Sécurisation matérielle de cryptographie post-quantique basée sur les isogénies entre courbes elliptiques

Sujet de thèse

L'objectif principal de cette thèse est de concevoir des protections qui augmenteront la résistance aux attaques physiques d'une implémentation de l'algorithme cryptographique SIKE (Supersingular Isogeny Key Encapsulation).

La navigation au travers des isogénies entre courbes elliptiques supersingulières permet de construire un protocole d'échange de clé de type Diffie-Hellman. SIKE est un outil d'encapsulation de clé basé sur cette primitive de cryptographie asymétrique. Il fait partie des nouveaux algorithmes cryptographiques s'exécutant sur un ordinateur classique mais résistant à un attaquant disposant d'un calculateur quantique. Ces algorithmes "post-quantiques" sont en cours de standardisation dans un concours international organisé par le NIST. Le niveau de sécurité de ces algorithmes est choisi de manière à rendre les chemins d'attaques mathématiques par cryptanalyse impossibles. Ceci motive les attaquants à explorer des chemins d'attaques alternatifs en tirant profit d'un accès physique à l'implémentation manipulant la clé secrète. Les attaques par analyse des émanations électromagnétiques d'un déchiffrement ou par perturbation de celui-ci par illumination laser ou électromagnétique sont des moyens efficaces pour attaquer l'implémentation d'un algorithme mathématiquement sûr. Des protections existent pour les implémentations de cryptographie classique et sont capables de complexifier ce chemin d'attaque en dissimulant les secrets manipulés. Par contre, il existe peu de propositions de contre-mesures pour protéger les implémentations de SIKE et la menace des attaques physiques sur les isogénies n'est que partiellement caractérisée. Cette thèse propose d'explorer ces deux problèmes.

Le doctorant commencera par prendre en main les concepts mathématiques et les implémentations existantes de SIKE. Il/Elle cherchera à identifier les pistes d'attaques physiques théoriques existantes dans la littérature et à en proposer de nouvelles. Par des démonstrations expérimentales d'attaques physiques par écoute et/ou perturbation, il/elle affinera la caractérisation de la menace. Il/Elle proposera et implémentera des contre-mesures qui pourront être algorithmiques, logicielles ou matérielles dans le but

de proposer une implémentation SIKE avec un haut niveau de résistance aux attaques physiques.

Le laboratoire SAS “Systèmes et Architectures Sécurisés” situé entre Aix-En-Povence et Marseille à Gardanne sur le campus Georges Charpak Provence accueillera le doctorant au sein de l'équipe de recherche commune entre le CEA et l'EMSE. Cette équipe dispose d'équipements de pointe avec des bancs d'attaque physique au niveau de l'état de l'art international. La thèse sera co-dirigée par Nadia El Mrabet (EMSE/SAS) et Luca De Feo (UVSQ/LMV) avec un co-encadrement par Simon Pontié (CEA/SAS). Cette équipe d'encadrement réunie un des inventeurs du protocole SIKE, une spécialiste des courbes elliptiques et un concepteur de contre-mesures aux attaques physiques.

Plus d'informations:

- https://www.simon.pontie.fr/sujet-these/sike/index.html
- https://www.emse.fr/~nadia.el-mrabet/
- https://defeo.lu/
- https://www.simon.pontie.fr/
- http://www.cea-tech.fr/cea-tech/Pages/en-regions/pfa-securite-physique-systemes-electroniques.aspx
- https://sike.org/

Financement

Le financement de thèse CEA envisagé sera attribué à un étudiant présentant un très bon dossier de candidature.

Profils recherchés

Le candidat/La candidate devra avoir un cursus Mathématique, Informatique ou Électronique avec de fortes capacités en mathématique. Une expérience en lien avec les attaques physiques n'est pas obligatoire.

La thèse démarrera en octobre 2019.

Candidature

Les candidatures sont fermées.