2021-03391 - PhD Position F/M Learning to Adaptively Attack and Defend Privacy of Machine Learning Systems

**Context**

In his/her journey to the doctoral thesis, the candidate will be supported by AI, PhD@Lille grant, and supervised by Debabrata Basu and Philippe Preux. Debabrata and Philippe are affiliated with the Schoo project-team (previously SequeL) of Inria Lille-Nord Europe. As a team, Schoo is internationally recognized for developing theories and algorithms for sequential learning and decision making, i.e. in the fields of bandits and reinforcement learning.

The project is expected to simulate the existing and new collaborations with researchers and groups working on data privacy, privacy-preserving machine learning, and reinforcement learning. Existing collaborators in such topics are distributed internationally at National University of Singapore, Grandes Écoles in Paris, and University of Oslo. In future, the candidate will be encouraged to visit the collaborators and work with them. The candidate will also be part of the HumAln alliance that aims toward studying humane impact of deploying AI.

From the application point of view, Schoo is involved in multiple projects that incorporates medical data, agricultural data, and e-commerce. Depending on the future development, we will be interested to deploy such private systems and algorithm for securing such applications involving individual data.

**Main activities**

The successful candidate is expected to:

1. Study the literature of privacy-preserving machine learning and reinforcement learning.
2. Design adaptive attacks on online and reinforcement learning systems.
3. Design adaptive defense mechanisms that can secure the data used in online machine learning, such as bandits and reinforcement learning.
4. Incorporating both attack and defense in a single framework of reinforcement learning that operates around data privacy.
5. Developing algorithms using standard programming languages like Python in order to validate their applicability.
6. Deploying algorithms using standard programming languages such as Python. C/C++
7. Some experience with implementation and experimentation (a plus)

The candidate should aim to publish the research results in premier machine learning (AAAI, AISTATS, ICML, UAI), NeurIPS and privacy enhancing technology (PoPETs, IEEE SSP) venues. Also, the candidate is expected to present his/her work orally in seminars, workshops, conferences, and also beyond academia towards more general audience.

Since the work involves and impacts the digital life of general public, the successful candidate should collaborate in writing scientific articles aiming towards the larger audience.

**Skills**

The candidate should preferably have the following skills:

- A strong background in mathematics/statistics
- A good knowledge of machine learning, statistics, and algorithms
- Broad interest for differential privacy or data privacy
- Knowledge of programming languages such as Python. C/C++
- Some experience with implementation and experimentation (a plus)
- A good command of English (a plus)

Please follow the instructions given in https://team.inria.fr/magnet/how-to-apply/ to set up your application file.

In brief, the application of the candidate should include his/her CV, an application letter (two or more) recommendation letters, and the school transcripts. It is recommended that the candidate
contacts Debrota and Philippe while preparing the application.

The deadline for application is 15th April, 2021.

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