SAT-Equiv: an efficient tool for equivalence properties

Véronique Cortier[1], Antoine Dallon[1,2], and Stéphanie Delaune[3]

[1] LORIA, CNRS, France
[2] LSV, CNRS & ENS Paris-Saclay, Université Paris-Saclay, France
[3] IRISA, CNRS, France

Automatic tools based on symbolic models have been successful in analyzing security protocols. Such tools are particularly adapted for trace properties (e.g. secrecy or authentication), while they often fail to analyse equivalence properties.

Equivalence properties can express a variety of security properties, including in particular privacy properties (vote privacy, anonymity, untraceability). Several decision procedures have already been proposed but the resulting tools are rather inefficient.

In this paper, we propose a novel algorithm, based on graph planning and SAT-solving, which significantly improves the efficiency of the analysis of equivalence properties. The resulting implementation, SAT-Equiv, can analyze several sessions where most tools have to stop after one or two sessions.