OPONENTSKÝ POSUDEK BAKALÁŘSKÉ PRÁCE

Autor práce: Tereza Hrubešová
Název: Klasický strukturální útok na Niederreiterův kryptosystém vytvořený nad GRS kódy
Vedoucí: prof. RNDr. Aleš Drápal, CSc., DSc.

Předložená práce obsahuje podrobný popis Sidelnikovova-Šestakovova útoku na Niederreiterův kryptosystém nad zobecněnými Reed-Solomonovými kódy spolu s využívanými teoretickými nástroji.

Text je kromě sručného úvodu a závěru rozčleněn do čtyř kapitol. První dvě kapitoly shrnují potřebné teoretické zázemí, první z nich zavádí lineární lomené transformace jako prvky grupy přirozeně působící na projektivní přímku a druhá je věnována Reed-Solomonovým kódům. Zbylé dvě části prezentují popis samotného Niederreiterova kryptosystému a útok využívající působení grupy lineárních lomený transformací na projekci množiny řešení jisté polynomiální rovnice.

Přestože má pomerně obsáhlý text především kompilační charakter, jeho vytvoření vyžadovalo od studentky pochopení a zpracování matematicky značně netriviálních myšlenek, které jsou obvykle ilustrovány na samostatně vytvořených příkladech, čímž studentka zjevně prokázala schopnost samostatné práce i práce s odbornou literaturou. Výsledný text je dobře uspořádaný a přes jistou strohost čtivý (například Kapitola 1 by si ovšem podrobnější komentáře zasloužila). Množství překlepů a drobných nepřesností je vzhledem k rozsahu práce velmi malé.

Práce Terezy Hrubešové *Klasický strukturální útok na Niederreiterův kryptosystém vytvořený nad GRS kódy* podle mého názoru beze zbytku naplnila zadání a obsahuje netriviální vlastní příspevek, proto ji rozhodně doporučuji uznat jako bakalářskou.

v Praze 26.8.2014 Jan Žemlička