



MATEMATICKO-FYZIKÁLNÍ
FAKULTA
Univerzita Karlova

Zápis o části státní závěrečné zkoušky Obhajoba diplomové práce

Akademický rok: 2021/2022

Jméno a příjmení studenta: Bc. David Tvrký
Identifikační číslo studenta: 39017111

Typ studijního programu: navazující magisterský
Studijní program: Matematika pro informační technologie
Studijní obor: Matematika pro informační technologie
ID studia: 672944

Název práce: Cryptanalytic attacks on the cipher PRINCE
Pracoviště práce: Katedra algebry (301. • 32-KA)
Jazyk práce: angličtina
Jazyk obhajoby: čeština
Vedoucí: Dr. rer. nat. Faruk Göloğlu
Oponent(i): RNDr. Vlastimil Klíma

Datum obhajoby: 09.06.2022 **Místo obhajoby:** Praha
Termín: řádný

Průběh obhajoby: Student pečlivou počítačovou prezentací vyložil obsah své práce. Přítomný vedoucí přednesl svůj posudek. Posudek nepřítomného oponenta byl přečten. Student se vyjádřil ve smyslu, že výtky oponenta přijímá, ovšem s výhradou, že sice některé obecnější známé generické metody vyložil krátce, avšak naopak dodal vysvětlení a argumentaci k článkům, ve kterých toto chybělo.

Výsledek obhajoby: výborně (1)

Předseda komise: prof. RNDr. Aleš Drápal, CSc., DSc.

Členové komise: Dr. rer. nat. Faruk Göloğlu

doc. RNDr. Iveta Hnětynková, Ph.D.

doc. Mgr. Štěpán Holub, Ph.D.

doc. RNDr. Přemysl Jedlička, Ph.D.

doc. Ing. Tomáš Pajdla, Ph.D.

doc. Mgr. Pavel Příhoda, Ph.D.

doc. Ing. Filip Šroubek, Ph.D., DSc.

doc. Mgr. et Mgr. Jan Žemlička, Ph.D.