Oponentský posudek diplomové práce

Pavel Hubáček: Gröbnerovy báze v kryptografii

Práce se zabývá využitím Gröbnerových bází k útokům proti moderním kryptosystémům. Text je rozdělen do dvou větších částí a k jeho vytvoření bylo využito několik monografií a množství článků a konferenčních příspěvků.

V první části se autor zabývá potřebným teoretickým zázemím ke Gröbnerovým bázím a moderními algoritmy na jejich výpočet. Hlavním cílem a motivací je pak schopnost řešit soustavy polynomiálních rovnic nad konečnými tělesy. Po stručném popisu původního Buchbergerova algoritmu je podrobně popsán Faugèrův vylepšený algoritmus F4. Z hlediska řešení soustav polynomiálních rovnic je také klíčová schopnost transformovat Gröbnerovu bázi vypočítanou vzhledem k jednomu uspořádání členů na bázi vzhledem k jinému uspořádání, zpravidla lexikografickému. K tomu slouží ve speciálním (leč velmi důležitém) případě algoritmus Faugèra, Gianniho, Lazarda a Mory. Zcela obecný algoritmus založený na tzv. Gröbnerových procházkách, k jehož pochopení je třeba určitý teoretický úvod, pak vytvořili Collart, Kalkbrener a Mall. Oba algoritmy jsou popsány a ilustrovány na příkladech.

Druhá část se zaměřuje kryptoanalytické útoky. Po zavedení obecného rámce se autor zabývá možností útoku na standardní široce používanou blokovou šifru AES a její "zmenšené" učební verze. Dále pak popisuje Bardův útok na šifru KeeLoq, používanou např. pro dálkové odemykání automobilů.

Práce je napsána srozumitelně a obsahuje mnoho zajímavého materiálu, co se teoretické i praktické stránky řešení soustav polynomiálních rovnic týče. Drobnější výtkou je pak místy nepečlivost při používání značení a patrně i jeho sjednocení z různých zdrojů. Jedná se např. o občasnou záměnu značení pro "leading term" a "leading monomial", používání značení normální formy bez zavedení a občas ne zcela jasné značení v kapitole o AES.

Předloženou práci doporučuji k obhajobě a navrhuji ohodnotit stupněm výborně.

V Praze dne 6. 9. 2010

RNDr. Jan Šťovíček, Ph.D.