UNIVERZA NA PRIMORSKEM
UNIVERSITÀ DEL LITORALE / UNIVERSITY OF PRIMORSKA

IAM
INŠTITUT ANDREJ MARUŠIČ
ISTITUTO ANDREJ MARUŠIČ
ANDREJ MARUŠIČ INSTITUTE

Muzejski trg 2, SI – 6000 Koper
Tel.: (+386 5) 611 75 91
Fax: (+386 5) 611 75 92
www.iam.upr.si
info@iam.upr.si

UNIVERZA NA PRIMORSKEM
UNIVERSITÀ DEL LITORALE
UNIVERSITY OF PRIMORSKA

Titov trg 4, SI – 6000 Koper
Tel.: + 386 5 611 75 00
Fax.: + 386 5 611 75 30
E-mail: info@upr.si
http://www.upr.si

Date of publication	31 May 2018
Deadline for submission	prolonged to 16 July 2018
Published	website Andrej Marušič Institute (UP IAM) in and the Employment Service of Slovenia

University of Primorska based on the Article 12 of the Act on Research and Development (Official Gazette of the Republic of Slovenia, No. 22/2006-UPB1, 61/2006-ZDru-1, 112/2007, 9/2011, 57/12-ZPOP-1A and 21/2018-ZNOrg) and the Article 112 of the Rules on procedure for (co)financing, Assessing and Monitoring the Implementation of Research Activities (Official Gazette of the Republic of Slovenia, No. 52/2016 and 79/17) publishes a

PUBLIC TENDER FOR YOUNG RESEARCHER CANDIDATE* IN 2018 IN THE FIELD OF CRYPTOGRAPHY

1. The Purpose of the Public Tender

The purpose of this Public Tender is the selection of the candidates for young researchers to be trained in the University of Primorska Andrej Marušič Institute (UP IAM) for obtaining a doctorate of science.

The candidates who have not yet enrolled in a doctoral degree study programme and will be selected in this tender shall also apply separately for the Tender for Enrolment to Doctoral Degree Study Programme UP Faculty of Mathematics, Natural Sciences and Information Technologies in the 2018/19 Academic Year.

2. Mentors and research fields

Candidates may apply for available position of a young researcher with selected mentor Prof. Enes Pasalic, PhD in the selected field of science and research according to the decision on the selection of mentors for the year 2018 submitted for the *Public call for the selection of mentors positions in the year 2018 – MR +*(Official Gazette of the Republic of Slovenia, No. 3/18) and confirmed by Slovenian Research Agency (N° of notification 6316-21/2017-74 dated 25 April 2018).

Only one candidate can be selected. In case more candidates compete, they will be ranked according to an overall grade achieved in all the selection criteria. The candidate selected will be the highest rated candidate. If the selected candidate resigns or fails to submit the required documents by the deadline specified in the Public Tender, the next candidate shall be admitted according to the overall grade achieved.

No.	MENTOR	RESEARCH FIELD	INSTITUTE OF THE UNIVERSITY OF PRIMORSKA
1	Prof. Enes Pasalic, PhD	Natural sciences and mathematics / Computer sciences	UP Andrej Marušič Institute

Young Researcher candidate in the field of CRIPTOGRAPHY will be trained at University of Primorska Andrej Marušič Institute (UP IAM) for obtaining a doctorate of science. Student's mentor will be Prof. Enes Pasalic, PhD, one of leading experts in symmetric-key cryptography.

The four-year doctoral study, which will begin in the Academic Year 2018/19, includes research work, publication of articles in international scientific journals, project work and teaching exercises as assistant.

The PhD student will conduct research in modern cryptography that includes some contemporary directions such as post-quantum cryptography and/or homomorphic encryption. The former branch of cryptography mainly concerns problem of specifying secure cryptographic primitives which are resistant in presence of quantum computers. In particular, the standard public key cryptography is affected and therefore many alternative approaches have been developed (lattice-based, code-based, multivariate-based cryptography) recently to protect these primitives once quantum computers become reality. Homomorphic encryption or more precisely Fully Homomorphic Encryption has been developed during the last decade but there still do not exist efficient solution for performing standard mathematical operations on the encrypted data instead of decrypting the data, performing such operations and encrypting the data again.

