Posudek vedoucího bakalářské práce

Název: Kryptografická kritéria pro Booleovské funkce
Autor: Radka Luňáčková

Shrnutí obsahu práce

Předložená práce se věnuje vybraným částem teorie Booleovkých funkcí. Cílem bylo popsat základní kryptografická kritéria a uvést jejich vztahy a vlastnosti.

Práce začíná popisem různých reprezentací Booleovských funkcí. Následuje kapitola 2 obsahující základy teorie těchto funkcí (korelace, pseudo-Booleovské funkce, Walsh-Hadamardova transformace, derivace). Poslední kapitola se věnuje vlastnostem (kriteriím) Booleovských funkcí podstatným pro kryptografii (algebraický stupeň, nelinearita, balancovanost, odolnost a korelační imunita).

Obsah práce vychází z přednášky „Teoretická kryptografie“. Nad její rámec jsou kapitoly 1.4 a 1.5, část kapitoly 2 a celá kapitoly 3.

Celkové hodnocení práce

Téma práce. Téma práce a její náročnost jsou přiměřené pro bakalářskou práci. Její zpracování vyžadovalo detailně pochopení obtížně čitelného textu o Booleovkých funkcích od C. Carleta [3]. Práce jednoznačně splnila zadání.

Vlastní příspěvek. Studentka zformulovala do tvrzení a vět část textu od C. Carleta [3]. K nim doplnila vlastní důkazy, rozepsala uvedené náznaku důkazů nebo doplnila chybějící kroky. Pro ilustraci doplnila vlastní příklady.

Matematická úroveň. Výborná.

Práce se zdroji. Všechny zdroje jsou správně citovány. U každé podkapitoly je jasné z čeho čerpá, a které části jsou původní.

Formální úprava. Výborná.

Závěr

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

Michal Hojsík
Katedra algebry
14.6.2013