Abstract:
As the NIST competition on postquantum cryptography begins, it becomes increasingly important to understand not just the theoretical, black-box security of lattice-based schemes, but also the security of implementations. In this talk, we will discuss recent developments in this area, and particularly fault and side-channel attacks on lattice-based signatures, some of which involved interesting mathematical techniques.