3. Conditions for applying to the Public Tender

The candidate for young researcher must meet the following conditions:

- in the 2018/19 Academic year he/she will be enrolled in Year 1, 2 or 3 of a doctoral degree study programme (Mathematical Sciences, field Cryptography, UP FAMNIT),
- age of up to 28 years (the year of birth is taken into consideration). The age limit is raised over 28 years, if a candidate for a young researcher has already completed one or two years of post-graduate doctoral studies without financial support. For each finished year a year can be added to the age limit,
- has completed the 2nd level of the Bologna study programme (Master's degree) in Mathematics or a Master's degree in studies similar to Mathematics (Computer and Information Sciences, Information Science and Mathematics, Natural Sciences) and an average grade for all examinations and coursework in both 1st and 2nd level of the Bologna study programme of at least 8,00 (including the grade of the graduation thesis in both study levels), or
- holds at least a undergraduate university study degree in Mathematics or in studies similar to Mathematics (Computer and Information Sciences, Information Science and Mathematics, Natural Sciences), obtained in a study programme adopted in the Republic of Slovenia before 11 June 2004 and an average grade for all examinations and coursework (excluding the grade of the graduation thesis) of at least 8,00, and meets the enrolment conditions for the doctoral study programme, or
- holds a comparable degree to that referred to the above-quoted third and fourth indent obtained at foreign universities.

If a young researcher's candidate at the signing of the agreement of training will be or is enrolled in a first or second year of the postgraduate doctoral study programme or has a Master of Sciences degree, obtained in a master's study programme adopted in the Republic of Slovenia before 11 June 2004, the average grade at the undergraduate level in a study programme adopted in the Republic of Slovenia before 11 June 2004 or of both 1st and 2nd level of the Bologna study programme in is not relevant, except in the case of re-enrolment in the first year of the doctoral study programme.

If the candidate for young researcher has used parental leave for a period of at least six months, considering one year for each child, the age limit shall be raised over 28 years. The same shall apply in the case of extended more than six months documented sick leave.

Candidates, who on signing the agreement of training, will be enrolled in an additional year of the third-level doctoral study or have already used that status, candidates who have already received funds by the Slovenian Research Agency (further on ARRS) from the Young Researchers Programme and candidates that have already obtained a PhD may not participate in the Public Tender.

The conditions for applying are determined in the Article 113 of the Rules on procedure for (co)financing, Assessing and Monitoring the Implementation of Research Activities (Official Gazette of the Republic of Slovenia, No. 52/2016 and 79/2017).

4. The candidate evaluation criteria

- the average grade of all examinations and coursework (excluding the grade of the graduation thesis) in the undergraduate university study programme adopted in the Republic of Slovenia before 11 June 2004 or in the 1st and 2nd level of the Bologna study programme, at least 80% of all examinations and coursework must be passed;
- a completed Master of Science course adopted in the Republic of Slovenia before 11 June 2004;
- enrolment in a 3rd level (doctoral) study programme;
- received awards and recognitions;
- published scientific articles;
- collaboration in research and development work;
- evaluation of the interview with the candidate.

The evaluation criteria are determined in the Article 114 of the Rules on procedure for (co)financing, Assessing and Monitoring the Implementation of Research Activities (Official Gazette of the Republic of Slovenia, No. 52/2016 and 79/2017) and in the *Confirmation and Evaluation Sheet*, that must be fulfilled by mentor and is annexed only for information purposes.

5. Duration of funding

ARRS shall finance the training of young researchers for obtaining the doctorate of science for:

- a maximum period of four years if they are enrolled in 3rd level of the Bologna study programme (the new programme).

The financing category of the young researcher is determined by the category of the research programme of the mentor. The determined financing category is valid for the entire period of training.

ARRS shall reduce the financing period defined in the first paragraph: by one year if the young researcher is already in the second year of postgraduate 3rd level studies on signing the agreement of training or by two years if the young researcher is already in the third year of postgraduate 3rd level studies.

According to the decision on the selection of mentors for the year 2018 (ARRS notification MR+) the financing of the young researcher starts on October 2018.

6. The application content

The application for the Public Tender must consist of **completed and undersigned:**

- **Application form (*UP-MRplus-Application/2018*) and**
- **separate annexes**:
  1. **biography,**
  2. **proof of education:**
     - **a photocopy of the graduation certificate with the annex to the certificate or written statement** (*UP-MR+/Statement/2018*) stating, that the candidate will graduate and submit the graduation certificate with annex to the certificate up to 21 September 2018 at the latest;
     - or **proof of the completed Master of Science course**
     - or **proof of enrolment in a postgraduate 3rd level study** (if the candidate is already enrolled in the programme);
  3. **official proof of the all passed examinations and coursework with the average grade** (excluding the grade of the graduation thesis) in the undergraduate 1st level and postgraduate 2nd level of the Bologna study programme or in a undergraduate study programme adopted in the Republic of Slovenia before 11 June 2004,
  4. **undersigned statement by the candidate stating that he has not received funding** in the Young Researchers Programme yet and that the postgraduate study during the training shall not be financed from the other public funds (*UP-MR+/Statement/2018*),
  5. **a photocopy of the valid identification document**,
  6. **undersigned statement by the candidate** (*UP-MR+/Statement/2018*) confirming that the personal information, given in the application, can be used for the records or registers as determined in the *Rules on procedure for (co)financing, Assessing and Monitoring the Implementation of Research Activities,*

7. **a photocopy proofing** possible parental leave or extended more than six months documented sick leave.

