**SCIS 2022** 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

# Implementations on identity-based signature schemes based on variants of CSIDH

Hyungrok Jo * Junji Shikata †

**Keywords:** post-quantum cryptography, isogeny-based cryptography, identity-based signature scheme, CSIDH, CsiIBS, forward-secure signature

## Abstract

Identity-based cryptography are one of main high functional applications for a modern society. The necessity for these proposals are enlarging especially as growing the pie of IoT (Internet of Things) among electronics industry. Recently, there are some suggestions of identity based identification schemes or signature schemes based on even isogeny walk problems, which are known as one of promising candidates for post-quantum cryptography (PQC for short).

In this paper, we measure the performances of two identity-based signature schemes, which are recently proposed by Peng et al. [8] CsiIBS (2020) and Shaw and Dutta [9] (ProvSec2021), respectively. Especially, since in Shaw and Dutta's work, there are no implementation results, we try to measure the proper parameter sets of their schemes. We also consider the best possibilities of each scheme by switching the underlying isogeny problems (CSIDH) to variants (CSURF) of CSIDH or other isogeny problems such as endomorphism computation problem towards high efficiencies.

## References

[1] Castryck, W., Lange, T., Martindale, C., Panny, L., & Renes, J., "CSIDH: an efficient post-quantum commutative group action." *In International Conference on the Theory and Application of Cryptology and Information Security*, pp. 395-427, Springer, Cham, 2018.

[2] Castryck, W., & Decru, T., "CSIDH on the surface." *In International Conference on Post-Quantum Cryptography* (PQCrypto 2020), Vol. 12100, pp. 111-129, Springer, 2020.

[3] De Feo, L., Jao, D., & Plût, J.,"Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies,", *Journal of Mathematical Cryptology*, 8(3), pp. 209-247, 2014.

[4] Eisenträger, K., Hallgren, S., Lauter, K., Morrison, T., & Petit, C., "Supersingular isogeny graphs and endomorphism rings: reductions and solutions," *In Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 329-368, Springer, Cham., 2018.

[5] Fan, X., Tian, S., Xu, X., & Li, B., "CSURF-TWO: CSIDH for the Ratio (2: 1),", *In International Conference on Information Security and Cryptology*, pp. 148-156, Springer, Cham., 2020.

[6] Galbraith, S. D., Petit, C., & Silva, J., "Identification protocols and signature schemes based on supersingular isogeny problems," *In International Conference on the Theory and Application of Cryptology and Information Security*, pp. 3-33, Springer, Cham., 2017.

[7] Kim, S., "On the Use of Twisted Montgomery Curves for CSIDH-Based Cryptography." *Journal of the Korea Institute of Information Security & Cryptology*, 31(3), pp. 497-508, 2021.

[8] Peng, C., Chen, J., Zhou, L., Choo, K. K. R., & He, D., "CsiIBS: A post-quantum identity-based signature scheme based on isogenies," *Journal of Information Security and Applications*, 54, 102504, 2020.

[9] Shaw, S., & Dutta, R., "Identification Scheme and Forward-Secure Signature in Identity-Based Setting from Isogenies," *In International Conference on Provable Security*, pp. 309-326, Springer, Cham, 2021.

* Yokohama National University, Institute of Advanced Sciences,79-5 Tokiwadai, Hodogaya-ku, Yokohama, Kanagawa (jo-hyungrok-xz@ynu.ac.jp)

† Yokohama National University, 79-7 Tokiwadai, Hodogaya-ku, Yokohama, Kanagawa (junji-shikata-rb@ynu.ac.jp)