Offer #2022-05411

Post-Doctoral Research Visit F/M Post-doctoral researcher in lattice algorithms, including parallel or quantum algorithms.

Contract type : Fixed-term contract

Renewable contract : Yes

Level of qualifications required : PhD or equivalent

Fonction : Post-Doctoral Research Visit

Context

Within the framework of a partnership

- the ERC Advanced Grant "Lattices in a Parallel and Quantum World" (PARQ)

The researcher will be hosted by the Computer Science Department of the Ecole normale supérieure (ENS), located in downtown Paris (5th arrondissement).

There are possibilities to extend the contract. There is flexibility for the starting date.

Assignment

For a better knowledge of the proposed research subject :

Lattices are mathematical objects which have emerged in the past twenty years as a key technique for public-key cryptography: the ongoing standardization of homomorphic encryption and the majority of the candidates to NIST's post-quantum standardization rely on the conjectured hardness of lattice problems.

The PARQ project aims at readying lattice-based cryptography for real-world deployment, by protecting it against the most powerful adversaries, from ASIC farms to quantum computers. It will study the best parallel and quantum algorithms for lattice problems, and propose automated tools to select safe parameters.

Collaboration :
The recruited person will be in connection with the P.I. Phong Nguyen, as well as Frédéric Magniez and Brice Minaud.

Main activities

The goal is to study the best parallel and quantum algorithms for lattice problems, as well as design new tools to select safe parameters for lattice-based cryptography.

Skills

Languages : English.

Other valued appreciated : Curiosity

Benefits package

- Subsidized meals
- Partial reimbursement of public transport costs
- Leave: 7 weeks of annual leave + 10 extra days off due to RTT (statutory reduction in working hours) + possibility of exceptional leave (sick children, moving home, etc.)
- Possibility of teleworking and flexible organization of working hours (after 12 months of employment)
- Professional equipment available (videoconferencing, loan of computer equipment, etc.)

- Social, cultural and sports events and activities
- Access to vocational training

Remuneration

Remuneration will be determined by degree and experience.

General Information

- **Theme/Domain :** Algorithmics, Computer Algebra and Cryptology
  Scientific computing (BAP E)
- **Town/city :** Paris
- **Inria Center :** Centre Inria de Paris
- **Starting date :** 2023-01-01
- **Duration of contract :** 12 months
- **Deadline to apply :** 2023-06-30

Contacts

- **Inria Team :** CASCADE
- **Recruiter :**
  Nguyen Phong-quang / Phong-Quang.Nguyen@inria.fr

About Inria

Inria is the French national research institute dedicated to digital science and technology. It employs 2,600 people. Its 200 agile project teams, generally run jointly with academic partners, include more than 3,500 scientists and engineers working to meet the challenges of digital technology, often at the interface with other disciplines. The Institute also employs numerous talents in over forty different professions. 900 research support staff contribute to the preparation and development of scientific and entrepreneurial projects that have a worldwide impact.

The keys to success

The candidate is expected:

- to have expertise in lattices and their algorithmic aspects, or quantum algorithms.
- to have obtained a PhD related to lattice algorithms or quantum algorithms.
- to have published in major conferences such as CRYPTO, EUROCRYPT, STOC, FOCS, SODA, QIP.

Warning : you must enter your e-mail address in order to save your application to Inria. Applications must be submitted online on the Inria website. Processing of applications sent from other channels is not guaranteed.

Instruction to apply

For each candidate, you will need to send :

- Your curriculum vitae
- Your two best publications
- Research statement
- Reference letters if possible

Defence Security :
This position is likely to be situated in a restricted area (ZRR), as defined in Decree No. 2011-1425 relating to the protection of national scientific and technical potential (PPST).Authorisation to enter an area is granted by the director of the unit, following a favourable Ministerial decision, as defined in the decree of 3 July 2012 relating to the PPST. An unfavourable Ministerial decision in respect of a position situated in a ZRR would result in the cancellation of the appointment.

Recruitment Policy :
As part of its diversity policy, all Inria positions are accessible to people with disabilities.