



MATEMATICKO-FYZIKÁLNÍ  
FAKULTA  
Univerzita Karlova

## Zápis o části státní závěrečné zkoušky Obhajoba diplomové práce

Akademický rok: 2022/2023

**Jméno a příjmení studenta:** Bc. Petr Sedláček  
**Identifikační číslo studenta:** 35100454

**Typ studijního programu:** navazující magisterský  
**Studijní program:** Matematika pro informační technologie  
**ID studia:** 704629

**Název práce:** Security of Trapdoor Permutations under Preimage Leakage  
**Pracoviště práce:** Informatický ústav Univerzity Karlovy (208. • 32-IUUK)  
**Jazyk práce:** angličtina  
**Jazyk obhajoby:** čeština  
**Vedoucí:** Mgr. Pavel Hubáček, Ph.D.  
**Oponent(i):** Dr. rer. nat. Faruk Göloğlu  
**Datum obhajoby:** 12.09.2023    **Místo obhajoby:** Praha  
**Termín:** řádný

**Průběh obhajoby:** Student velmi pečlivou prezentací představil výsledky své práce. Přítomný vedoucí i oponent seznámili přítomné se svými posudky. V krátké diskusi se ujasnila určitá informace týkající se síly jistého odhadu a míry jeho vylepšení studentem. Vzhledem k jednoznačnému názoru vedoucího i oponenta, a též vzhledem ke kvalitě prezentace, byla diskuse v neveřejné části velmi krátká.

**Výsledek obhajoby:** výborně (1)

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

**Členové komise:** Dr. rer. nat. Faruk Göloğlu .....

doc. Mgr. Štěpán Holub, Ph.D. ....

RNDr. Zuzana Patáková, Ph.D. ....

doc. Mgr. Pavel Příhoda, Ph.D. ....