Post-doc Proposal - Deadline 31st July 2024

{Lattice-Based, Class-Group-Based, Threshold} Cryptography

June 13, 2024

We have a **full-time two-years post-doc position** available. The recruited person will have the possibility to do research in cryptography. More precisely, we are searching for someone interested in cryptography based on lattice problems and/or class group problems. Moreover, we would like to investigate further on threshold solutions for both classes of problems.

Where? At the *Laboratoire d'Informatique, de Robotique et de Microélectronique de Montpellier* (short form: LIRMM, in English: Laboratory of Computer Science, Robotics and Microelectronics of Montpellier, website).

Who? The recruited person will be part of the very welcoming ECO research group (website). Given the topic, the postdoc will be most likely collaborating with Katharina Boudgoust (website) and Fabien Laguillaumie (website), but there are also other interesting research topics represented in the team: side-channel analysis, coding theory, computer algebra, information-theoretic cryptography.

What exactly? We leave the call on purpose rather general, as we want to encourage a wide spectrum of people to apply. The concrete research project can be adapted to the experience and wishes of the postdoc. Generally, Katharina is interested in many aspects of lattice-based cryptography. Together, we could for instance investigate threshold constructions of lattice-based primitives, such as threshold (ring) signatures or threshold decryption (e.g., building upon [BS23]). Other directions could be aggregate signatures (building upon [AAB+24]). Fabien is broadly interested in various aspects of discrete-log and class-group-based cryptography. Possible directions could be designing new primitives based on class-groups, or improving the existing ones.

Salary? The salary will depend on the work experience (after the PhD) of the person. But to give a rough estimate, it will be around 2000€ per month after taxes. There is funding for travel and attending schools/workshops/conferences. In France, you benefit from public social security.

Do I have to speak French? The clear answer is: NO, you don't have to be fluent in French in order to come to us. Even though the majority of the group is originally from France, everyone is happy to speak English at work. We can also help you with administrative things. Globally, Montpellier is pretty used to non-French speaking people, due to the many international students. Of course, it is always nice to be able to speak some words in the local language. To this end, free language courses are offered by the research institute.

When? The deadline for applying is **August 15th**. The starting date is flexible between October 2024 and January 2025.

Selection Criteria? We are preferably looking for a candidate with experience in designing public-key primitives. It is not mandatory to have knowledge on lattice-based or class-group-based cryptography. The postdoc could be your opportunity to learn about those exciting topics! It comes without saying (but we still write it, to be sure) that we are welcoming everyone, independent of their gender, sexual orientation, race, ethnicity, national origin, health status, or disability. We promote a friendly, safe, and supporting work environment.

How to apply? Last but not least, how to apply: Please send an e-mail to Katharina (e-mail) and Fabien (e-mail), including your CV, at least one paragraph on why you want to work with us, as well as the name of one person who we can contact for an informal recommendation. This person could be a former advisor or co-author.

References

AAB+24. Marius A. Aardal, Diego F. Aranha, Katharina Boudgoust, Sebastian Kolby, and Akira Takahashi. Aggregating falcon signatures with labrador. *IACR Cryptol. ePrint Arch.*, page 311, 2024.

BS23. Katharina Boudgoust and Peter Scholl. Simple threshold (fully homomorphic) encryption from LWE with polynomial modulus. In Jian Guo and Ron Steinfeld, editors, *ASIACRYPT 2023, Part I*, volume 14438 of *LNCS*, pages 371–404. Springer, Heidelberg, December 2023.