Exact Lattice-Based ZKPs

Ngoc Khanh Nguyen, King's College London

Abstract:
In this talk, we will discuss techniques to circumvent the obstacles from the previous talk and obtain "exact" zero-knowledge proofs from lattices. This will involve proving inner products (modulo q), integer relations, approximate range proofs, and product relations over the native ring. The talk is based on the joint work with Vadim Lyubashevsky and Maxime Plancon (IACR CRYPTO 2022).

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.