## Institute colloquium

# Lattices and cryptography: A match made in heaven

**Vinod Vaikuntanathan**
Massachusetts Institute of Technology

Host: Krzysztof Pietrzak

Integer Lattices are a formidable tool in mathematics and computer science, with numerous applications in number theory, coding theory and combinatorial optimization. Over the last three decades, lattices have proven themselves to be a veritable goldmine in the field of cryptography. In this talk, I will describe the evolution of lattices in cryptography -- from their early role as a powerful tool to break crypto-systems, their application in designing encryption and digital signature schemes with post-quantum security, and their triumph in the last decade in achieving long-anticipated cryptographic goals such as methods for computing on encrypted data.

**Monday, October 16, 2017 04:00pm - 05:00pm**
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.