DTELA/AC/AT/

0045

Public Selection for 1 Research Assignments, lasting 12 months, at the Dipartimento di Informatica Giovanni Degli Antoni in accordance with art. 22-ter of Law 240/2010

THE RECTOR

HAVING REGARD TO Law No. 168 of May 9, 1989, "Establishment of the Ministry of University and Scientific and Technological Research";

HAVING REGARD TO Law No. 240 of December 30, 2010, "Provisions on the organization of universities, academic staff and recruitment, as well as delegation to the Government to promote the quality and efficiency of the university system";

HAVING REGARD TO the Statute of the University of Milan, adopted pursuant to art. 2 of Law No. 240 of December 30, 2010, issued by Rectoral Decree on March 15, 2012, as last amended by Rectoral Decree on May 4, 2020;

HAVING REGARD TO the University Regulations for Administration, Finance, and Accounting, issued by Rectoral Decree No. 465 on January 30, 2019;

HAVING REGARD TO Decree-Law No. 45 of June 7, 2025, "Further urgent provisions regarding the implementation of the measures of the National Recovery and Resilience Plan and the start of the 2025/2026 school year," converted with amendments by Law No. 79 of June 5, 2025, with effect from June 7, 2025;

HAVING REGARD TO the resolution of July 8, 2025, by which the Academic Senate expressed a favorable opinion, and the resolution of July 22, 2025, by which the Board of Directors definitively approved the Regulations for the awarding of research assignments, pursuant to art. 22-ter of Law No. 240/2010;

NOTING THAT with Rectoral Decree No. 3882 of September 11th, 2025, the Regulations for the awarding of research assignments, pursuant to art. 22-ter of Law No. 240/2010, were issued;

HAVING REGARD TO the Decree of the Minister of Education, University and Research No. 592 of August 6, 2025, which sets the minimum amount for research assignments;

NOTING THAT the Dipartimento di Informatica Giovanni Degli Antoni on October 31, 2025 approved the activation of research assignments for the gross annual amount of 23.500,00 Euro,

in the scientific-disciplinary area of Mathematics And Computer Sciences for a duration of 12 months approving the related call for applications;

HAVING VERIFIED the economic availability on the aforementioned project;

HEREBY DECREES

Art. 1

Public selection based on qualifications and interview

1. A public selection is announced for the activation of **1 Research Assignments** aimed at introducing young scholars to research and innovation who have held a master's or single-cycle degree for no more than six years and possess a curriculum suitable for assisting with research activities, for a duration of **12 months**, in accordance with art. 22-ter of Law 240/2010:

Dipartimento di Informatica Giovanni Degli Antoni

Competition Code: 0045

Positions: 1

Duration: 12 months

Annual gross amount: 23.500,00 Euro

Scientific-disciplinary area: Mathematics And Computer Sciences

Maximum number of publications to submit at the candidate's discretion: 5

Foreign language required: English

Title and brief description of the Research Program:

Algebraic Methods in Cryptanalysis

The robustness analysis of certain ciphers is based on the idea that any mapping between vector spaces over a finite field Fq is, in fact, a polynomial mapping. The study of the complexity involved in solving (specific) polynomial systems over finite fields is therefore a fundamental tool for assessing the security of cryptographic protocols. In the implementation of cryptographic

primitives, efficient operations play a crucial role both in cryptography and in cryptanalysis. This project aims to obtain new results in the field of cipher security through innovative methodologies that may open new research directions. The focus will be on robustness testing of lightweight and post-quantum cryptographic algorithms recently submitted to various NIST competitions.

Tutor: Prof. Visconti Andrea

Location of activity: Dipartimento di Informatica Giovanni Degli Antoni

Art. 2

Admission Requirements

1. The following are eligible to participate in the selection:

- Candidates, whether Italian or foreign nationals, who, as of the application deadline, hold a master's degree in:
    - All master's degree, or equivalent.

