Offer #2025-08539

PhD Position F/M Formal Verification of Higher-Order, Probabilistic Programs

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 center at Université Côte d'Azur includes 42 research teams and 9 support services. The center's staff (about 500 people) is made up of scientists of di?erent nationalities, engineers, technicians and administrative staff. The teams are mainly located on the university campuses of Sophia Antipolis and Nice as well as Montpellier, in close collaboration with research and higher education laboratories and establishments (Université Côte d'Azur, CNRS, INRAE, INSERM ...), but also with the regional economic players.

With a presence in the fields of computational neuroscience and biology, data science and modeling, software engineering and certification, as well as collaborative robotics, the Inria Centre at Université Côte d'Azur is a major player in terms of scientific excellence through its results and collaborations at both European and international levels.

Context

This PhD thesis project is part of the ANR project HOPR (Higher-Order Probabilistic and resource-aware Reasoning) (ANR-24-CE48-5521-01) coordinated by P. Baillot, starting in 2025 and aiming at defining expressive logical frameworks, dealing in particular with higher-order computation and probabilities, which can serve to reason on cryptographic primitives and protocols and on differential privacy. The project has three partner sites: INRIA Lille/CRIStAL; INRIA Paris; IRISA Rennes and INRIA Sophia-Antipolis. It is starting in January 2025 for 4 years.

The recruited PhD student will carry out her/his research within the SPLITS and OLAS project-teams at INRIA Sophia Antipolis, under the supervision of B. Gregoire and M. Avanzini

Assignment

Randomized computation has emerged as a highly effective extension of the standard deterministic computational model, especially in recent decades. Randomization plays a key role among many areas of computer science, e.g., zin computational complexity, artificial intelligence, security and privacy.
Avoiding bugs in critical applications, such as cryptographic routines, necessitates the development of formal verification methods that account for probabilistic effects.

Dijkstra's weakest-precondition predicate transformers are certainly among the most effective tools in the field of program semantics and verification. Over the past decade, such constructions have been generalized to probabilistic programs: in this context, it is natural that the truth of a formula becomes quantitative in nature, e.g., truth values turn into probabilities. While this methodology is well-established for probabilistic imperative programs [Kozen, 1981; McIver and Morgan, 2005; Avanzini et al. 2023,2024], its extension to
higher-order programs remains underexplored. This is unfortunate, as e.g. game-based cryptographic proofs inherently center around the analysis of higher-order, probabilistic programs.

The aim of this PhD is to develop new program logics, such as type systems or higher-order logics, for the quantitative analysis of higher-order probabilistic programs. Predicate transformers can serve as a foundational tool towards this aim [Avanzini et al., 2021]. A key objective will then be to apply these developed methodologies to enhance the logical foundations of EasyCrypt [Barthe et al., 2012], a proof assistant designed for game-based cryptographic proofs, which has been extensively used in recent years to verify cryptographic routines, including post-quantum schemes such as Kyber [Almeida et al., 2024].

References:

[Almeida et al. 2024] José Bacelar Almeida, Santiago Arranz Olmos, Manuel Barbosa, Gilles Barthe, François Dupressoir, Benjamin Grégoire, Vincent Laporte, Jean-Christophe Léchenet, Cameron Low, Tiago Oliveira, Hugo Pacheco, Miguel Quaresma, Peter Schwabe, Pierre-Yves Strub: Formally Verifying Kyber - Episode V: Machine-Checked IND-CCA Security and Correctness of ML-KEM in EasyCrypt. CRYPTO (2) 2024: 384-421

[Avanzini et al. , 2024] Martin Avanzini, Gilles Barthe, Benjamin Grégoire, Georg Moser, Gabriele Vanoni: Hopping Proofs of Expectation-Based Properties: Applications to Skiplists and Security Proofs. Proc. ACM Program. Lang. 8(OOPSLA1): 784-809 (2024)

[Avanzini et al., 2023] Martin Avanzini, Georg Moser, Michael Schaper: Automated Expected Value Analysis of Recursive Programs. Proc. ACM Program. Lang. 7(PLDI): 1050-1072 (2023)

[Avanzini et al., 2021] Martin Avanzini, Gilles Barthe, Ugo Dal Lago: On continuation-passing transformations and expected cost analysis. Proc. ACM Program. Lang. 5(ICFP): 1-30 (2021)

[Barthe et al., 2012] Gilles Barthe, Juan Manuel Crespo, Benjamin Grégoire, César Kunz, Santiago Zanella Béguelin: Computer-Aided Cryptographic Proofs. ITP 2012: 11-27

[Kozen 1981] Dexter. Kozen. Semantics of Probabilistic Programs. J. Comput. Syst. Sci. 22, 3 (1981), 328–350. (1981)

[McIver and Morgan, 2005] Annabelle McIver and Carroll Morgan. Abstraction, refinement and proof for probabilistic systems. Springer Science & Business Media. (2005)

Main activities

- Carry out the PhD research project on Verification of Higher-Order, Probabilistic Programs.
- Collaborate with other team members and with the ANR HOPR project partners
- Disseminate research results, by publications and presentations at international conferences

Skills

The candidate should be fluent in English.

Some basic knowledge of either type systems, proof theory, proof systems or program verification is expected.

Knowledge in cryptography is a plus but not necessary.

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 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
- Contribution to mutual insurance (subject to conditions)

Remuneration

Gross Salary per month: 2200€ brut per month (year 2025) and 2300€ brut per month (year 2026).

General Information

- **Theme/Domain :** Proofs and Verification
  Scientific computing (BAP E)
- **Town/city :** Sophia Antipolis
- **Inria Center :** Centre Inria d'Université Côte d'Azur
- **Starting date :** 2025-09-01
- **Duration of contract :** 3 years
- **Deadline to apply :** 2025-07-31

Contacts

- **Inria Team :** OLAS
- **PhD Supervisor :**
  Avanzini Martin / martin.avanzini@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

Applications must be submitted online on the Inria website. Collecting applications by other channels is not guaranteed.

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.