Offer #2024-08303

Post-Doctoral Research Visit F/M Post-doc on the design and analysis of Symmetric Techniques for Advanced Protocols

Contract type : Fixed-term contract

Level of qualifications required : PhD or equivalent

Fonction : Post-Doctoral Research Visit

Context

The successfull applicant will work with Léo Perrin within the framework of the ERC grant ReSCALE, that deals with symmetric cryptographic primitives intended to closely integrate with modern public key protocols, called STAPs.

See https://who.paris.inria.fr/Leo.Perrin/rescale/rescale.html for more information about the context.

Assignment

With the help of the other members of the ReSCALE team, including Léo Perrin, the recruited person will work on expanding the knowledge of the academic community and of the industry about the best practices when designing "STAP"s.

Main activities

- Investigate the design and analysis of STAPs.
- Assist in the supervision of the PhD students of the project.

Skills

Technical skills and level required : good knowledge of Python/SAGE, very good knowledge of symmetric cryptography.

Languages : English

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 (after 6 months of employment) and flexible organization of working hours
- Professional equipment available (videoconferencing, loan of computer equipment, etc.)
- Social, cultural and sports events and activities
- Access to vocational training
- Social security coverage

General Information

- **Theme/Domain :** Algorithmics, Computer Algebra and Cryptology
  Information system (BAP E)
- **Town/city :** Paris
- **Inria Center :** Centre Inria de Paris
- **Starting date :** 2025-02-01
- **Duration of contract :** 2 years
- **Deadline to apply :** 2024-11-29

Contacts

- **Inria Team :** COSMIQ
- **Recruiter :**
  Perrin Leo / leo.perrin@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

Advanced knowledge of symmetric cryptography, and ideally some knowledge of the cryptographic protocols requireing STAPS (FHE, MPC...)

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

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.