Recent Advances and Challenges in Code-based Signatures

Violetta Weger

TU Munich

The National Institute of Standards and Technology (NIST) has recently announced that the standardization process for quantum-secure schemes will be reopened for digital signatures, with a particular interest in code-based schemes.

In this talk, I will present the two main approaches to obtain a code-based signature scheme, namely Hash-and-sign and through a zero-knowledge identification scheme, and discuss their respective strengths and weaknesses. Finally, we will look into some new improvements and open challenges.

Keywords: Code-based cryptography, signature scheme, post-quantum cryptography