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

Forschungspraxis

Solvers for the Code Equivalence Problem

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].

The McEliece cryptosystem is a promising candidate for asymmetric encryption.
However, many attempts at constructing a code-based signature scheme have resulted in impractical parameters or security problems.

NIST's announcement of a competetion dedicated to standardizing post-quantum signatures has lead to the publication of several new code-based schemes

In this work we consider LESS [2] a signature scheme based on the hardness of the code equivalence problem [3].
State-of-the-art solvers of the problem [4] are analysed and modifications are made to improve their performance.

References:

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

[2] Barenghi, A., Biasse, J. F., Persichetti, E., & Santini, P. (2021). LESS-FM: fine-tuning signatures from the code equivalence problem. In Post-Quantum Cryptography: 12th International Workshop, PQCrypto 2021, Daejeon, South Korea, July 20–22, 2021, Proceedings 12 (pp. 23-43). Springer International Publishing.

[3] Barenghi, A., Biasse, J. F., Persichetti, E., & Santini, P. (2022). On the computational hardness of the code equivalence problem in cryptography. Cryptology ePrint Archive.

[4] Beullens, W. (2021, July). Not enough LESS: An improved algorithm for solving code equivalence problems over F q. In Selected Areas in Cryptography: 27th International Conference, Halifax, NS, Canada (Virtual Event), October 21-23, 2020, Revised Selected Papers (pp. 387-403). Cham: Springer International Publishing.

Prerequisites

Channel coding

Security in Communications and Storage

Advisors

Sebastian Bitzer