Posudek vedoucího diplomové práce

Martin Jureček: Útoky na bitově orientované proudové šifry obsahující LFSR

Posuzovaná diplomová práce se zabývá studiem a implementací útoků na proudové šifry na bázi posuvných registrů s lineárními zpětnými vazbami. Její hlavní náplní je popis a implementace útoků na proudovou šifru A5/1.

Prvním z nich je základní verze Bihamovy Dunkelmanovy kryptoanalýzy založené na hledání tzv. „speciálních vnitřních stavů" šifry. Jde o velmi elegantní útok, který ovšem není náročný ani na pochopení ani na implementaci.

Proto za podstatné výsledky diplomové práce považuji implementaci Goličova útoku typu „rozděl a dobývej" a dále implementaci „korelačního útoku" podle Ekdahla a Johanssona na šifru A5/1.

Hlavní částí implementované varianty Goličova útoku je procházení stromu možností hodnot bitů vnitřního stavu šifry při průběžném přidávání lineárních rovnic do jejich aktuální soustavy. Zde narazil diplomant na problém spočívající v tom, že některé z přidávaných rovnic byly lineárně závislé na předchozích, v důsledku čehož byla výpočetní náročnost implementovaného algoritmu vyšší než u útoku hrubou silou.

Tento problém (a tudíž ani návrh jeho řešení) v Goličově článku nebyl zmíněn a pro diplomanta se stal vážnou překážkou v tom smyslu, že jeho implementace byly pomalejší než útok hrubou silou. Po značném úsilí se mu podařilo v literatuře najít a úspěšně aplikovat postup ze Sternovy a Porninovy varianty Goličova útoku spočívající v úpravách přidávaných rovnic tak, aby výsledná soustava byla připravena k eliminačnímu řešení. To vedlo k zásadnímu urychlení algoritmu.

Další podstatnou částí práce je implementace korelačního útoku Ekdahla a Johanssona na šifru A5/1. Jde o specifickou modifikaci korelačního útoku na případ šifry s nepravidelným krokováním. Útok proto obsahuje několik nestandardních kroků. Diplomant pracoval na této problematice zcela samostatně a teprve po dokončení práce mne požádal o konzultaci, v jejímž závěru jsem byl značně spokojen jak s jeho porozuměním řešené problematice, tak i s jeho zkušenostmi z provedené implementace.

Dotaz na diplomanta: Přepis vzorce (4.11) na vzorec (4.16) je na straně 43 uveden tak, jako by byl triviálně zřejmý. Jeho zdůvodnění je opravdu poměrně jednoduché, přesto se diplomanta pro upřesnění ptám:

- Jak je definována pravděpodobnost $p^{j}_{(t1,t2,t3)}$ na levé straně vztahu (4.16)?
- Jaké je pak korektní zdůvodnění platnosti (4.16) za předpokladu platnosti (4.11)?

Hodnocení diplomantovy práce
Posuzovaná diplomová práce včetně realizovaných implementací je výsledkem značného úsilí při řešení poměrně náročné problematiky. Diplomantovi evidentně podstatně více vyhovuje řešení dílčích problémů při implementaci již navržených algoritmů než teoretické rozbory. Přesto byl v průběhu práce nucen samostatně prostudovat a promyslet poměrně náročnou problematiku.

Závěrečné doporučení
Na základě výše uvedeného hodnocení a předpokladu správných odpovědí diplomanta na dotazy doporučuji diplomovou práci „Útoky na bitově orientované proudové šifry obsahující LFSR"

- PŘIJMOUT
- a hodnotit známkou:

Lipová-Lázně 12. 9. 2012
RNDr. B. Rudolf