Posudek vedoucího na bakalářskou práci
Jana Čížka nazvanou
Looking for weak states of RC4
by means of waiting tables

Jde o kvalitní bakalářskou práci, o které nemám pochyb, že by měla být hodnocena jako vynikající. Student formalizoval koncepty vedoucího práce způsobem, který je významným zlepšením původního stavu, a provedl pečlivou analýzu možné existence hledaných objektů při určitých omezeních na velikost.

Hledanými objekty jsou takzvané čekací tabulky, případně jejich grafová verze nazvaná čekací cesty. Cílem je najít injektivní periodickou čekací tabulku. Její existence by indikovala existenci slabých stavů v šifře RC4, což by mělo značný dopad na její důvěryhodnost.

První čtyři kapitoly práce se týkají především definic a ověřování jejich ekvivalence. Zde student prokázal velkou pečlivost a smysl pro detail. Ekvivalenci čekacích cest a čekacích tabulek, která byla dříve formulována pro periodický případ, dokázal i pro případ takzvaných úplných čekacích cest a tabulek, tedy i pro případ neperiodických, které již nelze dále prodloužit.

Protože není vůbec zřejmé, jak čekací cesty hledat, případně jak dokázat, že neexistují, navrhl jsem, aby byly hledány čekací cesty speciálního typu, který byl nazván vrcholově periodický. Pokud existují, tak každá z nich indukuje i jistou odvozenou strukturu, kterou je možno definovat nezávisle na existenci či neexistenci čekacích cest. Nazvali jsme ji IPW-matice, kde IPW je zkratka sousloví injective periodic waiting (matrix). Navrhl jsem, aby byly hledány IPW matice s nesoudělnými členy. Takové matice jsou v práci nazvány kanonické – ostatní IPW matice jsou jejich násobky. Student teorii IPW matic pečlivě zpracoval v kapitole 5, a zcela samostatně provedl klasifikaci IPW matic řádu 4. Dokázal, že existuje právě dvacet kanonických IPW matic řádu 4. U každé ověřil, že z ní není možné odvodit vrcholově periodickou čekací cestu. Výsledek práce tedy nepřinesl kýžený slabý stav šifry RC4. Plánuji do budoucna, že získané výsledky budu analyzovat tak, aby pojem IPW matice byl natolik zesílen, aby část kandidátů na analýzu bylo možno zamítnout na základě obecných vlastností (které je třeba objevit a formulovat) a odpadla tak nutnost každou z nich specificky zkoumat.

Práce téměř neobsahuje chyb. Je psána pečlivě, s porozuměním, a přináší nové výsledky. Jsem si vědom toho, že místy je její četba nesnadná. Domnívám se však, že je to především díky tomu, že je popisována struktura velice specifická a neintuitivní. Připouštím, že větší počet příkladů by srozumitelnosti napomoci mohl.

Navrhuji, aby práce byla přijata jako práce bakalářská a hodnocena stupněm výborně.

Aleš Drápal

V Praze 16. srpna 2018