Polynomial Commitments from Lattices

Ngoc Khanh Nguyen, King's College London

Abstract:
In this talk, we will consider more structured lattice-based commitment schemes, where the proof of knowledge of a valid opening admits fast (i.e., polylogarithmic in the message length) verification time. As an application, we will build a polynomial commitment scheme from the standard SIS assumption. This is based on joint work with Valerio Cini, Giulio Malavolta, and Hoeteck Wee (IACR CRYPTO 2024).

Biography:
Ngoc Khanh Nguyen is a Lecturer (Assistant Professor) in Cryptography in the Department of Informatics at King's College London. He was previously a postdoc at EPFL in Lausanne, Switzerland, hosted by Alessandro Chiesa. Khanh obtained his PhD at ETH Zurich and IBM Research Europe—Zurich. His main research interests are privacy-preserving cryptography and zero-knowledge proofs from lattice-based assumptions.