UNIVERZITA KARLOVA
Matematicko-fyzikální fakulta

Zápis o části státní závěrečné zkoušky
Obhajoba závěrečné práce

Akademický rok: 2018/2019

Jméno a příjmení studenta:	Bc. Marek Zpěváček
Datum narození:	05.10.1992
Typ studijního programu:	navazující magisterský
Studijní program:	Matematika
Studijní obor:	Matematika pro informační technologie
Zadavatel práce:	Katedra algebry (301. • 32-KA)
Název práce:	Důkazy bezpečností hashovacích funkcí
Jazyk práce:	čeština
Jazyk obhajoby:	čeština
Vedoucí:	doc. Mgr. Pavel Příhoda, Ph.D.
Oponent(i):	doc. Mgr. et Mgr. Jan Žemlička, Ph.D.
Datum obhajoby :	11.06.2019 **Místo obhajoby :** Praha
Průběh obhajoby:	Student představil výsledky své diplomové práce pomocí počítačové prezentace. Dobře uvedl do tématu a vhodným způsobem odlišil ideu výsledku od technických detailů. Přítomný vedoucí zdůraznil, že výsledek Ajtala, který byl předmětem zkoumání práce, má k tisíci citací, a přitom neexistuje zdroj, kde by důkazy potřebné pro odvození výsledku byly vyčerpávajícím a detailním způsobem uvedeny. Proti původnímu předpokladu se proto práce studenta omezila na rigorózní výklad Ajtalových výsledků. Posudek nepřítomného oponenta byl přečten. Diskuse byla krátká a týkala se hlavně otázky vztahu tématu práce k novějším výsledkům kryptografie založené na mřížích.
Výsledek obhajoby:	velmi dobře (2)
Předseda komise:	prof. RNDr. Aleš Drápal, CSc., DSc. .....
Členové komise:	doc. Mgr. Štěpán Holub, Ph.D. .....
	doc. Mgr. Pavel Příhoda, Ph.D. .....
	doc. RNDr. Petr Somberg, Ph.D. .....