POLITECNICO
MILANO 1863

Prot. n./Prot. no. 262298
Data/Date 10/11/2023
Rep. n. /Index no. 13702/2023

UOR-RPA SGPD – Servizio Gestione Personale Docente
RPA Enrico Eftimiadi
Firmatario/Signatory Prof. Sergio M. Savaresi

Oggetto Bando di selezione per il conferimento di assegni di ricerca

Subject Call to grant temporary research fellowships for research activities

Dipartimento di Elettronica, Informazione e Bioingegneria
Department of Electronics, Information and Bioengineering

Titolo del Programma di Ricerca

“Post-quantum Identification and Encryption Primitives Engineering”

Research Title

“Post-quantum Identification and Encryption Primitives Engineering”

Codice Procedura / Procedure Code: 2023_ASSEGNI_DEIB_125

Scadenza / Deadline 20/12/2023

POLITECNICO
MILANO 1863

SELECTION CALL TO GRANT TEMPORARY RESEARCH FELLOWSHIPS FOR RESEARCH ACTIVITIES UOR DEIB

HAVING REGARD to the Law of 9.5.1989, n. 168, and in particular Article 6, according to which the Universities are allowed to issue autonomous regulations;

HAVING REGARD to Law 24.12.1993, n. 537, "Corrective actions of public finance";

HAVING REGARD to the Decree of the President of the Republic of 28.12.2000, n. 445 - Consolidated laws and regulations on administrative documentation and subsequent amendments and additions;

HAVING REGARD to Legislative Decree n. 196 of 2003, "Code concerning the protection of personal data" and later amendments;

HAVING REGARD to the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data;

HAVING REGARD the Legislative Decree n. 198 of 11 April 2006 "Code on equal opportunities between man and woman, by virtue of Article 6 of Law No. 246 of 28 November 2005", and later amendments;

HAVING REGARD to the Law of 30.12.2010, n. 240, and in particular Article 22;

HAVING REGARD to Directorial Decree 29.7.2011, n. 336 "Determination of the call sectors grouped into call macro-sectors pursuant to Article 15 of Law 240/2010" and later amendments;

HAVING REGARD to Rector's Decree n. 41/AG of 17 May 2005, by which is issued the Regulation on the contribution for participation both in reserved internal examinations and in public entrance examinations organised by Politecnico di Milano;

HAVING REGARD to the Statute of Politecnico di Milano adopted by Rectoral Decree n. 623/AG on 23/2/2012, published on the O.J. of 2/3/2012, n. 52;

HAVING REGARD to Rectoral decree n. 667/AG of 28.02.2011 by which has been issued the Regulations for granting of temporary research fellowships for research activities on internally funded programmes, as amended by Rectoral Decrees No. 2471 of 02.10.2012, 3455 of 13.10.2014, 4674 of 19.12.2014, 2013 of 30.04.2015, 3398 of 29.07.2016, 8268 of 20.12.2017 and n. 6605 of 27.09.2018, 3983 of 29.05.2019 and further amended by Rectoral Decree no. 9232 of 23/12/2020;

HAVING REGARD to the Legislative Decree n.36 of 30/04/2022 "Further urgent measures for the implementation of the National Recovery and Resilence Plan (PNRR)" and in particular the art.14, paragraph 6-quaterdecies;

HAVING REGARD to the resolution of the Department of Department of Electronics, Information and Bioengineering by which it is approved the call proposal for a public selection for the assignment of n° 1 temporary research fellowship to carry out the research activity, on a fixed-term basis, within the programme called "Post-quantum Identification and Encryption Primitives Engineering";

HAVING REGARD to the D.D. 104 of 02/02/2022 (call PRIN 2022), within the framework of the National Recovery and Resilience Plan, Mission 4 Education and research – Component 2 From research to business – Investment 1.1, funded by the European Union – NextGenerationEU

PROVIDED the financial availability,

Article 1 - Scope of the contract

A public selection is hereby organized to grant n° 1 temporary research fellowship to grant research

activity, on a fixed-term basis:

