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

FK12 曲線上のペアリングにおける最終べきアルゴリズムの改良

Improvement of Algorithm for Computing Final Exponentiation for Pairing on FK12

池坂 和真 * 南條 由紀 * 小寺 雄太 * 日下 卓也 * 野上 保之 *
Kazuma Ikesaka Yuki Nanjo Yuta Kodera Takuya Kusaka Yasuyuki Nogami

キーワード ペアリング暗号，数体ふるい法，最終べき

楕円曲線上のペアリングは，ID ベース暗号やグループ署名などの様々な高機能暗号を実現するために重要なツールである．これらの高機能暗号を現実的なレベルで利用するためにペアリング計算の効率実装の関する研究が行われている．ペアリング暗号の安全性は，拡大体上の離散対数問題 (FFDLP) と楕円曲線上の離散対数問題 (ECDLP) を根拠としている．現時点で，ECDLP を解くためのアルゴリズムの劇的な改善は提案されていないが FFDLP を解くアルゴリズムとして 2016 年に拡大体上の数体ふるい法 (TNFS) の改良が提案された．ペアリングに用いられる拡大体に対しては，より効率的な数体ふるい法 (STNFS) が実行できることが報告されている．これらのアルゴリズムの改良に応じて，ペアリングの安全性評価の見直しや新たな推奨曲線の提案が行われている．これまでに推奨されてきた曲線として，BN12 曲線，BLS12 曲線， KSS16 曲線が挙げられる．この他，新たに推奨曲線に加わったものとして，Fotiadis と Konstantinou により [1] で示された埋め込み次数 12 の曲線 (FK12 曲線)，埋込み次数が素数の曲線，Cocks-Pinch 曲線などが挙げられる．これらの曲線上のペアリング計算量評価によると，BLS12 曲線， FK12 曲線，埋込み次数が 6 の Cocks-Pinch 曲線は，とくに効率的なペアリングを実現できると考えられる．本研究はこのうち FK12 曲線を対象とする．

楕円曲線上のペアリングは Miller ループと最終べきの計算の 2 つのステップからなり，最終べきの計算は曲線ごとに固定のべき指数により行う．さらに，このべき乗算は計算が容易な easy part と，それ以外の hard part に分割される．この hard part をどのように分割するか，またその分割結果をどのような計算手順で実行するかに最終べきの効率性は大きく左右される．最終べきの hard part の分割法については，主に p-進数展開法 [2] と格子ベースの手法 [3] が知られている．また，最適な計算手順を探索する方法として，加算鎖を利用する方法や計算結果の再利用を行うことができるような関係式を見出す手法が知られている．本研究の対象である FK12 曲線の最終べきの計算については，先行研究において格子ベースの手法を用いて最終べきを分割し，加算鎖の手法を用いてアルゴリズムを構成している [4]．しかし，アルゴリズムを構成する際には，計算結果を再利用できるような関係式を見出す手法を用いる方が計算効率の良いアルゴリズムを構成できる可能性がある．

本研究ではこの可能性を検証し，FK12 曲線上の最終べきのアルゴリズムの改善を行う．著者らは計算結果を再利用できるような関係式を探索し，既存手法のものとは異なる新たな最終べきの計算アルゴリズムを構成した．既存アルゴリズムと提案アルゴリズムの最終べきにかかる計算コストは素体上の乗算コスト m を用いて表すとそれぞれ $7803m$，$6525m$ で与えられる．これより，提案アルゴリズムは既存アルゴリズムよりも 16.4%少ない計算コストで最終べきを実行することができることが分かった．

参考文献

[1] G. Fotiadis and E. Konstantinou, “TNFS resistant families of pairing-friendly elliptic curves,” Theoretical Computer Science, vol. 800, pp. 73–89, 2019.

[2] M. Scott, N. Benger, M. Charlemagne, L. J. D. Perez, and E. J. Kachisa, “On the final exponentiation for calculating pairings on ordinary elliptic curves,” in International conference on pairing-based cryptography. Springer, pp. 78–88, 2009.

[3] L. Fuentes-Castaneda, E. Knapp, and F. Rodr ıguez-Henr ıquez, “Faster hashing to G2,” in International workshop on selected areas in cryptography. Springer, pp. 412–430, 2011.

[4] G. Fotiadis and C. Martindale, “Optimal TNFS-secure pairings on elliptic curves with composite embedding degree,” Cryptology ePrint Archive, Report 2019/555, 2019, https://eprint.iacr.org/2019/555.

* 岡山大学, 岡山県岡山市北区津島中 3-1-1, Okayama University, Tsushima–naka 3–1–1, Kita–ku, Okayama 700–8530, Japan