POSUDOK OPONENTA NA DIPLOMOVÚ PRÁCU:
Lenka Mišániková
PSO-algoritmy a možnosti jejich využití v kryptoanalýze

Predložená diplomová práca sa venuje využitiu algoritmu PSO v kryptoanalýze. Práca začína úvodom a popisom spojitej a diskrétnej verzie optimalizačného algoritmu PSO. Nasleduje kapitola o aplikácii tohoto algoritmu na jednoduchú zámenu. Zvyšok práce sa venuje možnostiam využitia PSO pri útokoch na blokovú šifru DES. V kapitole 4 autorka popisuje priamy útok na DES s nižším počtom rúnd a ukazuje, že pomocou PSO bola schopná nájsť kľúč pre DES s dvomi rundami. Kapitoly 5 a 6 obsahujú popis diferenčnej kryptoanalýzy a využitia PSO na hľadanie diferenčnej cesty pre DES.

Z formálnej stránky práca obsahuje značné množstvo preklepov (napríklad na strane 33 sú až tri na jednom riadku) ako aj niekoľko chýb (napríklad vo Vete 9 na strane 48 sú E_j a E_j^* výstupy expanzie a nie vstupy do S-boxov). Inak je výklad prevažne jasný. Vytknúť by sa dalo, že v kapitole 5 chýba popis určenia kľúču pri diferenčnej kryptoanalýze šifry DES a koniec popisu určenia kľúču pri znalosti vstupnej a výstupnej diferencie S-Boxu je nejasný (prečo nastane situácia, že pri k trojiciach budeme mať práve 1 počítadlo s hodnotou k?). Kapitola 6 mohla byť viac rozpracovaná.

Celkovo diplomantka preukázala porozumenie študovanej problematiky. Mohla ale namiesto testovania rôznych variant PSO pre substitučnú šifru venovať viac pozornosti použitiu PSO algoritmu na útok na DES a hľadanie diferenčnej charakteristiky. Prípadne sa autorka mohla zaoberať použitím PSO na kryptoanalýzu ďalších šifier.

Práca obsahuje analýzu neúspechu útoku na DES pomocou PSO. Prosím, aby pri prezentácii diplomantka odpovedala na nasledujúcu otázku: Aké vlastnosti by mala mať bloková alebo prúdová šifra aby sa dal na nájdenie kľúča úspešne použiť algoritmus PSO?

Predloženú prácu doporučujem uznať ako diplomovú a hodnotiť ju známkou *velmi dobře*.

Praha, 10.5.2011 Michal Hojsík