Department: Department of Electronics, Information and Bioengineering

Location: DIPARTIMENTO DI ELETTRONICA, INFORMAZIONE E BIOINGEGNERIA

Area: 09 - Industrial and Information Engineering

Academic Discipline: ING-INF/05 - INFORMATION PROCESSING SYSTEMS

Duration of the contract (months): 12

Expected start date of activity: 01 february 2024

Article 2 - Research Programme

Research Title (and research sub-programme):
Post-quantum Identification and Encryption Primitives Engineering
Implementing Protected Post-Quantum Primitives PRIN POINTER - ID-2022M2JLF2 - CUP D53D23008740006

Research programme description:
Post-Quantum (PQ) cryptographic algorithms built on error correcting codes are one of the most promising and timely research directions in the area of information security. Confidence in them is concrete, since code-based cryptosystems, along with those based on lattice structures, were selected in the final round of the NIST standardization effort for PQ cryptography. The research programme will tackle the efficient implementation of proposals to the additional call of the NIST post quantum standardization process, considering signature algorithms.
The activity carried out in this research programme will contribute to the Italian MUR PRIN 2022 project POst quantum Identification and eNcryption primiTives: dEsign and Realization (POINTER) ID-2022M2JLF2.

Starting and implementation of the research programme:
The research programme is expected to contribute to the realization of post quantum signature primitives, considering as a target use the one of digital identity documents. The approach will involve a critical evaluation of the primitives which have been submitted for the NIST additional call for post quantum signatures, considering in particular the ones based on hard problems from coding theory, due to the high confidence in the computational hardness of the problems which they provide. After the evaluation phase, a high efficiency implementation for the designated candidate will be realized. The implementation will consider the efficiency tradeoffs, picking either an ISA extension or a dedicated accelerator as a solution.

Activities that the Temporary Research Fellow will carry out, obligations of the Temporary Research Fellow and conditions :
The candidate is expected to be analyzing the current proposals to the NIST additional call and evaluate critically their computational and memory requirement. Once a scheme, compatible with implementations targeted to embedded systems is selected, the candidate will design and implement the said scheme, evaluating the possible strategies for hardware-accelerated realizations.

Countries and structures in which the research activity can be carried out:
EUROPA

Article 3 - Participation requirements

In order to participate to the selection procedure, candidates must possess **a "Laurea Magistrale" (equivalent to Master of Science) of the class (LM-32) Computer systems engineering or related degrees that are considered equated and equivalent ex lege or other possible qualifications that are considered equivalent ex lege to the corresponding degrees under the old educational system**[1]

If the academic qualification/s mentioned above is/are/was/were obtained abroad, it/they must be the official qualification/s of the foreign university system, issued by an institution officially recognized in the foreign system of reference. With reference to the Master of Science mentioned in the previous paragraph, if obtained abroad, this must be equivalent, for the sole purpose of selection, by type, level and correspondence of study subject, to the related Italian qualification indicated above and it can allow the access to a Ph.D. programme in Italy.
Equivalence, as regards the correspondence of study subjects, will be notified by the Head of the Department where the research activity will be carried out.
Candidates must have obtained the required academic qualifications by the deadline indicated in Article 4, in order for the application to be valid.

1 The Interministerial Decree 9.7.2009 relating to the **equivalence** between old university system degrees, laurea specialistica and laurea magistrale study programmes, is made available at the following link: https://www.miur.it/UserFiles/3160.pdf
The Interministerial Decrees that establish the **equipollence** of Italian academic qualifications applied to participation in public calls for application are available at the following link: http://www.istruzione.it/archivio/web/universita/equipollenze-titoli.html

Article 4 - Application and participation deadline

For the purposes of selection, the candidate must fill out and send, within the compulsory deadline of 20 december 2023 or s/he will be excluded from the call, the admission application, and the related signed summary, by accessing the Online Services of Politecnico di Milano - section Competitions and selections - Competitions/selections for entrusting of assignments/positions - Temporary Research Fellowships, and attach what required by the Call.
If the aforementioned deadline falls on a holiday, it will shift to the immediately next weekday other than a holiday.

Article 5 - Participation contribution

Applicants must pay by the deadline for submitting the application, and under penalty of exclusion from the selection procedure, a contribution fee of **25.82 Euro**, without the right to a refund in the event of non-participation for any reason, through the unified system for electronic payments to the public administration **PagoPA**, following the instructions of the online application submission procedure.

