The Practice of Cryptographic Protocol Verification

Michael Rusinowitch [1,2]

LORIA-INRIA-Lorraine
615, rue du Jardin Botanique, BP 101,
54602 Villers les Nancy Cedex
France

Abstract

We present CASRUL, a compiler for cryptographic protocols specifications. Its purpose is to verify the executability of protocols and to translate them into rewrite rules that can be used by several kinds of automatic or semi-automatic tools for finding design flaws. We also present a related complexity results concerning the protocol insecurity problem for a finite number of sessions. We show the problem is in NP without assuming bounds on messages and with non-atomic encryption keys. We also explain that in order to build an attack with a fixed number of sessions the intruder needs only to forge messages of linear size, provided that they are represented as dags.

For more information:
`http://www.loria.fr/equipes/protheo/SOFTWARES/CASRUL/`.

Key words: Cryptographic protocols, verification, complexity, non-atomic keys, CASRUL.

[1] Email: `Michael.Rusinowitch@loria.fr`
[2] The author is partially supported by *ACI Cryptologie VERNAM.*