Algorithmique des Isogénies de Variétés Abéliennes et Cryptographie Post-Quantique

Stage de recherche de Master 2

Encadrant : Pierre-Jean Spaenlehauer

Équipe CARAMBA, Inria Nancy – Grand Est

1 Contexte, motivation

La cryptographie basée sur les isogénies a connu un développement rapide durant ces dernières années, sous l'impulsion de l'invention en 2011 de SIDH [8], un système d'échange de clé basé sur les isogénies de courbes elliptiques supersingulières. Ce cryptosystème et ses variantes ont connu un fort engouement, notamment dû au fait qu'il promettait de résister aux attaques utilisant un ordinateur quantique. Malheureusement, des travaux récents ont permis de mettre en oeuvre des attaques dévastatrices sur SIDH, le rendant de fait obsolète [2, 9].

Cependant, le mouvement créé par SIDH a permis le développement d'une boîte à outils algorithmique diversifiée pour les isogénies de courbes elliptiques et a conduit également à la découverte d'autres constructions cryptographiques telles que CSIDH [4], SQISign [6], CSI-FiSh [1], etc.

Les faiblesses découvertes récemment montrent l'importance d'étudier des variantes qui peuvent se révéler résistantes aux attaques trouvées sur les systèmes les plus regardés. Une alternative possible consiste à étudier si les isogénies de variétés abéliennes peuvent servir de substitution aux isogénies de courbes elliptiques. Ceci est notamment motivé par le fait que les isogénies de courbes elliptiques sont des réalisations concrètes de la théorie de la multiplication complexe et de la théorie du corps de classes des corps quadratiques imaginaires, et elles permettent d'adopter un point de vue algorithmique sur ces théories. Ces concepts se généralisent partiellement aux variétés abéliennes via la théorie des corps CM. Des travaux récents [7, 5, 3] ont commencé à étudier ce qu'il était possible de faire avec ces objets, mais cette ligne de recherche a encore été assez peu explorée.

2 Objectifs du stage

Dans un premier temps, le stage consistera à se familiariser avec les variétés abéliennes — qui peuvent être vues comme des généralisations des courbes elliptiques — afin de construire un socle de connaissances théoriques. Ensuite, un objectif de ce stage de M2 sera de faire un état des lieux de la cryptographie basée sur les isogénies de variétés abéliennes de dimension 2 et plus. Le but sera d'étudier si des variantes de protocoles cryptographiques post-quantiques sur les courbes elliptiques peuvent se généraliser à ce contexte. Cet objectif est probablement très ambitieux, et on peut s'attendre à rencontrer de nombreux obstacles pratiques et algorithmiques sur le chemin qui mène à sa réalisation. Ce stage permettra d'identifier ces obstacles, et de réfléchir à proposer des solutions algorithmiques pour en surmonter. Par conséquent, le stage pourra bifurquer vers le développement d'outils algorithmiques pour les variétés abéliennes, avec une coloration de calcul formel et de géométrie arithmétique effective. Les résultats algorithmiques obtenus pourront donner lieu à des

implémentations. Les applications à la cryptographie serviront de boussole pour guider la direction générale que prendra le stage. Ce sujet nécessite un bagage assez conséquent à la fois en mathématiques (théorie des nombres, géométrie algébrique), et en informatique (algorithmique, calcul formel, complexité).

Ce stage pourra être prolongé par une thèse sur l'algorithmique des variétés abéliennes pour la cryptographie basée sur les isogénies.

Bibliographie

[1] Ward Beullens, Thorsten Kleinjung, et Frederik Vercauteren. CSI-FiSh: efficient isogeny based signatures through class group computations. Dans *International Conference on the Theory and Application of Cryptology and Information Security*, pages 227–247. Springer, 2019.

[2] Wouter Castryck et Thomas Decru. An efficient key recovery attack on SIDH (preliminary version). Cryptology ePrint Archive, Paper 2022/975, 2022. https://eprint.iacr.org/2022/975.

[3] Wouter Castryck, Thomas Decru, et Benjamin Smith. Hash functions from superspecial genus-2 curves using richelot isogenies. *Journal of Mathematical Cryptology*, 14(1):268–292, 2020.

[4] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, et Joost Renes. CSIDH: an efficient post-quantum commutative group action. Dans *International Conference on the Theory and Application of Cryptology and Information Security*, pages 395–427. Springer, 2018.

[5] Craig Costello et Benjamin Smith. The supersingular isogeny problem in genus 2 and beyond. Dans *International Conference on Post-Quantum Cryptography*, pages 151–168. Springer, 2020.

[6] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, et Benjamin Wesolowski. SQISign: compact post-quantum signatures from quaternions and isogenies. Dans *International Conference on the Theory and Application of Cryptology and Information Security*, pages 64–93. Springer, 2020.

[7] Eugène Victor Flynn et Yan Bo Ti. Genus two isogeny cryptography. Dans *International Conference on Post-Quantum Cryptography*, pages 286–306. Springer, 2019.

[8] David Jao et Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. Dans *International Workshop on Post-Quantum Cryptography*, pages 19–34. Springer, 2011.

[9] Damien Robert. Breaking SIDH in polynomial time. Cryptology ePrint Archive, Paper 2022/1038, 2022. https://eprint.iacr.org/2022/1038.