The degree must have been obtained no more than six years ago, and candidates must possess a curriculum suitable for assisting with research activities, which will be evaluated by the Selection Committee. Additionally, the following is required: a. Competence in the research sector or field:

- Extensive cryptographic knowledge related to cryptographic primitives and algorithms.
- Proven prior experience in cryptographic projects and/or experimental/theoretical thesis work in cryptography and/or international/national cryptographic competitions.
- Knowledge of algebra and programming languages.
- Good knowledge of the English language (written and spoken).
- Ability to work both independently and in a team.
- Knowledge of language: English

For qualifications obtained abroad, equivalence with the corresponding Italian qualifications is verified by the Selection Committee and the scientific leader of the research project for the sole purpose of participation in this specific selection or direct assignment.

2. The following may not participate in the selections:

- Permanent staff employed by universities, public research bodies, and institutions whose scientific specialization diploma has been recognized as equivalent to a PhD. pursuant to article 74, paragraph 4 of the Decree of the President of the Republic 11 July 1980, n. 382;

- Those who have benefited from contracts as a fixed-term Researcher pursuant to article 24 of Law 240 of 2010;
- Those who have a family relationship or affinity up to and including the 4th degree with a professor belonging to the Department that proposed the activation of the contract, or with the Rector, the General Director, or a member of the Board of Directors. A spousal relationship is not a reason for inadmissibility from the procedure.

Furthermore, the following may not participate:

- Those who are excluded from the enjoyment of civil and political rights;
- Those who have been dismissed, released, or declared to have forfeited a public employment position with a Public Administration.

The admission requirements must be met by the application deadline.

Art. 3

Submission and Sending of the Application

1. The application for participation in the selection must be submitted, under penalty of exclusion, **by 12:00 PM (Italian time) on December 15, 2025**.
2. The procedure for completing and submitting the application is entirely and exclusively electronic and must be done via the following access link to the

[Elixform procedure]

3. The procedure is divided into two phases:

    a. Registration To register, it is necessary to connect to the aforementioned link and, by following the instructions below, log in or register on the UNIMI website. After registration, the service will send a confirmation email to the email address provided during the procedure, containing the link for activating the credentials. Through these credentials, it is possible to access the ELIXFORM application by clicking the blue button "INIZIA NUOVA RICHIESTA" (START NEW REQUEST).

    b. Completion and Submission of the Application The candidate completes the application for the competition by following the instructions provided by the computer system, filling out the specific form that will be made available from the day the call is published on the University's website, and indicating the code of the competition they wish to participate in.

After completing the form, the candidate must print the application generated by the system, sign it at the bottom with a handwritten signature, and scan it as a PDF file (or, alternatively, sign the application digitally and upload the file in PAdES or CAdES format). The signature at the bottom of the application must be affixed exclusively by handwritten or digital signature. During the application period, the form can be completed—24 hours a day—from any connected computer. The electronic procedure for submitting applications and attachments will be strictly deactivated on the deadline day for the submission of said applications. Applications sent after the deadline will not be considered valid.

To complete the procedure, the candidate must upload the application, signed at the bottom with a handwritten signature and scanned as a PDF (or, alternatively, digitally signed in PAdES or CAdES format), and the following documents:

a) Curriculum vitae in PDF format, not exceeding 30 pages, dated, without any signature or initials. Curriculum vitae, filled out according to the template downloadable from: https://www.unimi.it/en/node/52938, as declared in the application, the curriculum serves as a self-declaration pursuant to arts. 46 and 47 of Presidential Decree 445/2000 regarding the possession of all qualifications listed therein;

b) A numbered, dated, and signed list of the publications submitted for evaluation purposes only, according to the same procedure described above, with a simultaneous self-declaration in lieu of an affidavit attesting to their conformity to the original, signed at the bottom with a handwritten signature and scanned as a PDF, or, alternatively, digitally signed in PAdES or CAdES format;

c) Publications in digital format (pdf), as specified below (it is possible to upload up to 5 files, less than 30 MB);

d) A PDF copy of a valid identification document;

e) A PDF copy of the tax code (codice fiscale);

f) In case of a Ph.D. obtained abroad: a copy of the academic recognition decree (ex-equivalence) of the foreign qualification or the non-academic recognition decree (ex-equivalence);

4. **Upon completion of the application submission**, the system will notify the receipt of the application and attachments by sending an email to the address provided by the candidate.

5. The electronic procedure for completing and submitting the application and attachments must be completed within the scheduled deadline.

