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

適切な素数選択による KLPT アルゴリズムを利用した同種写像構成計算
Isogeny Construction Using the KLPT Algorithm with Suitable Prime Numbers

高橋　康 * 神戸 祐太 † 安田 雅哉 † 横山 和弘 †
Yasushi Takahashi Yuta Kambe Masaya Yasuda Kazuhiro Yokoyama

キーワード 耐量子計算機暗号，同種写像，KLPT アルゴリズム

あらまし

超特異楕円曲線間の同種写像問題を利用した同種写像暗号は，耐量子計算機暗号の候補として期待されている．同種写像暗号には，SIKE や SIDH のように超特異楕円曲線間の同種写像問題を直接利用する方式の他に，超特異楕円曲線の同型類の集合への作用を利用する方式や，自己準同型環と四元数環の極大整環の間の対応 (Deuring 対応) を利用する方式が知られている．本研究では特に，Deuring 対応を利用する方式 (ここでは KLPT ベース同種写像暗号方式と呼ぶ) の高速化手法を提案する．この方式では，その鍵生成フェーズにおいて，以下の 2 つの計算ステップを必要とする; 1) 超特異楕円曲線間の同種写像問題と Deuring 対応によって対応する，以下のような極大整環上の類似問題を求解する; 2)smooth なイデアル J を用いて，与えられた E_0 と同種な E_J を計算する．

問題 (極大整環上の類似同種写像問題)．与えられた左 $\mathcal{O}$, イデアル I に対して，smooth なノルムを持つ I と同値な左 $\mathcal{O}$, イデアル J を見つけよ．ここで I と J が同値であるとは，Deuring 対応で I と J に対応する 2 つの楕円曲線 E_I, E_J は同型であることをいう．

ステップ 1 で出力されるイデアル J は，そのノルムが smooth であるほど，ステップ 2 の同種計算が効率的であることが知られている．この計算には Kohel-Lauter-Petit-Tignol アルゴリズム (KLPT アルゴリズム) が使用されるが，その実装例は少なく，MathCrypt2021 で発表された神戸らの研究 [3] はその数少ない例の一つである．この神戸らの実装および計算実験の成果の一つとして，イデアルのノルムの素因子 l に対して l-ねじれ部分群を定める F_{p^2} 上拡大体のサイズが大きい場合，同種写像構成計算の所要時間が大きくなることが明らかになった．

そこで本提案手法では，各ねじれ部分群を定める拡大体のサイズが小さいイデアルが出力されるよう，KLPT アルゴリズムで用いられる素数を選択する改良手法を提案する．設定として，最初の超特異楕円曲線 E_0 は与えられているとする．提案手法ではまず，ある程度大きい素数までの E_0 のねじれ部分群を定める拡大体のサイズ k を事前計算し，k が小さい順にリスト化する．そして，KLPT アルゴリズムを実行する際には，k が小さい素数ほどイデアルのノルムを構成する素因子として使用される頻度が高くなるように，素数選択部分に改良を加える．

本発表では，この改良手法を加えた KLPT アルゴリズムを用いて，step1 の計算実験及び，step2 で利用される核多項式を出力するまでの計算実験を行い，従来手法による計算時間との比較を行う．

参考文献

[1] Galbraith, S. D., et al.: Identification protocols and signature schemes based on supersingular isogeny problems. Asiacrypt 2017.

[2] Kohel, D., et al.: On the quaternion-isogeny path problem. LMS J. of Comp. and Math. 17.A (2014): 418-432.

[3] Kambe, Y., et al.: Solving the constructive Deuring correspondence via the Kohel-Lauter-Petit-Tignol algorithm. MathCrypt 2021.

* 富士通株式会社 〒 211–8588 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号. FUJITSU LTD., 4–1–1 Kamikodanaka, Nakahara-ku, Kawasaki, Kanagawa 211–8588, Japan. t-yasushi@fujitsu.com
† 立教大学 〒 171–8501 東京都豊島区西池袋 3–34–1. Rikkyo University, 3–34–1 Nishiikebukuro, Toshima-ku, Tokyo, 171–8501, Japan. yuta.kambe.math@gmail.com, {yasuda,kazuhiro}@rikkyo.ac.jp