Alternatively, **only for those who are unable to proceed with the aforementioned payment system** (in particular, in case of payments made abroad if the candidate is not a credit card holder, or in case the credit card is not accepted by the system), it is possible to proceed through a bank transfer on the Current Account registered to Politecnico di Milano - P.zza Leonardo da Vinci, 32 - 20133 Milan, with the following bank details:
IBAN: IT34T0569601620000001600X69 SWIFT: POSOIT22
Reason for payment: "(....) Procedure Code 2023_ASSEGNI_DEIB_125".

Is required to upload the payment receipt/authorization.

Article 6 - Exclusion and withdrawal

The candidate is provisionally admitted to the selection. The Head of the Procedure can decide, at any time, to **exclude from the selection** by fax, registered letter, telegram or PEC, for the following reasons:

- **the electronic submission of the admission application after the compulsory deadline mentioned in Article 4 of the call;**
- **failure to sign the application form summary;**
- **lack of a professional scientific curriculum vitae written in Italian or English;**
- **lack of the copy of a valid identity document**;
- **failure to pay the participatory contribution within the deadline provided;**
- **lack of compliance with requirements of Article 3 of the call;**
- **incompatibility situations of Article 14 of the call;**
- **Any other breach of the requirements of the call.**

If the reasons for the exclusion have been ascertained after the selection process, the Head of the Procedure **can withdraw the rights for participation in the selection;** the withdrawal of candidates will be applied to candidates that stated false declarations in the admission application for the selection or false declarations given, according to the Presidential Decree 445/2000.

Article 7 - Selection Board

The selection is carried out by a specialized Commission, appointed by Directorial Decree, whose members are designated by the Director of the Department concerned.

The Commission consists of three components chosen among professors and researchers with research experience on the topics subject of the call, guaranteeing, as a rule, adequate gender representation.

Article 8 - Selection procedure

The selection board proceeds to the selection, for which it has a total of **100 points**, by the evaluation of qualifications and curriculum vitae submitted by the candidate and the interview, taken through the procedures defined by the board, aimed at assessing the candidate's aptitude for the research object of the selection , according to the following criteria:

- **Relevance of qualifications with the research programme object of selection points 15**
- **Consistency of the candidate's overall profile with respect to the content of the research programme object of selection points 30**
- **Relevance of publications, thesis and scientific products presented with the research programme object of selection points 30**
- **Interview aimed at ascertaining the candidate's aptitude for the research object of the selection points 25**

Applicants can submit a **maximum of 4 publications and certified scientific products**, in addition to any final theses that were presented for the achievement of academic qualifications.
Texts accepted for publication will be evaluated. Abstracts of academic theses, scientific publications, texts accepted for publication and certified scientific products are also considered acceptable submissions.
Only the contents that are attached will be assessed.
If more than 4 publications and certified scientific products or abstracts are attached, only the first 4 will be evaluated.
Furthermore, the university graduation thesis/scientific publications/texts accepted for publication/scientific products (or related abstracts), in order to be evaluated, must be submitted and/or written/translated in one of the following languages: Italian, English, French, German and Spanish. The translated texts must be submitted together with the text in the original language.

The selection is considered as successfully passed with a minimum score of 70 points.

In the event of an equal score, holding a Ph.D. qualification, will be considered as preferential title for the assignment of the temporary research fellowship; the latter applies only to selection procedures where the PhD qualification is not a compulsory entry requirement. If all equally scoring candidates lack the Phd qualification, preference shall be accorded to the younger candidate.

Article 9 - Selection interview

The interview, aimed at assessing the candidate's aptitude for the research object of the selection, **will be held**, unless there is an impediment by one or more members of the selection board to be present or connected electronically and it is not possible to replace him/her/them[2], **on 18/01/2024 at 15:00 , exclusively by means of teleconference.**

Candidates must ensure that the workstation from which they will perform the interview is equipped with a webcam, essential for their recognition, as well as a microphone and headphones/audio speakers.
At the beginning of the interview, candidates must present a valid identity document to the Commission, preferably using the one previously attached to the application.

This call is also a convocation notification for candidates.

Failure to connect electronically to the interview, on the established date and time, or late connection, even if due to force majeure, will be considered as a waiver of participation in the selection.

[2] In this case, it will be responsibility of the P.A. notify candidates of any change of the interview date.

