Attacks on Code-Based Cryptosystems

Master's Thesis

To promote the standardization of post-quantum cryptosystems, the National Institute of Standards and Technology (NIST) has initiated a post-quantum cryptography competition in 2017. Among the submissions, there have been multiple code-based cryptosystems, e.g., Classic McEliece, BIKE, HQC, and more recently Fuleeca.

The student will be able to pick one type of attack and see if and how it can be applied to different code-based cryptosystems.

Scope of the Thesis

- **Either** understand how weak keys can be identified in the BIKE cryptosystem through the analysis of underlying Tanner graphs and then be used to attack BIKE [MM25] and investigate if this approach can be applied to other code-based cryptosystems or why this is not the case
- **Or** understand how lattices can be used to break code-based cryptosystems in the Lee metric [HW24; Hor+24] and investigate if this approach can be applied to other code-based cryptosystems or why this is not the case

Requirements

- Recommended background knowledge
  - Cryptography: basic knowledge about cryptosystems
  - Coding theory: We recommend the student to have visited the lecture "Codierungstheorie".
- Some affinity for linear algebra and interest in lattices
- Interest in the topic is strongly recommended

Contact

In case of interest or for further information, please contact Laurin Benz, `laurin.benz@kit.edu` (Room 251, Building 50.34) or Eva Hetzel, `eva.hetzel@kit.edu` (Room 250, Building 50.34).

References

[Hor+24] Anna-Lena Horlemann, Karan Khathuria, Marc Newman, Amin Sakzad, and Carlos Vela Cabello. "Lattice-based vulnerabilities in Lee metric post-quantum cryptosystems". In: *arXiv preprint arXiv:2409.16018* (2024).

[HW24] Felicitas Hörmann and Wessel van Woerden. "FuLeakage: breaking FuLeeca by learning attacks". In: *Annual International Cryptology Conference*. Springer. 2024, pp. 253–286.

[MM25] Gretchen L Matthews and Emily McMillon. "A combinatorial approach to avoiding weak keys in the BIKE cryptosystem". In: *Designs, Codes and Cryptography* (2025), pp. 1–24.