SCIS 2021 2021 Symposium on
Cryptography and Information Security
On-line, Jan. 19 – 22, 2021
The Institute of Electronics,
Information and Communication Engineers

BLS 曲線上のペアリングにおける効率的な最終べき計算方式
Efficient Final Exponentiation for Pairings over BLS Curves

林田 大輝 * 早坂 健一郎 * 照屋唯紀 †
Daiki Hayashida Kenichiro Hayasaka Tadanori Teruya

あらまし ペアリング演算は Miller loop と最終べきの二つの演算からなる．最終べきについては，個々の楕円曲線族に依存したヒューリスティックな手順を含むアルゴリズムがこれまで用いられてきた．本研究では，楕円曲線上に定義されるペアリングの計算における最終べきについて，個々の楕円曲線に依存せず，ヒューリスティックな手順を含まない最終べき計算方式を初めて提案する．具体的には，二つの方式を提案する．一つ目は，円分多項式の構造を利用した，従来法を一般化した方式であり，任意の楕円曲線族に適用可能である．二つ目は，斉次円分多項式を利用した，埋め込み次数が 2^m, 3^n, 2^m3^n $(m, n \geq 1)$ の楕円曲線族に適用可能な方式である．両提案方式により，全ての Barreto-Lynn-Scott (BLS) 曲線において効率的な最終べき計算の存在が保証される．特に後者の方式は，対応する全ての BLS 曲線に対して既存のアルゴリズムよりも効率的な新しいアルゴリズムを与える．

キーワード ペアリング，最終べき，Barreto-Lynn-Scott (BLS) 曲線，円分多項式

1 はじめに

ペアリングを用いる暗号として，ID ベース暗号 [7] や関数型暗号 [20]，Boneh-Lynn-Shacham (BLS) 署名 [8] などが知られている．ペアリングの安全性は，楕円曲線上の離散対数問題と有限体上の離散対数問題の安全性により決定される．近年，Kim らの exTNFS [16, 17] による新たな有限体上の離散対数問題に対する数体篩法で離散対数問題の安全性が見直されたため，各セキュリティレベルにおける楕円曲線の候補に変化が見られている．例えば 128 ビットセキュリティにおいては BLS12 曲線が新たな候補として注目されている [14].

ところが，128 ビット・192 ビット・256 ビットセキュリティレベルそれぞれについて最良の楕円曲線を選択するためには，安全性・効率性・互換性・機能，全ての要素を考慮する必要があり，容易ではない．特に，ペアリングを用いる暗号方式において，ペアリングの計算量はボトルネックであるため，その効率化は重要な課題である．

ペアリングを計算するアルゴリズムは，大きく分けて，Miller loop と最終べきの二つからなる．最終べきを効率的に計算するには，べき部分をどのように分解するか，また，得られた分解に対してどのような計算手順を踏むかを検討することが重要である．

分解については大きく分けて 3 つのアプローチが存在する：p 進展開方式 [2, 3, 6, 4, 24, 25, 19]，lattice-based 方式 [1, 4, 10, 22]，特定の曲線パラメータの関係式を利用した方式 [23] である．また，最適な計算手順を探索する方式として，addition-chain 方式 [21] が知られている．いずれの方式においても，そのアルゴリズムは個々の楕円曲線もしくは楕円曲線パラメータに依存しており，分解もしくは計算手順探索においてその曲線独自の調整を行うことで，最終べき計算の効率化を図っている．

このように，先行研究における最終べき計算アルゴリズムはヒューリスティックな手順を含んでいる．したがって，新しい曲線に対して効率的な最終べきの計算方法を定めるには，新たにその曲線独自の最終べき計算アルゴリズムを従来方式を利用して構成する必要があり，その際，その方式に含まれるヒューリスティックな手続きを人手で与えながら試行錯誤する必要があるため，容易ではない．これらのことから従来方式，実利用が期待できるようなペアリング暗号に適した楕円曲線について，効率的な最終べき計算アルゴリズムの存在を自動的に保証するものではなく，効率的かつ統一的なアルゴリズムは知られていないのが現状である．

1.1 関連研究

最終べき計算において，p 進展開方式を用いた文献は [2, 3, 6, 4, 24, 25, 19] など数多くの曲線に対して研究さ

* 三菱電機株式会社 情報技術総合研究所 〒 247–8501 神奈川県鎌倉市大船 5-1-1.
† 産業技術総合研究所 〒 135-0064 東京都江東区青海 2-4-7.

れている．また，白勢ら [25] はこの方式を任意の BLS 曲線に拡張している．lattice-based 方式を用いた文献は [1, 4, 10, 22] などがあげられる．BLS27 曲線に限定されているが，曲線パラメータの多項式を利用した方式 [23] も提案されている．これらの方式は，効率的な計算アルゴリズムを構成するために，最終べきにおける分解部分もしくは計算手順を探索する部分で個々の楕円曲線に依存したヒューリスティックな手順を含んでいる．

1.2 貢献

本研究では，個々の楕円曲線に依存せず，ヒューリスティックな手順を含まない最終べき計算方式を二つ提案する．

一つ目の提案方式は，円分多項式の構造を利用した p 進展開方式を一般化した方式であり，任意の楕円曲線族に適用可能である．従来の p 進展開方式は個々の楕円曲線に依存しており，展開で得られた係数同士の関係性を探索するというヒューリスティックな手順を含んでいたが，この方式ではその係数同士の関係性を任意の楕円曲線族に対して記述する．したがって，この方式により，すべての BLS 曲線において効率的な最終べき計算アルゴリズムの存在が保証される．また，この方式はこれまで各 BLS 曲線で提案されてきた最良の最終べきアルゴリズムを出力する．なお，BLS 曲線に対する最終べき一般化を提案した文献 [25] とは，独立した研究である．

二つ目の提案方式は，斉次円分多項式を利用した，埋め込み次数が $k = 2^m$, $k = 3^n$, $k = 2^m 3^n$ $(m, n \geq 1)$ の楕円曲線族に適用可能な方式である．この方式では，従来のように hard part を分解し，各係数を求めるという方法を取らず，hard part を 2 変数多項式と考えて直接的に因数分解を与えることで，ヒューリスティックな手順を含まないアルゴリズムを実現する．またこの方式は，対応するすべての BLS 曲線に対して既存のアルゴリズムよりも効率的な新しいアルゴリズムを与える．なお二つ目の提案方式は，白勢らの方式 [25] 及び一つ目の提案方式よりも効率的である．

2 準備

この章では，本稿で用いる楕円曲線やペアリングの数学的な定義及び基本的な性質を述べる．

2.1 楕円曲線

有限体 $\mathbb{F}_p$ $(p > 3)$ 上の楕円曲線 $E/\mathbb{F}_p$ とは，$E/\mathbb{F}_p : y^2 = x^3 + ax + b$ で与えられ，係数 $a, b \in \mathbb{F}_p$ は $4a^3 + 27b^2 \neq 0$ を満たす．定義体が文脈から明らかな場合は単に，楕円曲線 E と書く．

整数 $t = p + 1 - \#E(\mathbb{F}_p)$ を E のトレースと呼び，$t \equiv 0 \bmod p$ であるとき，E を超特異楕円曲線，そうでないときを通常曲線と呼ぶ．E が通常曲線であるとき，CM (complex multiplication) 判別式 D とは，ある整数 V に対して，$DV^2 = 4p - t^2$ を満たす平方因子を持たない整数である．

整数 r を $r \mid \#E(\mathbb{F}_p)$ かつ $r^2 \nmid \#E(\mathbb{F}_p)$ を満たす素数とするとき，E の埋め込み次数 k とは，$r \mid (p^k - 1)$ を満たす最小の正整数のことである．CM 法により，5 つ組 (p, r, t, k, D) に対して，対応する楕円曲線 E を構成することができる．k や D が明らかな場合は単に 3 つ組 (p, r, t) と書くこともある．

