Offer #2025-08955

PhD Position F/M New tools for quantum symmetric cryptanalysis

Contract type : Fixed-term contract

Level of qualifications required : Graduate degree or equivalent

Fonction : PhD Position

About the research centre or Inria department

The Inria Rennes - Bretagne Atlantique Centre is one of Inria's eight centres and has more than thirty research teams. The Inria Center is a major and recognized player in the field of digital sciences. It is at the heart of a rich R&D and innovation ecosystem: highly innovative PMEs, large industrial groups, competitiveness clusters, research and higher education players, laboratories of excellence, technological research institute, etc.

Context

The development of quantum computing devices impacts severely the security guarantees of asymmetric cryptography, leading to an ongoing transition to post-quantum, i.e., quantum-secure, cryptosystems. Fortunately, mainstream symmetric primitives are considered robust against hypothetical quantum adversaries. However, our confidence in the security of symmetric cryptosystems is upheld by a rigorous cryptanalysis effort. This effort needs to continue in the context of post-quantum
security.

This PhD position takes place within the QATS project, which studies the cryptanalysis of symmetric primitives (block ciphers, hash functions...) using quantum algorithms. QATS is both focused on the systematization of new attack techniques, and the development of automatic tools that allow to find attacks.

Assignment

The PhD candidate will study attacks based on quantum convolution algorithms (which have been used recently in linear cryptanalysis), and their application to block cipher cryptanalysis, as well as the automatization of these techniques.

More information on the research to be carried out in this project as well as relevant bibliographic references are available on this document.

Main activities

The PhD candidate will contribute to the research activities of the CAPSULE team and the QATS project.

- Design new attack algorithms based on quantum convolutions
- Analyze existing and new attacks and design automatic tools to search for them

The candidate will also communicate her/his work through publications and communications in conferences, workshops or seminars.

Skills

The ideal candidate will have the following skills:

- A strong level in English for written and oral communication
- Relational skills (working in a team)
- A background in cryptography and / or algorithmics
- Programming skills in Python or other languages
- Notions of quantum computing

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

Remuneration

Salary gross : 2200€

General Information

- **Theme/Domain :** Algorithmics, Computer Algebra and Cryptology
- **Town/city :** Rennes
- **Inria Center :** Centre Inria de l'Université de Rennes
- **Starting date :** 2025-09-15
- **Duration of contract :** 3 years
- **Deadline to apply :** 2025-07-31

Contacts

- **Inria Team :** CAPSULE
- **PhD Supervisor :**
  Schrottenloher Andre / andre.schrottenloher@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

Please submit online : your resume, cover letter and letters of recommendation eventually

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.