POSUDOK OPONENTA NA DIPLOMOVÚ PRÁCU:
Lucie Marková, Analýza návrhu nových hašovacích funkcí pro soutěž SHA-3

Predložená diplomová práca sa venuje použitiu linearizačného rámca v analýze hašovacích funkcí konštrukcie ARX.

Práca začína krátkym, trochu neprehľadným úvodom do problematiky (kapitola 1) za ktorým nasleduje stručný popis práve prebiehajúcej súťaže o nový štandard SHA-3 (kapitola 2). Kapitola 3 popisuje hešovaciu funkciu BLAKE-32.

Vlastný obsah diplomovej práce začína popisom linearizačného rámca v kapitole 4. Tá obsahuje prevzaté, ale aj vlastné výsledky diplomantky. Na niektorých miestach je ale tažké tieto od seba odlíšiť, pretože autorka v jednotlivých podkapitolách a v nich uvedených definíciach a tvrdeniach nie vždy uvádza zdroj.

Zaujímavé výsledky sa nachádzajú v podkapitole 4.3, ktorá sa zaoberá diferenciami v prípade modulárneho pričítania konštanty. Je však na škodu, že práca popísaná v tejto podkapitole nie je dotiahnutá do konca. Podkapitola 4.4 by mohla byť prehladnejšia, prípadne viac rozpracovaná.

Kapitola 5 popisuje aplikáciu linearizačného rámca na kompresnú funkciu hešovacej funkcie BLAKE-32. Konkrétne obsahuje odvodenie a overenie matíc linearizovanej verzie kompresnej funkcie, zoznam vektorov malej váhy kódov určených týmito maticami a popis "zlého" diferenciálu pre BLAKE-32. Aj táto kapitola bohužial ostala nedokončená.

Vybrané poznámky k práci:

- Na str. 12 chýba definícia premenných $c_0, \ldots, c_7$.
- V celej práci sú v popise BLAKE-32 uvedené rotácie slov nesprávnym smerom (rotácie doľava namiesto správneho doprava, napr. strana 13).
- V Kap. 4.1 chýba motivácia pre definíciu 4.2.3.
- V Kap. 4.1 mohla autorka spojiť Lemma 4.2.4 a 4.2.5 a zjednodušiť tým výklad.
- Str. 28, 3. odstavec má byť $p_0 = 1$ a ani $p_0 = 0$.
- Str. 31 predposledná veta nie je spávna. Pre dané M a dané δ máme jedinú možnosť voľby M'.

Celkovo je predložená práca na dobrej formálnej úrovni a obsahuje vlastné výsledky, ktoré ale ostali nedokončené. Doporučujem ju preto prijať a navrhujem hodnotenie známkou . . . .

Praha, 19.1.2011

Michal Hojsík