## Institute colloquium

# Institute Colloquium: Secure distributed computing - from theory to practice

**Ivan Bjerre Damgård**
Aarhus University

Host:

Secure distributed computation is a field in cryptography that has seen an amazing and extremely fast development in recent years. From pure theory in the late 80s to practically useful systems today, with performance improvements of several orders of magnitude over the last 5 years. The technology has very useful, but seemingly paradoxical properties: it allows a network of machines to compute on confidential data, even though none of them can actually look at the data. This has countless applications, including cloud security, auctions, electronic voting and many types of market designs in general. In this talk, I will introduce the basic idea and survey some of the techniques that have recently given us tremendous efficiency improvements.

**Monday, March 24, 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.