Design and Cryptanalysis in Quantum-Safe Cryptography

Mots clés: Array

- Directeur de thèse: Ludovic Perret
- Co-directeur de thèse: Jean-Charles Faugère
- Co-encadrant(s):
- Unité de recherche: Laboratoire d'informatique de Paris 6
- Ecole doctorale: École Doctorale Informatique, Télécommunications, Électronique de Paris
- Domaine scientifique principal: Sciences et technologies de l'information et de la communication

Résumé du projet de recherche (Langue 1)

The goal of Quantum-Safe Cryptography is to design cryptographic primitives which are secure against a classical and quantum adversary. This is a well-established academic topic mainly motivated by Shor’s milestone quantum algorithm breaking the public cryptosystems deployed in practice.

In this thesis, we will be mainly concerned by multivariate cryptography which is defined as the set of cryptographic schemes using the computational hardness of solving a system of non-linear equations (PoSSo). This is a classical candidate in quantum-safe cryptography. A first goal of the thesis is to improve the efficiency of an asymmetric scheme based on a noisy variant of PoSSo. This will also require to understand the hardness of this noisy variant of PoSSo.