptographic protocols tailored to the Maude-NPA tool. This tool is a model-checker for cryptographic protocol analysis that allows for the incorporation of different equational theories and operates in the unbounded session model without the use of data or control abstraction.

An important contribution of this thesis is relative to theoretical aspects of protocol verification in Maude-NPA. First, we define a forwards operational semantics, using rewriting logic as the theoretical framework and the Maude programming language as tool support. This is the first time that a forwards rewriting-based semantics is given for Maude-NPA. Second, we also study the problem that arises in cryptographic protocol analysis when it is necessary to guarantee that certain terms generated during a state exploration are in normal form with respect to the protocol equational theory.

We also study techniques to extend Maude-NPA capabilities to support the verification of a wider class of protocols and security properties. First, we present a framework to specify and verify sequential protocol compositions in which one or more child protocols make use of infor-

mation obtained from running a parent protocol. Second, we present a theoretical framework to specify and verify protocol indistinguishability in Maude-NPA. This kind of properties aim to verify that an attacker cannot distinguish between two versions of a protocol: for example, one using one secret and one using another, as it happens in electronic voting protocols.

Finally, this thesis contributes to improve the efficiency of protocol verification in Maude-NPA. We define several techniques which drastically reduce the state space, and can often yield a finite state space, so that whether the desired security property holds or not can in fact be decided automatically, in spite of the general undecidability of such problems.