Posudek oponenta bakalářské práce

Název: Bezpečnost šifrování zpráv závisejících na klíči
Autorka: Kristina Hostáková

Shrnutí obsahu práce

Práce se zabývá šifrovacími schématy, která jsou bezpečná i v případě, že šifrujeme zprávy, které jsou funkcí tajného klíče. Dvě taková schémata práce rozebírá a dokazuje jejich bezpečnost (za předpokladu, že jistý mřížový problém je těžký). Jedná se o zajímavé a důležité téma, které kombinuje lineární algebru, teorii pravděpodobnosti, a dokonce dojde i na samoopravné kódy.

Celkové hodnocení práce

Téma práce. Téma je přiměřeně náročné. Jsem přesvědčený, že autorka zadání splnila.

Vlastní příspěvek. Vlastní příspěvek spočívá v kompilaci informací z několika článků a doplnění detailů důkazů bezpečnosti schémat. Příspěvek je přiměřený.

Matematická úroveň. Výsledky jsou matematicky korektní a na dobré úrovni. Výjimkou je důkaz lemmatu 15, který obsahuje jistou mezeru (viz níže).

Bohužel si zkoumaná šifrovací schémata vyžadují mnoho výpočtů a podat je čtivně není snadné. Důkazová část práce tak trpí obtížnou stravitelností, což je také má hlavní výtka.

Především bych ocenil v důkazech lepší rozlišení technických podrobností od důležitých konstrukcí – občas není pro stromy vidět les. Dále velké množství nových proměnných zavedených v textu znamená, že hlavní část práce nelze číst bez častého listování dopředu a zpět. Situaci ještě zhoršuje to, že se vedle sebe někdy vyskytují například různé proměnné označené $\mathbf{b}_i$, $\overline{\mathbf{b}_i}$ a b (str. 26).

Práce se zdroji. Na dvou místech mi chybí citace pro používaná tvrzení: Ocenil bych informaci, kde se v literatuře nachází důkaz Lemmatu 27 a ze kterého zdroje pochází dolní mez pro parametr α ve vzorci (4.1) na str. 20.

Mimo těchto dvou kazů je autorčina práce se zdroji velmi dobrá.

Formální úprava. Jsem všeobecně spokojený s jazykovou i typografickou úpravou. Nalezl jsem několik drobných překlepů a pár stylisticky problematických míst (viz níže), ale vzhledem k rozsahu práce je obého obdivuhodně málo.

Připomínky a otázky

1. Str. 2: V úvodu ve třetím odstavci bych se přimlouval za omezení trpného rodu.
2. Str. 7: Na první pohled není jasné, jak spočteme integrál v důkazu tvrzení 5. V zájmu čtenářského pohodlí by se slušelo říci, že použijeme per partes.
3. V důkazu lemmatu 15 (KDM bezpečnost na konstantní funkce implikuje IND-CPA bezpečnost) je potřeba se při převodu útočníků vyrovnat s tím, že náhodný šifrový text ve hrách pro IND-CPA a KDM bezpečnost vzniká pokaždé jinak – v jednom případě jde o zašifrovaný náhodný otevřený text, ve druhém případě o zašifrovaný řetězec nul. Bohužel o této potíži důkaz mlčí.

4. Z hlediska lepšího porozumění mi přijde užitečné už při zavedení problému Learning With Errors (LWE) rovnou zmínit, že jde vlastně o zašumělou soustavu lineárních rovnic.

5. Osobně se mi stylisticky nelíbí formulace „Přes volbu $X \leftarrow D$ je s velkou pravděpodobností [tvrzení],“ kde D je pravděpodobnostní rozdělení (lemmata 32, 33, 34 a 35). Oč jde, jsem pochopil, až když jsem si text přeložil do angličtiny. Přijde mi lepší psát klasicky „Buď $X \leftarrow D$ náhodná proměnná. Potom skoro jistě [tvrzení].“ Nemohu ale vyloučit, že se „přes volbu“ v české kryptografické literatuře bežně používá a já o tom nevím.

6. Str. 26 v rovnici (4.16) je, myslím, špatně znaménko ve formuli

$$\bar{b}_i = s_i - \bar{A}_i^T s,$$

   správně by tu mělo být

$$\bar{b}_i = s_i + \bar{A}_i^T s.$$

   Naštěstí tato chyba nezmění výsledek dalších kalkulací.

7. Na str. 33 na 5. řádku ve vzorečku pro $T_0(y)$ chybí uzavírací závorka.

8. Str. 36, řádek 5: Překlep v pádě „ve většině vědeckých článcích“.

Závěr

Práce je solidní, ovšem náročná na pochopení a lemmata 15 a 27 nejsou dostatečně dokázaná (v prvním případě je v důkaze mezera, ve druhém je důkaz plně ponechán na čtenáři). Přes tyto výtky práci považuji za velmi dobrou a doporučuji ji **uznat** jako bakalářskou práci.

Návrh klasifikace oponent sdělí předsedovi zkušební subkomise.

Alexandr Kazda
Department of Mathematics
Vanderbilt University
Nashville, USA
30. srpna 2013