PhD position in computer science
in LJK, Grenoble, France

Title: Robust and Certified High Performance Algebraic Computing
Keywords: computer linear algebra, fault tolerance, interactive certificates, parallel computing, C/C++

INFORMATIONS
Location: University Grenoble Alpes, France at the Laboratoire Jean Kuntzmann (LJK: ljk.imag.fr)
Duration: 3 years
Starting date: September 2016
Salary: approx. 1 400 € (monthly net salary including French health care coverage)
Contact: Jean-Guillaume Dumas, Clément Pernet - {jgdumas,pernet}@imag.fr
Application: please send a CV by email to (Jean-Guillaume.Dumas@imag.fr and Clement.Pernet@imag.fr) together with the contact information (e-mail addresses) of one or two references who could recommend your application.
Deadline for application: March 15th, 2016.

CONTEXT
Motivated by a wide range of applications, including algebraic cryptanalysis, experimental mathematics, etc., high performance algebraic computing has developed rapidly over the recent years. Exact linear algebra plays the role of a building block there, and is therefore an active field of research on both the theoretical and practical aspects of algorithmic design and implementation. In the context of large scale distributed computations, the reliability of the remote computing nodes is becoming increasingly questionable. First, the increase in scale of the parallelism being used makes the natural failure rates of the memory of a computing resource no longer negligible. This has motivated the development of the field of algorithm based fault tolerance, adapting the techniques of coding theory to a new range of applications. Second the use of computing resources provided by a third party also requires a level of confidence in the results returned. Interactive proof protocols can be applied in this framework to certify the exactness of a computation. Although interactive proofs protocols are already fairly well understood from a theoretical complexity point of view, their implementation to a practical framework is a rich field of investigation.

In this context the Ph.D. candidate will be expected to investigate in the following themes:

- exact linear algebra algorithmic and implementation for high performance algebraic computing: for instance, this could be the computation of the QR decomposition over a finite field and the rationals, with applications to computing normal forms over the integers and reducing euclidean lattices;
- fault tolerance by coding theoretic approaches: designing new evaluation codes or adapting existing ones, under constraints arising from the applications, such as preserving the sparsity, enabling early termination and using soft decision decoding techniques;
- effective interactive proofs and certification protocols: for instance, protecting privacy in an external database, while certifying that the database actually produced the right output or certifying that the correct computations have been performed on some sparse or structured matrices, ...

The Ph.D candidate will be under the supervision of Jean-Guillaume Dumas and Clément Pernet, at the Laboratoire Jean Kuntzmann, in Grenoble. The main outcome of the research is several publications in international journals or conferences, and the development of code, integrated to open-source libraries and software such as fflas-ffpack, LinBox and SageMath.

QUALIFICATIONS
The candidate must hold a Master degree (or any equivalent degree) in either computer science or in computational mathematics. He/She must be an experienced C/C++ programmer, with good knowledge in basic algebra (finite fields, polynomials), linear algebra, and their computational aspects in general. An experience with either advanced linear algebra, its application to cryptology or coding theory, interactive proofs or parallelization of scientific computing code will be appreciated.