Generic Syndrome Decoding Problem and its application to Cryptography

André Chailloux, Simona Etinski

Syndrome Decoding problem is one of the central problems in coding theory as well as in code-based cryptography. The problem is known to be NP-complete and, for conveniently chosen parameters, exponentially hard for both classical and quantum algorithms. As such, it is proposed as a basis of classical protocols resistant to quantum attacks, i.e., post-quantum protocols. In the original version of a problem, we observe a binary code, described via its parity check matrix, a syndrome corresponding the errors occurred during transmission, and we know the number of errors occurred, i.e. their Hamming weight. The goal is then to find the errors and their positions.

In our work, we extended this problem to a more general case, where the code, syndrome and the errors are given over a general finite field. We are primarily interested in the non-binary finite fields and the weight of the errors that takes into account not only the number of errors occurred but also their relative contributions. Focusing on Lee weight function, we show the problem in this more general setting remains exponentially hard for conveniently chosen parameters for both classical and quantum algorithms. Moreover, we showed that the problem is harder in the Lee weight setting in comparison to the original Hamming weight setting. Our results are presented at PQCrypto2021, and the paper is available at arxiv.

After obtaining promising results for Lee weight version of a problem, we decided to use a generic version of syndrome decoding to create a signature scheme. The goal is to have a smaller signature size than the already existing schemes, which is their major drawback. Starting from a well analyzed Stern's identification scheme, we a constructed a signature scheme based on the generic version of a problem. To preserve a zero-knowledge property that guarantees no leak of information, we use a version of a problem named permuted kernel problem that asymptotically behaves the same as syndrome decoding problem. In this talk, we will give a brief description of the scheme and present the results on the reduced signature sizes. The talk will be given by Simona Etinski.