Posudek oponenta na diplomovou práci Michala Botky

Předložená diplomová práce má slibně založené rozvržení, ale celkový výsledný dojem je slabší. Chybí výraznější vlastní vklad, látka je málo provázaná, některé části jsou vyloženy bez odpovídající diskuse kvality algoritmu, chybí souvislosti a není řádně vyloženo, kam celé úsilí míří. Výklad je místy zbytečně formální, až přetížený značením a pojmy (například na straně 15-16 by výklad usnadnilo, kdyby diplomant vyložil roli přidaných t proměnných, které vlastně slouží k záznamu provedených úprav na sloupcích vlevo). Celkový rozsah vzhledem k míře vlastní práce není příliš velký.

Jako klad vidím, že diplomant vykládané látce zjevně slušně porozuměl a pochopil ji. V práci je také velmi málo drobných formálních nedostatků a úroveň matematického vyjadřování je velmi dobrá. (Drobné nepřesnosti se samozřejmě najdou vždy: několikrát jsem si všiml, že diplomant píše *ekvivaletní*; v Lemma 5.7 je chybný poslední index).

Prosím, aby při práci prezentaci byly zodpovězeny tyto otázky:

- V kapitole 3 jde o popis S-boxu σ aproximací jeho "grafu" $S(\sigma)$ složeného z dvojic $(x, \sigma(x))$ jako množiny nul. Proč je tento popis výhodný? Jsou nějaké důvody, proč se soustředit právě na něj a ne třeba na vyjádření jednotlivých složek $\sigma = (\sigma_1, \ldots, \sigma_n)$ booleovskými polynomy?
- V případě AES mluvíte o 23 nalezených kvadratických polynomech. Je v tomto případě $S(\sigma) = N(W)$ nebo je $S(\sigma)$ vlastní podmnožinou $N(W)$?
- Proč se celá práce zabývá pouze kvadratickými polynomy? Má to nějaký jiný důvod než, že jsou chápány jako nejbližší aproximace linearity?

Doporučuji práci uznat jako diplomovou a hodnotit ji známkou ...

V Praze 30.1.2009

Aleš Drápal