Master's Thesis

Decoding of Interleaved Codes

Interleaving is a decoding method that allows correcting burst errors beyond the unique decoding radius with reasonable complexity. It is already in use for improving the performance of Reed-Solomon codes in storage applications such as CD and DVD. However, for many codes it is unclear how to use interleaving to decode up to their designed minimum distance. This work will focus on codes with application to security, i.e., code-based cryptography. Here interleaving has the potential to increase the security level for a given key size.

Advisors

Julian Renner, Lukas Holzbaur