Posudek vedoucího bakalářské práce

Název: Multilineární zobrazení nad celými čísly
Autor: František Havránek

Shrnutí obsahu práce

Text Františka Havránka prezentuje návrh kryptografického protokolu publikovaný v nedávných článcích J.-S. Corona, T. Lepointa a M. Tibouchiho. Konstrukce založená na Diffie-Hellmanovu schématu sdíleného tajemství jako základní stavební kámen využívá multilineární zobrazení nad celými čísly. Práce je rozčleněna kromě úvodu a závěru na čtyři části. První kapitola zavádí potřebnou terminologii spolu s ověřením jejích vlastností, především jde o klíčové pojmy kódu úrovně k a délky šumu. Druhá část se věnuje problému redukce kódových slov, která umožňuje ponechat modul uvažovaných hodnot mezi tajnými parametry, a třetí kapitola popisuje proces znáhodnění kódu, jenž zabezpečuje dobré kryptografické vlastnosti schématu. Nejrozsáhlejší závěrečná část se zabývá centrální otázkou protokolu, jíž je získání společného klíče.

Celkové hodnocení práce

Téma práce. Téma práce bylo kompilační, od studenta vyžadovalo především porozumění nepříliš čtenářsky přívětivě napsaného článku a jeho následné zpracování a doplnění do srozumitelného a korektního matematického textu. Zadání bylo podle mého mínění vhodné pro obor Matematické metody informační bezpečnost a bylo studentem v zásadě naplněno.

Vlastní příspěvek. Primárním zdrojem práce byl článek, který opravoval prolomenou verzi kryptosystému navrženého týmiž autory. Student tudíž pracoval s partiemi dvou statí, které doplnil o řadu detailů i pojmů a matematicky je upřesnil. Nejvýraznějším přínosem textu je zavedení množin $C^k_\rho(m)$, které studentovi umožnily korektní uchopení uzávěrových vlastností kódů úrovně k slova m pro danou délku šumu, které jsou klíčové pro prezentované schéma.

Matematická úroveň. Matematická úroveň práce je podle mého mínění velmi dobrá a formulace jsou vesměs korektní.

Práce se zdroji. Ačkoli je práce kompilací, která v podstatě sleduje strukturu hlavního zpracovávaného článku, díky rozšíření terminologie a doplnění argumentace a není výsledný text na zdrojích zásadně formulačně závislý.

Formální úprava. Po formální stránce se textu nedá mnoho vytknout, jazykových a stylistických nepřesností je v textu množství přiměřené jeho rozsahu.

Připomínky a otázky

S připomínkami a otázkami, které jsem vznášel průběžně k pracovním verzím práce, se student úspěšně vyrovnal a ve finálním textu už jsem významnější nedostatky nepostřehl.

Závěr

Práce Františka Havránka *Multilineární zobrazení nad celými čísly* podle mého názoru splnila zadání a doporučuji ji uznat jako bakalářskou.

Návrh klasifikace vedoucí práce sdělí předsedovi zkušební (sub)komise.

Jan Žemlička
Katedra algebry
5.9.2018