

Projet d'Initiation à la Recherche ou Projet d'Innovation-Recherche (barrer)

Nom du laboratoire ou de l'entreprise/établissement :

INSA-Toulouse / LAAS-CNRS

TUTEUR(S)

NOM-Prénom Tel Mel

- MIGLIORE Vincent (+33) 5 61 33 78 85, migliore@insa-toulouse.fr

-

Tuteurs INSA si projet industriel:

Prénom NOM

Mel:

TITRE DU PROJET

Attaques par canaux auxiliaires sur des modules de cryptographie quantique

MOT-CLES

Cryptographie, attaques par canaux auxiliaires

DESCRIPTIF (RESUME), indiquer l'enjeu sociétal de l'INSA de Toulouse s'il y a lieu

La montée en puissance de la faisabilité de concevoir des ordinateurs quantiques a donné lieu à un élan de modernisation des primitives cryptographiques afin d'éviter de casser les canaux de communication actuels réputés sûrs.

Cependant, même dans ce contexte, les attaques par canaux auxiliaires (attaque visant à extraire des variables internes sensibles des algorithmes pendant leur exécution sur une puce) ont montrés leur capacité à réduire significativement le niveau de sécurité attendu une fois les primitives déployées sur des vrais systèmes.

Récemment, les circuits quantiques ont également fait l'objet d'attaques [1] montrant l'importance de traiter les problèmes de canaux auxiliaires bien en amont et avant le déploiement à large échelle de ces dispositifs.

L'objectif de ce PIR est d'étudier les attaques par canaux auxiliaires ciblant les dispositifs de communication quantique, notamment en faisant une analyse de vulnérabilité des dispositifs acquis à l'INSA-Toulouse intégrant le protocole de communication BB-84.

Descriptif du projet :

- 1. Etat de l'art sur les protocoles de communication quantiques et des attaques par canaux auxiliaires ciblant les circuits classiques et quantiques.*
 - 2. Analyse de vulnérabilité de ces protocoles*
 - 3. Preuve de concept d'attaque sur le dispositif de communication quantique présent à l'INSA-Toulouse basé sur la protocole BB-84.*
 - 4. Proposition de contre-mesures*
- [1] Ferhat Erata , Chuanqi Xu , Ruzica Piskac and Jakub Szefer, « Quantum Circuit Reconstruction from Power Side-Channel Attacks on Quantum Computer Controllers », TCHES, 2024

PROFIL DES ETUDIANTS SOUHAITE (1 seul choix par projet)

☐ IR-SI : spécialité Informatique parcours Systèmes Informatiques

PRIORITE : si vous posez plusieurs sujets, indiquer ici la priorité de ce sujet (1= plus prioritaire)