Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

ZÁZNAM O PRŮBĚHU OBHAJOBY

DISERTAČNÍ PRÁCE

Název práce: Využití algebraických a kombinatorických metod při studiu hašovacích funkcí (Algebraic and combinatorial methods for the study of hash functions)

Jazyk práce: anglicky

Jméno studenta: RNDr. Daniel Joščák

Studijní program: Matematika

Studijní obor: 4M1 Algebra, teorie čísel a matematická logika

Školitel: doc. RNDr. Jiří Tůma, DrSc.

Oponenti: Mgr.Robert El Bashir, Dr.
Ing. Tomáš Rosa, Ph.D.

Členové komise:
Mgr. Libor Barto, PhD.
Mgr. Robert El Bashir, Dr.
Mgr.Emil Jeřábek, Ph.D.
prof. RNDr. Jan Krajíček, DrSc.
prof. RNDr. Ing. Petr Němec, DrSc.
doc. RNDr. Vítězslav Švejdar CSc.
Dr. Neil Thapen
prof. RNDr. Jan Trlifaj, CSc., DSc.

Datum obhajoby: 23.9.2015

Průběh obhajoby:
Obhajoby se zúčastnil uchazeč, 8 členů komise, oba oponenti a školitel. Komise konstatovala, že všechny podmínky pro konání obhajoby byly splněny a seznámila se s cv uchazeče a s přehledem jeho publikací. Po vyjádření školitele uchazeč vyložil obsah své disertace. Oponenti přednesli hlavní body svých posudků a položili několik dotazů: Dr.El Bashir se zeptal na možná rozšíření výsledků z 1.kap. na další případy AX rovnic a na vztah kolizí popsaných ve 3.kap. ke kolizím, které našly známé algoritmy. Ing.Rosa se zeptal na možnost vnoření konstrukce kolizí popsané v disertaci do známých algoritmů. Kandidát tyto dotazy zodpověděl ke

spokojenosti oponentů a fundovaně reagoval i v následné diskusi o dalších možných směrech výzkumu. Ve všeobecné rozpravě se předseda komise zeptal na genezi disertace, která obsahuje výsledky získané v delším období, prof.Trlifaj se dotázal, jak zasadní je omezení délky slov na 32 bitů, a doc.Tůma zmínil, že jedna z dokázaných matematických vět pomohla najít řadu chyb v existující literatuře o hašovacích funkcích. Uchazeč s přehledem zodpověděl všechny dotazy. Po tajném hlasování vyhlásil předseda komise kladný výsledek a konstatoval, že uchazeč svoji disertaci obhájil a získal titul Ph.D.

Počet publikací: 5

Výsledek hlasování:
Počet členů s právem hlasovacím: 8
Počet přítomných členů: 8
Odevzdáno hlasů kladných: 8
Odevzdáno hlasů neplatných: 0
Odevzdáno hlasů záporných: 0

Výsledek obhajoby: prospěl

Předseda nebo místopředseda komise: prof. RNDr. Jan Krajíček, DrSc.