Model Checking Randomized Security Protocols

A. Prasad Sistla
University of Illinois at Chicago, USA
sistla@uic.edu

Abstract

The design of security protocols is extremely subtle and is prone to serious faults. Many tools for automatic analysis of such protocols have been developed. However, none of them have the ability to model protocols that use explicit randomization. Such randomized protocols are being increasingly used in systems to provide privacy and anonymity guarantees. In this talk we consider the problem of automatic verification of randomized security protocols. We consider verification of secrecy and indistinguishability properties under a powerful threat model of Dolev-Yao adversary. We present some complexity bounds on verification of these properties. We also describe practical algorithms for checking indistinguishability. These algorithms have been implemented in the tool SPAN and have been experimentally evaluated. The talk concludes with future challenges.

(Joint work with: Matt Bauer, Rohit Chadha and Mahesh Viswanathan)

2012 ACM Subject Classification Theory of computation → Logic and verification

Keywords and phrases Randomized Protocols, Verification

Digital Object Identifier 10.4230/LIPIcs.FSTTCS.2018.2

Category Invited Paper

38th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2018).
Editors: Sumit Ganguly and Paritosh Pandya; Article No. 2; pp. 2:1–2:1

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany