Adam Christov:
Kryptografie založená na teorii kvazigrup

posudek vedoucího práce

Předložená práce je inspirována kryptosystémem MQQ pro kryptografii s veřejným klíčem a zabývá se teorií kvadratických kvazigrup, které se v tomto systému používají ke generování klíčů. Hlavním výsledkem práce je šikovný popis kvadratických kvazigrup (Věta 2.40), na jehož základě lze dále rozvíjet jejich teorii; v předložené práci konkrétně popis izotopů kvadratických lup a především dva algoritmy (kap. 3), které umožňují tyto kvazigrupy vytvářet mnohem efektivněji než bylo dosud známo.

Práce sestává z větší části z vlastních výsledků, algebraickou teorií kvadratických kvazigrup se nikdo dosud nezabýval. Práce využívá základní poznatky z teorie Booleovských funkcí a bilineárních forem. 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