Oponentský posudek diplomové práce

Autor práce: Aleš Fuchs
Název: Aplikace Gröbnerových bází v kryptografii
Vedoucí: Jan Šťovíček

Předkládaná práce představuje stručný souhrn využití komutativní i nekomutativní teorie Gröbnerových bází v kryptografii, konkrétně pro konstrukci asymetrického kryptosystému Poly Cracker.

Práce je rozdělena do pěti kapitol. Po úvodu je v druhé části stručně, bez důkazů prezentována klasické teorie Gröbnerových bází okruhu polynomů konečně mnoha komutujících neurčitých nad tělesem. Následující obsáhlá kapitola je věnována budování teorie Gröbnerových bází ve volné nekomutativní algebře nad tělesem. Předposlední, stěžejní kapitola se zabývá popisem a kryptoanalýzou komutativní a nekomutativní verze kryptosystému Poly Cracker, který je na teorii Gröbnerových bází založen. Součástí kapiotoly je ilustrace fungování kryptosystému na několika příkladech spolu s popisem útoků a ochraných opatření. V závěrečné části je kromě shrnutí dosažených cílů naznačen další možný směr výzkumu.

Práce je napsána přístupným stylem a vzhledem k rozsahu obsahuje text jen minimum věcných a jazykových nedostatků či nepřesností (např: *uspořádání* zavedené v Poznámce 2.1.3 je spíše pseudouspořádání, symbol *Span* z kapitoly 3 pro podprostor vektorového prostoru generovaný množinou není zaveden, okruh R v definici 4.2.4 není specifikován). Ačkoli je práce v souladu se zadáním z podstatné části kompilační, téma od autora vyžadovalo prostudování rozsáhlého souboru literatury. Jeho zpracování do podoby čtivého a dobře srozumitelného textu se zdařilo především v kapitole věnované nekomutativním volným algebrám. Část zabývající se kryptosystému Poly Cracker je v tomto ohledu poněkud méně povedená. Přes značné množství použitých a citovaných prací (a možná právě kvůli němu) je text matematicky poněkud povrchní. Pravděpodobně by mu prospělo zúžení výběru článků ve prospěch detailnější prezentace (často spíše heuristických) úvah. Oponent přitom nevylučuje, že povrchnost textu souvisí s mírou zajímavosti citovaných výsledků. Nejvýraznější slabinou předložené práce je nepříliš výrazný vlastní studentův přínos nad pouhou, byť zdařilou kompilaci a překlad do češtiny. Oponent v práci nepostřehl ani návrh konkrétní implementace kryptosystému nebo útoku ani alespoň jasný pokus o vylepšení stávajících algoritmů po teoretické stránce, ačkoli právě k naplnění druhého bodu byl při práci s nekomutativními Gröbnerovými bázemi autor nejblíže.

Přes uvedené výhrady předložená práce Aleše Fuchse *Aplikace Gröbnerových bází v kryptografii* naplnila zadání, doporučuji uznat jako diplomovou a navrhuji ji ohodnotit známkou **velmi dobře**. V případě, že se student při prezentaci práce úspěšně vypořádá s uvedenými výhradami a přesvědčí komisi o významu vlastního přínosu v celku práce, nemá oponent námitek proti hodnocení výborně.

v Praze 12.9.2008 Jan Žemlička