ROMA TRE
UNIVERSITÀ DEGLI STUDI

Dipartimento di Matematica e Fisica

Rep. n.: 27/2023 Prot. n. 1756/2023
Date: November 28, 2023

The English language version of the call does not have legal value in itself, and thus does not supersede the Italian version of the call (BANDO).

The integral version is available at the following links:
http://host.uniroma3.it/uffici/ricerca/assegni-di-ricerca.aspx
http://matematicafisica.uniroma3.it//dipartimento/bandi-e-concorsi/bandi-per-assegni-di-ricerca/

Art.1

Pursuant to the "Regolamento di Ateneo per gli assegni di Ricerca" a public selection process is established to award ONE grant for temporary research fellowship ("*assegno di ricerca*") for a period-renewable – of **12 (twelve) months** in the Mathematics and Physics Department:

The allowance is subjected to:

- the provisions of the article 4 of Law 13/08/1984, n. 476 (fiscal treatment);
- the provisions of article 2, paragraphs 26 and following, of the law 08/08/1995, n. 335, as further amended (social security);
- the provided in article 1, paragraph 788 of Law 27/12/2006, n. 296, as further amended (sick leave);
- the provisions of the Decree of the Minister of Labour and Social Welfare 12/07/2007, published in the Official Gazette no. 247 of 23/10/2007 (maternity).

Apart from the cases provided for and regulated by the above provisions, it is possible to suspend the research activity for a pre-determined number of months. Suspensions are given by the Board of the Department; at the end of the suspension the "*assegno di ricerca*" will resume or will be permanently stopped.

In all cases of suspension, the payment is immediately interrupted until the date of restart of the activities, certified by the Head of the Department.

In the case of anticipate conclusion of the research activity, the monthly installment will be paid proportionally.

ROMA TRE
UNIVERSITÀ DEGLI STUDI

Dipartimento di Matematica e Fisica

PROJECT TO WHICH THE GRANT REFERS
Cryptography and Cybersecurity Laboratory of Mathematics and Physics Department

TITLE OF THE RESEARCH PROGRAMME OF THE ANNUAL GRANT:
Exploring Multiparty Computation and Number Theory: Algorithmic and Algebraic Perspectives

DESCRIPTION OF THE ANNUAL GRANT RESEARCH PROGRAMME
The primary objective of this research program is to investigate the intersection of Multiparty Computation (MPC) and Number Theory, with a specific focus on algorithmic and algebraic aspects. The aim is to develop novel algorithms, protocols, and theoretical frameworks that leverage on Number Theory by applying its principles to MPC to enhance the efficiency and security of computations.

APPLICATION PROFILE
This research program aims to contribute to the growing body of knowledge at the intersection of Multiparty Computation and Number Theory, with a specific emphasis on advancing algorithmic and algebraic aspects for practical applications in secure and collaborative computations.
Candidates must hold a Ph.D. in mathematics, computer science, or computer engineering concerning topics related to cryptography by the deadline for submitting the application.
The interview will preferably take place in person. In case of proven needs, the committee will consider the possibility of interviewing candidates online through the Teams platform.

Research Plan:

1. **Literature Review:**
   - Conduct an in-depth review of existing literature on Multiparty Computation, focusing on its applications and challenges, in particular in view of post-quantum cryptography.
   - Investigate the state-of-the-art in Number Theory algorithms and identify areas where they can be effectively applied to MPC techniques.
   - Explore algebraic structures in the context of MPC and Number Theory, aiming to identify new ways to exploit these structures for more efficient computations.
   - Investigate the impact of number theoretic properties on the design and security of MPC protocols.
2. **Algorithmic Design:**
   - Develop new algorithms that leverage Number Theory such as modular arithmetic, factorization, and discrete logarithm calculations in use in a context of MPC for performing key operations.
   - Explore ways to distribute the computational load among multiple parties to improve efficiency and scalability.
3. **Protocols for Secure Computation:**
   - Investigate techniques of MPC based on homomorphic encryption and zero-knowledge proofs to enhance the privacy and security of computations.
   - Provide a theoretical analysis of the proposed algorithms, proving their correctness, security guarantees, and computational complexity.
   - Explore the theoretical limits and trade-offs associated with the intersection of Multiparty Computation and Number Theory.
4. **Efficiency Analysis:**
   - Perform a comprehensive analysis of the computational efficiency of the proposed algorithms and protocols.
   - Compare the performance metrics with existing methods to evaluate the practicality and effectiveness of the developed approaches.

