Assistant Professorship of Coding for Communications and Data Storage
TUM Department of Electrical and Computer Engineering
Technical University of Munich

Forschungspraxis

LRPC Codes and Their Application to Cryptography

The realistic threat of a quantum supercomputer has motivated research on post-quantum cryptography. Assuming an attack of a sufficiently large quantum computer, several classical public-key algorithms as RSA become insecure since computationally intensive mathematical problems become easy-to-solve.

The National Institute of Standards and Technology (NIST) has therefore initiated a process to solicit, evaluate, and standardize quantum-resistant public-key cryptographic algorithms, where one promising candidate is based on Low Rank Parity Check (LRPC) codes.

The first task of this research internship is to understand and implement LRPC codes and their known decoding algorithms [1] in the computer algebra system SageMath. Then, existing cryptosystems based on LRPC codes should be investigated [2] and the security of new variants should be determined.

[1] https://arxiv.org/abs/1904.00357

[2] https://pqc-rollo.org/

Prerequisites

Basics of Channel Coding

Basics of Python Programming

Advisors

Thomas Jerkovits, Julian Renner
Hannes Bartz (Deutsches Zentrum für Luft und Raumfahrt)