Journée thématique GDR SoC2 et GDR sécurité informatique :

# Algorithmes de chiffrement post-quantiques et sécurité matérielle

**Date** : 10 novembre 2021

**Lieu :** Laboratoire LIP6, salle 105 tour 26-25 1er étage
4, Place Jussieu, 75252 Paris

**Organisateurs :**

- Pierre-Louis Cayrel (Laboratoire Hubert Curien, UJM, Saint-Étienne)
- Cédric Marchand (École Centrale de Lyon - INL)

---

## Contexte :

Avec l'arrivée de l'ordinateur quantique, les algorithmes de chiffrement et de signature basés sur des problématiques « *traditionnelles* » de théorie des nombres à savoir le logarithme discret ou le problème de factorisation d'entiers, pourront être *cassés* dans un temps raisonnable. Les algorithmes de cryptographie post-quantiques ont pour but de fournir une solution à cette nouvelle ère informatique qui s'annonce. Les problèmes, sur lesquels la sécurité de ces cryptosystèmes repose, sont d'une autre nature (recherche de plus court vecteur dans un réseau, décodage d'un code aléatoire ou encore résolution de systèmes multivariés). Cette différence leur profère une sécurité supérieure face aux attaques utilisant un algorithme quantique. Cependant, une implémentation peut être mathématiquement sûre, ne pas avoir de faiblesse algorithmique ou reposer sur un problème mathématique qui, même pour un ordinateur quantique, serait considérer comme très difficile à résoudre (dans un temps raisonnable) ; il est possible d'utiliser d'autre biais pour l'attaquer. C'est ce qui est fait avec les attaques matérielles et notamment les attaques par canaux auxiliaires et les attaques par injection de fautes. La question qu'il convient alors de se poser est la suivante :

Quelle est la robustesse des algorithmes post-quantiques face aux attaques matérielles ?

Le but de cette journée est de rassembler la communauté française travaillant sur cette thématique pour s'intéresser aux implantations matérielles de ce type d'algorithmes, aux attaques matérielles visant ces implantations et à leurs contremesures.

**Intervenants :**

**Brice Colombier**, Univ Grenoble Alpes, CNRS, Grenoble INP, TIMAGrenobleFrance
Titre: Attaque physique sur le cryptosystème basé sur les codes correcteurs d'erreurs *Classic McEliece*

**Nicolas Aragon**, Université de Limoges, France

Titre: Implementation of the LRPC (Low Rank Parity Check) based cryptosystems

**Arnaud Tisserand**, CNRS, Lab-STICC UMR 6285 and Université Bretagne Sud, Lorient, France

Titre: Retour d'expérience en implantation HLS de PQC LWE sur FPGA »

**Simon Pontié**, CEA-Leti, Université Grenoble Alpes, F-38000 Grenoble, France

Titre: SIKE: injection de fautes et contre-mesure sur la génération de clés

**Nadia El Mrabet**, Mines Saint-Étienne, CEA-Tech, Centre CMP, F-13541 Gardanne, France

Titre: ROLLO : implémentation embarquée et attaques par canaux auxiliaires

**Inscription :**

L'inscription est gratuite mais obligatoire car le nombre de places est limité (40 places).
Pour vous inscrire, merci de remplir le formulaire suivant :

https://forms.office.com/Pages/ResponsePage.aspx?id=q_kijCAAokKtCYgKgUlXq5GsTHAMZIRMspHOVnPjeY9UNlRTRkJDU0tTREExUk5CSzI0WEMwUEE4NS4u