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

Montgomery 曲線の x 座標を用いた 3-同種計算の最小演算コスト
The minimal cost of operations on 3-isogeny computation via x-coordinates of Montgomery curves

守谷 共起 * 小貫 啓史 * 相川 勇輔 † 高木 剛 *
Tomoki Moriya Hiroshi Onuki Yusuke Aikawa Tsuyoshi Takagi

キーワード 同種写像暗号，耐量子暗号，同種写像計算，Montgomery 曲線，数論アルゴリズム

あらまし

楕円曲線間の同種写像を用いた同種写像暗号は量子計算機に耐性のある公開鍵暗号方式（耐量子暗号）の候補の 1 つであり，SIDH[4] や CSIDH[1] などのプリミティブが知られている．同種写像暗号には鍵長が短いというメリットがあり，IC チップや IoT 機器などメモリ制約が厳しい環境での利用が期待されている．

一方で，同種写像暗号ではスカラー倍や同種写像計算などのコストの高い計算を大量に行う必要があり，耐量子暗号の他の候補である格子暗号や多変数多項式暗号と比較して非効率であるというデメリットがある．同種写像暗号を効率化するために，1 つの座標で記述できる同種写像計算の公式が用いられる．その中で最も利用されているものとして，Montgomery 曲線の x 座標を用いた公式がある [6, 2, 5]．これらの論文ではいくつかの異なる形の公式が提案されており，同種写像計算の乗算 **M**，2 乗算 **S** の回数も変化している．

本研究では，Montgomery 曲線の x 座標を用いた上記の同種写像計算公式の違いについて解析を行った．まず，複数の計算公式の差が，division polynomial と呼ばれる楕円曲線の群構造から決まる多項式を因子に持つような分数多項式になるということを証明した．この事実を利用して，本研究では射影座標を用いた 3-同種写像の演算コストの最小値が $2\mathbf{M} + 3\mathbf{S}$ となることを証明した．

現在知られている最も効率的な射影座標を用いた 3-同種計算公式は，Costello らによって提案された

$$(-27X^4 + 18X^2Z^2 + Z^4 : 4XZ^3)$$

である [3]．この公式は [2, Appendix A] によると $2\mathbf{M}+3\mathbf{S}$ で計算できるため，本研究よりこの公式が理論的にも最も効率的に計算できる 3-同種計算公式の一つであることが示せた．

* 東京大学大学院 情報理工学系研究科 数理情報学専攻, 東京都文京区本郷 7-3-1. Department of Mathematical Informatics, The University of Tokyo, 7-3-1, Hongo, Bunkyo-ku, Tokyo. {tomoki_moriya,onuki,takagi}@mist.i.u-tokyo.ac.jp
† 三菱電機 情報技術総合研究所, 神奈川県鎌倉市大船 5-1-1. Information Technology R&D Center, Mistubishi Electric Corporation, 5-1-1, Ofuna, Kamakura-shi, Kanagawa. Aikawa.Yusuke@bc.MitsubishiElectric.co.jp

参考文献

[1] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: an efficient post-quantum commutative group action. In *International Conference on the Theory and Application of Cryptology and Information Security–ASIACRYPT 2018*, pages 395–427. Springer, 2018.

[2] Craig Costello and Huseyin Hisil. A simple and compact algorithm for SIDH with arbitrary degree isogenies. In *International Conference on the Theory and Application of Cryptology and Information Security–ASIACRYPT 2017*, pages 303–329. Springer, 2017.

[3] Craig Costello, Patrick Longa, and Michael Naehrig. Efficient algorithms for supersingular isogeny Diffie-Hellman. In *Annual International Cryptology Conference*, pages 572–601. Springer, 2016.

[4] David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In *International Workshop on Post-Quantum Cryptography–PQCrypto 2011*, pages 19–34. Springer, 2011.

[5] Michael Meyer and Steffen Reith. A faster way to the CSIDH. In *International Conference on Cryptology in India–INDOCRYPT 2018*, pages 137–152. Springer, 2018.

[6] Joost Renes. Computing isogenies between Montgomery curves using the action of (0, 0). In *International Conference on Post-Quantum Cryptography–PQCrypto 2018*, pages 229–247. Springer, 2018.