6. The procedure is considered complete upon the submission of the application and attachments; if the submission is incomplete, the application will not be considered.

7. Candidates whose applications are incomplete, not submitted within the deadline, or submitted through a method other than those specified above will not be admitted to the selection.

8. In the event of the unavailability of the described electronic procedure, the University of Milan reserves the right to communicate alternative methods for submitting applications through its website.

9. Any change in the address, telephone number, or email address that the candidate chooses for the purpose of the procedure must be promptly communicated to this University using the email address: incarichi.ricerca@unimi.it .

10. Candidates with disabilities are invited to indicate in their application any need for aids or support measures related to their disability, as well as any need for additional time to complete the tests, in accordance with Law 5.2.1992 n.104.

11. All qualifications that the candidate intends to submit must be held by the application deadline and must be listed exclusively on the **curriculum** prepared by the University downloadable from: https://www.unimi.it/en/node/52938.

12. In the application, the candidate declares, under their own responsibility:

    a) The citizenship held;
    b) That they meet the requirements referred to in art. 2;
    c) That they are not excluded from the enjoyment of civil and political rights;
    d) That they have not been dismissed, released, or declared to have forfeited a public employment position with a Public Administration;
    e) That they do not hold another employment relationship, including part-time or fixed-term, with public or private entities;
    f) That they have not benefited from contracts as a fixed-term Researcher pursuant to art. 24 of Law n.240/2010;
    g) That they do not have a degree of family relationship or affinity, up to and including the fourth degree, with a professor belonging to the Department that requested the position and is making the call, or with the Rector, the General Director, or a member of the University's Board of Directors.

13. The Administration reserves the right to carry out checks, including spot checks, on the truthfulness of the self-declarations.

14. It is not permitted to refer to documents submitted to this or other administrations, or to documents attached to the application for another selection procedure.

Art. 4

Application for Admission by Foreign Candidates

1. Foreign citizens, in addition to the provisions of the previous article, must declare in their application for participation:

- that they enjoy civil and political rights in their country of origin, or the reasons for the lack of such a requirement.

2. The qualifications that European Union citizens intend to submit must be listed on their CV.

   Non-EU citizens:

   • If <u>in possession</u> of a valid residence permit: may use the self-certifications and affidavits referred to in Articles 46 and 47 of Presidential Decree No. 445 of December 28, 2000, when proving personal status, facts, and qualifications that can be certified or attested by Italian public or private entities.

   • If **<u>not</u>** <u>in possession</u> of a valid residence permit: must list on their CV the qualifications they intend to submit for evaluation by the Commission, attaching a self-certification attesting to the original.

   All documentation must be submitted in one or more compressed PDF folders

3. The Administration reserves the right to conduct appropriate checks on the truthfulness of the content of the self-declarations.
4. Non-EU citizens must, upon request by the Administration, at any time and in any case upon potential employment, provide qualifications and certificates issued by the competent authorities of their country of citizenship or non-EU countries, legalized by the competent Italian consular authorities or by an official translator.

Art. 5

Publications

1. The scientific publications that candidates intend to submit must be numbered in progressive order, corresponding to the relative dated and signed list, and must be submitted **exclusively in digital format, as PDF**, each of which must not exceed 30MB.
2. The candidate is required to respect the maximum number of publications to be submitted as specified in art. 1. If the list in the curriculum vitae contains a number of publications greater than that established by art. 1, **only the publications that fall within the aforementioned limits according to the ascending order of the list will be taken into consideration for evaluation. In case of discrepancy between the list and the publications submitted, the list shall prevail**.
3. Only publications and texts accepted for publication according to current regulations are eligible for evaluation. Internal memos and departmental reports are not evaluable.
4. Texts or articles accepted for publication by the application deadline must be submitted together with the publisher's acceptance document.

5. Publications included in the list but not submitted, or the submission of publications not included in the list attached to the application, will not be considered by the Selection Committee.

6. For publications edited in Italy, the requirements provided by Law No. 106 of 15 April 2004 and the related regulation issued by Presidential Decree No. 252 of 3 May 2006 apply.

7. For all publications, both published in Italy and abroad, the following must be indicated: a) the date and, if possible, the place of publication; b) ISBN, or ISSN, or DOI code, or another equivalent.

