Posudek vedoucího na diplomovou práci

# Aleš Fuchs: Aplikace Gröbnerových bází v kryptografii

Cílem diplomové práce bylo seznámit se s teorií Gröbnerových bází pro okruhy polynomů i volných nekomutativních algeber nad tělesem, prostudovat návrhy kryptosystémů na této teorii založené a analyzovat jejich bezpečnost a praktickou použitelnost. Zvláštní důraz byl kladen na systém navržený před sedmi lety T. S. Raiem, jehož bezpečnost jeho autor odůvodňuje mimo jiné tím, že pro mnohé konečně generované ideály ve volných algebrách nad tělesem neexistuje konečná Gröbnerova báze.

Práce je mimo úvodu a závěru členěna do tří kapitol. V první z nich je podán pěkný přehled dobře známých faktů ohledně Gröbnerových bází pro okruhy polynomů. Druhá, která na ní staví, se zaměřuje na modifikaci této teorie pro volné nekomutativní algebry. Je zde popsán patřičně upravený Buchbergerův algoritmus a s důkazem prezentováno kritérium pro existenci konečných Gröbnerových bází. Třetí kapitola pak přehledně pojednává o variantách kryptosystému Polly Cracker a útocích na něj.

Cíle byly splněny a výsledkem je pěkná přehledová práce sestavená na základě takřka třiceti zdrojů.

Mojí hlavní výtkou je poněkud uspěchaný konec a nedotažená analýza důsledků argumentů z článku Barkeeho a spoluautorů. Ačkoliv jejich slova platila kryptosystémům založeným na Gröbnerových bázích v okruzích komutativních polynomů, po přečtení posuzované práce je vidět, že podobný argument bude velice pravděpodobně fungovat i pro volné algebry. Důsledkem by pak bylo, že argument T. S. Raie o nekonečnosti Gröbnerovy báze není zcela relevantní, protože pro útok stačí vždy počítat jen její dobře specifikovanou konečnou část. Toto vše bylo bohužel ponecháno jako úkol zvídavému čtenáři.

Předloženou práci **doporučuji k obhajobě**, v závislosti na jejímž průběhu navrhuji práci ohodnotit stupněm **výborně** nebo **velmi dobře**.

V Praze dne 12. 9. 2011 RNDr. Jan Šťovíček, Ph.D.