Offer #2025-08946

Post-Doctoral Research Visit F/M Solid Basis for Symmetric Cryptography: Towards a generalization of cryptanalysis techniques, and new links between cryptanalysis and security arguments

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 (you can choose between)

- not applicable,
- collaboration between 2 Inria teams: *****,
- collaboration ({team_Inria} and the start-up *****,
- project/programme/European fund *****,
- public with {French National Research Agency (ANR), local and regional authorities, academic partners, *****]
- value-creation and technology transfer contracts with *****

a package/model/prototype/application/interface/infrastructure/other specify ***
more specifically dedicated to *****.**

Is regular travel foreseen for this post ? “Do not hesitate to make this known and to ensure that "travel expenses are covered within the limits of the scale in force".

Assignment

The recruted post-doc will work on the context of the ERC SoBaSyC, both regarding objective 1 (One toolbox to rule them all) and 2 (solid arguments for future desgins).

Symmetric cryptography, essential for enabling secure communications, has benefited from
an explosion of new results in the last two decades, in big part due to several standardization
efforts: many public competitions have been launched since 1997, where the community
proposes cryptographic constructions and simultaneously evaluates their security and per-
formance. The security of symmetric cryptography is based on cryptanalysis: we only gain
confidence in a symmetric cryptographic function through extensive and continuous scrutiny.
However, the current context has not allowed the community to digest all the new findings,
as can be seen from several recurrent issues. The two main ones are:
1) primitives proposed at top-tier venues often get broken by slight modifications of already
known techniques;
2) published cryptanalysis at top conferences sometimes include mistakes or are suboptimal.
They are also often re-invented and re-named.
The main challenge of SoBaSyC is to establish solid bases for symmetric cryptography.
Using cryptanalysis as the starting point, my aim is to unify the knowledge obtained through
the years on the different families of attacks, to transform it with an algorithmic approach
and to endow it with optimizations. The final result will be a toolbox congregating all
our newly proposed optimized algorithms, that will provide the best known attacks on a
given construction, through an easy application. Next, I plan to derive from this algorithmic
approach some theoretical bounds, as well as some properties that I will include in the security
proofs of symmetric constructions, providing more meaningful and realistic security arguments.
This would allow, for the first time, to ensure that any newly proposed primitive or construction
is already resistant to all known attacks, and will considerably increase the confidence on these
functions. It will also save a considerable amount of time and allow the field to

advance, at
last, on solid ground.

Main activities

Typical post-doc activities, working on reserach topics in the proposed subject, writing papers, participating on a group.

Skills

Technical skills and level required :

Languages :

Relational skills :

Other valued appreciated :

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 :** 2025-09-01
- **Duration of contract :** 2 years
- **Deadline to apply :** 2025-06-22

Contacts

- **Inria Team :** COSMIQ
- **Recruiter :**
  Naya Plasencia María / Maria.Naya_Plasencia@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

There you can provide a "broad outline" of the collaborator you are looking for what you consider to be necessary and sufficient, and which may combine :

- tastes and appetencies,
- area of excellence,
- personality or character traits,
- cross-disciplinary knowledge and expertise...

This section enables the more formal list of skills to be completed and 'lightened' (reduced) :

- "Essential qualities in order to fulfil this assignment are feeling at ease in an environment of scientific dynamics and wanting to learn and listen."
- " Passionate about innovation, with expertise in Ruby on Rails development and strong influencing skills. A thesis in the field of **** is a real asset."

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.