8. Publications must be submitted in their original language. If this is a language other than Italian, French, English, German, or Spanish, the publications must be translated into Italian, with the translation certified as conforming to the foreign text, prepared by the competent diplomatic or consular representation or by an official translator.

Art. 6

Research activities

The Fellowship implies carrying out the activities briefly mentioned below at Dipartimento di Informatica Giovanni Degli Antoni of the Università degli Studi di Milano and under the supervision of Prof. Visconti Andrea of the activities mentioned below:

1. Understand the properties of stream ciphers, symmetric, asymmetric, or hash functions selected by the research team, and to analyze the implementations of these functions as presented in the literature;

2. Construct an algebraic representation of selected ciphers, analyzing both their theoretical strengths and weaknesses;

3. Evaluate the robustness of the algebraic representation using specific tools such as Singular and Magma in conjunction with experimental analysis;

4. Collect data from the experimental analysis, with appropriate documentation of the steps taken;

5. Dissemination of the results obtained through appropriate publications

Art. 7

Withdrawal from the Selection Procedure

1. Candidates who intend to withdraw from the selection procedure for which they have submitted an application may send a withdrawal declaration to the Contracts and Scholarships Office, to the email address **incarichi.ricerca@unimi.it** , attaching a photocopy of their identification document.

2. The candidate's absence on the day of the oral examination is considered a manifestation of their will to withdraw from the selection procedure.

Art. 8

Exclusion from the Selection

1. Candidates are admitted to the selection on a conditional basis.
2. Exclusion due to the lack of one of the requirements set forth in this call for applications is ordered by a reasoned decree of the Rector.
3. If the reasons for exclusion are ascertained after the selection has been completed, the Rector will order the forfeiture of any right resulting from participation in the selection; forfeiture will also be ordered for candidates for whom a declaration made in the application for admission to the selection or a declaration made pursuant to Presidential Decree 445/2000 is found to be untruthful.

Art. 9

Establishment of the Selection Committee

1. The selection procedures are carried out by a committee composed of 4 members proposed by the Department Council, one of whom serves as a substitute.
2. For the establishment of the Selection Committee, the rules on incompatibility and conflicts of interest are observed.
3. The composition of the Committee is published on the University's website.
4. Any requests for recusal of one or more committee members by the candidates may be submitted to the Rector within 10 days from the date of publication of the Rectoral Decree appointing the Committee on the University's website. The recusal request, duly signed and dated, with an attached copy of a valid identification document, must be sent to the certified email address **unimi@postecert.it** and to the email address **incarichi.ricerca@unimi.it** .

Art. 10

Duties of the Selection Committee

1. During its first meeting, the Committee shall appoint a President and a Secretary from within its members.
2. The Committee, having reviewed the evaluation criteria established by the Regulations, shall conduct a comparative evaluation of the candidates based on their curricula, qualifications, and publications submitted by them, and the results of an interview, evaluating their scientific qualification, research aptitudes, and required competencies.
3. The Committee has a maximum of 100 points, 50 of which can be assigned to qualifications and 50 to the interview. The points are assigned to qualifications according to the criteria determined in the following paragraph.

4. Candidates are evaluated comparatively based on the following criteria and according to the point distribution specified and elaborated by the Committee during the preliminary meeting and reported in the "criteria minutes," drafted by the Committee itself:

   a) Any other qualifications besides the degree obtained by the candidate, up to a maximum of **15** points;

   b) Relevance and significance of previously performed research activities, as well as any work experience, in relation to the contents of the research program subject to the selection, up to a maximum of **25** points;

   c) Relevance of the attached publications (maximum 5) to the research program subject to the selection, up to a maximum of **10** points;

   d) Oral examination aimed at verifying the suitability for carrying out the research activity subject to the selection, as well as evaluating knowledge of the English language and/or other languages relevant to the research, up to a maximum of **50** points.

5. The Committee proceeds with the evaluation based on each criterion in the preceding paragraph and assigns a score to each of the points from a) to d), accompanied by a reasoned analytical judgment on each item. Candidates not admitted to the interview will be notified before the oral exam.
6. The Committee draws up a merit ranking taking into account the scores achieved by the candidates. The selection is considered successfully passed with a score of 60 points or higher.
7. In the case of a tie in scores, preference is given to the candidate with the younger age.