Article 10 - Approval of the Procedure and Ranking list

The decree approving the procedure and the ranking list of the winner candidates and other suitable candidates for selection will be published on the Official Noticeboard of Politecnico di Milano and on the Politecnico Web site.
The publication on the Web site counts as official notification to candidates pursuant to the law.
From the date of publication of the aforementioned decree, it will start the terms for submitting appeals.

Article 11 - Conditions for execution of the contract and the commencement of activities

The candidate declared winner of the selection who has obtained abroad the qualifications required in Article 3 above , if these qualifications have not already been declared equivalent in accordance with the legislation in force, must send to the Teaching Staff Management Service, before signing the contract or they will forfeit the right to sign it:

- the original or authenticated copy of the foreign academic qualification, legalised[3] and accompanied by a certified or sworn translation (in Italian, English, French or Spanish if written in a language different from those mentioned above);
- the diploma supplement, or the certificate of equivalence of qualification, or the transcripts of examinations taken relating to the degree required for participation[4].

For non-EU candidates who are not yet in possession of an Italian Residence Permit, this submission must be compulsorily carried out before the starting of activity.

Non-EU candidate declared winner of the selection procedure and who obtained the qualification listed in Article 3 above in Italy and who, on the date of the application's submission do not yet has a residence permit in Italy , must provide the originals or copies authenticated by Italian Authorities of the academic qualifications obtained in Italy which are required for admission to this selection procedure (Art. 3 of the Call) to the Teaching Staff Management Service before the starting of the activity.

Non-EU candidate who, at the date of the application's submission, has a residence permit in Italy or has the receipt for the residence permit request in Italy, **if declared winner of the selection procedure**, must show the original copy of the residence permit (or the receipt for the residence permit request) to the Visiting Professor Welcome Office, by and no later than the date set for the contract's execution. Failure to provide the document will result in the automatic forfeiture of the right to enter into the contract.

Non-EU candidate who, at the date of the application's submission, do not yet has a residence permit in Italy , if declared winner of the selection procedure, must compulsorily obtain authorisation from the Prefecture, which is necessary to apply for an entry visa. Activities can only commence after the above-mentioned visa has been presented to the Visiting Professor Welcome Office. Failure to provide the document will make it impossible to commence the activity.

The Administration reserves the right to carry out controls on the declarations produced regarding qualifications (obtained in Italy or abroad) and on publications/thesis/scientific products submitted.

3 Please note that in the countries which signed The Hague Convention of 5 October 1961 regarding the abolition of the legalisation of public documents obtained abroad, the need to legalise documents issued by foreign authorities is replaced by another formality: affixing an "apostille" by the competent authority internally designated by each State.
Moreover, it is not mandatory to legalise qualifications or to affix The Hague Apostille if the qualification has been issued by one of the countries that ratified the Brussels Convention of 25 May 1987 or if the qualification has been issued by a German institution (Italian-German Convention on the exemption of public deeds from legalisation).
For information concerning the legalisation of foreign qualifications, please visit the website of the Ministry of Foreign Affairs and International Cooperation http://www.esteri.it/MAE/IT/Italiani_nel_Mondo/ServiziConsolari/TraduzioneLegalizzazioneDocumenti.htm?LANG=IT;
or the CIMEA Web site http://www.cimea.it/
or the Hague Convention website https://www.hcch.net/en/instruments/conventions/specialised- sections/apostille

4 The diploma supplement, the certificate of equivalence of qualification and the examination transcripts are not required for those who hold a Research Doctorate.

Article 12 - Contract

The temporary research fellowship to carry out the research activity is governed by a specific individual

contract.

The contract regulates the collaboration on the basis of the following criteria: flexibility according to the needs of the activity, continuous activity, temporally defined, commitment not merely occasional, coordination with the overall activity of the University, close relation to the realization of a research programme, autonomous development of collaboration within the programme, absence of predefined working hours.

By signing the contract, the temporary research fellows will carry out the online course on security provided by the University available on the online service portal of Politecnico under the field "data - security training courses" and submit, within 30 days from the beginning of the activity, copy of the related certificate to the Department where the research activity will take place.

At the end of the contract, the temporary research fellow is required to submit a written report on the research activity carried out and on the results achieved within the project. In case that the report will not be submitted, it will not be possible to renew the temporary research fellowship or sign a contract for a new temporary research fellowship.

