Oponentský posudek bakalářské práce

Jana Čížka

nazvané

Looking for Weak States of RC4 by Means of Waiting Tables

V předložené práci student navazuje na předchozí práci Drápala a Hojsíka z roku 2006, ve které byly zavedeny takzvané *čekací tabulky* (Waiting Tables). Nalezení čekací tabulky určitých vlastností by mělo za následek významné snížení bezpečnosti šifry RC4.

Práce je rozdělena do pěti kapitol. V první kapitole je připomenuta šifra RC4. Ve druhé jsou představeny čekací tabulky a dokázány jejich vlastnosti. Totéž je pak uděláno pro *čekací cesty* (Waiting Paths) v kapitole třetí. Čtvrtá kapitola se věnuje dokázání ekvivalence mezi čekacími tabulkami a čekacími cestami. V poslední (nejdelší) kapitole je pak problém nalezení vhodné čekací cesty (a ekvivalentně čekací tabulky) redukován na nalezení matice IPW-matrix, z které by se čekací cesta dala odvodit. Ve zbytku kapitoly (23 stran) jsou pak klasifikovány IPW matice řádů jedna až čtyři. Bohužel se ale ukázalo, že ani jedna z uvažovaných matic neindukuje vhodnou čekací cestu. Výsledek práce tedy (zatím) nepřinesl úspěch ve zlomení šifry RC4.

Dle mého soudu se jedná o velmi kvalitní bakalářskou práci s jen malým množství chyb (které patrně vznikly jen nepozorností při kopírování textu). Všechno je velmi precizně zadefinováno a přehledně dokázáno. Zdroje jsou řádně ocitovány. Vlastní příspěvek autora je značný.

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

V Praze dne 5. září 2018

Milan Boháček

Digitálně podepsal Mgr. Milan Boháček
DN: c=CZ, 2.5.4.97=NTRCZ-04389921, o=Milan Boháček [IČ 04389921], ou=1, cn=Mgr. Milan Boháček, sn=Boháček, givenName=Milan, serialNumber=P543081
Datum: 2018.09.05 11:40:46 +02'00'