2.2 楕円曲線族

上記の楕円曲線パラメータ t, r, p が変数を x とする $\mathbb{Q}$ 上の多項式 $t(x), r(x), p(x)$ でパラメータ付けすることができる楕円曲線族について解説する [11]．楕円曲線族の定義を述べる前に，いくつか用語の定義をする．多項式 $a(x) \in \mathbb{Q}[x]$ が素数表現を持つとは，定数でない先頭項係数が正の既約多項式であって，$a(n) \in \mathbb{Z}$ となる $n \in \mathbb{Z}$ が存在し，$\gcd(\{a(n) \mid n, a(n) \in \mathbb{Z}\}) = 1$ である．多項式 $a(x)$ が整値であるとは，任意の $n \in \mathbb{Z}$ に対して $a(n) \in \mathbb{Z}$ であることをいう．

定義 1 ([11])．$t(x), r(x), p(x) \in \mathbb{Q}[x]$ を 0 でない多項式とする．正整数 k と平方非剰余の正整数 D が与えられたとき，3 つ組 (t, r, p) が埋め込み次数 k，判別式 D の楕円曲線族をパラメータ付けするとは，次の条件が満たされるときを言う：

(1) $p(x)$ は素数表現を持つ．
(2) $r(x)$ は定数でない先頭項係数が正の既約多項式であって整値である．
(3) $r(x) \mid p(x) + 1 - t(x)$ が成立する．
(4) $r(x) \mid \Phi_k(t(x) - 1)$ が成立する．ここで，Φ_k は k 次円分多項式である．
(5) 方程式 $Dy^2 = 4p(x) - t(x)^2$ が無限個の整数解 (x, y) を持つ．

埋め込み次数 k と判別式 D，多項式 $t(x), r(x), p(x)$ を定めたとしても楕円曲線 E は一意に決定されない．あくまでそれらのパラメータは族を定めるにすぎず，暗号技術として利用する上で適切な楕円曲線をただ一つに決定するには $r(x), p(x)$ を同時に素数にするようなパラメータ $x = z_0$ が必要であることに注意されたい．

2.3 Barreto-Lynn-Scott 曲線

楕円曲線族の一つである Barreto-Lynn-Scott (BLS) 曲線（族）について解説する．BLS 曲線は Barreto ら [5] によって提案された楕円曲線族であり，18 で割れない任意の埋め込み次数 k に対して存在する [5, 11]．ここでは代表的な埋め込み次数の BLS 曲線を紹介する．

埋め込み次数が $k = 2^m 3$ $(m > 0)$ の BLS 曲線は次のようにパラメータ付けされる：

$$\begin{cases} t(x) = x + 1, \\ r(x) = \Phi_k(x), \\ p(x) = (x-1)^2 r(x)/3 + x. \end{cases}$$

ここで，Φ_k は k 次円分多項式である．

2.4 ペアリング

$E/\mathbb{F}_p$ を埋め込み次数 k の楕円曲線，r を $\#E(\mathbb{F}_p)$ の最大素因数，π_p を E のフロベニウス自己準同型写像とする．

定義 2. 楕円曲線 E の部分群

$$\mathbb{G}_1 := E[r] \cap \mathrm{Ker}(\pi_p - 1) = E(\mathbb{F}_p)[r],$$
$$\mathbb{G}_2 := E[r] \cap \mathrm{Ker}(\pi_p - [p]) \subset E(\mathbb{F}_{p^k})[r]$$

をそれぞれ，*base field* 部分群，*trace-zero* 部分群と呼ぶ．また，$\mathbb{F}_{p^k}^*$ の位数 r の部分群を $\mathbb{G}_T$ と書く．

E 上のペアリングとは写像 $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ (or $e : \mathbb{G}_2 \times \mathbb{G}_1 \to \mathbb{G}_T$) であって次の性質をもつものをいう．

双線形性: 任意の点 $P \in \mathbb{G}_1, Q \in \mathbb{G}_2$ と任意の数 $a \in \mathbb{Z}$ に対して，$e([a]P, Q) = e(P, [a]Q) = e(P, Q)^a$ が成立する．

非退化性: $e(P, Q) = 1$ であるための必要十分条件は $P = \mathcal{O}$ または $Q = \mathcal{O}$ である．

ここでは特に BLS 曲線上のペアリングについて述べる．BLS 曲線 E 上の Ate ペアリングは

$$e_{z_0} : \mathbb{G}_2 \times \mathbb{G}_1 \to \mathbb{G}_T, (Q, P) \mapsto f_{z_0,Q}(P)^{(p^k-1)/r}$$

で定義される双線形写像である．ここで，多項式 $p(x), r(x)$ に整数 z_0 を代入したものを p, r と書く．BLS 曲線の場合，Miller loop 部分が単純に Miller 関数 $f_{z_0,Q}$ のみで記述することができるため計算効率が良い．

3 最終べき

最終べきとは，Miller loop で得られた値を $(p^k - 1)/r$ べき乗する計算過程である．埋め込み次数の定義より，r は $\Phi_k(p)$ を割るので，最終べきのべき指数は

$$\frac{p^k - 1}{r} = \frac{p^k - 1}{\Phi_k(p)} \cdot \frac{\Phi_k(p)}{r}$$

と二つの因子に分解することができる．円分多項式の定義より，前半部分が整数になることは明らかである．この前半のべき乗を計算する部分を easy part，後半のべき乗を計算する部分を hard part と呼ぶ．easy part は p の線形和で書くことができ，p 乗，すなわちフロベニウス演算は一般に高速に処理することができるため，計算コストが小さい．一方，hard part の計算は高コストであるため，その効率化がこれまでに提案されてきた．

本章では，最終べき hard part 計算の従来方式を簡単に解説した後，本稿における最終べきの課題設定を解説する．

3.1 既存研究

最終べき計算は，べき指数を分解する過程とその分解を用いた効率的な計算手順回路を探索する過程に分けることができる．最終べき分解方式として，p 進展開方式 [19]，lattice-based 方式 [12]，特定の楕円曲線の多項式パラメータを利用した方式 [23] が知られている．以下では，それら方式を簡単に述べる．

3.1.1 p 進展開方式

p 進展開方式とは，最終べきの hard part を p 進展開によって分解する方式であり，アイデアとしてはもっとも単純である．べき指数 $d(x) = \Phi_k(p(x))/r(x)$ を p に関する多項式と考えて，p 進展開を施す：

$$d(x) = \sum_i \lambda_i(x) p(x)^i.$$

ただし，$\deg \lambda_i < \deg p$ である．

この展開は個々の楕円曲線パラメータに依存しているが，ヒューリスティックは存在せず，係数 λ_i は一意に決定される．次に，この分解を用いた効率的な計算手順回路に対しては，各係数 $\lambda_i(x)$ 同士の関係性をヒューリスティックに発見する必要がある．なお，計算手順回路の探索については係数同士の関係性を見出すことに加えて，addition-chain 方式を利用する文献 [2] も存在するが，p 進展開方式の本質は係数 λ_i の関係性を手作業で発見することにある．現在では，p 進展開方式が最も主流であり，数多くの曲線に対して，係数 $\lambda_i(x)$ 及びそれらの関係式が導出されている．

我々の一つ目の提案方式は，この p 進展開方式を任意の楕円曲線族に拡張したものであり，係数 $\lambda_i(x)$ 同士の関係性をヒューリスティックなしに記述する．

3.1.2 lattice-based 方式

最終べきのべき指数 $d(x)$ は，代わりに $d'(x) = a(x)d(x)$ を用いてもペアリングの性質を損なわない．ただし，多項式 $a(x)$ は $r(x)$ と互いに素である必要がある．このとき，lattice-based 方式とは，効率的な最終べき計算アルゴリズムを構成することができるべき指数 $d'(x)$ を発見する方式である．具体的な手順は次のとおりである．ま

ず，方程式

$$\begin{pmatrix} d(x) \\ xd(x) \\ \vdots \\ x^{\deg p-1} \end{pmatrix} = M' \left(\begin{pmatrix} 1 \\ p \\ \vdots \\ p^{\varphi(k)-1} \end{pmatrix} \bigotimes \begin{pmatrix} 1 \\ x \\ \vdots \\ x^{\deg p-1} \end{pmatrix} \right)$$

