Posudek vedoucího bakalářské práce

**Název:** MQ problém
**Autor:** Adolf Středa

## Shrnutí obsahu práce

Hlavním cílem předložené práce je podat popis útoků na některé varianty kryptosystémů založených na takzvaném MQ-problému, tedy na obtížnosti řešení systému polynomiálních rovnic více neznámých nad konečným tělesem. První dvě kapitoly, které tvoří matematickou expozici práce, uvádí čtenáře do problematiky afinních transformací, kvadratických polynomů $n$ neurčitých nad konečným tělesem $\mathbb{F}_q$ a jejich reprezentace jako polynomů jedné neznámé nad rozšířením $\mathbb{F}_{q^n}$ spolu s popisem kryptosystému HFE, jenž využívá MQ-problém pro kvadratické polynomy více neurčitých. Třetí část je věnována stručnému přehledu základních známých útoků na HFE, útoky pomocí linearizace, relinearizace a Gröbnerových bazí. Nejobsáhlejší čtvrtá kapitola prezentuje útoky na varianty kryptosystému HFEm a HFEz.

## Celkové hodnocení práce

**Téma práce.** Ačkoli se kryptosystémy založené na NP-úplném MQ-problému zdály být nadějnými kandidáty pro praktické využití v postkvantové kryptografii, valná většina navržených schémat takových kryptosystémů byla záhy prolomena. Tématem práce proto bylo vedle obecného matematického popisu variant MQ-problému především vysvětlení několika útoků na konkrétní schémata. Úlohu, již považuji za adekvátní nároku na bakalářskou práci, se podle mého mínění podařilo splnit.

**Vlastní příspěvek.** Student srozumitelně a za použití vlastní argumentace vysvětlil otázku reprezentace polynomiálních vektorů více neurčitých pomocí polynomů nad rozšířeným tělesem, která je klíčová pro všechny varianty schémat HFE. Za velmi užitečné považují rovněž ilustrace zdařile prezentovaných známých útoků na příkladech malé dimenze.

**Matematická úroveň.** Matematická úroveň práce je podle mého mínění dobrá, formulace jsou korektní a snadno srozumitelné. Výsledný text svědčí o studentově vhledu do zkoumané problematiky.

**Práce se zdroji.** Text práce sice vychází z několika zdrojů, ovšem sepsaný text je výsledkem autorova vlastního přístupu a formulací, tudíž práce formulační závislostí na zdrojích netrpí.

**Formální úprava.** Text se velmi dobře čte a množství jazykových a stylistických nepřesností je zanedbatelné.

## Připomínky a otázky

1. Připomínky k textu jsem vznášel průběžně k pracovním variantám během sepisování práce a k závěrečné podobě už žádné připomínky nemám.

## Závěr

Práci považuji za kvalitní a doporučuji ji uznat jako bakalářskou práci.

*Návrh klasifikace vedoucí sdělí předsedovi zkušební (sub)komise.*

Jan Žemlička
Katedra algebry
17.6.2016