Information Set Decoding – An Attack On The McEliece Cryptosystem

Fabio Fürst

Master's thesis in Mathematics

In today's digital world, public-key cryptography is absolutely essential for ensuring cyber security. However, if one day it were possible to build powerful quantum computers, most of today's cryptosystems would be completely insecure due to quantum algorithms from Shor. For this reason, alternatives are being sought. Robert J. McEliece proposed such an alternative in 1978 – a code-based cryptosystem, which is believed to withstand quantum attacks. The present master's thesis presents this alternative and examines it. First, coding theory on which the McEliece cryptosystem is based is introduced. The system is then explained and analyzed. In particular, the currently best attacks on McEliece's cryptosystem are being studied in order to estimate its security. All these attacks are basically generic decoding algorithms for linear codes based on so called information set decoding. Finally, the advantages and disadvantages of McEliece's code-based encryption scheme are discussed. In summary, it can be said that the McEliece cryptosystem has the serious disadvantage that the size of the public key is extremely large compared to today's cryptosystems.

Supervisor: Prof. Dr. Elisa Gorla (University of Neuchâtel)
Co-supervisor: Prof. Dr. Emanuele Delucchi (University of Fribourg)