**2019-01951 - PhD Position F/M Semantics and Compilation of State Machines in an Interactive Theorem Prover**

**Type de contrat :** CDD de la fonction publique  
**Niveau de diplôme exigé :** Bac + 5 ou équivalent  
**Fonction :** Doctorant  
**Niveau d’expérience souhaité :** jusqu’à 3 ans

**Contexte et atouts du poste**

The FidelIR project, for “Fidelity in Reactive Systems Design and Compilation”, is funded by a French government “Young Researcher” grant (ANR JIC). Its goal is to extend the Vélus verified Lustre compiler with state machines and techniques for interactively verifying models. The grant includes funding for national and international travel to participate in workshops and conferences.

Lustre is a synchronous language closely related to the industrial Scade tool which supports Model-Based Development (MBD) of critical embedded control software. It’s a programming language with a formal semantics for block-diagram specifications.

The Vélus compiler is developed in OCaml and the Coq Interactive Theorem Prover (ITP). It successively transforms source programs into the Clight language used by CompCert. The overall correctness theorem states that the stream-based semantics of the source program is preserved by the generated assembly code.

Vélus is developed in the Inria PARKAS team located at the École normale supérieure in the heart of Paris. Development is led by Timothy Bourke and involves collaboration with experts in synchronous languages (Marc Pouzet), verified compilation (Xavier Leroy) and automatic verification (Cesare Tinelli).

**Mission confiée**

Initial work on the Vélus compiler treated the basic features of Lustre: simple equations, initialized delays, and function instantiations. Recent PhD work has extended the semantic model and compilation passes with the modular reset construct from the Scade language. This PhD would focus on progressively adding state machines. Please see the Vélus website for other scientific references.

The first challenge is to adapt existing state machine semantic models for use within an interactive theorem prover. The definitions must be consistent with intuitions about the construct, suitable for verifying compilation passes, and amenable to program verification. State machines are compiled by rewriting them into a smaller subset of the language. The second challenge is to implement the rewrite rules as a functional program in Coq and to prove that it preserves the semantics of source programs.

The PhD student will work closely with other team members to develop semantic models, compilation passes, and correctness proofs for the state machine construct. Results will be communicated to international workshops, conferences, and journals.

Over the three years of the PhD scholarship, a hard-working candidate would master advanced concepts in programming languages and their semantics, become an expert in interactive theorem proving and its application to compiler development, and contribute to extending the state-of-the-art in formal techniques for model-based development. Students join a passionate research group. They learn how to analyze and solve challenging technical problems, present results at workshops and conferences, write scientific articles, and collaborate with other researchers. At the end of a successful PhD, the candidate will be well prepared to continue a research career or contribute to cutting edge developments in industry.

**Principales activités**

1. Master relevant background knowledge on synchronous language semantics and compilation, and interactive theorem proving by reading books and research articles.
2. Develop a plan of action based on successfully treating various state machine features described in the literature.
3. Extend the existing Vélus compiler with required constructs and define semantic models for them in the Coq ITP.
4. Implement compilation algorithms in Coq and develop proofs of semantic preservation.
5. Document the results in scientific articles and a PhD thesis.

**Additional activities:**

1. Participate in workshops and team activities.
2. (Optional) Contribute to teaching by supervising lab and tutorial sessions.

**Compétences**

**Languages:** French or English.

**Avantages**

- Subsidized meals

---

**Informations générales**

- **Thème/Domaine :** Preuves et vérification  
- **Ville :** Paris  
- **Centre Inria :** CRI de Paris  
- **Date de prise de fonction souhaitée :** 2020-01-01  
- **Durée du contrat :** 3 ans  
- **Date limite pour postuler :** 2019-10-31

**Contacts**

- **Equipe Inria :** PARKAS  
- **Directeur de thèse :** Bourke Timothy  
  Timothy.Bourke@inria.fr

**A propos d’Inria**

Inria, l’institut national de recherche dédié aux sciences du numérique, promeut l’excellence scientifique et le transfert pour avoir le plus grand impact. Il emploie 2400 personnes. Ses 200 équipes-projets agiles, en général communes avec des partenaires académiques, impliquent plus de 3000 scientifiques pour relever les défis des sciences informatiques et mathématiques, souvent à l’interface d’autres disciplines. Inria travaille avec de nombreuses entreprises et a accompagné la création de plus de 160 start-up. L’institut s’efforce ainsi de répondre aux enjeux de la transformation numérique de la science, de la société et de l’économie.

**L’essentiel pour réussir**

You are passionate (but not fanatic!) about functional languages and interactive proof assistants. You are not (just) interested in the theory of logic, but really motivated to apply it to real-world problems. Tenacity and a taste for simplicity are essential character traits for this work.

Ideally, you have had some exposure to interactive theorem proving in your undergraduate or masters programs—just to be sure that the subject suits you.

A curiosity to master new topics, an openness to criticism, a willingness to learn and improve, and a critical mind are essential.

Knowledge of Lustre, Scade, or Model-Based Development is optional.

Any PhD involves focusing on a narrow topic for three (long!) years. Additionally, developing large projects in interactive theorem provers requires a particular kind of tenacity and stamina.

It would be possible to undertake a five month (M2) internship in the team before beginning the PhD (or deciding not to).

**Consignes pour postuler**

**Sécurité défense :**

Ce poste est susceptible d’être affecté dans une zone à régime restrictif (ZRR), telle que définie dans le décret n°2011-1425 relatif à la protection du potentiel
- 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

Attention: Les candidatures doivent être déposées en ligne sur le site Inria. Le traitement des candidatures adressées par d'autres canaux n'est pas garanti.