# Offer #2020-02974

# Researcher in the Tools for Proofs project of MSR-Inria Joint Centre

**Contract type :** Fixed-term contract

**Level of qualifications required :** PhD or equivalent

**Fonction :** Tempary Research Position

**Level of experience :** From 3 to 5 years

## Context

The Microsoft Research-INRIA Joint Centre is offering a 24-month position for a contractual researcher to contribute to the design and further development of the TLA+ Proof System (TLAPS, http://msr-inria.com/projects/tools-for-proofs).

The researcher will be hosted by the VeriDis team (https://team.inria.fr/veridis/) located at the Inria Nancy – Grand Est research center in Nancy, France. He or she will closely collaborate with the other members of the Tools for Proofs for project, in particular Damien Doligez and Leslie Lamport.

## Assignment

TLA+ is a language for specifying and reasoning about systems, including concurrent and distributed systems. It is based on first-order logic, set theory, and temporal logic. TLA+ and its tools have been used in industry for more than a decade. More recently, we have extended TLA+ by a language for writing structured formal proofs and have developed TLAPS, a proof checker that contains an interpreter for the proof language and interfaces with different back-end provers, including SMT solvers, the tableau prover Zenon that supports set-theoretic constructions, and a declarative encoding of TLA+ set theory as an object logic in the logical framework Isabelle. TLAPS is integrated into the TLA+ Toolbox, an IDE for TLA+ (http://lamport.azurewebsites.net/tla/tla.html).

Although it is still under active development, TLAPS is already quite powerful and has been used for several verification projects, in particular in the realm of distributed algorithms (e.g., http://lamport.azurewebsites.net/tla/byzpaxos.html).

The current version of TLAPS handles the "action" part of TLA+: first-order formulas with primed and unprimed variables that represent the values of a variable before and after a transition. It also supports the propositional fragment of temporal logic. This fragment is enough for proving safety properties (invariants and step simulation). Preliminary support for the full temporal logic of TLA+, which will allow us to prove liveness and refinement properties, has been implemented, but requires further refinement.

## Main activities

The contractual researcher (post-doctoral) position is funded for 24 months by the Microsoft Research - Inria Joint Centre. You will work together with the members of the TLA+ project, including Damien Doligez, Leslie Lamport, and Stephan Merz on extending the TLA+ Proof System. Your main objective will be to provide full support for temporal reasoning in TLAPS so that it can be released to users of the prover. You will also be able to work on extensions of existing functionality, including the following items:

- Module instantiation. The TLA+ language contains a module system, and modules can have constant and variable parameters in order to make them generic and reusable. When a module is instantiated, parameters can be replaced by constant- and state-level expressions, and these instantiations must be taken into account when generating proof obligations for back-end provers.
- Improved backend provers. The current backend provers provide decent support for proof obligations mixing first-order logic, elementary set theory, functions, and integer arithmetic. Reasoning about other important data structures such as finite sequences requires low-level user interaction. We are interested in exploiting advances in automatic deduction techniques, such as support for relevant theories in SMT solvers, for enabling a higher degree of automation of such

proof steps.
- Rigorous validation of soundness. Computing proof obligations involves some subtle transformations, such as distributing the prime operator of TLA+ or handling instantiated ENABLED expressions. We are working on a precise definition of the semantics of the proof language that would help us ensure the soundness of these transformations and give guidelines to the implementation.
- Checking SMT proofs. The SMT backend handles most of the proof obligations that occur in practice. The current version of TLAPS assumes the external SMT solver to be correct, but we are interested in reconstructing proofs provided by SMT solvers within Isabelle/TLA+. The Zenon backend already benefits from proof reconstruction.
- Performance issues. Proof projects can be large, and TLAPS implements mechanisms, such as fingerprinting proof obligations, that are intended to make the tool scale. Performance bottlenecks should be monitored and avoided, whenever possible.
- Case studies and proof libraries. Our work on TLAPS is validated by carrying out case studies, and we provide libraries of lemmas that are useful for many proof projects.

We do not expect to be able to address all of these issues within 24 months. The choice of items will be made jointly with the researcher, also depending on his or her interests and background.

## Skills

You should hold a PhD degree in computer science and have solid knowledge of mathematical logic, as well as implementation skills related to symbolic theorem proving. TLAPS is mainly implemented in OCaml, but some Java programming will be necessary for interfacing TLAPS with the other TLA+ tools. Experience with temporal and modal logics, with interactive theorem provers or with Eclipse could be valuable.

## 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

From 2632 euros gross monthly (according to degree and experience)

## General Information

- **Theme/Domain :** Proofs and Verification
  Software engineering (BAP E)
- **Town/city :** Villers lès Nancy
- **Inria Center :** Centre Inria de l'Université de Lorraine
- **Starting date :** 2020-10-01
- **Duration of contract :** 2 years
- **Deadline to apply :** 2020-10-02

## Contacts

- **Inria Team :** VERIDIS
- **Recruiter :**
  Merz Stephan / Stephan.Merz@loria.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

Work on TLAPS provides the opportunity to learn about issues of using deductive verification in practice, and there are possibilities to produce publishable

research. However, the main focus is on the implementation of components of our tool chain that are missing or need improvement.

Given the geographical distribution of the members of the team, we highly value a good balance between the ability to work in a team and the capacity to propose initiatives.

**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.