を満たす行列 $M' \in M_{\deg p,\varphi(k)\deg p}(\mathbb{Q})$ を求める．ここで，記号 $\bigotimes$ はクロネッカー積である．次に，得られた行列の要素が整数になるように各行に定数倍をかけて行列 $M \in M_{\deg p,\varphi(k)\deg p}(\mathbb{Z})$ を得る．次に，行列 M の基底を LLL アルゴリズムを用いて簡約化する．最後に，得られた最短ベクトルの小さなスカラー倍に対する線形和を全探索し，最終べき計算の addition-chain が小さくなるような $d'(x)$ を決定する．この探索はべき指数を分解する過程と計算手順回路を探索する手順を含んだヒューリスティックな操作であり，個々の楕円曲線に依存している．

なお，この方式によって得られる最終べき計算アルゴリズムが最適であるかどうかは知られていない．実際，[10] では BLS15 曲線に対して lattice-based 方式が適用されているが，p 進展開を検討した [25, 15] の方が効率的であることが報告されている．同様に，BLS21 曲線においても [22] で lattice-based 方式の最終べき計算アルゴリズムが提案されているが，p 進展開を検討した [24] の方が効率的である．

3.1.3 多項式パラメータを利用した方式

[23] では，BLS27 曲線の最終べきを楕円曲線の多項式パラメータを利用して計算している．BLS27 曲線の $r(x), p(x)$ は，

$$r(x) = \Phi_{27}(x)/3,\ p(x) = (x-1)^2 r(x) + x$$

で与えられる．この関係式を利用して，最終べきを次のように分解している:

$$d(x) = (x-1)^2(p^9+x^9+1)(p^8+xp^7+\cdots+x^7p+x^8)+3.$$

この方式は，p 進展開方式や lattice-based 方式と異なり，分解にヒューリスティックが存在しないが， [23] では BLS27 曲線に依存した形で述べられている．

我々の提案する 2 つ目の方式はこのアイデアに基づいている．第 5 章で，この方式が楕円曲線族にまで拡張可能であり，斉次円分多項式を用いて分解を記述できることを示す．

なお，[23] では述べられていないが，上記の等式の一部分はさらに，

$$p^8+xp^7+\cdots+x^7p+x^8 = (p^2+xp+x^2)(p^6+x^3p^3+p^6)$$

と分解することができ，こちらの方がより効率的な最終べき計算アルゴリズムを与える [15].

3.2 最終べきにおける課題

最終べきで計算するべき指数は，楕円曲線を固定したときに（一意ではないが）決定可能であり，最終べきは拡大体演算とべき乗の組み合わせで計算可能であるため，それらの算術回路で表現することができる．したがって，効率的に計算できる最終べきの算術回路を探索することが重要であり，そのような算術回路を発見するには結局のところ，hard part の分解を適切に与えることが本質である．

従来方式によって提案された最終べき計算アルゴリズムは，個々の楕円曲線に依存しており，分解過程もしくは計算手順回路探索過程において，アルゴリズムを効率的にするためのヒューリスティックな調整を行っている．そのため，新たな楕円曲線に対して効率的な最終べき計算アルゴリズムを得るためには，従来方式を利用してその曲線に特化したヒューリスティックな調整を行う必要がある．本稿では，そのような調整が無い方法を提案する．

4 提案方式 1

この章では，前章で述べた $p(x)$ 進展開を用いた最終べき分解方式を任意の楕円曲線族に拡張できることを示す．

E を楕円曲線族に属する楕円曲線とする．このとき，定義 1 における関係式を用いると，E に関する多項式パラメータ $p(x), r(x), t(x)$ は，次のような関係性を持つ：

$$\begin{cases} r(x) = \Phi_k(T(x))/h_2(x), \\ p(x) = h_1(x)r(x) + T(x), \\ t(x) = T(x) + 1. \end{cases} \tag{1}$$

