Mathematics and CS Seminar

Subversion-resistant zero knowledge (Georg Fuchsbauer, ENS Paris)

Georg Fuchsbauer
ENS Paris

Host: Krzysztof Pietrzak

Motivated by the subversion of trusted public parameters in mass-surveillance activities, we study the security of non-interactive zero-knowledge (NIZK) proofs in the presence of a maliciously chosen common reference string. We provide definitions for subversion-resistant soundness and zero knowledge. After showing that subversion-soundness is impossible for NIZKs, we construct a subversion-ZK proof system.We then turn to ZK-SNARKs (succinct non-interactive arguments of knowledge), which are NIZK systems with short and efficiently verifiable proofs, used e.g. in cryptocurrencies such as Zcash. We show that under plausible hardness assumptions, many SNARK schemes proposed in the literature are subversion-ZK or can be made at very little cost.

Thursday, October 12, 2017 02:00pm - 03:30pm
Meeting room 2nd floor / Central Bldg. (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.