Art. 11

Work Schedule

1. The Committee may use electronic tools for collegiate work and may hold its meetings remotely. The interview may also be conducted electronically.
2. The interview is public and will take place on **January 9, 2026 at 11:00 AM**. Candidates are required to constantly consult the pages dedicated to this procedure, the updating of which is considered notification for all purposes.
3. The Committee must conclude its work within forty days from the date of publication of the appointment decree and, once the work is completed, transmit the records to the Head of the procedure.
4. The Rector by decree ensures the regularity of the acts and approves the merit ranking.

Art. 12

Awarding of Contracts

1. The research assignments are awarded, based on the merit ranking, within 30 days of the approval of the documents.

2. The ranking list is valid for three months from the approval of the documents and must be used on a rolling basis in the following cases:

- Inability to finalize the contract due to a lack of the requirements declared in the application;
- Withdrawal from the contract by the candidate(s) called to fill the position;
- Failure to start work or withdrawal by the successful candidate within 30 days from the start of the contract.

3. If the competition is not attended or has no successful candidate, a new call for applications for the research assignment may be issued upon request by the relevant department.

Art. 13

Contract Stipulation

1. The contract specifies: a) the start and end date of the collaboration; b) the required research activities; c) the financial compensation and the funding source for the contract; d) the Scientific-Disciplinary Area and the GSD; e) the Department where the work will be performed and the Tutor to whom to refer to agree on the methods of performance.
2. The collaboration contract is signed by the holder of the assignment and the Rector.

Art. 14

Methods of Collaboration Performance

1. The research fellow is required to carry out the activity specified in the collaboration contract and has the right to use the facilities and equipment of the reference Department for this purpose. Research activities may be carried out in part at external facilities only with the express authorization of the Tutor and the Department Council; this must be communicated to the University Administration.
2. The research fellow is subject to health checks provided for by Legislative Decree No. 81/2008 at the expense of the University.
3. The activity must be carried out continuously, within the limits of the research program and according to the instructions given by the Tutor, who is also responsible for verifying it. The activity must be suspended during the period of mandatory maternity leave. It can also be suspended for serious illness or serious family reasons, or for leave related to

parental leave. The periods of suspension, with the exception of mandatory maternity leave, which, according to current regulations, entails an automatic extension of the contract, can be made up at the end of the natural expiry of the contract, upon agreement with the Tutor and in compliance with the limits imposed by the available funding. A total period of justified absence not exceeding thirty days per year does not constitute a suspension and, consequently, does not need to be made up.

4. During the period of leave related to childbirth, female research fellows are entitled to a maternity allowance disbursed by INPS in accordance with current regulations. In case of sick leave lasting more than four days, research assignment holders are entitled to a daily sickness allowance within the limits provided by law. During the period of mandatory maternity leave, the allowance paid by INPS pursuant to art. 5 of the Decree of July 12, 2007, is supplemented by the university up to the full amount of the research assignment compensation.

Art. 15

Contract Duration

1. The contract has a duration of **12 months** and starts on the first day of the month following the signing date, unless a reasoned request for a waiver is made by the candidate in agreement with the tutor, and in any case for a period not exceeding 90 days.

Art. 16

Termination of the Collaboration

1. The termination of the collaboration is determined by the expiry of the term or by the withdrawal of one of the parties and by any other cause of termination provided for by current regulations. The holder of the research assignment who intends to withdraw from the contract must provide written notice to the Rector and the department with at least thirty days' notice. Failure to provide notice will result in the withholding of compensation proportional to the period of missed notice.

2. The violation by the research fellow of the provisions contained in the "Code of Ethics and Conduct of the University of Milan," and the obligations established by Presidential Decree No. 62 of April 16, 2013, concerning "Regulations on the code of conduct for public employees in accordance with article 54 of Legislative Decree No. 165 of 30 March 2001," as amended by Presidential Decree No. 81 of June 13, 2023, may constitute just cause for withdrawal pursuant to art. 2119 of the Civil Code.

3. The cancellation of the selection procedure is a condition for the termination of the contract, without the obligation of notice.

