Un protocole d'échange de clé post-quantique avec des modules de Drinfeld

Antoine Leudière

La cryptographie post-quantique naît de la nécessité de se prémunir — avec des ordinateurs classiques — des attaques menées par des ordinateurs quantiques. Cette discipline est particulièrement florissante depuis l'ouverture en 2017 de la compétition de standardisation du NIST (`https://csrc.nist.gov/projects/post-quantum-cryptography/`). Plusieurs classes de solutions sont en compétition : cryptographie multivariée, des réseaux, des codes correcteurs, ou encore, des isogénies de courbes elliptiques. C'est cette dernière qui nous intéresse, notamment les protocoles d'échange de clé basés sur une action de groupe simplement transitive facile à calculer et difficile à inverser.

Une isogénie de courbes elliptiques est un morphisme (au sens de la géométrie algébrique) de courbes elliptiques qui est aussi un morphisme de groupes. Les cryptosystèmes basés sur ces dernières misent en général sur la difficulté de trouver une isogénie entre deux courbes elliptiques isogènes données, citons CRS ([Cou96], [RS06]) et CSIDH ([Cas+18]). Dans ce paradigme, les clés sont de tailles relativement courte. Néanmoins, les performances de CRS sont peu compétitives ; quant à CSIDH, il est difficile sur un ordinateur classique de calculer la structure du groupe considéré. Dans ce contexte, il est naturel de chercher à adapter ces constructions à d'autres objets mathématiques.

C'est ici que les modules de Drinfeld entrent en jeu. Un module de Drinfeld est une construction algébrique issue de l'arithmétique des corps de fonctions. Ces objets ont des propriétés algébriques extraordinairement proches de celles des courbes elliptiques, à ceci près qu'un module de Drinfeld induit une loi de $\mathbb{F}_q[X]$-module sur la clôture algébrique $\overline{\mathbb{F}_q}$ et non de $\mathbb{Z}$-module sur les points de la courbe elliptique.

Nous proposons un nouveau protocole d'échange de clé, non-interactif, basé sur une action de groupe simplement transitive, facile à calculer et difficile à inverser. La construction, que nous décrirons dans cet exposé, mime celles de CRS et permet de déterminer l'ordre du groupe considéré en temps polynomial. Nous nous intéresserons aussi au problème mathématique sur lequel repose la sécurité du protocole. Nous évoquerons enfin des résultats expérimentaux qui suggèrent que le calcul de l'action de groupe est compétitif avec CSIDH.

Travail commun avec Pierre-Jean Spaenlehauer et Emmanuel Thomé.

Références

[Cas+18] Wouter Castryck et al. "CSIDH : An efficient post-quantum commutative group action". In : *Asiacrypt* (2018), p. 395-427. URL : `https://link.springer.com/chapter/10.1007/978-3-030-03332-3_15`.

[Cou96] Jean-Marc Couveignes. "Hard homogeneous spaces". 1996. URL : `https://eprint.iacr.org/2006/291.pdf`.

[DJP11] Luca De Feo, David Jao et Jérôme Plût. "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies". In : *PQCrypto* (2011), p. 19-34. URL : `https://eprint.iacr.org/2011/506.pdf`.

[RS06] Alexander Rostovtsev et Anton Stolbunov. "Public-key cryptosystem based on isogenies". 2006. URL : `https://eprint.iacr.org/2006/145`.