Associate Professorship of Coding and Cryptography
TUM Department of Electrical and Computer Engineering
Technical University of Munich

Master's Thesis

Efficient Implementation of Decryption Algorithms in Rank-Based Cryptography

Many Rank-based cryptosystems require decoding of Gabidulin codes in their decryption algorithm. In this work, the student should compare the theoretical complexity of different Gabidulin code decoders. Based on the theoretical complexity analysis, the students should decide on the most promising decoding algorithms. Then, the algorithms should be implemented in C and their performance should be compared on a microcontroller.

Prerequisites

- Good knowledge about rank-metric codes (e.g. by taking the course Coding Theory for Storage and Networks)

- Good knowledge about cryptography (e.g. by taking the course Security in Communications and Storage)

- Very good knowledge of the Programming language C

Advisors

Julian Renner