Bern-Fribourg Graduate Seminar

a seminar for Master and PhD students

Thursday 2nd June, 2022: 17:15 - 18:00

Room B7, Exakte Wissenschaften, Bern

Audhild Høgåsen

University of Bern

Lattice-based cryptography for electronic voting

Abstract

An electronic voting system lets voters participate in an election from wherever they want, using their own devices. We present how to construct an electronic voting system with building blocks like encryption, commitments and zero-knowledge protocols, and we explain how the use of return codes can provide individual verifiability to the voters. We explain why quantum computers are not only a future threat of integrity of electronic voting systems, but also a threat of privacy of votes cast today. We present lattice-based building blocks that can be used to contruct a post-quantum secure cryptographic voting scheme.