POSUDOK VEDÚCEHO NA BAKALÁRSKU PRÁCU:

Ondřej Väter

Triangulační algoritmus pro systémy nelineárních rovnic

Práca Ondřeja Vätera sa venuje takzvanému Triangulačnému algoritmu a jeho využitiu pre hľadanie správ spĺňajúcich danú diferenčnú cestu. Po úvode nasleduje detailný popis šifry Rijndael a definície potrebných pojmov. Práca pokračuje popisom Triangulačného algoritmu a jeho aplikáciou na sústavu rovníc odvodenú z diferenčnej stopy pre 5-rundový Rijndael. Posledné dve kapitoly sa venujú využitiu získaných výsledkov na nájdenie kolízie pre uvedenú hešovaciu funkciu a popisu implementačnej časti bakalárskej práce. Väčší rozsah práce je spôsobený potrebným detailným popisom šifry Rijndael, veľkým počtom obrázkov vhodne ilustrujúcich popisované diferenčné stopy, ako aj uvedením získaných rovníc v kapitole 3.

Okrem úvodných kapitol obsahuje práca prevažne vlastné výsledky. Pozitívne hodnotím napríklad autorovo spracovanie a analýzu Triangulačného algoritmu, ktoré výrazne rozširujú neformálny popis uvedený v citovanom článku. Vlastným netriviálnym výsledkom je taktiež postup umožňujúci trianguláciu sústavy rovníc v kapitole 4 spolu s implementáciou Triangulačného algoritmu a konštrukciou kolízií v kapitole 5.

Z formálnej a jazykovej stránky ale práca obsahuje značné množstvo nedostatkov, ktoré miestami znižujú čitateľnosť textu a tým celkovú kvalitu práce. Taktiež autorova formalizácia uvádzaných pojmov je v niektorých prípadoch neprehľadná.

Prácu doporučujem uznať ako bakalársku a hodnotiť ju známkou . . . .

Praha, 27.8.2012 Michal Hojsík