REGISTRATION FORM FOR CZECH SCIENTIFIC INSTITUTION

1. Research institution data (name and address):

Faculty of Informatics
Masaryk University
Botanická 68a
Brno 602 00

2. Type of research institution: Public university (veřejná vysoká škola)

3. Head of the institution: prof. RNDr. Jiří Zlatuška, CSc. — Dean

4. Contact information of designated person(s) for applicants:

prof. RNDr. Petr Hliněný, Ph.D. – Vice-Dean for Research, Development, and Doctoral Studies
hlineny@fi.muni.cz
Faculty of Informatics, Masaryk University
Botanická 68a, Brno 602 00

5. Research discipline in which the strong international position of the institution ensures establishing a Dioscuri Centre:

Natural Sciences and Technology: *Computer science and informatics* - informatics and information systems, computer science,scientific computing, intelligent systems

6. Description of important research achievements from the selected discipline from the last 5 years including a list of the most important publications, patents, or other results:

Top publications

- JANČÁR, Ján, Vladimír SEDLÁĞEK, Petr ŠVENDA a Marek SÝS. Minerva: The curse of ECDSA nonces. In Amir Moradi, Mehdi Tibouchi. **IACR Transactions on Cryptographic Hardware and Embedded Systems.** Ruhr-University of Bochum, 2020. s. 281-308. ISSN 2569-2925. doi:10.13154/tches.v2020.i4.281-308.
- GRZESIK, Andrzej, Daniel KRÁĽ a Laszlo Miklos LOVASZ. Elusive extremal graphs. **Proceedings of the London mathematical society.** Cambridge: Cambridge University Press, 2020, No. 121, 6, p. 1685-1736. ISSN 0024-6115. doi:10.1112/plms.12382.
- KOUŘIL, David, Ladislav ČMOLÍK, Barbora KOZLÍKOVÁ, Hsiang-Yun WU, Graham JOHNSON, David S. GOODSELL, Arthur OLSON, Eduard M. GROELLER a Ivan VIOLA. Labels on Levels: Labeling of Multi-Scale Multi- Instance and Crowded 3D Biological Environments. **IEEE Transactions on Visualization and Computer Graphics.** 2019, No. 25, p. 977-986. ISSN 1077-2626. doi:10.1109/TVCG.2018.2864491.
- MAIER-HEIN, Lena, Annika REINKE, Michal KOZUBEK, Anne L. MARTEL, Tal ARBEL, Matthias EISENMANN, Allan HANBURY, Pierre JANNIN, Henning MÜLLER, Sinan ONOGUR, Julio SAEZ-RODRIGUEZ, Bram VAN GINNEKEN, Annette KOPP-SCHNEIDER a Bennett A. LANDMAN. BIAS: Transparent reporting of biomedical image analysis challenges. **Medical Image Analysis.** Elsevier, 2020, No. 66, December, p. "101796", 7 p. ISSN 1361-8415. doi:10.1016/j.media.2020.101796.
- KLAŠKA, David, Antonín KUČERA, Tomáš LAMSER a Vojtěch ŘEHÁK. Automatic Synthesis of Efficient Regular Strategies in Adversarial Patrolling Games. In **Proceedings of the 2018 International Conference on Autonomous Agents & Multiagent Systems.** Richland, SC, 2018. p. 659-666. ISBN 978-1- 5108-6808-3. doi:10.5555/3237383.3237481.
- AGRAWAL, Sheshansh, Krishnendu CHATTERJEE a Petr NOVOTNÝ. Lexicographic ranking supermartingales: an efficient approach to termination ofprobabilistic programs. In **PACMPL (Proceedings of** POPL'18). New York, NY, USA: ACM, 2018. p. 34:1--34:32. ISSN 2475-1421.
- NEMEC, Matúš, Marek SÝS, Petr ŠVENDA, Dušan KLINEC a Václav MATYÁŠ. The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli. In **Proceedings of the 2017** ACM SIGSAC **Conference** on**Computer and Communications Security.** New York, NY, USA: ACM, 2017. s. 1631-1648. ISBN 978-1-4503-4946-8. doi:10.1145/3133956.3133969.

Other achievements

October 2017: A newly discovered vulnerability in generation of RSA keys used by a software library adopted in **cryptographic smartcards,** security tokens and other secure hardware chips manufactured by Infineon Technologies AG allows for a practical factorization attack, in which the attacker computes the private part of an RSA key. Thisserious vulnerability affected, e.g, the **government ID cards** in Estonia and Slovakia.

