Institute colloquium

Institute Colloquium: Physical zero-knowledge

Moni Naor
Weizmann Institute

Host:

Zero-knowledge proofs are protocols that prove an assertion without revealing any information beyond that assertion s validity. Zero-knowledge proofs were first introduced by Goldwasser, Micali, and Rackoff in 1985.
The power of zero-knowledge proofs is quite remarkable: anything that can be proved efficiently can be proved with a zero-knowledge protocol, under the cryptographic assumption that one-way functions exist.
What happens when we move to physical properties? For instance, is it possible to prove that two DNA-fingerprints match, or that they do not match, without revealing any further information about the fingerprints? Is it possible to prove that two objects have the same design without revealing the design itself? Zero-knowledge is not as well-developed in the context of problems that are inherently physical.
In this talk I will describe the notion of zero-knowledge digital domain and then discuss recent work (with Ben Fisch and Daniel Freund, Crypto 2014) on protocols that prove physical properties of physical objects without revealing further information.

Monday, October 20, 2014 04:30pm - 05:30pm
Raiffeisen Lecture Hall, 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.