Pavel Hubáček: Gröbnerovy báze v kryptografii

posudek vedoucího práce

Práce představuje úvod do algebraické kryptoanalýzy. V první části jsou shrnuty sofistikovanější techniky výpočtu Gröbnerových bází s aplikací na řešení soustav polynomiálních rovnic (algoritmy F4, FGLM, Gröbnerovy procházky). V druhé části je vysvětlena vlastní technika algebraických útoků na konkrétním příkladě šifer AES a KeyLoq. Tyto útoky byly v rámci práce reimplementovány a bylo dosaženo srovnatelných výsledků s literaturou.

Přestože práce neobsahuje původní výsledky (což ani nebylo cílem), je velmi přínosná především tím, že je v ní zpracováno aktuální téma, kterým se v Praze nikdo nezabývá. Student postupoval samostatně, zpracoval velké množství materiálů a podstatně těžil ze svého semestrálního pobytu na univerzitě v Linci. Zpracování práce je, až na drobné chyby v angličtině, na vysoké úrovni. Snad jen druhou část kazí několik drobných chyb, typu záměna charakteristiky a velikosti tělesa v definici 4.3, nebo vyjádření čísla 63 na str. 38 (jestli tomu dobře rozumím, 63=1+2+...+2^5, tedy odpovídající polynom je 1+theta+...+theta^5).

Práci navrhuji uznat jako diplomovou a hodnotit stupněm **výborně**.

V Praze, 10.9.2010

David Stanovský

[redacted]