In this work an attack upon Wieschebrink's version of Niederreiter cryptosystem using GRS codes by Couvreur et. al. from 2014 is described.
Relevant notions of error-correcting code theory are presented, definitions of McEliece scheme, Niederreiter scheme and their respective Wieschebrink's modifications are shown.
A description of the attack using distinguisher as described by Couvreur et. al. Based on componentwise code products and shortened codes properties follows, as does Sidelnikov-Shestakov attack on Niederreiter scheme with relevant group theory notions.
Implementation details are also outlined.
The attack is then summarized and its complexity is mentioned.
The attack duration measured by the C++ implementation is presented in the last chapter.
The program implementing the cryptosystem as well as the attack is located in the appendix with the program documentation.