Résistance des implémentations cryptographiques basées sur les isogénies à une attaque matérielle

Élise Tasso[1,2], Luca De Feo[3], Nadia El Mrabet[4], and Simon Pontié[1,2]

[1]CEA Tech, Centre CMP, Équipe Commune CEA Tech - Mines Saint-Étienne, F-13541 Gardanne, France
[2]Université Grenoble Alpes, CEA, Leti, F-38000 Grenoble, France
[3]IBM Research, Zurich, Suisse
[4]Mines Saint-Étienne, CEA-Tech, Centre CMP, 13541 Gardanne, France

En 1994, Shor a montré avec son algorithme de factorisation que les ordinateurs quantiques représentaient une menace pour la cryptographie asymétrique classique. Le National Institute of Standards and Technology (NIST) a alors lancé un concours de standardisation en 2016 afin que des équipes de chercheurs du monde entier proposent des algorithmes implantables sur ordinateurs classiques résistant aux attaques d'ordinateurs quantiques. Les candidats sont divisés en deux catégories : ceux pour le chiffrement et l'encapsulation de clef, et ceux pour la signature. Ils reposnt sur divers outils mathématiques. Nous allons nous intéresser à SIKE (Supersingular isogeny key encapsulation), le seul basé sur les isogénies entre courbes elliptiques. C'est un candidat alternatif au troisième round du concours : le NIST encourage à poursuivre les recherches à son sujet, mais on ignore encore s'il sera standardisé.
Tous les candidats encore en lice sont censés résister à la cryptanalyse. Toutefois, leurs implémentations peuvent être vulnérables à des attaques matérielles, où l'attaquant a un accès physique à la carte où s'exécute l'algorithme. On peut réaliser des attaques passives, où l'on observe l'exécution de l'algorithme en prenant des mesures de tension, d'émission électromagnétique ou de temps d'exécution par exemple, sans modification du fonctionnement, mais aussi des attaques actives, où l'on perturbe celui-ci en injectant des fautes à l'aide d'un laser ou d'un champ électromagnétique, entre autres. Des attaques des deux types ont été proposées pour la cryptographie basée sur les isogénies dans la littérature, mais peu ont été testées en laboratoire. Nous allons présenter une attaque matérielle sur SIKE en commençant par décrire la théorie qui la sous-tend, puis en expliquant comment nous l'avons mis en pratique en laboratoire. Nous finirons par présenter une contremesure idoine.

Mots-clefs : cryptographie post-quantique - SIKE - courbes elliptiques - isogénies - attaque matérielle.