Posudek vedoucího bakalářské práce

Název: Bezpečnost šifrování zpráv závisejících na klíči
Autor: Kristina Hostáková

Shrnutí obsahu práce

Práce se zabývá šifrovacími schématy, která jsou bezpečná i v případě, kdy šifrujeme zprávy závisející na klíči, tzv. KDM-bezpečnými schématy. Po zavedení základních pojmů v první kapitole se práce ve 2. kapitole věnuje obecné definici šifrovacího schématu a jeho kryptografických vlastností, zejména pak KDM-bezpečnosti. Další kapitola postihuje základy mřižkové kryptografie nutné pro popis schémat z následujících kapitol, především pak definuje problém LWE (Learning With Errors) a LPN (Learinig of Parity with Noise). Kapitoly 4 a 5 obsahují popis asymetrického resp. symetrického schématu, která jsou bezpečná vzhledem k affiním funkcím soukromých klíčů. Jde o schémata autorů Applebaum et al. (CRYPTO 2009), která jsou však v práci pojednána daleko podrobněji. Přestože se nepodařilo (zejména z důvodu omezeného rozsahu práce) dokázat všechna pomocná lemmata, klíčové části důkazu KDM-bezpečnosti jsou přítomny a čtenáře daleko lépe přesvědčí o platnosti hlavních tezí než původní článek, který vesměs pomocná lemmata nedokazuje.

Celkové hodnocení práce

Téma práce. Práce patří mezi obtížnější, neboť k jejímu úspěšnému sepsání bylo nutné kromě znalosti velkého množství běžně probíraných témat (samoopravné kódy, pravděpodobnost, složitost) i proniknutí do oblasti mřížkové kryptografie. Zadání práce bylo beze zbytku splněno.

Vlastní příspěvek. Práce poskytuje některé chybějící části důkazu KDM-bezpečnosti popisovaných schémat, což lze označit za primární přínos textu. Práce dále obsahuje vlastním způsobem zpracované obecné definice kryptografických vlastností šifrovacích schémat pomocí her/experimentů.

Matematická úroveň. Velmi dobrá.

Práce se zdroji. Všechny zdroje jsou správně citovány.

Formální úprava. Text je psán přehledně a bez zjevných gramatických a typografických chyb.

Závěr

Práci považuji za vynikající a doporučuji ji uznat jako bakalářskou práci.

Michal Hojsík
Katedra algebry
14.8.2013