Posudek vedoucího na diplomovou práci

## Lenka Mišániková, **PSO-algoritmy a možnosti jejich využití v kryptoanalýze**

Tématem předložené práce bylo prozkoumat možnosti využití jedné z moderních a populárních heuristik – particle swarm optimization, zkráceně PSO – v kryptoanalýze, zejména pak při hledání diferenčních cest. Je třeba předeslat, že jde o téma v literatuře dosud nepříliš zkoumané a jak se v průběhu práce ukázalo, také dosti náročné.

Po krátkém úvodu je ve druhé kapitole popsán algoritmus PSO původně navržený pro použití ve spojitém prostoru. Tento algoritmus se snaží optimalizovat hodnotu nějaké účelové funkce tak, že v prostoru všech možných řešení zvolí na počátku náhodně nějakou počáteční množinu, její prvky jsou nazývány částice, tyto částice spolu komunikují a snaží se vylepšit svoji polohu (tj. hodnotu účelové funkce) na základě znalosti svých předchozích poloh a také poloh částic ve svém okolí a hodnot jejich účelových funkcí. Každá částice se v každém kroku snaží změnit svoji polohu tak, aby zlepšila hodnotu účelové funkce.

Ve druhé kapitole jsou také uvedeny různé možnosti jak definovat  Jsou zde uvedeny různé možnosti jak definovat topologii částic a také jak upravit základní PSO algoritmus pro případ pohybu v diskrétním prostředí, což je také případ, kdy PSO aplikujeme v kryptoanalýze šifer, kdy prostorem všech možných řešení je prostor klíčů.

Ve třetí kapitole je zkoumána možnost aplikace PSO algoritmu na řešení jednoduché záměny. Tato kapitola je až příliš podrobná, moje hlavní výhrada spočívá v tom, že autorka zkoumala pouze variantu jednoduché záměny s abecedou o 27 znacích, kromě 26 písmen ještě navíc mezeru. Tato varianta jednoduché záměny je ještě jednodušší na řešení než obvyklejší varianta pouze s 26 písmeny. Při porovnání výsledků dosažených pomocí PSO s vásledky pomocí jiných heuristik v PhD disertaci A.J.Clarka mi schází sdělení, kterou variantu jednoduché záměny A.J.Clark zkoumal.

Ve čtvrté kapitola je podrobně popsána šifra DES a PSO aplikována přímo na nalezení klíče. Autorka podrobně a přesvědčivě vysvětluje obtíže přímé aplikace – není vůbec jasné, jak zvolit vhodnou účelovou funkci a na základě experimentů ukazuje, že maximální počet rund, pro které je možné doufat v úspěch PSO v prolomení DES je čtyři. Při obhajobě bych rád požádal o podrobnější vysvětlení obrázku 4.5 na str. 41. Chybí zde popis os a další údaje, které jsou pro pochopení těchto výsledků nutné.

Další kapitola je velmi stručný úvod do diferenciální kryptoanalýzy DES. Moje hlavní výhrada zde spočívá v neuvedení citace Stinsonovy knihy, ze které je celá část 5.1 převzata včetně značení.

V šesté kapitole je pak algoritmus PSO použit na hledání diferenčních cest s vysokou pravděpodobností pro jednu až pět rund DES.  K tomuto účelu bylo třeba provést řadu modifikací původního PSO algoritmu, aby bylo možné získat vůbec nějaké výsledky.

Moje hlavní připomínky k práci.

1. V práci je obrovské množství překlepů, autorka závěrečné redakci práce zjevně nevěnovala dost času.

2. Nedbalé formulace na řadě míst. Tak například nevím, jak rozumět výroku *„jednoduchá zámena zachováva nielen rozdelenie frekvencií jednotlivých znakov, ale a jich rozmiestnenie“* na str. 21, nebo použití výrazu *„odšifrovať 4-kolový DES“* ve smyslu „prolomit 4-kolový DES“.
3. Nekonzistentnost značení. Tak například na str. 22 aurotka oznámí, že nadále bude místo značení *gb* (globál best) používat *lb* (locl best), ale hned na str. 24 se opět *gb* objevuje.
4. Nedostatečné uvádění zdrojů.Opominutí Stinsonovy knihy v části 5.1. jsem už zmínil, stejně tak obrázky 5.1, 6.1 nebo 6.2 se zdají být převzaté z nějaké práce, ale zdroj u nich není uveden. Tyto problémy se vyskytují pouze v kapitolách 5 a 6, které byly psány až jako poslední.
5. Dosažené výsledky jsou popisovány pouze slovně v částech 4.3., 4.4 a kapitole 6 a lze je v podstatě považovat za sdělení, že toto autorka vyzkoušela a toto ji vyšlo, bez jakéhokoliv dalšího zdůvodnění nebo naznačení dalšího možného postupu.

Přes všechny tyto výhrady jsem vzhledem k obtížnosti tématu přesvědčen, že práci je možné přijmout jako práci diplomovou a navrhuji hodnotit ji známkou

Dne 11.5.2011

Doc. RNDr. Jiří Tůma, DrSc.