Analyse de sécurité quantique de OSIDH

Contexte. Le stage se déroulera au LORIA (Nancy), au sein de l'équipe CARAMBA. Il sera encadré par Xavier Bonnetain.

Contact. `xavier.bonnetain@inria.fr`

Description. L'avènement d'un ordinateur quantique efficace permettrait de casser totalement les cryptosystèmes à clé publique RSA et Diffie-Hellman, qui sont ceux généralement utilisés à l'heure actuelle. Cette catastrophe annoncée a permi le développement de la cryptographie *post-quantique*, qui vise à concevoir et analyser des remplaçants resistant à l'ordinateur quantique.

Parmi les systèmes proposés, les constructions à base d'isogénies ont une place particulière : leur développement est plutôt récent, elles utilisent des outils proches des constructions pré-quantiques, et reposent sur des hypothèses de sécurité spécifiques qui ont été encore peu étudiées. Cela a par exemple été observé sur la construction la plus aboutie, le protocole d'échange de clé SIKE [AKC+17], qui a été cassé cette année [CD22, Rob22]. Néanmoins, d'autres constructions plus récentes n'ont pas les faiblesses de SIKE. On peut par exemple citer CSIDH [CLM+18], un système d'échange de clé non-interactif, et sa généralisation OSIDH [CK20].

L'objectif de ce stage est d'étudier la sécurité quantique de OSIDH. Pour cela, plusieurs pistes pourront être explorées :

Approche classique. La sécurité de OSIDH dans un contexte classique a été étudiée [DF22], et la meilleure attaque proposée utilise un algorithme de réduction de réseau en norme infinie. Une version quantique de cet algorithme donnerait directement une attaque sur OSIDH.

Décalage caché. La sécurité de CSIDH repose sur le problème du *décalage caché*, pour lesquels il existe des algorithmes quantiques sous-exponentiels [CJS14, BS20, Pei20]. Le cadre de OSIDH est différent, mais si de tels algorithmes sont appliquables, cela pourrait donner des attaques quantiques bien meilleures.

Réduction de réseau quantique. Des travaux récents [CLZ22] ont montré que certains problèmes de réseau en norme infinie, difficiles classiquement, peuvent être résolus quantiquement en temps polynomial. Si à l'heure actuelle, l'intérêt cryptographique de ces algorithmes n'est pas clair, on pourra étudier leur applicabilité à OSIDH.

References

[AKC+17] Reza Azarderakhsh, Brian Koziel, Matt Campagna, Brian LaMacchia, Craig Costello, Patrick Longa, Luca De Feo, Michael Naehrig, Basil Hess, Joost Renes, Amir Jalali, Vladimir Soukharev, David Jao, and David Urbanik. Supersingular isogeny key encapsulation, 2017.

[BS20] Xavier Bonnetain and André Schrottenloher. Quantum security analysis of CSIDH. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology*

- *EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part II*, volume 12106 of *Lecture Notes in Computer Science*, pages 493–522. Springer, 2020.

[CD22] Wouter Castryck and Thomas Decru. An efficient key recovery attack on SIDH (preliminary version). *IACR Cryptol. ePrint Arch.*, page 975, 2022.

[CJS14] Andrew M. Childs, David Jao, and Vladimir Soukharev. Constructing elliptic curve isogenies in quantum subexponential time. *J. Math. Cryptol.*, 8(1):1–29, 2014.

[CK20] Leonardo Colò and David Kohel. Orienting supersingular isogeny graphs. *Journal of Mathematical Cryptology*, 14(1):414–437, 2020.

[CLM+18] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: an efficient post-quantum commutative group action. In Thomas Peyrin and Steven D. Galbraith, editors, *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part III*, volume 11274 of *Lecture Notes in Computer Science*, pages 395–427. Springer, 2018.

[CLZ22] Yilei Chen, Qipeng Liu, and Mark Zhandry. Quantum algorithms for variants of average-case lattice problems via filtering. In Orr Dunkelman and Stefan Dziembowski, editors, *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III*, volume 13277 of *Lecture Notes in Computer Science*, pages 372–401. Springer, 2022.

[DF22] Pierrick Dartois and Luca De Feo. On the security of OSIDH. In Goichiro Hanaoka, Junji Shikata, and Yohei Watanabe, editors, *Public-Key Cryptography - PKC 2022 - 25th IACR International Conference on Practice and Theory of Public-Key Cryptography, Virtual Event, March 8-11, 2022, Proceedings, Part I*, volume 13177 of *Lecture Notes in Computer Science*, pages 52–81. Springer, 2022.

[Pei20] Chris Peikert. He gives c-sieves on the CSIDH. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part II*, volume 12106 of *Lecture Notes in Computer Science*, pages 463–492. Springer, 2020.

[Rob22] Damien Robert. Breaking SIDH in polynomial time. *IACR Cryptol. ePrint Arch.*, page 1038, 2022.