Programma Partenariato Esteso "SEcurity and RIghts in the CyberSpace" - Acronimo SERICS, Codice Programma PE_00000014, - CUP H73C22000880001, Avviso n. 341 del 15/03/2022 - Piano Nazionale di Ripresa e Resilienza (PNRR), Missione 4 Istruzione e ricerca – Componente 2 Dalla ricerca all'impresa – Investimento 1.3, finanziato dall'Unione europea – NextGenerationEU

Rep. n.: 24/2024 Prot. n. 2068/2024
Date: December 19, 2024

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

PROJECT TO WHICH THE GRANT REFERS
"Advanced and Quantum-safe Solutions for Digital Identity and digital Tracing" (AQuSDIT)"-
CUP H73C22000880001
TITLE OF THE RESEARCH PROGRAMME OF THE ANNUAL GRANT:
Logical Methods and Formal Verification of Post-Quantum Cryptographic Algorithms
DESCRIPTION OF THE ANNUAL GRANT RESEARCH PROGRAMME
The Lean is a modern proof assistant developed by Microsoft Research, integrating assisted proof and automated deduction features, making it an ideal tool for verifying cryptographic properties. Compared to tools like Coq and Z3, Lean offers an approach that enables the integration of model theory methods into automated verification.
In cryptography, Lean allows for the formal description and validation of complex protocols and algorithms, combining assisted and automated proofs. Its flexibility and integration with SMT solvers like Z3 make it suitable for handling combinations of logical properties typical of cryptography, simplifying formal verification and enhancing code security through advanced computer-assisted deduction methods.
This research program aims to study and develop specialized languages for the formal description and verification of cryptographic algorithms and protocols. The goal is to create tools that enable precise and rigorous representation of security and correctness properties of protocols, with a focus on aspects such as secrecy, integrity, authenticity, and resistance to attacks. These languages are intended to support assisted automatic verification, facilitating the identification and resolution of vulnerabilities in cryptographic structures. Through the development of these languages, the program seeks to provide reliable and formally validated tools for designing secure cryptographic systems, with potential applications across various fields, from cybersecurity to digital authentication and sensitive data protection.
Automated proof methods will be applied to lattice-based encryption and signature schemes with advanced features, such as Attribute-Based Encryption and Threshold Signatures.

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 Lean, will be considered preferential. A PhD in Mathematics, Computer Science or Engineering is required.

Telematic Interview.

GROSS AMOUNT (paid in monthly installments): **€ 25.000,00 comprehensive of all fees due by the Administration.**

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:

Programma Partenariato Esteso "SEcurity and RIghts in the CyberSpace" - Acronimo SERICS, Codice Programma PE_00000014, - CUP H73C22000880001, Avviso n. 341 del 15/03/2022 - Piano Nazionale di Ripresa e Resilienza (PNRR), Missione 4 Istruzione e ricerca – Componente 2 Dalla ricerca all'impresa – Investimento 1.3, finanziato dall'Unione europea – NextGenerationEU

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 Degree in Mathematics**, **computer science, or computer engineering**
- 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 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: ricerca.matematicafisica@uniroma3.it and marco.pedicini@uniroma3.it attaching a copy of a valid identity document and MUST BE SUBMITTED within the final deadline of January 10, 2025; 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 awarded to students enrolled in undergraduate, Master, Ph.D with scholarship 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

Upon appointment, selected candidates must provide self-certification of the following personal details, tax and social security information, and personal attributes:

1. Personal data.
2. Tax data/social security data.
3. The absence of scholarships.
4. Non-tenured employment status at Universities, Astronomical, Astrophysical and Vesuvian Observatories, Public Institutions, and Research Institutions, in accordance with art. 8 of D.P.C.M. 30.12.93, n.593, and subsequent amendments and additions, ENEA, and ASI.
5. The absence of any familial relationship up to and including the fourth degree of kinship or affinity with a professor affiliated with the Department where the grant will be held, or with the Rector, the Administrative Director, or a member of the University's Board of Directors.
6. Non-enrollment in any bachelor's, master's, or master's degree program, PhD with scholarship, or medical specialization.
7. The absence of any other research grants or fixed-term researcher contracts.

