Andrea Frisová:
Kryptografie založená na teorii kvazigrup

posudek vedoucího práce

Předložená práce je inspirována proudovou šifrou Edon-80 a zabývá se analýzou procesu, který generuje pseudonáhodnou posloupnost. Stěžejním parametrem tohoto procesu je volba čtyřprvkových kvazigrup. Práce si klade za cíl určit, které kvazigrupy jsou vhodné. Výsledkem je argument, že centrální kvazigrupy vhodné nejsou, protože výsledná posloupnost má krátkou periodu. (Přesné znění viz přehled výsledků na str.55)

Práce využívá klasifikaci čtyřprvkových kvazigrup pomocí izotopie na abelovské grupy. Pro centrální kvazigrupy lze daný problém převést na výpočty v grupovém okruhu automorfismů grupy Z4, resp. Z2xZ2, které vedou na komplikované rovnosti s binomickými koeficienty modulo 4 resp. 2 (kapitoly 4,5). Výpočty jsou elementární, leč technicky dosti náročné, využívá se řada pomocných vlastností (kap.3).

Práce sestává z větší části z vlastních výsledků (zejména klíčové kapitoly 4,5). Studentka postupovala samostatně, výsledky jsou netriviální, správné a patrně budou základem pro publikaci. Práce je sepsána dosti pečlivě a bez chyb.

Předloženou práci proto doporučuji uznat jako diplomovou a ohodnotit stupněm **výborně.**

V Praze, 19.5.2009
David Stanovský