ここで，$h_1(x), h_2(x), T(x) \in \mathbb{Q}[x]$ である．このとき，次の定理が成立する．

定理 3 ([15]). *k 次円分多項式 $\Phi_k(x)$ を $\Phi_k(x) = \sum_{i=0}^{d} c_i x^i \in \mathbb{Z}[x]$ とおく．このとき，*

$$\Phi_k(p(x))/r(x) = h_1(x)\left(\sum_{i=0}^{d-1} \lambda_i(x)p(x)^i\right) + h_2(x)$$

が成立する． ここで，

$$\begin{cases} \lambda_{d-1}(x) = c_d, \\ \lambda_i(x) = T(x)\lambda_{i+1}(x) + c_{i+1} \end{cases}$$

である．

証明 (概略). 円分多項式 $\Phi_k(x)$ に $p(x)$ を代入すると，

$$\Phi_k(p(x)) = \sum_{i=0}^{d} c_i p(x)^i \tag{2}$$

となる．定義 1 から，これは $r(x)$ で割れる．係数 λ_i は $T(x)$ 倍だけずれるが帰納的（漸化式的）に定義されてい

ることに注目する．多項式 $T(x), r(x), p(x)$ は式 (1) を満たすから，

$$p(x)^i = h_1(x)r(x)p(x)^{i-1} + T(x)p(x)^{i-1} \qquad (3)$$

が成立する．右辺の $p(x)$ の次数を落としていき，式 (2) と組み合わせる．式 (3) の後半部分から $r(x)$ を括り出すために，式 (1) を用いる．すなわち，

$$r(x)h_2(x) = \Phi_k(T(x)) = \sum_{i=0}^{d} c_i T(x)^i$$

を利用することで定理 3 を得る． □

Algorithm 1 は，定理 3 を適用した任意の楕円曲線族上の最終べきにおける hard part の計算アルゴリズムである．分数のべき乗の計算コストが大きいため，ステップ 1,2 では，多項式 $h_1, h_2 \in \mathbb{Q}[x]$ の係数の分母を払っている．その操作によりペアリングの値が変化するが，第 3.2 節で述べた通り，$\gcd(c, r) = 1$ であればペアリングの性質を損なわない．また，ステップ 5 では順次，T べき乗算を繰り返す．最終べき計算ではここのステップの計算量が最も大きい．BLS 曲線の場合，トレースの形が $t(x) = x + 1$ であるため，このステップは他の曲線族に比べて効率的になり，このアルゴリズムは特に BLS 曲線に適していると言ってよい．このことから，定理 3 は任意の BLS 曲線に対する効率的な最終べき計算アルゴリズムの存在を保証している．

Algorithm 1 最終べき hard part 計算アルゴリズム

Input: $E = (p(x), r(x), t(x), z_0)$，$f \in \mathbb{F}_{p^k}$

Output: $f^{c \cdot \frac{\Phi_k(p(z_0))}{r(z_0)}}$

1: Set $c = \mathrm{lcm}(c_1, c_2)$, where c_1, c_2 are smallest integers such that $c_1 h_1 \in \mathbb{Z}[x], c_2 h_2 \in \mathbb{Z}[x]$ and $\gcd(c, r) = 1$.
2: $h_1 \leftarrow ch_1, h_2 \leftarrow ch_2$
3: $f \leftarrow f^{h_1}, f' \leftarrow f^{h_2}, g_{d-1} \leftarrow f^{c_d}$
4: **for** $i = d - 1$ downto 1 **do**
5: $\quad g_{i-1} \leftarrow g_i^T \cdot f^{c_i}$
6: **end for**
7: **for** $i = 1$ to $d - 1$ **do**
8: $\quad f \leftarrow g_i^{p^i}$
9: **end for**
10: $f \leftarrow f \cdot f'$
11: **return** f

5 提案方式 2

前節では，任意の埋め込み次数を持つ楕円曲線族に対する最終べき分解の一般化を示した．本節では，埋め込み次数が $k = 2^m$, $k = 3^n$, $k = 2^m 3^n$ $(m, n \geq 1)$ である楕円曲線族に対する定理 3 よりも効率的な最終べき分解を与える．この方式は [23] における多項式パラメータを利用した方式の一般化といえる．

