# Stručná charakteristika uchazeče k habilitačnímu řízení na ČVUT v Praze

---

Uchazeč: Dr.-Ing. Martin Novotný

**A) V oblasti pedagogické**

1) Počet doktorandů, pro které byl uchazeč ustanoven školitelem, resp. školitelem specialistou a kteří úspěšně obhájili disertační práci:
   - celkem 2:
     Ing. Vojtěch Miškovský, Ph.D. – obhajoba 29.04.2020 (školitel specialista)
     Ing. Petr Socha, Ph.D. – obhajoba 10.11.2023 (školitel)
   - Dále vede jako školitel specialista tyto doktorandy po úspěšně složené SDZ:
     Ing. Stanislav Jeřábek (odevzdal disertační práci 31.08.2023)
     Ing. Jiří Khun
   - Dále vede jako školitel tyto doktorandy:
     Ing. David Pokorný (po odborné rozpravě, přihlášený k SDZ v dubnu 2023)
     Ing. Tomáš Přeučil (odborná rozprava plánována na 14.02.2023, přihlášený k SDZ v dubnu 2023)
2) Počet obhájených diplomových/bakalářských prací, které uchazeč vedl:
   - Celkem 60+, z toho v období 2014-23:
     6 diplomových prací (z toho 3 byly oceněny cenu děkana)
     13 bakalářských prací (z toho 7 bylo oceněno cenou děkana)
3) Jeden nejvýznamnější počin uchazeče v oblasti výuky:
   - Zavedení nového předmětu NI-BVS Bezpečnost vestavných systémů
4) Hodnocení uchazeče ve studentské anketě v posledních 4 semestrech:
   - ZS 2021/2022: 1,13 (96 známek)
   - LS 2021/2022: 1,09 (44 známek)
   - ZS 2022/2023: 1,21 (76 známek)
   - LS 2022/2023: 1,18 (40 známek)

**B) V oblasti tvůrčí**

1) Tři významné původní výsledky tvůrčí činnosti nebo arch. či uměl. realizace:

   Za hodnocené období 10 let:

   - Socha, P., Brejník, J., Balasch, J., Novotný, M., & Mentens, N. (2020). Side-channel countermeasures utilizing dynamic logic reconfiguration: Protecting AES/Rijndael and Serpent encryption in hardware. Microprocessors and Microsystems, 78, 103208. (2 citace ve WoS, 3 citace ve Scopus – po odečtení autocitací)
   - Socha, P., Miškovský, V., Kubátová, H., & Novotný, M. (2017, April). Optimization of Pearson correlation coefficient calculation for DPA and comparison of different approaches. In 2017 IEEE 20th International Symposium on Design and Diagnostics of Electronic Circuits & Systems (DDECS) (pp. 184-189). IEEE. (10 citací ve WoS, 12 citací ve Scopus – po odečtení autocitací)
   - Pokorný, D., Socha, P., & Novotný, M. (2021, February). Side-channel attack on Rainbow post-quantum signature. In 2021 Design, Automation & Test in Europe Conference & Exhibition (DATE) (pp. 565-568). IEEE. (2 citace ve WoS, 6 citací ve Scopus – po odečtení autocitací)

   Celkově:

   - Güneysu, T., Kasper, T., Novotný, M., Paar, C., & Rupp, A. (2008). Cryptanalysis with COPACOBANA. IEEE Transactions on computers, 57(11), 1498-1513. (66 citací ve WoS, 93 citací ve Scopus – po odečtení autocitací)
     (*pozn: rok 2008, před obdobím 2014-2023*)
   - Gendrullis, T., Novotný, M., & Rupp, A. (2008, August). A real-world attack breaking A5/1 within hours. In International Workshop on Cryptographic Hardware and Embedded Systems (pp. 266-282). Springer, Berlin, Heidelberg. (20 citací ve WoS, 26 citací ve Scopus – po odečtení autocitací)
     (*pozn: rok 2008, před obdobím 2014-2023*)