Employment under this call falls within the untenured ongoing continuous collaboration category.

To the temporary research fellowship, for what concerns tax matters, it must be applied the provisions of article 4 of the law n. 476 of 13 August 1984, as well as, for social security, those referred in Article 2, paragraphs 26 et seq., of the Law n. 335 of 8 August 1995, and subsequent amendments, for compulsory abstention from work for maternity, the provisions of the Decree of the Ministry of Labour and Social Policies of 12 July 2007, published in the Official Journal n. 247 of 23 October 2007, and, with regard to sick leave, the provisions of the Article 1, paragraph 788, of the Law n. 296 of 27 December 2006, and subsequent amendments, as far as they can be compatible. During the period of compulsory maternity leave, the maternity subsidy paid by INPS in accordance with article 5 of the above-mentioned decree of 12 July 2007 is supplemented by Politecnico di Milano up to the total amount of the temporary research fellowship.

Citizens of EU countries, who are not able to produce the S1 model related to health assistance in their country of origin, can ask to ASL offices for instructions regarding the registration fee to the Italian National Health Service.

The Politecnico di Milano will provide the contracting part insurance coverage for civil liability funded with specific budget items.
The Politecnico di Milano will withhold from the grant salary Euro 3,97 for each solar year, for the additional insurance premium "Students, Research Fellows and Similar Roles Accidents", to cover expenses for any injuries sustained during the performance of all activities related to the research grant.

Article 13 - Amount of the Temporary Research Fellowship

The amount of the temporary research fellowship, referred to the contract duration (see article 1 of this call), paid as deferred monthly instalments, is **Euro 19367** with only deductible expenses included and charged to the contractor.

Article 14 - Incompatibility

The temporary research fellowship cannot be allocated to employees, either in public or private scheme,

including part-time and fixed-term contracts.

The temporary research fellowship cannot be assigned to those enrolled in laurea study programmes, laurea Specialistica or Laurea Magistrale (equivalent to Master of Science) programme, Ph.D. programme with scholarships or medical specialization, in Italy or abroad, and it implies to place in unpaid leave the employee in service with public administrations other than those referred to in the fifth paragraph of this article.

The participation to the selection is not allowed to subjects with a degree of kinship or affinity within the fourth degree (included) with:

- a full and associate professor of the Department that issued this call;
- the Rector;
- the Director General;
- a Member of the Board of Governors.

Those who have already signed contracts for temporary research fellowships pursuant to Article 22 of Law 240/2010 may not participate in this selection, for a number of 6 years, with the exclusion of the period in which the temporary research fellowship was obtained for Ph.D. programme without scholarship, within the maximum limit of the legal duration of the programme. Similarly, those who are not able to carry out the research activity for the entire period provided in Article 1 of the call cannot participate in the selection process, due to the exceeding of the time limits established by Article 22, third paragraph of Law 240/2010 as supplemented by Article 6, paragraph 2bis of the Decree-Law 192/2014, as well as by Article 22 ninth paragraph, Law 240/2010 [5].

The holders of temporary research fellowships cannot be full employees of Universities, institutions and public research and experimentation bodies, of the National Agency for New Technologies, Energy and Sustainable Economic Development (ENEA), of the Italian Space Agency (ASI) and of institutions whose scientific diploma has been recognized as equivalent to a Ph.D. programme according to Article 74, fourth paragraph, of the Presidential Decree n. 382 of 11 July 1980.

The holder of temporary research fellowship can carry out professional activities and sign contracts that fall within the self-employment contracts, provided that carrying out this activity will not provide a lack of performance in the research activity subject of the contract and upon written authorization by the Head of the Structure, after consultation with the Head of the research or programme. These activities are considered as not compatible with the temporary research fellowship in the event of lack of the aforementioned authorization.

The holder of the temporary research fellowship cannot carry out activities that could lead to a situation of conflict of interest with the activities of Politecnico di Milano.

The temporary research fellowship cannot be combined with other fellowships and scholarships except with those granted by national or foreign institutions, useful as integration for research activities abroad for the same holders of the temporary research fellowships.

The temporary research fellow can attend Ph.D. courses, also as extra courses and without the right to scholarship, always subject to pass the admission tests.

