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

Seminar

MRD Codes and Their Application to Code-Based Cryptography

Rank-matric codes are codes that live in a vector space that is endowed with a different metric than the Hamming metric: in the rank-metric the distance between two codewords, represented as matrices over a smaller field, is defined as the rank of their difference.

MRD codes are a special class of rank-metric codes that attain a bound analogous to the Singleton bound. They have interesting connections to many topics in discrete mathematics and have promissing applications to various code-based cryptosystems.

In this seminar work, the student will study the properties and construction of MRD codes, in particular Gabidulin codes, and one or more cryptosystems that are based on these codes. The goal is to understand and summarize parts of Ch. 2 & 3 of [1], and Ch. 3 & 4 of [2].

Main papers:

[1] H. Bartz, L. Holzbaur, H. Liu, S. Puchinger, J. Renner, A. Wachter-Zeh (2022). “Rank-Metric Codes and Their Applications”. arXiv: 2203.12384 https://arxiv.org/pdf/2203.12384.pdf

[2] K. Marshall, (2016). “A study of cryptographic systems based on Rank metric codes”, Dissertation, University of Zurich https://www.zora.uzh.ch/id/eprint/127105/1/Diss%20Kyle.pdf

Other recommended papers:

[3] T. Randrianarisoa, (2018). “Rank metric codes, codes using linear complexity and applications to public key cryptosystems”, Dissertation, University of Zurich
https://www.zora.uzh.ch/id/eprint/153545/1/153545.pdf

[4] E. Gorla (2019). “Rank-metric codes”. arXiv: 1902.02650 https://arxiv.org/pdf/1902.02650.pdf

[5] E. Gorla and A. Ravagnani. (2018). “Codes endowed with the rank metric”. In: Network Coding and Subspace Designs. Springer. 3–23.
https://link.springer.com/content/pdf/10.1007/978-3-319-70293-3.pdf

Prerequisites

- Proficiency in linear algebra
- Some knowledge of finite fields
- Some experience with coding theory

Advisors

Hugo Sauerbier Couvée