GROSS AMOUNT (paid in monthly installments): **€ 32.000,00 comprehensive of all fees due by the Administration.**

Art. 2

To participate to the selection, it is mandatory to have achieved:

- a **PhD Degree in Mathematics**, **computer science, or computer engineering** concerning topics related to cryptography by the deadline for submitting the application, or equivalent title, obtained either in Italy or abroad. In the latter case the candidate must provide a copy of the PhD certificate and an English or Italian translation when the certificate is in another language. Unless the translation has legal value, the candidate should also attach a self-declaration asserting that the translation corresponds to the original.

- a **scientific and professional curriculum** suitable for carrying out the research activity for which the candidate is competing.

Should the PhD or Master Degree have been obtained abroad, the title should be declared equivalent, solely for selection purposes, by the Council of the Mathematics and Physics Department.
The candidate must possess all the required qualifications within the deadline specified in paragraph 3, under penalty of exclusion.

Art. 3

The signed and dated application form, compiled following the template attached at the bottom of the Call (**ANNEX A**) must be sent to the **Mathematics and Physics Department of Roma Tre University – Research Area**
by ordinary e-mail to the address: amm.matematicafisica@uniroma3.it attaching a copy of a valid identity document
and MUST BE SUBMITTED within the final deadline of **January 20, 2024**; otherwise the applicant will be excluded.

Application must include:

- **Appropriate scientific and professional curriculum demonstrating aptitude for research activities;**
- **Self-declaration for the Degrees (ANNEX B);**
- (if any) **list of other titles and or previous scientific publications, and a self-declaration asserting that all the documents and the publications correspond to the originals (ANNEX C).**

Art. 4

The Committee will define the criteria of the selection before proceeding with the evaluation.

Art. 5

1. The research grant cannot be held by students enrolled in undergraduate, Master, Ph.D. or medical specialization in Italy or abroad, and involves placement on unpaid leave or employee with public administration other than those referred to in point .3 below.

2. Participation in the selection is not allowed for spouses, relatives and akin up to and including the 4th degree of the:
- Teaching staff of the Department which has issued this notice;
- Rector;
- General Director;
- Members of the Board Directors.

3. Permanent employees of Universities, Research Institutes or public bodies, the National Institute for New Technologies, Energy and Sustainable Economic Development (ENEA), the Italian Space Agency (ASI) and institutions whose scientific specialization qualification have been recognized as equivalent to a Ph.D pursuant paragraph, of Presidential Decree no. 382 of July 1980, cannot participate in the selection.
4. The research grant cannot be combined with any scholarships, except those awarded by national or foreign institutes to supplement research activities of said temporary research fellows with permanence abroad.
5. The grant for carrying out research activities is governed by a specific individual contract, based on the following criteria: flexibility in meeting the needs of the activity, continuity, time allocation (not sporadic), coordination with the overall activities of the Department, close relationship with the implementation of a research program, autonomous activity within the scope of the program and absence of pre-determined working hours.

Art. 6

For all matters not included here we refer to the laws and rules regarding the "assegni di ricerca"

Roma, November 28, 2023

Rep. N. 27/2023

Head of Mathematics and Physics Department of Roma Tre University
Prof. Roberto Raimondi

ROBERTO RAIMONDI
28.11.2023 10:37:55
GMT+01:00

ROMA TRE
UNIVERSITÀ DEGLI STUDI

Dipartimento di Matematica e Fisica

ANNEX A

APPLICATION FORM

Head of Mathematics and Physics Department of Roma Tre University

The undersigned (name and surname) ..... born

in.....(.....)

date....., place of residence..... (.....) post code ……..

C. F. (fiscal code)…….. (if available)

address for the competition:

town….....(state.....) Street …….....Post Code.....

Telephone number ..... Mobile Phone . …….

E-mail ……..

