We PQ-TLS Chair Offer

Junior Research Leader

Quantum Security for Post-Quantum Cryptography

General information

Funding project: PEPR QUANTIQUE
Type of contract: Research Chair in Post-Quantum Cryptography
Contract period: 3+ years
Expected starting date: March 2024

Context

Cryptography is at the heart of many secure devices for ensuring confidentiality, integrity and authenticity of communications, programs and data. The security of the current asymmetric cryptography relies on problems that are easy to break with a quantum computer. In practice, the real threat of quantum computing is predicted to be operational in decades. However, through the National Institute of Standards and Technologies (NIST) impulsion, the community decided to move on a stronger cryptography, resilient to attacks from classical and quantum computers. This cryptography is called post-quantum cryptography (also called quantum-safe cryptography or quantum-resistant cryptography).

PQ-TLS is a 5-year research project driven by the French National Research Agency (ANR) and the France 2030 strategy under the frameworks of the Priority Research Programs and Equipment (PEPR). PQ-TLS aims at studying the security of post-quantum cryptosystems.

Mission description

The candidate will study the security of hard problems on which many post-quantum cryptosystems are built against quantum adversaries either lattice-based, code-based, isogeny-based or multivariate cryptography. For instance, the security of hard problems has been studied, but it is frequent that specialized instances of the hard problems are used. Moreover, it is only conjectured that there are no quantum adversaries against these hard problems, but there is no proof. It could also be interested to study the security proofs of these cryptosystems in the QROM model.

Localisation

The offer localisation will be determined by the candidate's employer, and the best team fitted to the subject.

Offer requirements

The candidate must have at least 2 years of experience after their PhD and have research experience in quantum cryptanalysis and in the development of quantum algorithms.
To already be employed by one of the following institutions: Rennes University, CNRS, Inria, CEA, Limoges Université, Rouen Normandie University, Bordeaux University, Jean Monnet Saint-Etienne University, Versailles Saint-Quentin University, ENS Lyon, Bretagne Occidentale University

How to apply

Please send your application to pierre-alain.fouque@univ-rennes1.fr and marilou.gaborel@irisa.fr.

Required documents:

- Detailed CV with list of publications
- Two letters of recommendation
- Short research statement (1 page max)

Application Process

- Your application is reviewed by our committee
- Your application is accepted: it will be reviewed by the pilots and the ANR
- They accept you application: Oral presentation in front of the committee, and recruitment if approved.