SEMINARIO

Departamento de Sistemas Informáticos y Computación

Facultad de Informática
Universidad Complutense de Madrid

11-5-2010

14:00
Sala de Grados
Facultad de Informática

Automated Certification of Code-Based Cryptographic Proofs

Gilles Barthe
IMDEA Software

Certicrypt is a framework that enables the machine-checked verification of cryptographic proofs using the Coq proof assistant. To date, CertiCrypt has been used to check the security of standard signature and encryption schemes, in particular the OAEP padding scheme. The talk will survey the design and applications of CertiCrypt, and will discuss ongoing work on the automation of cryptographic proofs.

****

Gilles Barthe received a Ph.D. degree in Mathematics from the University of Manchester, UK, and an Habilitation for Computer Science from the University of Nice, France.
He is currently a research professor at IMDEA Software.
His main research interests are formal methods, programming languages, software security, cryptography, and foundations of mathematics and computer science.
He has published over 80 refereed papers in these areas, and has been coordinator of many national and international projects, and of the FP6 FET integrated project "MOBIUS: Mobility, Ubiquity and Security" for enabling proof-carrying code for Java on mobile devices.
He is an editor of the Journal of Automated Reasoning.

Después de la presentación habrá un pequeño refrigerio en la Sala de reuniones.