Posudek vedoucího na bakalářskou práci
Terezy Hrubešové nazvanou
Klasický strukturální útok na Niederreiterův kryptosystém
vytvořený nad GRS kódy

Obsah práce vyplývá z názvu. Téma se ukázalo být pro bakalářskou práci vhodné a přiměřené. Studentka problematice porozuměla a postup Sidelnikova a Šestakova rozpracovala do míry podrobnosti, která ho činí přímočaře přístupným studentům bakalářského studia. Navíc postup autorů útoku ilustrovala na množství příkladů. V práci je též opraveno malé, ale relativně významné přehlédnutí týkající se složitosti jimi navrženého algoritmu. To, že si studentka chyby všimla, dosvědčuje, že problematiku si opravdu dobře osvojila. Po formální stránce je práce zcela v pořádku. Drobné výtky by formulovat možné bylo, ale zdá se mi, že za podrobnější rozvedení nestojí. Matematická úroveň plně odpovídá bakalářskému stupni a rovněž nemám výhrad. Pro studentku nebylo úplně jednoduché pochopit a formálně uchopit roli symetrie v útoku, takže jsem považoval za vhodné, aby práci začala popisem akce grupy a popisem struktury grupy lineárních lomených transformací. Tím myslím došlo k vhodnému propojení znalostí získaných v různých přednáškách bakalářského stupně.

Práce neobsahuje původní výsledky v užším slova smyslu. Její formální kvalita, netriviálnost tématu a pečlivost zpracování mě však vedou k návrhu, aby byla přijata jako práce bakalářská a hodnocena stupněm výborně. Jsem si vědom toho, že ve srovnání s pracemi, které skutečně přinášejí nové výsledky, se to může jevit jako příliš kladné hodnocení. Beru to ale tak. že se při návrhu hodnocení mám opírat především o dokument "Standardy bakalářských prací Matematika – Odborné obory". Mnou navržené hodnocení samozřejmě vychází z předpokladu, že i ústní projev při vlastní obhajobě bude mít odpovídající úroveň.

Aleš Drápal

V Praze 1. srpna 2014