Thesis defense

Michal Rybar's Thesis Defense: (The exact security of) Message Authentication Codes

Michal Rybar
IST Austria

Host: Sandra Siegert

Message authentication is one of the basic tasks in cryptography. Even though message authentication codes are around for decades, for many of them their exact security is not known. In the talk you will see two examples of algorithms where it was worth re-visiting their proofs of security. New proofs for these constructions will be explained, as well as new matching attacks. Together, they expose the true security of both constructions.

==========

Michal Rybár is a Ph.D. candidate in the Pietrzak group, working on message authentication codes and symmetric cryptography. He obtained his Master's degree from the University of Bristol in the United Kingdom, before he joined IST in 2012.

Friday, June 9, 2017 09:00am - 10:00am
Big Seminar room Ground floor / Office Bldg West (I21.EG.101)

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.