Programma Partenariato Esteso "SEcurity and RIghts in the CyberSpace" - Acronimo SERICS, Codice Programma PE_00000014, - CUP H73C22000880001, Avviso n. 341 del 15/03/2022 - Piano Nazionale di Ripresa e Resilienza (PNRR), Missione 4 Istruzione e ricerca – Componente 2 Dalla ricerca all'impresa – Investimento 1.3, finanziato dall'Unione europea – NextGenerationEU

8. Adherence to the overall utilization limits stipulated in paragraphs 3 and 9 of Article 22 of Law 240/2010.

Art. 7

The legally binding commencement date of the research collaboration, including any potential renewals thereof, shall be the first day of the month, and it will remain in effect until the conclusion of the stipulated contractual period. The actual initiation of research activities, duly certified by the Department's Director, shall be determined by the date on which the awardee assumes their position. This date shall also signify the initiation of economic compensation, commencing with the first scheduled salary payment. In the event of a candidate's withdrawal or delayed acceptance among eligible candidates, the subsequent candidate in the ranked order will assume the position, provided they are available. The assignee's responsibilities must exhibit continuity or adhere to a predetermined temporal framework. These responsibilities must align with the overall objectives of the Department and must directly contribute to the execution of the research program or a specific project phase. The assignee is expected to work autonomously without prescribed working hours. The contractual arrangement associated with the grant explicitly excludes any form of teaching activities for the grant recipient. Any allocation of teaching support duties to the assignee necessitates a distinct directive from the Department. Engaging in compensated assignments by the assignee, other than their public administrative employment, which mandates unpaid leave, requires prior authorization from the Departmental Council, in consultation with the research head. Such authorization must confirm compatibility with the grant related responsibilities. Throughout the duration of their service at the University, the grant recipient will be covered by insurance against accidents resulting from their activities performed in the course of their grant-related work. It is important to note that the grant does not confer any entitlements concerning access to University roles.

Art. 8

Any renewal of the check for an additional 12 months beyond the original term provided is decided by the Department Council following the verification carried out by an Investigative Committee, appointed by the Department Director, on the activities carried out and the results obtained by the grant holder (taking into priority the research products carried out), illustrated in a report prepared by the same grant holder.

Art. 9

Pursuant to Law No. 241 of August 7, 1990, the person in charge of the procedure is Research Area Mathematics and Physics Department.

PIETRO
CAPUTO
19.12.2024
20:12:25
GMT+02:00

Roma, December 19, 2024

Rep. N.24/2024

Head of Mathematics and Physics Department of Roma Tre University
Prof. Pietro Caputo

Programma Partenariato Esteso "SEcurity and RIghts in the CyberSpace" - Acronimo SERICS, Codice Programma PE_00000014, - CUP H73C22000880001, Avviso n. 341 del 15/03/2022 - Piano Nazionale di Ripresa e Resilienza (PNRR), Missione 4 Istruzione e ricerca – Componente 2 Dalla ricerca all'impresa – Investimento 1.3, finanziato dall'Unione europea – NextGenerationEU

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 Post-Quantum Cryptographic Algorithms"

Rep. n.24/2024 Prot. n. 2068/2024 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)

Programma Partenariato Esteso “SEcurity and RIghts in the CyberSpace” - Acronimo SERICS, Codice Programma PE_00000014, - CUP H73C22000880001, Avviso n. 341 del 15/03/2022 - Piano Nazionale di Ripresa e Resilienza (PNRR), Missione 4 Istruzione e ricerca – Componente 2 Dalla ricerca all’impresa – Investimento 1.3, finanziato dall’Unione europea – NextGenerationEU

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

Programma Partenariato Esteso "SEcurity and RIghts in the CyberSpace" - Acronimo SERICS, Codice Programma PE_00000014, - CUP H73C22000880001, Avviso n. 341 del 15/03/2022 - Piano Nazionale di Ripresa e Resilienza (PNRR), Missione 4 Istruzione e ricerca – Componente 2 Dalla ricerca all'impresa – Investimento 1.3, finanziato dall'Unione europea – NextGenerationEU

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)