Offer #2025-09077

PhD Position F/M Attack Modelling of Symmetric Primitives

Contract type : Fixed-term contract

Level of qualifications required : Graduate degree or equivalent

Fonction : PhD Position

Context

The main objective of the PhD project is to propose new attack modellings of symmetric primitives.
It will be carried out in the CARAMBA team at Loria, in Nancy, within the framework of the project CRYPTANALYSE of the PEPR CYBERSÉCURITÉ.

Business travels, in France or abroad, could be considered to disseminate the scientific results, in particular at conferences. Travel expenses are covered within the limits of the scale in force.

Assignment

Context

When designing a symmetric-key primitive, trying to attack it (a.k.a cryptanalysis) is the main approach we have to assess its security. Particular care shall be taken to the analysis of statistical attacks, which are among the most efficient approaches known to date. The
two most famous examples are differential and linear cryptanalysis, but many other variants were proposed afterwards, including the differential-linear technique and the boomerang attacks, to cite a few.

Unfortunately, no efficient ways exist to identify statistical defects, and the generic approach is to study each of the small components to deduce how the property evolves round after round through the primitive. On the bright side, several techniques have been recently introduced to automate this process with computer programs, saving cryptanalysts from having to do it manually. It however remains imperfect as the descriptions of the problem in the programs (known as the modelling techniques) are generally simplifications that are not always accurate, and are often unsuitable for lightweight constructions.

PhD proposal

In recent years many new iterative frameworks that aim at capturing more accurately the probability have been proposed. While their theory is in general sound, they are harder to use, and it is less clear how to efficiently find distinguishers with these approaches.
The aim of this PhD is to propose new modelling techniques for automated search of symmetric distinguishers and attacks.

Main activities

The core activities of this PhD thesis include:

- Study the state-of-the-art in the modelling of attacks and the recents theoretical frameworks giving estimates of the probability of distinguishers,
- Develop new methods for modelling the search of efficient parameters for a cryptanalysis,
- Write and publish the scientific results in scientific journals and conferences.

Skills

- Solid knowledge in the domain of cryptography.
- Solid programming skills (Python, Sagemath, C).
- Strong communication abilities.
- Fluency in English (written and spoken)

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

Remuneration

2200€ gross/month

General Information

- **Theme/Domain :** Algorithmics, Computer Algebra and Cryptology
- **Town/city :** Villers lès Nancy

- **Inria Center :** Centre Inria de l'Université de Lorraine
- **Starting date :** 2025-10-01
- **Duration of contract :** 3 years
- **Deadline to apply :** 2025-08-02

Contacts

- **Inria Team :** CARAMBA
- **PhD Supervisor :**
  Bonnetain Xavier / xavier.bonnetain@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.