Oponentský posudek bakalářské práce „Triangulační algoritmus pro systémy nelineárních rovnic“

Cílem bakalářské práce Ondřeje Vätera bylo aplikovat triangulační algoritmus, jakousi obdobu Gaussovy eliminace pro jistý typ soustav nelineárních rovnic, v kryptoanalytickém kontextu.

Samotný algoritmus představili autoři Khovratovich, Biryukov a Nikolic v článku „Speeding up Collision Search for Byte-Oriented Hash Functions“ publikovaném roku 2009. Pan Väter ve své práci algoritmus formálně popsal, ukázal úskalí jeho aplikace na několika příkladech a posléze jej uplatnil při ověřování platnosti diferenční stopy v rámci snahy o nalezení kolize pro hashovací funkci, jež vznikne při použití šifry Rijndael v Daviesově-Mayerově módu. Konkrétně byla zkoumána 5rundovní varianta šifry Rijndael a pro náhodný inicializační vektor byly zkonstruonány dvě zprávy se stejnou hodnotou hash. V rámci implementace umístěné na přiloženém DVD se pracovalo se zprávami různých délek, až po 1 GB.

Po strukturní stránce práci není v podstatě co vytknout. Pokud jde o stránku věcnou, několik menších pochybení by se již našlo, například: Z toho, jak je zformulována Definice 1.2, plyne, že každý kryptosystém je blokovou šifrou, bez ohledu na zvolené n. Podobně formulace Definice 1.7 je přinejmenším krkolomná. V posledním odstavci na straně 6 se mluví o isomorfismu operací sčítání, což striktně vzato nedává smysl. Na prvním řádku Konvencí pro pseudokód (strana 10) jsou otočené „definitorické rovnosti“.

Co ovšem nejvíce sráží kvalitu práce dolů, je její formální a jazyková stránka. Čeština pokulhává nejen na rovině pravopisné, nejčastěji jde o chybějící čárky v souvětích či různé překlepy a špatně zvolené pády (např. v Definici 3.1 „. . . lze hodnota a_l určit jednoznačně. . . “), ale především na rovině stylistické (úvod, 5. kapitola). Navíc podobně svévolně a nejistě jako s jazykem, zachází autor i s grafickou podobou práce. Formátování v rámci důkazu Věty 3.27 (strana 36 a 37) je v tomto smyslu ukázkovým příkladem. . . Na druhou stranu, zařazení a provedení obrázků šifrových diagramů si zaslouží pochvalu.

Text Ondřeje Vätera „Triangulační algoritmus pro systémy nelineárních rovnic“ **doporučuji uznat jako bakalářskou práci.** Autor splnil cíl specifikovaný v zadání a jednoznačně prokázal schopnost samostatně pracovat v oboru.