POSUDOK OPONENTA NA DIPLOMOVÚ PRÁCU:

Martin Jureček
Útoky na bitově orientované proudové šifry obsahující LFSR

Predložená diplomová práca sa venuje analýze známych útokov na prúdovú šifru A5/1. Práca začína úvodom popisujúcim lineárne posuvné registre a šifru A5/1. Ďalšie kapitoly sa postupne venujú trom útokom na túto šifru.

Oproti prvej verzii diplomovej práce autor mimo iné vylepšil popis lineárnych posuvných registrov, zlepšil popis útoku od Golića a doplnil kapitolu o korelačných útokoch od Ekdahla a Johanssona. Práca je dobre čitateľná a z jazykovej stránky, s výnimkou anglického abstraktu, obsahuje len malé množstvo chýb.

Negatíva práce: Autor v práci používa značne neformálne vyjadrovanie. Na viacerých miestach práce je výklad nejasný - autor v popise útokov opakovane uvádza tvrdenia bez bližšieho zdôvodnenia alebo dôkazu. Pritom by často stačilo doplniť pár výrazov alebo viet na objasnenie. Autor opäť namiesto termínu "lineárne nezávislé rovnice" používa napríklad "lineárne a na sebe nezávislé rovnice" prípadne "navzájom nezávislé rovnice". V popise Golićovho útoku autor zisťuje počet získaných lineárne nezávislých rovníc (algoritmus 3.2, bod 4). V texte ale opakovane (napríklad str. 25, prvý odstavec, str. 28 prvý odstavec) výsledok považuje iba za celkový počet rovníc a nie počet lineárne nezávislých rovníc. Negatívne taktiež hodnotím fakt, že skoro každý z citovaných zdrojov má v zozname literatúry iný formát.

Na väčšinu tu uvedených nedostatkov bol už autor upozornený v predošlom posudku. V tom bol taktiež požiadaný o dôkladnú analýzu mechanizmu vzniku lineárne závislých rovníc. V predloženej práci ale autor uvádza iba príklady takýchto rovníc spolu s tvrdením, že mechanizmus ich vzniku "je nám neznámy".

Napriek týmto nedostatkom považujem doplnenie práce za dostatočné a *doporučujem* ju uznať ako diplomovú.

Praha, 13.9.2011 Michal Hojsík