U LISBOA | UNIVERSIDADE DE LISBOA

CENTRO DE MATEMÁTICA E APLICAÇÕES FUNDAMENTAIS
Av. Prof. Gama Pinto 2, 1649-003 LISBOA, PORTUGAL Tel. (351) 217 904 700

Mês de: DEZEMBRO 2013

SEMINÁRIO DE LÓGICA MATEMÁTICA

Dia 12 de Dezembro (quinta-feira), às 15 horas, na Sala B3-01

LOGIC FOR SECURITY (aka KLEISTIC LOGIC)

Carlos Caleiro
(SQIG - Instituto de Telecomunicações & IST - Universidade de Lisboa)

Abstract:

Cryptographic protocols are widely used to provide secure communication over insecure networks, and much work is devoted to ensure their correctness. Symbolic approaches to this task have achieved significant success: based on them, several automated protocol verification tools have been implemented, and these have been successful in finding many protocol attacks. In this talk, we overview this exciting area of applied logic, covering the ground from the plain old Dolev-Yao intruder to computational indistinguishability, and from provable security to attack search. We highlight three of our own contributions to the field: (1) the use of distributed temporal logic as a metalevel tool for evaluating the correctness of simplification techniques used in protocol model-checkers; (2) the improvement of existing algorithms for security relevant problems in equational reasoning over the algebraic properties of cryptographic functions; and (3) the development of a symbolic probabilistic model of an attacker with cryptanalytical capabilities and its application to the analysis of offline guessing attacks.

Local:
INSTITUTO PARA A INVESTIGAÇÃO INTERDISCIPLINAR
Av. Prof. Gama Pinto, 2
1649-003 Lisboa