Radical CTIDH

Andreas Hellenbrand
andreas.hellenbrand@hs-rm.de
RheinMain University of Applied Sciences, Wiebsaden

36th Crypto Day, 14./15. March 2024

We present a first performance evaluation for the usage radical isogenies in CTIDH [1], which is currently the state-of-the-art constant-time instantiation of Commutative Supersingular Isogeny Diffie-Hellman (CSIDH) [5]. Our approach introduces a new keyspace that allows the usage of 2- and 4-isogenies on the surface, together with a novel hybrid strategy for including radical isogenies of small odd degrees.

Radical isogenies were first presented by Castryck & Decru in 2020 in the form of 2-actions on the surface and are built around chaining the computation of isogenies, such that multiple isogenies of the same degree can be performed from a single kernel point [3]. Follow-up work introduced new and more efficient formulas for more degrees [2, 7, 4]. Radical isogenies for constant-time implementations were analyzed in [6]. However, to allow for even degree isogenies on the surface, these parameters relied on a prime with 513 or 514 bits, which are unsuitable for optimized implementations as they do not align with 64-bit registers. Therefore, we present a new 511-bit prime called RADICAL-512. This new prime allows for equally fast assembly-optimized arithmetic as the original CSIDH-512 prime.

We include radical isogenies into CTIDH using a novel hybrid approach, in which isogenies of small degrees are used for radical isogenies and CTIDH batches. This allows us to combine the benefits of both worlds.

While the first benchmarks of our implementation only indicate tiny improvements of 1-2% compared to CSIDH-512, the results of this work provide relevant insight into the importance of selecting parameters, as seen by the new RADICAL-512 prime. Further, we provide first results on the performance of Radical isogenies in a performance-optimized constant-time setting.

References

[1] Gustavo Banegas, Daniel J. Bernstein, Fabio Campos, Tung Chou, Tanja Lange, Michael Meyer, Benjamin Smith & Jana Sotáková (2021). CTIDH: faster constant-time CSIDH. volume 2021, 351–387. URL https://doi.org/10.46586/tches.v2021.i4.351-387.

[2] Wouter Castryck (2021). CSIDH On The Surface (CSURF). Isogeny-based Cryptography School - July 2021. URL https://homes.esat.kuleuven.be/~wcastryc/summer_school_csurf.pdf.

crypto day matters 36 (2024)
Beiträge vom 36. Kryptotag, 14.-15. MÃ¤rz 2024, Regensburg.
doi:10.18420/cdm-2024-36-33

[3] Wouter Castryck & Thomas Decru (2020). CSIDH on the Surface. In *Post-Quantum Cryptography - 11th International Conference, PQCrypto 2020, Paris, France, April 15-17, 2020, Proceedings*, Jintai Ding & Jean-Pierre Tillich, editors, volume 12100 of *Lecture Notes in Computer Science*, 111–129. Springer. URL https://doi.org/10.1007/978-3-030-44223-1_7.

[4] Wouter Castryck, Thomas Decru, Marc Houben & Frederik Vercauteren (2022). Horizontal Racewalking Using Radical Isogenies. In *Advances in Cryptology - ASIACRYPT 2022 - 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5-9, 2022, Proceedings, Part II*, Shweta Agrawal & Dongdai Lin, editors, volume 13792 of *Lecture Notes in Computer Science*, 67–96. Springer. URL https://doi.org/10.1007/978-3-031-22966-4_3.

[5] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny & Joost Renes (2018). CSIDH: An Efficient Post-Quantum Commutative Group Action. In *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*, Thomas Peyrin & Steven D. Galbraith, editors, volume 11274 of *Lecture Notes in Computer Science*, 395–427. Springer. URL https://doi.org/10.1007/978-3-030-03332-3_15.

[6] Jesús-Javier Chi-Domínguez & Krijn Reijnders (2022). Fully Projective Radical Isogenies in Constant-Time. In *Topics in Cryptology – CT-RSA 2022*, Steven D. Galbraith, editor, 73–95. Springer International Publishing, Cham. ISBN 978-3-030-95312-6.

[7] Hiroshi Onuki & Tomoki Moriya (2022). Radical Isogenies on Montgomery Curves. In *Public-Key Cryptography – PKC 2022*, Goichiro Hanaoka, Junji Shikata & Yohei Watanabe, editors, 473–497. Springer International Publishing, Cham. ISBN 978-3-030-97121-2.