FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

Posudek na bakalářskou práci Jana Frnky

“Kryptografie na copánkových grupách”

Copánkové grupy si prožily svůj vzestup a pád v kryptografii v prvním desetiletí tohoto století. Postupně bylo navrženo několik protokolů založených na různých variantách problému konjugace, to stimulovalo rychlý rozvoj algoritmů pro počítání v copánkových grupách a výsledkem byl prudký pokles důvěry v jednosměrnost navržených funkcí. Práce velmi poctivě shrnuje prodělaný vývoj.

Téma je přesto aktuální: potřeba postkvantové kryptografie vyvolává duchy nejrůznějších zavržených principů a snaží se najít varianty, které by mohly posloužit návrhu nových jednosměrných funkcí. Jedno takové téma je představené v závěru: problém příslušnosti podgrupě.

Prvních cca 35 stran popisuje základní teorii copánkových grup s důrazem na výpočetní aspekty: normální forma slov, řešení problému slov (několik algoritmů různé síly), problém konjugace a jeho částečná řešení pomocí různých variant *summit sets*. Třetí kapitola se věnuje třem kryptografickým protokolům a útokům, které je částečně prolamují.

Práci považuji po obsahové i formální stránce za velmi zdařilou. Práce je kompilací mnoha zdrojů, převedení do jednotné terminologie a značení je povedené. Práce je zpracována velmi pečlivě, neobsahuje prakticky žádné překlepy.

Jednu připomínku mám k rozsahu. Není v možnostech oponentů pečlivě prostudovat padesát stránek textu, je tedy možné, že jsem nějaké podstatné chyby přehlédl; nicméně v těch částech, které jsem studoval podrobně, žádné chyby nebyly. Na druhou stranu, student pojal předhled výsledků velmi poctivě, jde o cenné shrnutí mnoha zdrojů se všemi podstatnými detaily a mnoha odkazy na doplňující informace. Z tohoto důvodu rozhodnutí podat práci (příliš) dlouhou respektuji a honotím ve výsledku kladně.

Drobné připomínky k textu:

- bylo by dobré někde zmínit (nebo i dokázat?), že centrum grupy B_n, je generované čtvercem fundamentálního copánku (využilo by se při diskusi centralizátorů);
- lepší vysvětlení by zasloužila poznámka na konci str. 13;
- podmínka (2) z Lemmatu 8 by možná posloužila jako přirozenější definice S(B);
- není mi jasné, jak může mít algoritmus polynomiální časovou a exponenciální prostorovou složitost (sekce 2.1.3 na začátku);
- u *subgroup membership* není a priori jasné, jak je podgrupa zadaná;
- str. 39 nahoře: co je parametr *p*?

Department of Algebra
Sokolovská 49/83, 186 75 Praha 8, Czech Republic
ka@karlin.mff.cuni.cz
+420 95155 3242

- prezentace sekce 3.1.2 by mohla být promyšlenější, např nevím, proč se přeznačuje grupová operace, o zobrazení *d* bychom mohli mluvit jako o homomorfismu,
- str. 42 nahoře: pokud mám více informací na vstupu, neznamená to a priori komplikaci, ta informace by mohla jít nějak využít
- proč je v Algoritmu 6 rozsah *i* od -5 do 5 ?
- str. 45, poslední odstavec před nadpisem: není mi úplně jasné, jaké jsou výsledky experimentu, znamená to, že Gebhardtův algoritmus prolomí CSP vždy?
- str. 50 uprostřed, určení vzoru matice asi nebude nemožné, jen (díky neprostosti zobrazení) není ten vzor jednoznačný a například konjugace v obrazu nemusí znamenat konjugaci ve vzoru;
- sekce 3.3, návrh vlastního protokolu: pokus o návrh cením, ale není mi jasné, jak spočítat generátory centralizátoru *C(b),* navíc celkem přirozeně by se mezi těmito generátory měl vyskytovat sám prvek *b*, což je problém; v druhém bodě algoritmu na str. 51 je zřejmě překlep, má být B_n *mínus C(b)*, jinak by nefungoval test na nenáležení centralizátoru.

Komplexnější připomínku mám k prezentaci složitosti diskutovaných algoritmů. Chybí mi nějaký přehled, které parametry jsou pro který algoritmus podstatné, souhrnná diskuse časové vs. prostorové složitosti. Tato fakta jsou uvedena u každého algoritmu, ale ne systematicky, čtenář tak poněkud tápe v tom, které parametry jsou pro který problém kritické. U útoků pak není vždy jasně popsané, s jakou pravděpodobností algoritmy fungují, co jsou kritické paramtery a kde jsou složitostní limity. To je asi jediné místo v práci, kde by diskuse mohla být podrobnější.

Žádný z popsaných problémů není podstatný, s prací jsem celkově velmi spokojen a doporučuji ji k obhajobě.

David Stanovský
oponent