Code-Based Cryptography - an Overview

Anna-Lena Horlemann-Trautmann

University of St. Gallen, Switzerland

In code-based cryptography we design asymmetric cryptosystems based on error-correcting codes. These cryptosystems are of great interest, because they are believed to be secure against attacks running on quantum computers - contrary to the currently used RSA and elliptic curve cryptosystems. We give an introduction to the topic and explain the basic ideas and design of code-based cryptosystems. Then we show that using other coding metrics than the classical Hamming metric can decrease the size of the public key, while achieving the same security level. Finally, we will explain some vulnerabilities and attacks on these systems, and pose some open questions for future research.

Faculty of Mathematics and Statistics, University of St. Gallen, Bodanstrasse 6, 9000 St. Gallen, Switzerland
anna-lena.horlemann@unisg.ch