Offer #2024-08486

PhD Position F/M PhD position on Verification of Differential Privacy

Contract type : Fixed-term contract

Level of qualifications required : Graduate degree or equivalent

Fonction : PhD Position

Level of experience : Recently graduated

About the research centre or Inria department

The Inria University of Lille centre, created in 2008, employs 360 people including 305 scientists in 15 research teams. Recognised for its strong involvement in the socio-economic development of the Hauts-De-France region, the Inria University of Lille centre pursues a close relationship with large companies and SMEs. By promoting synergies between researchers and industrialists, Inria participates in the transfer of skills and expertise in digital technologies and provides access to the best European and international research for the benefit of innovation and companies, particularly in the region.For more than 10 years, the Inria University of Lille centre has been located at the heart of Lille's university and scientific ecosystem, as well as at the heart of Frenchtech, with a technology showroom based on Avenue de Bretagne in Lille, on the EuraTechnologies site of economic excellence dedicated to information and communication technologies (ICT).

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 in the SyCoMoRES project-team at INRIA Lille / CRIStAL, under the supervision of P. Baillot.

Assignment

When computing values from sensitive datasets such as e.g. medical records, it is of crucial importance to guarantee some privacy properties. Methods based on anonymization are not sufficient in general because clever combinations with other data sources can lead to some privacy breaches. Differential privacy (DP) [DR14] is a quantitative notion of privacy that provides strong confidentiality guarantees and at the same time is flexible enough to allow for useful computations on private data. Technically it relies on the notion of program sensitivity, which is a bound relating the distance between two outputs of a program to the distance between the two inputs. DP has become a gold standard for data privacy. However, manually checking that large programs are differentially private can be both tedious and subtle. For this reason some formal methods approaches to sensitivity analysis and DP have been developed in the last decade [BGHP16]. Among them one can mention for instance approaches based on Hoare logics [BKOB12, BGG+16] and approaches based on type systems [RP10, GHH+13, NDA+19, TDA+23, jwdABG23, SB24]. The first line of work has been developed for programs in imperative languages while the second one is for programs from functional languages.

In this PhD project we propose to develop a program logic approach for reasoning on the DP of probabilistic higher-order functional programs. The goal is to obtain in this way a general and expressive approach for proving DP properties of such programs, which would allow both to verify the correctness of basic primitives or mechanisms, and to ensure that the composition of high-level functions satisfies the properties. In particular an interest of such a program logic will be to verify that the rules of a typing system for DP are sound.

References

[BGG+16] Gilles Barthe, Marco Gaboardi, Benjamin Grégoire, Justin Hsu, and Pierre-Yves Strub. Proving differential privacy via probabilistic couplings. In Proceedings of LICS 2016, pages 749–758. ACM, 2016.

[BGHP16] Gilles Barthe, Marco Gaboardi, Justin Hsu, and Benjamin C. Pierce. Programming language techniques for differential privacy. ACM SIGLOG News,

3(1) :34–53, 2016.

[BKOB12] Gilles Barthe, Boris Köpf, Federico Olmedo, and Santiago Zanella Béguelin. Probabilistic relational reasoning for differential privacy. In John Field and Michael Hicks, editors, Proceedings of the 39th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2012, Philadelphia, Pennsylvania, USA, January 22-28, 2012, pages 97–110. ACM, 2012.

[DR14] Cynthia Dwork and Aaron Roth. The algorithmic foundations of differential privacy. Found. Trends Theor. Comput. Sci., 9(3-4) :211–407, 2014.

[GHH+13] Marco Gaboardi, Andreas Haeberlen, Justin Hsu, Arjun Narayan, and Benjamin C. Pierce. Linear dependent types for differential privacy. In Proceedings of POPL ’13, pages 357–370. ACM, 2013.

[jwdABG23] june wunder, Arthur Azevedo de Amorim, Patrick Baillot, and Marco Gaboardi. Bunched Fuzz : Sensitivity for vector metrics. In Proceedings of ESOP 2023, volume 13990 of LNCS, pages 451–478. Springer, 2023.

[NDA+19] Joseph P. Near, David Darais, Chike Abuah, Tim Stevens, Pranav Gaddamadugu, Lun Wang, Neel Somani, Mu Zhang, Nikhil Sharma, Alex Shan, and Dawn Song. Duet : an expressive higher-order language and linear type system for statically enforcing differential privacy. Proc. ACM Program. Lang., 3(OOPSLA), 2019.

[RP10] Jason Reed and Benjamin C. Pierce. Distance makes the types grow stronger : a calculus for differential privacy. In ICFP 2010. ACM, 2010.

[SB24] Victor Sannier and Patrick Baillot. A linear type system for lˆp-metric sensitivity analysis. In 9th International Conference on Formal Structures for Computation and Deduction, FSCD 2024, volume 299 of LIPIcs, pages 12 :1–12 :22. Schloss Dagstuhl - Leibniz-Zentrum fu?r Informatik, 2024.

[TDA+23] Matías Toro, David Darais, Chike Abuah, Joseph P. Near, Damián Árquez, Federico Olmedo, and Éric Tanter. Contextual linear types for differential privacy. ACM Trans. Program. Lang. Syst., 45(2) :8 :1–8 :69, 2023.

Main activities

- Carry out the PhD research project on Verification of Differential Privacy
- Collaborate with other SyCoMoRES 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.

Some knowledge of differential privacy would be appreciated but is not compulsory.

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
- Social security coverage

General Information

- **Theme/Domain :** Proofs and Verification
- **Town/city :** Villeneuve d'Ascq

- **Inria Center :** Centre Inria de l'Université de Lille
- **Starting date :** 2025-09-01
- **Duration of contract :** 3 years
- **Deadline to apply :** 2025-05-14

Contacts

- **Inria Team :** SYCOMORES (DIR-LIL)
- **PhD Supervisor :**
  Baillot Patrick / patrick.baillot@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.