ROMA TRE
UNIVERSITÀ DEGLI STUDI

Dipartimento di Matematica e Fisica

Rep. n.: 19/2021 Prot. n. 1074/2021
Date: December 16, 2021

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:

RESEARCH PROJECT:
Logical Methods and Formal Verification of Cryptographic Algorithms

Starting in the seventies, many programming languages were born to ensure correctness of source code. These languages applied logical specification and formal verification of properties that programs have to guarantee. Most of these programming languages have syntactic structures derived from functional programming (e.g. standard ML introduced by Milner in 1970) and type assignment systems based on logical solvers (variants of proof-checkers, SMT). While increasing constructs and type systems, one quickly comes across combinations (of languages and/or type systems) that are undecidable (for particular situations involving second-order types, like in Wells' undecidability of type assignment for System F). For this reason, at a certain historical moment, some authors embarked on the development of systems, called proof-assistants (for assisted demonstration), by expanding the expressivity of the language and leaving the sphere of properties that can be proven automatically (decidable) and require an external guide to the type derivation algorithm. From a theoretical point of view, one of these approaches is formalized with the calculus of constructions by Thierry Coquand which is the basis of the Coq software which is precisely the paradigmatic example of proof assistants.
Some of these have become industry standards, for instance, the Z3 language introduced in 2012 (developed by Microsoft). Among automated proof systems, some are variants/specializations of others, and in the specific case of cryptographic protocols (by this we mean algorithms based on the combination of several primitives), they were born as spin-offs of the more general ones; for example, Gilles Barthe's EasyCrypt derives from Coq. A different approach consists in considering a programming language (with some constraints in the type system) and using compilation time to check statements on the code. This is the path taken by F-star which has recently proven both to be able to certify code used in practice and to produce a compiled file which, in addition to having a certificate of correctness (based on the verification of (dependent) types), has proved to be more effective than the initial one. It finally seems that with the new methods it is possible to have a language/compiler that guarantees the specification. This research program aims to study and eventually develop specialized languages for the description and formal verification of cryptographic algorithms and protocols.
APPLICATION PROFILE
This research fellow will collaborate with the Logic and Theoretical Computer Science Group on topics related to the formal specification of algorithms and the verification of cryptographic systems. Knowledge of formal verification systems such as Z3 or proof assistants such as Coq, Matita, Idris, Lean, Easycrypt or compilers ensuring formal correctness such as FStar will be considered preferential. A PhD in Mathematics, Computer Science or Engineering in Computer Science is required.
Telematic Interview.

GROSS AMOUNT (paid in monthly installments): **€ 27.513,00 comprehensive of all fees due by the Administration.**

The allowances 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.

Art. 2

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

- a PhD in Physics or Mathematics, Computer Science or Engineering in Computer Science
- a proven scientific and professional curriculum suitable for carrying out the research activity for which you are competing, possibly certified by the possession of additional research training qualifications or documented and suitable experience for research activity already carried out. Should the Master's Degree have been obtained abroad, the course must be declared equivalent, solely for selection purposes, by the Academic Senate of the University. The candidate must possess the required qualification 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 addressed 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

MUST BE SUBMITTED within the final deadline of January 16, 2022; 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 (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 awarded to 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, December 16, 2021

Rep. N. 19/2021

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

This document complies with the original kept in the archives of the Department

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)……..

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

"Logical Methods and Formal Verification of Cryptographic Algorithms"

Rep. n. 19/2021 Prot. n. 1074/2021 which will take place at 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 ;
- □ 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

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)