---

5 Article 22, third paragraph, law 240/2010 states that *"the total duration of the relations established under this article, including any renewals, may not [...] exceed four years, with the exclusion of the period in which the temporary research fellowship was obtained for Ph.D. programme, within the maximum limit of the legal duration of the programme".*
Article 6, paragraph 2 of the Legislative Decree 192/2014 states that *"The total duration of the relations established under Article 22, paragraph 3, of the law of 30 December 2010, n. 240,* ***is extended for two years".***
Article 22, ninth paragraph, Law 240/2010 states that *"The total duration of the relationships established with the holders of the temporary research fellowships as referred in this article and of the contracts as referred in Article 24, which also existed with different universities, state, non-state or telematic universities, as well as with entities as mentioned in paragraph 1 of this article, with the same subject, cannot, in any case, exceed twelve years, even if it is a non-continuous period. For calculation of duration of the aforementioned relations, the periods spent on maternity or sick leave, according to current legislation, are not relevant.".*

Article 15 - Personal Data Treatment

Pursuant to EU Regulation no. 679/2016, applicants are informed that the processing of personal data supplied by them will be processed, either on paper or electronically, for the sole purpose of this procedure and the possible establishment of the employment relationship and for the purposes related to its management.

The processing will be carried out by the persons in charge of the procedure, as well as by the selection board, also with the use of computerized procedures, in the ways and within the limits necessary to pursue the aforementioned purposes, even in the event of any communication to third parties.

The provision of such data is necessary for the assessment, for the verification of the participation requirements and the actual possession of the declared academic qualifications. Failure to provide such information may preclude such obligations and, in the cases provided for in the notice, may result in the exclusion from the selection procedure.
Further data may be requested to candidates for the sole purpose mentioned above.

The collected data may be communicated to any subjects entitled under the law n. 241/1990, the legislative decree 33/2013 and any subsequent amendments and additions.

The data will be stored, in accordance with the provisions of current legislation, for a period of time not exceeding that necessary to achieve the purposes for which they are processed.

Pursuant to GDPR 2016/679, the Politecnico di Milano may publish on the University website the Curriculum Vitae of the successful candidates as attached to the application form, for institutional purposes and in compliance with Legislative Decree no. 33 of 14 March 2013 (Transparency Decree) as amended by Legislative Decree 97 of 2016. It is understood that, in addition to the complete Curriculum Vitae, it will be possible to provide a specific Curriculum Vitae, without personal data, for the sole purpose of the publication on the University website.

The subjects are granted the rights referred to in the third chapter of EU Regulation no. 679/2016, in particular, the right to access their personal data, to request correction, updating and cancellation, if incomplete, erroneous or collected in violation of the law, and to oppose to their processing for legitimate reasons. Further information is available on the University website at www.polimi.it/privacy.
Complaints can be filed with a specific request to the person responsible for the protection of personal data, point of contact: privacy@polimi.it.

The Data Controller of the Politecnico di Milano is the General Manager delegated by the Rector pro-tempore - contact: dirgen@polimi.it.
Responsible for the processing: the Human Resources and Organization Manager.

Article 16 - Head of the procedure

According to what provided by Article 5 of the Law n. 241 of 7 August 1990 and subsequent amendments, the Head of the procedure for this Call is Enrico Eftimiadi, Human resources and organization - Teaching Staff ManagementService, phone (+39) 02.2399.2272 - (+39) 02.2399.2150 - (+39) 02.2399.2240 - (+39) 02.2399.2156 E-Mail: assegniricerca@polimi.it - Italian Certified E-Mail (in Italian: PEC, Posta Elettronica Certificata) pecateneo@cert.polimi.it.

Article 17 - Final Provisions

For anything not provided in this call, please consult the provisions of the "Regulations for granting of temporary research fellowships for research activities on internally funded programmes" indicated in the premises and available at the following link: https://www.normativa.polimi.it/personale/docenti, as well as applicable laws.

Article 18 - Advertising

This call for applications is advertised on the Politecnico's Official Noticeboard, on the website of Politecnico, of the MIUR and on that of the European Union.

The Head of Department
Prof. Savaresi Sergio Matteo
Signed Savaresi Sergio Matteo

Digitally signed pursuant to Italian Law - Legislative Decree 7.3.2005, No. 82, as amended (subsequent modifications and integrations).