Offer #2024-08028

PhD Position F/M Security of ASCON and Lightweight Symmetric Primitives against Quantum Attackers

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 Centre at Rennes University is one of Inria's eight centres and has more than thirty research teams. The Inria Centre 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

This PhD position takes place within the ASCON-CAT project, which studies the resistance of the ASCON cipher family against quantum attacks. ASCON-CAT aims at combining the expertise of its members in cryptography, quantum computing and physical implementations to assess the security levels of ASCON, and increase our understanding of the quantum security of symmetric cryptosystems as a whole.

In 2018, the NIST launched a competition to select a new family of lightweight symmetric authenticated encryption algorithms, therefore recognizing the importance that lightweight cryptography has taken in industrial applications and research. After five years of competition, ASCON was selected for standardization, and is now expected to become a major commercial standard. In parallel, many other lightweight designs have been proposed throughout the competition and later on.

Mainstream symmetric primitives are widely believed to retain a good level of security against hypothetical quantum adversaries. However, the past few years have shown that a lot can be said about the quantum security of symmetric ciphers.The goal of ASCON-CAT is to tackle this challenge on the high-profile target ASCON. Within this project, the goal of this PhD will be to analyze the impact of quantum cryptanalysis families on ASCON and develop dedicated attacks.

The ASCON-CAT project is a collaboration between Alice&Bob (Paris), Thales SIX (Gennevilliers) and Inria Rennes.The PhD student will be jointly supervised with the cryptography group at Thales SIX and is expected to collaborate regularly with the group.

Assignment

The PhD candidate will study different categories of attacks and analyze their impact on the ASCON cipher family and related targets. These categories will notably include:

- Linear and differential attacks
- Algebraic attacks (including Meet-in-the-middle attacks on hashing or Duplex encryption modes

It is expected that some of the observations made on ASCON and / or cryptanalysis techniques will lead to results on other similar lightweight primitives.

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 collaborate with the ASCON-CAT project partners.

- Analyze existing families of attacks and build a bibliography of applicable attacks
- Design new attack algorithms and analyze their costs

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
- Possibility of teleworking (90 days per year) and flexible organization of working hours
- Partial payment of insurance costs

Remuneration

Monthly gross salary: 2100€ during the 2 1st years and 2200€ during the 3rd year.

General Information

- **Theme/Domain :** Algorithmics, Computer Algebra and Cryptology
- **Town/city :** Rennes
- **Inria Center :** Centre Inria de l'Université de Rennes
- **Starting date :** 2024-10-01
- **Duration of contract :** 3 years
- **Deadline to apply :** 2024-08-22

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.

The keys to success

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.