Posudek vedoucího bakalářské práce

Název: Kryptografie na copánkových grupách
Autor: Jan Frnka

Shrnutí obsahu práce

Práce se zabývá kryptografií na copánkových grupách. V první kapitole jsou představeny základní definice, tvrzení a prostředky pro popis kryptografických schémat a útoků na ně. Na ty navazuje popis problémů, na kterých jsou postaveny „trapdoor“ funkce používané v odvozených schématech – především „word problem“ postavený na problematice nejednoznačnosti zápisu copánků a „conjugacy problem“, kde slevíme z požadavku identity na ekvivalenci danou konjugací. Třetí kapitola se již věnuje kryptosystémům postaveným na copánkových grupách od obecných schémat po schémata specifická pro copánkové grupy. Následně jsou na tato schémata popsány útoky. Z počátku se práce věnuje útokům postavených na nástrojích z předchozích teoretických a popisných kapitol. Následně se dostává i k útokům využívající specifičnosti klíčů kryptografických schémat (délkový útok) a obecnému útoku za pomocí reprezentací. V závěru kapitoly se student věnuje dalším potenciálním „trapdoor“ funkcím a navrhuje schémata, která by z nich šla sestavit.

Celkové hodnocení práce

Téma práce. Téma práce bylo na bakalářskou práci zvoleno spíše náročné. Požadovaná literatura a materiály trpěly značnou nekonzistencí v dokazovacím aparátu. Student se s tímto problémem dokázal vypořádat, zadání práce bylo jednoznačně naplněno.

Vlastní příspěvek Vlastní příspěvek studenta je na několika úrovních. Práce si vyžádala mnoha kompromisů na úrovni dokazovacího aparátu, kdy student zvolil kompromis mezi formalistickým algebraickým přístupem a intuitivistickým geometrickým přístupem za účelem dobré čtivosti práce při zachování požadované úrovně formalismu. Student se dále zabývá dalšími potenciálními cestami pro konstrukci kryptografických schémat postavených na dalších možných „trapdoor“ funkcích nad copánkovými grupami.

Matematická úroveň Práce obsahuje rigorózně zformulovaný matematický text v průběhu většiny kapitol. Matematická úroveň práce je nadprůměrná vzhledem k tématu z oblasti aplikované matematiky (kryptografie).

Práce se zdroji Student si vypůjčuje mnohé definice, především v kompilační části práce. Při přechodu do dokazovací části se již student často odchyluje od primárních zdrojů právě za účelem vyvážení formalismu a přístupnosti tématu pro čtenáře z aplikovaných oborů.

Formální úprava Formální úprava je na velmi dobré úrovni. Práce je psaná kvalitní češtinou s důrazem na dobrou čtivost této práce.

Závěr

Práce Jana Frnky „Kryptografie na copánkových grupách“ splňuje zadání a dosahuje požadované úrovně. Proto práci doporučuji k přijetí s hodnocením *výborně*.

Adolf Středa
Katedra algebry
12.6.2024