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

Forschungspraxis, Master's Thesis

Code-based Cryptography: Information Set Decoding

Due to the recent advances in quantum computers, the search for cryptosystems that survive quantum attacks is of great interest. Code-based cryptography is a promising candidate, since it is build on the NP-hard problem of decoding a random code [1].

In order to solve the generic decoding problem, algorithms from the information set decoding (ISD) family can be used.
During the last 60 years, small improvements to this approach were made.

Recently, new variants of the classical decoding problem were proposed [2,3,4].
This work adapts strategies for the classical problem to one of the new settings.
The goal is to develop decoding algorithms, analyse their complexity and do a (proof of concept) implementation.
There is also a webpage which provides instances that we can attempt to solve.

If you are interested, please write an email, then we'll discuss the details.

References:

[1] Weger, V., Gassner, N., & Rosenthal, J. (2022). A Survey on Code-Based Cryptography. arXiv preprint arXiv:2201.07119.

[2] Bricout, R., Chailloux, A., Debris-Alazard, T., & Lequesne, M. (2020). Ternary syndrome decoding with large weight. In Selected Areas in Cryptography–SAC 2019: 26th International Conference, Waterloo, ON, Canada, August 12–16, 2019, Revised Selected Papers 26 (pp. 437-466). Springer International Publishing.

[3] Weger, V., Khathuria, K., Horlemann, A. L., Battaglioni, M., Santini, P., & Persichetti, E. (2020). On the hardness of the Lee syndrome decoding problem. arXiv preprint arXiv:2002.12785.

[4] Baldi, M., Battaglioni, M., Chiaraluce, F., Horlemann-Trautmann, A. L., Persichetti, E., Santini, P., & Weger, V. (2020). A new path to code-based signatures via identification schemes with restricted errors. arXiv preprint arXiv:2008.06403.

Prerequisites

Channel coding

Security in Communications and Storage

Advisors

Sebastian Bitzer