ulm university universität ulm

Bachelor/Master Thesis: Subfield Subcodes of One-Point Hermitian Codes

M.Sc. Cornelia Ott (cornelia.ott@uni-ulm.de), Institute of Communications Engineering

Introduction

When transmitting data over a channel, errors can occur due to noise on the channel. The task of channel coding is, to encode the message before transmitting by adding redundancy to the information, such that errors can be detected and corrected. This can be realized with different error correcting codes, e.g., one-point Hermitian codes wich belong to the class of algebraic geometry codes (AG codes).

Motivation

The security of the most public key cryptosystems relies on either the integer factorizing problem or on the discrete logarithm problem. In case a quantum computer would come to exist, these problems can be easily solved using Shor's Algorithm. Therefore the search for cryptosystems that are resistant to attacks by a quantum computer is becoming increasingly important, the so-called *Post-Quantum Cryptography*.
In the seventies R. J. McEliece introduced a public key cryptosystem [McE78] based on the problem of decoding a general linear error correcting code. At that time, this cryptosystem was not practical because it requires very large key sizes. But since the McEliece Cryptosystem is resistant to attacks by quantum computers it is now of great interest. The security of the McEliece Cryptosystem is dependent on the choice of the error correcting code. In [McE78] McEliece used binary goppa codes. Using these codes the system is unbroken up to now. In order to reduce the key size several alternative codes were used, e.g., AG codes, but most of them are broken by polynomial time attacks.
In [CMP17] a polynomial time algorithm is given which attacks the McEliece Cryptosystem based on AG codes (with arbitrary curves and genus). Subfield subcodes of AG codes are not affected and shall hence be studied within this thesis.

Task

The major part of the Masterthesis is to work out and summarize the necessary basics of one-point Hermitian codes using for example [Kam12] and to construct different examples of one-point Hermitian codes and their subfield subcodes. Furthermore an extensive literature recherche should be done in order to find out which codes are most suitable in the McEliece Cryptosystem.

Requirements

Interest in channel coding and cryptography.

Literature

[CMP17] A. Couvreur, I. Márquez-Corbella, and R. Pellikaan.
Cryptanalysis of McEliece Cryptosystem Based on Algebraic Geometry Codes and Their Subcodes.
IEEE Transactions on Information Theory, 63(8):5404–5418, Aug 2017.

[Kam12] Sabine Kampf.
Decoding Hermitian codes-an engineering approach.
PhD thesis, Universität Ulm, 2012.

[McE78] Robert J McEliece.
A public-key cryptosystem based on algebraic.
Coding Thv, 4244:114–116, 1978.