Modèles d'apprentissage profond appliqués aux attaques par canaux auxiliaires contre les implémentations sécurisées d'algorithmes de cryptographie post-quantique

Mamadou Kolon Barry* and Farid Mokrane[1]

[1]Laboratoire Analyse, Géométrie et Applications – Laboratoire Analyse, Géométrie et Applications, LAGA, CNRS, UMR 7539, F-93430, Villetaneuse, France. – Institut Galilée, 99 avenue Jean-Baptiste Clément, F-93430, Villetaneuse, France, France

Résumé

L'organisme américain de normalisation National Institute of Standards and Technology (NIST) a lancé en 2016 un programme visant à définir un nouveau standard cryptographique résistant aux ordinateurs quantiques. Ce processus de sélection est arrivé à son terme et plusieurs premiers standards ont été publiés en 2023 et 2024. Cependant, au-delà de la sécurité mathématique de ces constructions, leur robustesse face aux attaques physiques reste une question ouverte, notamment face aux attaques par canaux auxiliaires (Side-Channel Attacks, SCA).
Les produits sécurisés par des mécanismes cryptographiques embarqués peuvent en effet être vulnérables à ces attaques. Les attaques par canaux auxiliaires exploitent des fuites physiques telles que la consommation d'énergie, le temps d'exécution ou encore les émissions électromagnétiques afin d'extraire des informations sensibles. Aujourd'hui, ces attaques peuvent être rendues plus efficaces grâce à l'utilisation de méthodes d'apprentissage profond (deep learning), capables d'extraire automatiquement des caractéristiques pertinentes à partir de signaux complexes.

L'objectif de cette thèse est d'explorer de nouvelles méthodes d'apprentissage automatique et de les adapter au contexte des attaques par canaux auxiliaires afin d'améliorer les performances des attaques contre les implémentations sécurisées d'algorithmes de cryptographie post-quantique.

Par ailleurs, l'usage intensif d'appareils mobiles connectés aux réseaux internet et téléphoniques augmente les risques liés aux attaques matérielles. La question de la sécurité de ces dispositifs devient donc cruciale. Les mécanismes de protection tels que le masquage ou la randomisation doivent être réévalués face à des attaquants capables d'exploiter des modèles de deep learning puissants.
La problématique principale de cette thèse est donc la suivante : les protections matérielles actuelles sont-elles suffisantes pour empêcher les attaques par canaux auxiliaires basées sur le deep learning contre les algorithmes de cryptographie post-quantique ?

*Intervenant