



Report on part of state final examination Defence of master's thesis

Academic year: 2024/2025

Student's name and surname: Bc. Berenika Richterová
Student's ID: 50863837

Type of the study programme: Master's (post-Bachelor)
Study programme: Mathematics for Information Technologies
Study ID: 753590

Title of the thesis: On security of adaptor signatures
Thesis department: Computer Science Institute of Charles University (208. • 32-IUUK)

Language of the thesis: English
Language of defence: English
Supervisor: Mgr. Pavel Hubáček, Ph.D.
Reviewer(s): doc. Faruk Göloğlu, Dr. rer. nat.
Date of defence: 02.06.2025 **Venue of defence:** Praha
Attempt: regular

Examination proceedings: The student presented her thesis on the security of adaptor signatures. Her supervisor explained practical aspects of the work. The opponent among other things made more precise his objection on the definition of security of signatures for ECDSA. The student answered another question from the opponent. Committee approved the grading suggested by the supervisor and the referee.

Result of defence: excellent (1)

Chair of the committee: Příhoda Pavel, doc. Mgr., Ph.D.

Committee members: Göloğlu Faruk, doc., Dr. rer. nat.

Hnětynková Iveta, doc. RNDr., Ph.D.

Holub Štěpán, doc. Mgr., Ph.D.

Jedlička Přemysl, doc. RNDr., Ph.D.

Patáková Zuzana, RNDr., Ph.D.

Tichý Petr, doc. RNDr., Ph.D.

