Mathematics and CS Seminar

Computer-aided cryptography

Gilles Barthe
IMDEA Software Institute

Host: Krzysztof Pietrzak

We need cryptography that we can trust. Yet the design, analysis, and implementation of cryptographic libraries is a challenging task, that requires insights across various areas of mathematics and computer science. Computer-aided cryptography is a young research area which aims to provide methods based on formal methods, and in particular program synthesis and program verification for exploring the design space of cryptographic constructions and for building zero-defect cryptographic libraries. The talk will reflect on the challenges, benefits and opportunities for applying computer-aided formal methods in cryptography.

Thursday, June 7, 2018 09:00am - 10:00am
Mondi Seminar Room 2, Central Building

This invitation is valid as a ticket for the ISTA Shuttle from and to Heiligenstadt Station. Please find a schedule of the ISTA Shuttle on our webpage: https://ista.ac.at/en/campus/how-to-get-here/ The ISTA Shuttle bus is marked ISTA Shuttle (#142) and has the Institute Logo printed on the side.