# Stanovisko habilitační komise k návrhu na jmenování docentem

| | |
|---|---|
| **Masarykova univerzita** | |
| **Fakulta** | Fakulta informatiky |
| **Obor řízení** | Informatika |
| **Uchazeč** | RNDr. Petr Švenda, Ph.D. |
| **Pracoviště uchazeče** | Fakulta informatiky, Masarykova univerzita |
| **Habilitační práce** | Examining and exploiting randomness for cryptography |
| **Složení komise** | |
| **Předseda** | prof. RNDr. Antonín Kučera, Ph.D.<br>*Fakulta informatiky, Masarykova univerzita* |
| **Členové** | prof. RNDr. Otokar Grošek, Ph.D.<br>*FEL STU Bratislava*<br>doc. Dr. Ing. Petr Hanáček<br>*FIT VUT v Brně*<br>doc. Mgr. Jan Obdržálek, PhD.<br>*Fakulta informatiky, Masarykova univerzita*<br>prof. Ing. Petr Tůma, Dr.<br>*MFF UK v Praze* |

## Hodnocení vědecké / umělecké kvalifikace uchazeče

Výzkumná činnost uchazeče je zaměřena na vybrané problémy z oblasti aplikované bezpečnosti. Dosavadní publikační činnost zahrnuje 25 článků ve sbornících mezinárodních konferencí, dvě publikace v časopisech indexovaných databází SCOPUS, a pět dalších publikací nespadajících do výše uvedených kategorií. Vynikající úroveň mají zejména příspěvky z oblasti analýzy RSA klíčů, což lze doložit nejen jejich přijetím na prestižní konferenci USENIX (a získáním ocenění za nejlepší příspěvek na této konferenci), ale rovněž praktickým dopadem těchto výsledků, zejména odhalením nekalých praktik dodavatele identifikačních karet pro vládu v Estonsku. Za tyto výsledky získal uchazeč rovněž cenu rektora Masarykovy univerzity.

Uchazeč v podkladech uvádí 76 citací, z toho 10 v databázi WoS a 31 v databázi Google Scholar. Podle dat dostupných v dubnu 2019 je ale aktuální počet citací ve WoS 25 (15 bez autocitací) a v Google Scholar 329 (220 bez autocitací). Citační ohlas tedy lze považovat za přiměřený, i když nikoliv nadprůměrný.

Komise obdržela rovněž podpůrný dopis od Ing. Jaroslava Šmída, náměstka ředitele Národního úřadu pro kybernetickou bezpečnost, který vysoce oceňuje přínos uchazeče při řešení problémů souvisejících s analýzou čipových karet.

**Závěr**: Vědecká / umělecká kvalifikace uchazeče **odpovídá** požadavkům standardně kladeným na uchazeče v rámci habilitačních řízení v oboru Informatika.

## Hodnocení pedagogické způsobilosti uchazeče

Objem a struktura výuky uchazeče odpovídá pozici odborného asistenta. Na Fakultě informatiky vyučuje kurzy zaměřené na bezpečnost, kryptografii a programování. Vedl cekem 53 bakalářských a 44 magisterských prací, v současné době se podílí rovněž na vedení doktorského studenta.

Velmi pozitivně je třeba hodnotit skutečnost, že uchazeč dokáže zapojit studenty do aktivní vědecké práce a zúročit výsledky této spolupráce i ve formě vynikajících publikací. Dalším indikátorem vynikajících pedagogických kvalit uchazeče je udělení ceny pro nejlepšího pedagoga Masarykovy univerzity.

Většina členů komise byla přítomna přednášce uchazeče pro odbornou veřejnost v rámci habilitačního řízení na téma "Analysis and use of RSA keypair generation bias", která jasně demonstrovala nejen jeho skvělou odbornou erudici, ale rovněž schopnost zaujmout posluchače jasným, zajímavým a výborně strukturovaným výkladem.

**Závěr**: Pedagogická způsobilost uchazeče **odpovídá** požadavkům standardně kladeným na uchazeče v rámci habilitačních řízení v oboru Informatika.

## Hodnocení habilitační práce uchazeče

Habilitační práce uchazeče je souborem deseti vybraných prací opatřených úvodem v rozsahu zhruba padesáti stran. Komise stanovila čtyři oponenty:

Prof. Ross Anderson, University of Cambridge, UK Prof. Kenny Paterson, University of London, UK; ETH Zurich, Switzerland Prof. Krzysztof Pietrzak, Institute of Science and Technology Austria, Austria Prof. Vincent Rijmen, KU Leuven, Belgium

Všechny posudky jsou kladné a vyzdvihují velmi vysokou kvalitu a význam prací z oblasti analýzy RSA klíčů. Výsledky v dalších dvou oblastech, kterým je habilitační práce věnována (adaptivní testování náhodnosti a problémy v oblasti bezdrátových senzorových sítí) jsou hodnoceny rovněž pozitivně. Posudky neobsahují negativní komentáře ani explicitní výhrady.

**Závěr**: Úroveň habilitační práce uchazeče **odpovídá** požadavkům standardně kladeným na habilitační práce v oboru Informatika.

MUNI

# Stanovisko habilitační komise k návrhu na jmenování docentem

**Výsledek tajného hlasování komise**

Hlasování se uskutečnilo: elektronicky

| | | |
|---|---|---|
| Počet členů komise | | 5 |
| Počet odevzdaných hlasů | | 5 |
| z toho | kladných | 5 |
| | záporných | 0 |

**Návrh komise**

Na základě výsledku tajného hlasování následujícího po zhodnocení vědecké / umělecké kvalifikace, pedagogické způsobilosti a úrovně habilitační práce uchazeče předkládá komise Vědecké radě Fakulty informatiky Masarykovy univerzity návrh **jmenovat uchazeče docentem** v oboru Informatika.

V Brně dne 22.04.2019

prof. RNDr. Antonín Kučera, Ph.D. .....