Adam Christov: Kryptografie založená na teorii kvazigrup

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Předloženou práci považuji za velmi zdařilou. Týká se více základů matematické teorie kvazigrup než bylo asi původně očekáváno. Za hlavní přínos práce považuji vybudování abstraktního pojetí kvadratických lup (teorémy 2.48 a 2.50) a použití abstraktního popisu kvadratických kvazigrup (teoréma 2.40) pro hledání kvadratických kvazigrup pomocí izotopismů (výsledky jsou shrnuté v tabulce 2.2).

Dosažené výsledky umožňují efektivnější generování kvadratických kvazigrup v kryptosystému navrženém trojicí autorů Gligoroski, Markovski, Knapskog.

Angličtina práce je velmi slušná, byť místy by potřebovala ještě mírně zlepšit. To však za podrobnější rozbor nestojí.

Doporučuji, aby práce byla uznána jako diplomová a hodnocena známkou

V Praze 18. května 2009

Aleš Drápal