ASKS

to participate in the competition for the assignment of the grant for the research program titled

"Exploring Multiparty Computation and Number Theory: Algorithmic and Algebraic Perspectives"

Rep. n. 27/2023 Prot. n. 1756/2023 which will take place in the **Mathematics and Physics Department**

DECLARE UNDER ITS RESPONSIBILITY:

1) Citizenship.....;

2) declares to have obtained the degree in..... and obtained in date .....

at the University of..... with the grade of .....;

3) declares to have obtained the PhD in.....

obtained in date ....., at the University of .....;

4) To not receive any kind of other scholarships with the exception of those which are useful to integrate, with trip abroad, the research activity. Or to give up the above scholarship if she/he wins the contest.
5) To not have L.240/2010 research grants for a total period of more than 60 months.
6) To not be an official at the Universities, Astronomical Observatories , Astrophysical and Vesuvian , public bodies and institutions of research in art. 8 of D.P.C.M. 12/30/93, 593 and subsequent amendments and supplements, ENEA and ASI.
7) To not have a degree of consanguinity or affinity up to the fourth degree, with a professor at the Department in which the research grant will be carried out, and even with the Rector, the General Manager or a member of the Board of Governors.
8) To be aware of all the rules contained in the announcement.
9) To undertake to inform the University of any changes of their residence or address.

Attached:

- □ Personal declaration of graduation, indicating the title of the thesis discussed and the final mark. In the case of degree obtained abroad the title of the appropriate equivalence must be accompanied or to be submitted to the Department Council for recognizing the sole purpose insolvency - ANNEX B ;
- □ Declaration attesting the possession of a PhD; in the case of PhD obtained abroad the title of the appropriate equivalence must be accompanied or to be submitted to the Department Council for recognizing the sole purpose insolvency - ANNEX B ;
- □ (optional) List of publications and any other qualifications useful for the assessment of the Commission ;
- □ Detailed scientific and professional curriculum showing the suitability of the research activity to be carried out.

I authorize the Roma Tre University to the processing of personal data, in accordance with law . n . 196 of 30/06/03 .

Date, _____ _____

(original signature)

ROMA TRE
UNIVERSITÀ DEGLI STUDI

Dipartimento di Matematica e Fisica

ANNEX B

DECLARATION SUBSTITUTE FOR CERTIFICATE PREPARED IN SIMPLE PAPER
(DPR 28/12/2000, n° 445 "*Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*)

The undersigned..... (C. F. fiscal number…….....)

born in..... in date....., address.....

..... telephone number ....., mobile phone .....,

e-mail …… aware that false declarations are punishable under the Criminal Code and other rules in force

DECLARE

1b. **Please fill in this box if you obtained the degree from a non Italian University**

declares to have obtained the degree in

_____

obtained in date_____/_____/_____ at the University of_____

Faculty of_____, with the grade of_____/_____

Please fill in this part only if you have already obtained a PhD

(optional)

2. declares to have obtained the PhD in.....,
at the University of .....,
the PhD defense took place in date …….
the title of the PhD thesis is: .....

I authorize the Roma Tre University to the processing of personal data, in accordance with law . n . 196 of 30/06/03 .

Date, _____ _____
(original signature)

Please attach a copy of an identification document, for example your passport

ROMA TRE
UNIVERSITÀ DEGLI STUDI

Dipartimento di Matematica e Fisica

ANNEX C

DECLARATION SUBSTITUTE FOR CERTIFICATE PREPARED IN SIMPLE PAPER
(DPR 28/12/2000, n° 445 "*Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*)

The undersigned..... (fiscal number …….....)
born in..... (.....) in date....., address..... (.....)
Street ....., telephone number ....., Mobile phone. .....,
e-mail …… aware that false declarations are punishable under the Criminal Code and other rules in force

(DECLARES THAT ALL THE COPIES OF THE TITLES, OF THE PUBBLICATIONS, AND ANY OTHER QUALIFICATIONS ATTACHED TO THIS APPLICATION FORM ARE FULLY COMPLIANT WITH ORIGINAL.)

I authorize the Roma Tre University to the processing of personal data, in accordance with law . n . 196 of 30/06/03 .

Date, _____ _____
(original signature)