2) H index s vyloučením autocitací:
   - WoS: 6
   - Scopus: 6
3) Počet citací WOS/Scopus/ohlasů arch. díla, vždy s vyloučením autocitací:
   - WoS: celkem 167, z toho 140 v období 2014-2023
   - Scopus: celkem 221, z toho 180 v období 2014-2023
   - WoS + Scopus: celkem 236, z toho **191** v období 2014-2023
4) Mobilita (pobyt na zahraničním pracovišti – místo, délka a výsledek pobytu):
   - Ruhr-University Bochum
     Horst-Görtz Institute
     Chair for Embedded Security (prof. Christof Paar)
     Universitätsstraße 150
     44801 Bochum, Germany
     1.2.2007 - 31.7.2007, 1.9.2007 - 31.8.2008 (celkem 18 měsíců)
     *Výsledky pobytu*: Hardwarová podpora výpočetně náročné kryptoanalýzy, článek v IEEE Transaction on Computers, článek na konferenci CHES 2008, obhájená disertační práce (titul Dr.-Ing.)
   - Università della Svizzera italiana (dr. Francesco Regazzoni)
     via Buffi 13
     6900 Lugano, Switzerland
     15.01.2024 - 14.02.2024 (1 měsíc)
     Výsledky pobytu: Práce na obvodu pro hardwarovou (FPGA) podporu Möbiovy transformace pro řešení soustavy Boolských rovnic, Studie přenositelnosti tohoto obvodu na cluster obvodů FPGA.
5) Dva nejvýznamnější grantové projekty, kde byl uchazeč v pozici řešitel či spoluřešitel (navrhovatel či spolunavrhovatel): ERC, H2020, apod.:
   - DRASTIC: Dynamically Reconfigurable Architectures for Side-channel analysis protecTIon of Cryptographic implementations. Projekt CELSA/17/033 (Central Europe Leuven Strategic Alliance, https://celsalliance.eu/). Účastníci projektu: KU Leuven (Belgium) a ČVUT v Praze, 2017-2019.
   - Tools for AI-enhanced Security Verification of Cryptographic Devices (Nástroje pro verifikaci bezpečnosti kryptografických zařízení s využitím AI). Grant VJ02010010 byl podpořen Ministerstvem vnitra ČR ve veřejné soutěži 2.VS IMPAKT 1, 2022-2025.
6) Příklad(y) uplatnění výsledků uchazeče v praxi:

- Ing. David Röhlich: firmware pro počítadlo cestujících ve vestibulu metra (1993)
- DataCon, s.r.o.: firmware pro záznamové zařízení KoroDat (1994)
- 2N telekomunikace, a.s.: firmware pro kódový zámek (1996)
- 2N telekomunikace, a.s.: firmware pro Vrátník/Vrátník 2000/výtahový hlásič (1999 – 2008)
- CESNET: Vstupně/výstupní rozhraní pro JPEGencoder a JPEGdecoder (2010)
- Lešikar, a.s.: Odolnost tachografických snímačů TSAES a TS3DES vůči rozdílové odběrové analýze (2018-2019)

7) Nejvýznamnější uznání komunitou (vč. ocenění v arch. či uměl. soutěži):
   - Pořádání IACR konference Cryptographic Hardware and Embedded Systems (CHES 2023)
8) Nejvýznamnější počin služby komunitě:
   - General co-Chair konference CHES 2023 v Praze (https://ches.iacr.org/2023/contact.php)
   - General Chair konference CARDIS 2019 v Praze (https://cardis2019.fit.cvut.cz/committee.html)
   - Program Chair Euromicro conference on Digital System Design (DSD) 2018 (https://dsd-seaa2018.fit.cvut.cz/dsd/index.php?sec=comm#page_header)
   - Program co-Chair Euromicro conference on Digital System Design (DSD) 2017 (https://dsd-seaa2017.ocg.at//dsd2017.html)
   - člen ediční rady časopisu MICPRO (https://www.sciencedirect.com/journal/microprocessors-and-microsystems/about/editorial-board)
   - Program co-chair sekce Architecture and Hardware for Security Applications (AHSA) na konferenci DSD (2016 – dosud)
   - Člen programového výboru mezinárodních konferencí (DATE – track DT6: 2022 – dosud, DSD: 2013 – dosud, PESW: 2014 – dosud)
   - Založení Embedded Security Lab na ČVUT v Praze, FIT

**V Praze dne 8.11.2024**

**Habilitační komise:**

**prof. Ing. Jiří Jakovenko, Ph.D. (předseda)**

---

**prof. Ing. Viktor Fischer, CSc.**

---

**prof. Ing. Lukáš Sekanina, Ph.D.**

---

**prof. Ing. Václav Matoušek, CSc.**

---

**prof. Ing. Pavel Čičák. Ph.D.**

---

prof. Ing. Lukáš Sekanina, Ph.D. _____

prof. Ing. Václav Matoušek, CSc. _____

prof. Ing. Pavel Čičák. Ph.D. _____