



Institute for Research in Fundamental Sciences
School of Computer Science

Operational and Epistemic Approaches to Protocol Analysis: Bridging the Gap

MohammadReza Mousavi
Eindhoven University of Technology
The Netherlands

Place: Hall 1, IPM, Niavaran, Shahid Bahonar Sq., Tehran, Iran

Date: August 4, 2010 (13 Mordad 1389), 16:00 - 17:30

Abstract:

Operational models of security protocols, on one hand, are readable and conveniently match their implementation (at a certain abstraction level). Epistemic models, on the other hand, are appropriate for specifying knowledge-related properties such as anonymity or secrecy. These two approaches to specification and verification have so far developed in parallel and one has either to define ad-hoc correctness criteria for the operational model or use complicated epistemic models to specify the operational behavior. We work towards bridging this gap by proposing a combined framework which allows for modeling the behavior of a protocol in a process language with an operational semantics and supports reasoning about properties expressed in a rich logic which combines temporal and epistemic operators.