7. List of no more than 3 important research projects in the selected discipline awarded in national and international calls to the institution in the last 5 years:

Cyber Security Network of Competence Centres for Europe - CyberSec4Europe

prof. Václav Matyáš

H2020

547916 £

Models, Algorithms, and Tools for Solving Adversarial Security Problems

prof. Antonín Kučera

US ARMY

344736 USD

Classification of brain tumors using advanced techniques of multimodal diffusion MRI data

prof. Kozubek

Ministry of Health - applied research

7425000 CZK

8. Description of the available laboratory and office space for a Dioscuri Centre:

Scientific research at FI is organized rather informally, within flexible research groups which can quickly respond to current challenges and trends in the scientific world. Thereare around twenty active laboratories at the faculty in which researchers and students perform leading-edge research, often in cooperation with companies located in the science and technology park directly in the FI building.

Office space and standard computing equipment and support will be provided for a newresearch group. The standard institutional background also includes seminar and meeting rooms and access to supercomputing resources.

Importantly, the Faculty of Informatics premises include also the **CERIT-SP:** Science & Technology Park and Business Incubator. Since 2014, this Technology Park has hosted around 20 Hitech IT companies within an office space of 2,200 sqm directly in the FI buildings. This park offers unique opportunities for more applied research and technology transfer in collaboration with students, researchers and the companies in the park.

9. List of the available research equipment for a Dioscuri Centre:

As stated above, we offer incoming researchers standard office and computing equipment, and access to the **CERIT-SP** Science & Technology Park and Business Incubator in thefaculty building. For special research needs in areas for which the standard office equipment and infrastructure are not sufficient, we offer the following specially equipped laboratories:

- Centre for Biomedical Image Analysis — microscopy imaging, related specialcomputing equipment
- The Human Computer Interaction Laboratory — equipment for virtual andaugmented reality
- Centre for Research on Cryptography and Security — equipment for research withsmartcards, IoT and other cryptography and security research
- Cybersecurity Laboratory (CYBERSEC) — cybersecurity monitoring and training environment, unique KYPO cyber range
- Design and Architecture of Digital Systems Laboratory — hardware, FPGA andsignal processing tools and measurement
- Research laboratory Sitola - advanced technologies for high-performancecomputing, big data processing, and high-speed networking

10. List of the additional benefits (other than listed in the conditions for hosting a DC, see invitation) that the Institution declares to provide for a Dioscuri Centre (i.e.: additional funds, personal benefits, dual career options, relocation support or other):

Our faculty offers an opportunity not only to get involved in cutting-edge research, but provides complete project support and English-speaking administrative staff, and also full support during the onboarding process. Tenure track positions are offered to scientists interested in participating in research at FI and contributing to its further development.

The Faculty of Informatics is a proud holder of the HR Award HRS4R. In April 2021 the Faculty of Informatics, Masaryk University, successfully completed the Initial Phase and has been successfully certificated by the European Commission. The personnel policy and work with human resources is a part of the Faculty's Long-term strategy and the part of the HR Award is entrusted, by the Organizational Rules of the Faculty, to the Office for Research and Development, Projects and Partners.

Masaryk University (MU) also has the Gender Equality Plan for 2020-2025 according tothe goals of the European Union.

11. Other information about the internationalization of the research institution, international researchers employed at the institution, the availability of English language seminars etc.:

The Faculty of Informatics (FI) was founded in 1994 as the first Faculty of Informatics in the Czech Republic. Today, with a steady increase of interest to study, it provides Computer Science education at all levels of university studies for two thousand students in Czech and English. The faculty offers 2 master's programmes ("Computer Systems, Communication and Security", "Software Systems and Services Management"), and also a doctoral study programme "Computer Science" with 2 specializations in English. Currently, there are 13 students from abroad attending the English doctoral programme, but all our doctoral students conduct their research in English regardless of the official study language.

The Faculty of Informatics is committed to offering excellent conditions for research and international collaboration in computer science, and for employment of international research and academic staff. Currently, international research staff includes Achim Blumensath, Bruno Rossi, Bacem Mbarek, Hind Bangui, Simone Kriglstein, Daniel R. E. Giraldo.

The faculty also regularly offers Postdoc positions to international applicants in all areasof CS. We currently host four international postdocs.

The Faculty of Informatics regularly invites distinguished foreign and domestic **scientists** to give plenary lectures at the weekly **Informatics Colloquium** (with a tradition datingback to 1997) and on additional important occasions.

Masaryk University awards honorary degrees to outstanding personalities and we are proud that in the field of Computer Science this award has been given to personalities such as prof. Donald Knuth, prof. Charles Bennett, prof. Thomas A. Henzinger, prof. Javier Esparza, etc.

On the other hand, the excellent international standing of our scientists is witnessed not only by numerous international projects they are involved in (see examples listed above), but also by international prizes and awards they have got, among which we mention the following three outstanding examples: prof. Jozef Gruska (Computer Pioneer Award 1996, IEEE Computer Society), prof. Antonín Kučera (Friedrich Wilhelm Bessel Research Award, 2016), and prof. Daniel Král' (Fellow of the American Mathematical Society, 2020 class).