POSUDEK VEDOUCÍHO/OPONENTA BAKALÁŘSKÉ PRÁCE

Název: Kryptografická kritéria pro Booleovské funkce
Autor: Radka Luňáčková

Shrnutí obsahu práce

Práce pojednává o booleovských funkcích a jejich použití v kryptografii. První kapitola se zabývá různými způsoby jak zadat booleovskou funkci. Druhá kapitola se zabývý především Wlash-Hadamardovo transformací . V poslední kapitole pak autorka využívá zavedených pojmů a výsledků předchozích dvou kapitol ke studiu algebraického stupně booleovské funkce, její vzdálenosti od množiny afinních funkcí, balancovaností a korelační imunitou, což jsou všechno charakteristiky booleovských funkcí důležité pro jejich kryptografické použití.

Celkové hodnocení práce

Téma práce přiměřeně náročné, text splňuje zadání práce.

Vlastní příspěvek autorky spočívá v podrobnějších důkazech některých tvrzení převzatých z literatury, případně v doplnění a ilustraci pojmů na vlastních příkladech.

Matematická úroveň je velmi dobrá, prakticky celá práce je rigorózně a korektně formulovaný matematický text.

Práce se zdroji. Zdroje jsou správně a úplně citovány.

Formální úprava práce je na velmi dobré úrovni.

Následuje pár připomínek.

1. Autorka v důkazech občas neuvádí na příslušných místech odkud nějaký krok důkazu plyne. Například v prvním odstavci důkazu Věty 4 se mluví o počtu polynomů jedné proměnné nad tělesem o 2^n prvcích. Ve skutečnosti se ale jedná počet polynomů nad tímto tělesem stupně nejvýše 2^n-1, tento předpoklad je ale ve znění věty správně uveden. Podobných příkladů by se v práci našlo více.
2. V jednom případě (poznámka za definicí 13 na str. 16) se v práci používá pojem stupně booleovské funkce, který ale zaveden až na str. 24 v definici 19.

Závěr

Práci považuji velmi dobrou a doporučuji ji uznat jako bakalářskou práci.

Jméno oponenta: Jiří Tůma
Pracoviště: katedra algebry
Datum: 17.6.2013