Michal Hojsík: Proudová šifra RC4

Posudek vedoucího diplomové práce

Proudová šifra RC4 je mezi proudovými šiframi realizovanými programovým vybavením tou nejpoužívanější. V práci je nejprve popsán její chod, dále jsou zmíněny všechny běžně uváděné a publikované útoky na tuto šifru, a pak je vytvořen tabulkový model jejích vnitřních parciálních stavů. Zbytek práce je věnován popisu tohoto modelu a hledání jeho vlastností.

Za nejvýznamnější v práci považuji právě ono vytvoření tabulkového modelu, které studium setrvalých stavů postavilo na pevnou matematickou bázi. Cílem je dokázat, že žádné setrvalé stavy neexistují (až na triviálního Finneyho stav). To se nepodařilo, byť je možné, že k cíli není daleko. Některé vedlejší výsledky (např. regularita čtvercové matice odvozené z lineárního uspořádání a ekvivalence) jsou zajímavé samy o sobě. Rovně se podařilo dokázat, že netriviálního setrvalé stavy neexistují, pokud počet parciálních stavů je menší než pět.

Je zřejmé, že i v případě, kdy se podaří po matematické stránce problém dořešit, bude ještě dlouhá cesta k jeho plnému kryptologickému vytěžení. Na druhou stranu abstrakce v práci předložená jde daleko za rámec dosavadních úvah o RC4, je originální a otevírá zcela novou linii výzkumu.

Po matematické stránce je práce kvalitní, avšak co do výkladu místy příliš formální. Zejména popis transformace, která vede od vlastní šifry k vytvoření tabulkového modelu by potřeboval paralelně s formálním popisem podat i popis neformální a vhodně ilustrovaný.

Práce je popsána v angličtině slušné úrovně, třebaže ne bezchybné (tak např. „focuse“ místo „focus“ na straně 5, „periodical“ místo „periodic“ na straně 29, a jiné drobnosti).

Jistou výtku lze vyslovit i ve směru, že některé výsledky zůstaly implicitně dokázané, avšak ne explicitně formulované – tím je například popis všech setrvalých stavů na čtyřech sloupcích pro neinjektivní případ.

Vzhledem k uvedenému navrhuji uznat předloženou práci jako práci diplomovou a hodnotit ji známkou výborně.

V Praze 22. května 2006

Aleš Drápal

[redacted]