Offer #2025-09198

PhD Position F/M Estimating precisely the efficiency of cryptanalysis techniques for symmetric primitives intended for advanced protocols

Contract type : Fixed-term contract

Level of qualifications required : Graduate degree or equivalent

Fonction : PhD Position

Context

This thesis will be co-supervised by Yann Rotella (UVSQ) and Léo Perrin (COSMIQ, Inria). It will be financed by the ERC project ReSCALE, and will take place at the "centre Inria de Paris", within the COSMIQ team.

Assignment

The candidate will be expected to do research on both the theoretical and the practical (i.e. implementation) aspects of various cryptanalysis techniques that are of particular relevance when analysing symmetric primitives intended for advanced protocols.

Main activities

The aim of this thesis is to precisely understand how the complexity of some cryptanalysis techniques scales with the various parameters of a cryptosystem.

The candidate will then be expected to investigate this topic, publish scientific papers (and possibly computer programs) describing their results, and to present them at the relevant conferences or seminars.

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 :** 2025-10-01
- **Duration of contract :** 3 years
- **Deadline to apply :** 2025-08-21

Contacts

- **Inria Team :** COSMIQ
- **PhD Supervisor :**
  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.

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.