Mathematics and CS Seminar

Compactness in Cryptography

Giulio Malavolta
Simons Institute

Host: Krzysztof Pietrzak

The communication complexity of secure protocols is a fundamental question of the theory of computation and has important repercussions in the development of real-life systems. As an example, the recent surge in popularity of cryptocurrencies has been enabled and accompanied by advancements in the construction of more compact cryptographic machinery.In this talk we discuss how to meet the boundaries of compactness in cryptography and how to exploit succinct communication to construct systems with new surprising properties. Specifically, we consider the problem of computing functions on encrypted data: We show how to construct (i) homomorphic encryption schemes with optimal ciphertext expansion and (ii) time-lock puzzles where multiple puzzles can be compressed into a single one, containing only the function output. Then we survey the applications of these results along with the implication of cryptographic compactness in different contexts, such as proof systems and scalable blockchains.

Thursday, January 16, 2020 10:00am - 11:00am
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.