JMA-745

Commutative Supersingular Isogeny Diffie Hellman Key Exchange Using Edward Curves

Krishnaprabha R

Researcher, Amrita Viswa Vidyapeetham Ettimadai

*Corresponding author's e-mail: krishnaprabha.kpr@gmail.com

ABSTRACT

In a post-quantum environment, we suggest a productive commutative group action appropriate for non-interactive key exchange. The Diffie–Hellman key exchange technique resulted from group action runs quickly and permits public key validation at extremely minimal cost. Castryck presented the isogeny-based CSIDH key exchange protocol in 2018. In this paper CSIDH is based on supersingular elliptic curve isogenies. The ideal class group action on the Fp-isomorphism classes of Montgomery curves serves as its foundation. The original CSIDH technique represented points as x-coordinates over Montgomery curves, requiring a computation over Fp.On Edwards curves, a unique coordinate known as the w coordinate is used to compute group operations and isogenies. We must take into account points defined over Fp^4 if we attempt to compute the class group action on Edwards curves using the w-coordinate in a manner similar to that on Montgomery curves. Consequently, it is not an easy operation to calculate the class group action on Edwards curves with w coordinates over just Fp. We construct the new CSIDH algorithm using Edwards curves with w-coordinates over Fp.

Keywords: Supersingular Isogeny, Edwards curves, CSIDH

How to Cite

Krishnaprabha R, "Commutative Supersingular Isogeny Diffie Hellman Key Exchange Using Edward Curves", *AIJR Abstracts*, pp. 36–36, Feb. 2024.

DOI: 10.21467/abstracts.165 ISBN: 978-81-965621-7-5 (eBook), 978-81-965621-4-4 (Paperback)