Andrea Frisová: Kryptografie založená na teorii kvazigrup

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Předloženou diplomovou práci považuji za velmi kvalitní a pečlivou. Z šíře možných témat se věnuje růstu period v šifře Edon 80. Délka period byla odhadována heuristicky a pomocí statistických metod. Určit rozložení period exaktně se jeví být jako náročný úkol. V práci tento úkol řešen není, pouze jsou vytvořeny nástroje, které snad v budoucnu umožní jeho vyřešení.

Hlavním z takových nástrojů je přenesení problému hledání period do period posloupností prvků grupového okruhu. Tyto posloupnosti vznikají jako koeficienty v polynomech více proměnných nad příslušným grupovým okruhem, pokud prvky klíče považujeme za proměnné, jejichž dosazením konkrétní periodickou posloupnost teprve obdržíme. Její periodičnost přitom lze odhadnout na základě period posloupností koeficientů.

Látka je komplikovaná a tak lze přijmout, že v prvním přiblížení je řešen problém pouze pro centrální kvazigrupy, které se ovšem ve vlastní šifře Edon 80 fakticky nevyskytují. Ostatně řešení již pro mediální kvazigrupy není lehké a vyžaduje aplikaci netriviálních poznatků z teorie čísel.

Formálně je práce na vysoké úrovni a nemám žádné výhrady.

Doporučuji, aby práce byla uznána jako diplomová a hodnocena známkou výborně

V Praze 18. května 2009

Aleš Drápal