Posudek oponenta bakalářské práce

Název: Multilineární zobrazení nad celými čísly
Autor: František Havránek

Shrnutí obsahu práce

Práce podává podrobný a srozumitelný popis schématu navrženého autory Coronem, Lepointem a Tibouchim, které s využitím multilineárních zobrazení nad $\mathbb{Z}$ umožňuje dohodu více účastníků na bezpečném klíči během nezabezpečené komunikace. Jedná se o rešerši celkem sofistikovaného článku (přesněji vlastně dvou článků), kde ovšem student doplnil spoustu chybějících detailů, včetně klíčových odhadů změny velikosti šumu kódových slov při rozličných transformacích, které je nutno s těmito slovy provádět. Je pravda, že pár drobností — jako např. konstrukce matice H a čísel α_i, β_i v sekci 4.2 — v práci nakonec rozvedeno není, ale vzhledem k již tak lehce nadstandardnímu rozsahu to považuji za pochopitelné.

Celkové hodnocení práce

Téma práce. Téma se mi jeví jako přiměřené pro bakalářskou práci, byť relativně náročnější vzhledem k množství technikálií (uhlídání odhadů různých parametrů apod.), s nimiž se student musel potýkat. Je třeba obratem dodat, že se pan Havránek se všemi nástrahami vypořádal velice dobře. Ve vlastním zpracování tématu se bohužel nakonec nedostalo na kryptoanalýzu, čímž nebylo cele naplněno zadání práce. Vzhledem k náročnosti popisné části bych tento nedostatek ovšem nepovažoval za nikterak zásadní.

Vlastní příspěvek. Za významný autorův příspěvek považuji doplnění mnoha detailů na místech, která byla ve zdrojových článcích pojednána příliš kuse či prakticky vůbec. Celkově se mu povedlo podat téma velmi srozumitelně a přístupně pro čtenáře–matematika.

Matematická úroveň. Matematická úroveň práce je velice dobrá. Z textu je patrné, že student podávané problematice skutečně porozuměl. Vyzdvihl bych, že hlavní náplní práce jsou skutečně **matematické** metody a nejedná se ani v nejmenším o inženýrský text o jisté oblasti informační bezpečnosti, jak tomu občas bývá. Zásadní výtku bych ovšem měl k nešvaru zamlčet tu a tam ve znění tvrzení nějaký předpoklad, který se později vyjeví v průběhu dokazování jako dodatečná podmínka, již je nutno uvažovat, aby vše fungovalo, jak má. Tuto praxi z kryptologie chápu, ale v konečném důsledku vede k tomu, že — přísně vzato — tvrzení tak, jak je formulováno, neplatí. Jako příklad uvádím Tvrzení 2.3 a Tvrzení 4.4 a poznámky za nimi připojené. Nakonec: trochu jsem postrádal nějakou motivaci před Tvrzením 2.4, v níž by se osvětlily jeho předpoklady, konkrétně např. $k + l \leq \kappa$.

Práce se zdroji. Zdroje jsou správně citovány. Nejsem si vědom, že by práce obsahovala (netriviální) otrocky přeložené pasáže.

Formální úprava. Formální úprava práce je vynikající. Zde lze stěží co vytknout. Text je velmi pěkně strukturován, stylisticky bez větších prohřešků a obsahuje naprosté minimum překlepů.

Připomínky a otázky

1. V poznámce na straně 13 se uvádí, že kódové slovo c_1 je prvním redukovaným slovem. Nemá být správně $\hat{c}_1$?

2. Co znamená ϖ_{j_i} na posledním řádku důkazu Tvrzení 3.2 a odkaz [CLT15] na prvním řádku důkazu Tvrzení 3.3?

3. Podle čeho volí nezávislá autorita číslo n? Kromě řádově rozdílné bitové délky mezi (po dvou různými) prvočísly g_i a p_i, $i = 1, \ldots, n$, jsou ještě nějaká omezení na jejich vzájemné vztahy?

Závěr

Práci považuji za vynikající a **doporučuji** ji **uznat** jako bakalářskou práci.

Mgr. Jan Šaroch, Ph.D.
Katedra algebry MFF UK
V Praze dne 5. září 2018.