The mathematical department IRMAR (http://irmar.univ-rennes1.fr/), part of Rennes 1 University in the west of France, is advertising a 2-year post-doctoral position in the area of **computational number theory and algebraic geometry for code-based or isogeny-based post-quantum cryptography**.

It includes the following topics:

- Code-based private information retrieval (PIR) protocol;
- Code-based secret sharing schemes;
- Algebraic codes and/or asymptotically good towers of curves for verifiable computing;
- Number of rational points of embedded varieties defined over a finite field;
- Isogeny computation with elliptic curves, higher genus curves, complex multiplication ;
- Computation with abelian varieties, theta functions ;
- Explicit methods for moduli spaces of curves and abelian varieties.

The list above is indicative and not exhaustive. Candidates are invited to design their research proposal around other topics, provided that they are **closely related** to algebraic geometry and code-based cryptography.

Candidates must hold a PhD thesis or equivalent in mathematics or computer science, together with a strong research record.

Applications and requests for further information should be directed to

- Jade Nardi if related to code theory (jade.nardi@univ-rennes1.fr),
- David Lubicz for curve based cryptography (david.lubicz@univ-rennes1.fr).

Applicants should send detailed curriculum vitae, list of publications, a short research proposal.