If the candidate for young researcher has not obtained a degree in the undergraduate programme or postgraduate programme (2nd level) or a master study programme **in the Republic of Slovenia** must submit further documents:

- **decision of the higher education institution on the recognition** of the foreign education with a view to access to education in the Republic of Slovenia and
- **conversion of the average grade of the undergraduate study** according to the Slovenian higher education evaluation system and considering the evaluation system of higher education abroad, obtained by the training organisation, or
- **written statement** (*UP-MR+/Statement/2018*) stating, that the candidate will submit the decision of the higher education institution on the recognition of the foreign education with a view to access to education in the Republic of Slovenia with the conversion of the average grade of the undergraduate study up to 21 September 2018 at the latest.

The candidate may also include following separate annexes:

- proof of received awards and recognitions,
- proof of published scientific articles (authorship or co-authorship),
- description of the candidates' previous collaboration in the research and development work.

7. The deadline and the method for submission of applications

Applications with annexes must be submitted in sealed envelopes marked **»Ne odpiraj – prijava na javni razpis za mladega raziskovalca pri mentorju prof. dr. Enesu Pasalicu«** / **»Do not open – Application for Public Tender for Young Researchers for mentor Prof. Enes Pasalic, PhD« with first name, last name and full address of the candidate. The applications must be**:

- **delivered personally in the UP IAM headquarters, Muzejski trg 2, SI-6000 Koper** every working day from 8 a.m. till 2 p.m., or
- **sent by mail** on address **UP IAM, Muzejski trg 2, SI-6000 Koper.**

Candidates must submit their applications **till Monday, 16 July 2018 by 2 p.m.** An application shall also be timely if delivered by registered post **from Slovenia** till **16 July 2018** (postal stamp). Application delivered **from abroad** should be delivered in the UP IAM headquarters, Muzejski trg 2, SI-6000 Koper till **16 July 2018. Late applications will not be considered**.

8. The deadline by which the applicants will be informed on the Public Tender results

The candidates will be informed on the Public Tender results according to the *Employment Relationships Act* (The Official Gazette of the Republic of Slovenia, No. 21/2013 and 52/2016).

9. The Public Tender documentation

The Public Tender documentation with the conditions for candidates and instructions on how to apply are available on the UP IAM website (www.iam.upr.si/sl/) and in the headquarters of UP IAM, Muzejski trg 2, SI-6000 Koper till the Public Tender deadline.

The application documentation includes:

- The application form for the candidate for young researcher (*UP-MR+/Application/2018*),
- Instructions on how to apply,
- Form *UP-MR+/Statement/2018,*
- Form *Confirmation and Evaluation Sheet* (fulfilled by mentor) – informative purpose.

10. Additional information and warnings

Candidates who have already received public funds for postgraduate study cannot be financed in the Young Researcher Programme. Additional information on the Public Tender can be obtained in the administrative office UP Andrej Marušič Institute (on telephone and e-mail) and by mentors (on e-mail):

UP MEMBER	TELEPHONE	E-MAIL	MENTOR'S NAME AND LAST NAME	E-MAIL
Andrej Marušič Institute	+ 386 (0) 5 611 75 90	sandra.penko@upr.si	Prof. Enes Pasalic, PhD	enes. pasalic@upr.si

Assoc. Prof. Vito Vitrih, PhD
Director UP IAM

Prof. Dragan Marušič, PhD,
Rector of the University of Primorska

Useful links:

- *Rules on procedure for (co)financing, Assessing and Monitoring the Implementation of Research Activities* (Official Gazette of the Republic of Slovenia, No. 52/2016 and 79/17)
- Slovenian Research Agency – Young Researchers
- Ministry of Education, Science and Sport, ENIC/NARIC CENTRE
- University of Primorska
- UP Andrej Marušič Institute
- Call for enrolment for postgraduate study programmes 2018/19 UP FAMNIT.

* The terms, written in masculine, are used as neutral for male and female.