Mathematics and CS Seminar

Security of data encapsulation mechanisms in the multi-user setting

Federico Giacon
RUB Bochum

Host: Krzysztof Pietrzak

In practice, public key encryption (PKE) is routinely implemented by combining two cryptographic primitives: a key encapsulation mechanism
(KEM) and a data encapsulation mechanism (DEM). The known notion of multi-user security for PKE allows the adversary to query a challenge encryption oracle on related messages addressing different users. We extend this idea to multi-user security notions for KEMs and DEMs, which give rise to a very natural composition theorem. We then expand on the security of deterministic DEMs by studying their resilience against certain generic attacks. The effectiveness of the latter motivates our definition of an augmented data encapsulation mechanism
(ADEM): a DEM that takes besides key and message an additional "tag"
input for encapsulation. In the corresponding security model the tag is randomly picked during challenge encapsulation, and given to the adversary together with the ciphertext. To provide a better understanding of this principle we propose some ADEM constructions based on the CTR mode of operation using idealized primitives. We analyze the security of our schemes, as well as of standard DEMs, and relate them to each other.

Thursday, May 18, 2017 01:00pm - 02:00pm
Computer Science Room (I01.2OG.)

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.