4. Any other cause for the termination of the relationship is governed by the relevant laws in force.

Art. 17

Incompatibility and Additional Assignments

1. Research assignments are incompatible with:

   - any other employment relationship, including part-time or fixed-term, with public and private entities;

   - holding research grants, including those held at other universities or public research institutions;

   - scholarships or research grants of any kind awarded by national or foreign institutions, except those exclusively aimed at international mobility for research purposes;

   - holding research contracts pursuant to Article 22 of Law 240/2010 (research contracts);

   - holding post-doc contracts pursuant to Article 22-bis of Law 240/2010 (post-doc positions);

   - holding fixed-term research contracts pursuant to Article 24 of Law 240/2010 (RTT).

2. A research assignment is not compatible with attending degree courses, specialized or master's degree courses, Ph.D. or medical specialization courses, in Italy or abroad, without prejudice to the possibility of implementing specific research funding programs of the European Union within the framework of the Marie Skłodowska-Curie (MSCA) program, and it entails unpaid leave for employees serving in public administrations.

3. The total duration of relationships established with holders of positions referred to in arts. 22, 22-bis, and 22-ter and contracts referred to in art. 24, including with different universities (state, non-state, or online), with institutions of Higher Education in Art, Music, and Dance, with institutions whose scientific specialization diploma has been recognized as equivalent to a Ph.D. title pursuant to art. 74, paragraph 4, of Presidential Decree No. 382/1980, and with public research bodies, may not in any case exceed eleven years, even if not continuous. For the purpose of the duration of the aforementioned relationships, periods spent on maternity or paternity leave or for health reasons according to current regulations are not taken into account.

4. Research assignments do not give rise to rights regarding access to University roles, nor can they be computed for the purposes of art. 20 of Legislative Decree 25/5/2017, n. 75.

5. The holder of a research assignment may carry out a limited self-employment activity, subject to agreement with the Tutor and written communication to the competent office, provided that such activity is declared by the department where they work as compatible

with the research activity they are required to perform and does not entail a conflict of interest.

- Activities as a speaker in seminars, conventions, conferences, and journalistic activities carried out outside the University are compatible with the research assignment;
- Pursuant to art. 45 of the University's General Regulations, the holder of a research assignment may act as a Trainer or Tutor, by registering in the appropriate lists and receiving the related compensation provided by the Board of Directors.

Overall, the self-employment activity may not exceed a gross annual income limit of 15,000 euros.

Art. 18

Economic, Tax, Social Security, and Insurance Treatment

1. The amount of the research assignment is **Euro 23.500,00** gross per year.
2. For the research assignments referred to in this article, the provisions of art. 4 of Law No. 476 of August 13, 1984, apply for tax matters; the provisions of art. 2, paragraphs 26 et seq., of Law No. 335 of August 8, 1995, apply for social security matters; the provisions of the Decree of the Minister of Labour and Social Security of July 12, 2007, published in the Official Gazette No. 247 of October 23, 2007, apply for mandatory maternity leave; and art. 1, paragraph 788, of Law No. 296 of December 27, 2006, applies for sick leave.
3. Regarding risks from accidents and civil liability, the University provides the relevant insurance coverage.

Art. 19

Personal Data Processing

1. The personal data provided by the candidate will be collected and processed by the University as the Data Controller in compliance with EU Regulation 679/2016 (General Data Protection Regulation or, more briefly, GDPR) as well as Legislative Decree No. 196/2003 (Code on the protection of personal data) and its subsequent amendments and additions, for purposes related to the performance of the public selection. The privacy notice is available at this page.

Art. 20

Head of the Procedure

1. The Head of the selection procedure related to this call for applications is the Head of the Self-Employment and Similar Sector - Dr. Anna Tavano – email: **anna.tavano@unimi.it** .

2. Information or clarifications regarding the methods of application submission can be requested from the Contracts and Research Grants Office, email: **incarichi.ricerca@unimi.it** .

Art. 21

Final Provisions

1. For anything not expressly provided for in this call for applications, the provisions of the regulations cited in the premises of this decree, as well as the current laws on the subject, apply where applicable.

THE RECTOR

Marina Brambilla