V práci je popsán útok na Wieschebrinkovu verzi Niederreterova kryptosystému využívajícího GRS kódy podle Couvreur et. al. z roku 2014.
Jsou zde definovány relevantní pojmy teorie samoopravných kódů, McEliecovo schéma, Niederreiterovo schéma a dále Wieschebrinkovy modifikace obou schémat.
Následuje popis samotného útoku obsahující distinguishera podle Couvreura et. al.
založeného na vlastnostech součinu kódů po složkách a vlastnostech zkrácených kódů.
Také je představen Sidelnikův-Šestakův útok na Niederreiterovo schéma a s ním spojené pojmy teorie grup a problémy implementace.
Útok je poté shrnut a je odhadnuta jeho časová složitost.
V poslední kapitole jsou uvedeny reálné časy útoků naměřené pomocí implementace v jazyce C++.
Přílohou práce je program včetně dokumentace, který implementuje kryptosystém i útok na něj.