Posudek vedoucího na bakalářskou práci
Miroslava Homera nazvanou
Útok na Wieschebrinkovu verziu Niederreiterovho systému

Wieschbrink se pokusil zachránit použití GRS kódů v McEliece–Niederreiterově schématu přidáním náhodných sloupců do generující matice, která je součástí veřejného klíče. Nedávno Tillberg a jeho spolupracovníci publikovali několik významných článků, kterými vyzdvihli význam součinu kódů pro útoky na McEliece–Niederreiterovo schéma. Jednou (spíše vedlejší) aplikací je i rozbití Wieschbrinkova návrhu metodou testování dimenze čtverce propíchnutého kódu daného generující maticí veřejného klíče.

Pan Homer si vytkl za cíl celý tento útok popsat a naprogramovat. Nalezení oněch náhodných pozic ve vektorech kódu tvoří, z hlediska programování i popisu, jen část celého projektu. Značnou pozornost bylo třeba také věnovat již dříve popsanému útoku Sidelnikova a Šestakova, na který je popisovaný útok po odstranění náhodných sloupců redukován. Útok Sidelnikova a Šestakova je popsán na stranách 22–29 předkládané práce a opírá se o zpracování v bakalářské práci slečny Hrubešové. Ta ovšem programovou realizaci útoku neřešila. Výklad pana Homera je více algoritmicky orientován, a rozšiřuje rozsah parametrů, pro které lze útok provést. Nejde tedy o zcela přímočaré převzetí již zpracované látky.

Rozsah i kvalita práce naplňují a převyšují parametry kladené na bakalářskou práci. Je mi ovšem trochu líto, že se autorovi nepodařilo hlouběji proniknout do problematiky Hypotézy 3.3. Domnívám se, že její řešení není až tak obtížné, a že autoři článku, ve kterém je publikována jakožto experimentální fakt, se vážněji o její řešení nepokusili, protože v kontextu jejich článku šlo o věc okrajovou.

Práci jsem připomínkoval průběžně. Je pravděpodobné, že nějaké formální chyby lze v práci nalézt. Nebude jich však mnoho.

Navrhuji, aby práce byla přijata jako práce bakalářská a hodnocena stupněm *výborně*.

Aleš Drápal

V Praze 20. srpna 2015