MATEMATICKO-FYZIKÁLNÍ
FAKULTA
Univerzita Karlova

Zápis o části státní závěrečné zkoušky
Obhajoba diplomové práce

Akademický rok: 2021/2022

Jméno a příjmení studenta:	Bc. Jan Oupický
Identifikační číslo studenta:	98484842
Typ studijního programu:	navazující magisterský
Studijní program:	Matematika
Studijní obor:	Matematika pro informační technologie
ID studia:	627522
Název práce:	Theoretical foundations of cryptosystems based on isogenies of supersingular elliptic curves
Pracoviště práce:	Katedra algebry (301. • 32-KA)
Jazyk práce:	angličtina
Jazyk obhajoby:	čeština
Vedoucí:	prof. RNDr. Aleš Drápal, CSc., DSc.
Oponent(i):	doc. Mgr. et Mgr. Jan Žemlička, Ph.D.
Datum obhajoby:	11.02.2022 **Místo obhajoby:** Praha
Termín:	řádný
Průběh obhajoby:	Ve velmi pěkné počítačové prezentaci student s přehledem vytýčil hlavní témata obsahu práce. Vedoucí práce i oponent se shodli na tom, že práce, byť kompilační, má svým rozsahem a hloubkou potřebných znalostí značný význam, neboť uceleně prezentuje teoretické základy i praktickou implementaci systémů CSIDH a SIDH. V diskusi student zodpověděl otázky, které se vyskytly v posudcích. Krátká diskuse se týkala odolnosti vůči útokům založeným na kvantových počítačích.
Výsledek obhajoby:	výborně (1)
Předseda komise:	prof. RNDr. Aleš Drápal, CSc., DSc. .....
Členové komise:	doc. RNDr. Iveta Hnětynková, Ph.D. .....
	doc. Mgr. Štěpán Holub, Ph.D. .....
	doc. RNDr. Přemysl Jedlička, Ph.D. .....
	doc. Ing. Tomáš Pajdla, Ph.D. .....

RNDr. Zuzana Patáková, Ph.D. .....

doc. Mgr. Pavel Příhoda, Ph.D. .....

doc. RNDr. Petr Somberg, Ph.D. .....

doc. RNDr. Petr Tichý, Ph.D. .....

doc. RNDr. Jiří Tůma, DrSc. .....

doc. Mgr. et Mgr. Jan Žemlička, Ph.D. .....