PQ-TLS Chair Offer

Junior Research Leader

Formal Analysis for Post-Quantum Cryptography Protocols

General information

Funding project: PEPR QUANTIQUE
PQ-TLS
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 developing innovative and efficient protocols for of post-quantum cryptography.

Mission description

Nearly all security protocols rely on public-key cryptography using RSA or Elliptic Curve. With the threat of quantum attackers, the transition of all currently deployed cryptographic protocols must be studied. Typically, we would like to study new designs for TLS, IPSec, Signal, SSH or Wireguard protocols in the context of Post-Quantum cryptography using formal methods. Among those, TLS would be a target of particular interest: there are many proposals for TLS, but there are still many issues with these proposals.

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 the formal analysis of security protocol. Knowledge in post-quantum cryptography would be a plus.
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.