分解を記述するに際し，斉次円分多項式という新たな道具を導入する．

定義 4. 任意の正整数 n に対して，n 次斉次円分多項式 $\Psi_n(x, y)$ を

$$\Psi_n(x, y) := \begin{cases} y^{\varphi(n)}\Phi_n(x/y) & \text{if } n > 1, \\ 1 & \text{if } n = 1 \end{cases}$$

と定義する．ここで，φ はオイラー関数である．

斉次円分多項式を 2 変数多項式として定義したが，本稿では，$y = p$ と固定して，1 変数多項式として扱う．斉次円分多項式の性質として，次の補題は重要である．

補題 5. m を 2 以上の整数とする．このとき，多項式 $x^{m-1} + px^{m-2} + \cdots + p^{m-2}x + p^{m-1}$ は斉次円分多項式の積で表すことができる：

$$\sum_{j=0}^{m-1} p^j x^{m-1-j} = \prod_{i|m} \Psi_i(x, p).$$

証明. この補題は円分多項式の性質 $x^m - 1 = \prod_{i|m} \Phi_i(x)$ とオイラー関数の性質 $\sum_{i|n} \varphi(i) = n$ から容易に導かれる．実際，

$$x^{m-1} + x^{m-2} + \cdots + x^2 + x + 1 = \prod_{\substack{i|m \\ i \neq 1}} \Phi_i(x)$$

が成立するので，$x = x/p$ を代入し，両辺に p^{m-1} を掛けると，

$$x^{m-1} + px^{m-2} + \cdots + p^{m-1} = p^{m-1} \prod_{\substack{i|m \\ i \neq 1}} \Phi_i(x/p)$$

が成立する．斉次円分多項式の定義及びオイラー関数の性質より，補題 5 を得る． □

さて，楕円曲線 E が楕円曲線族に属するとき，その多項式パラメータは式 (1) を満たすので，任意の正整数 i に対して，

$$p^i = h_1 r p^{i-1} + T p^{i-1}$$

が成立していることに注意されたい．この関係式を利用して，最終べきの分解を導出する．

次数が $k = 2^m$ であるとき，k 次円分多項式は $\Phi_k(x) = x^{k/2} + 1$ と表すことができるので，

$$\begin{aligned} \Phi_k(p) &= p^{k/2} + 1 \\ &= h_1 r(T^{k/2-1} + pT^{k/2-2} + \cdots + p^{k/2-2}T + p^{k/2-1}) \\ &\quad + T^{k/2} + 1 \\ &= h_1 r(T^{k/2-1} + pT^{k/2-2} + \cdots + p^{k/2-2}T + p^{k/2-1}) \\ &\quad + h_2 r \end{aligned}$$

である．この式に補題 5 を適用すると次の定理を得る．

定理 6. 正整数 m に対して，楕円曲線 E が埋め込み次数 $k = 2^m$ の楕円曲線族に属するとき，E 上のペアリングに対する最終べきの *hard part* は次のように分解することができる：

$$\frac{\Phi_k(p)}{r} = h_1 \left(\prod_{i|(k/2)} \Psi_i(T,p) \right) + h_2.$$

ここで，多項式 h_1, h_2, T は式 *(1)* を満たしている．

これらの議論は埋め込み次数が $k = 3^m$, $k = 2^m 3^n$ であっても同様に成立する．ここでは結果のみ述べる．

定理 7. 正整数 m に対して，楕円曲線 E が埋め込み次数 $k = 3^m$ の楕円曲線族に属するとき，E 上のペアリングに対する最終べきの *hard part* は次のように分解することができる：

$$\frac{\Phi_k(p)}{r} = h_1 \left(\prod_{i|(k/3)} \Psi_i(T,p) \right) (T^{k/3} + p^{k/3} + 1) + h_2.$$

ここで，多項式 h_1, h_2, T は式 *(1)* を満たしている．

定理 8. 正整数 m, n に対して，楕円曲線 E が埋め込み次数 $k = 2^m 3^n$ の楕円曲線族に属するとき，E 上のペアリングに対する最終べきの *hard part* は次のように分解することができる：

$$\frac{\Phi_k(p)}{r} = h_1 \left(\prod_{i|(k/6)} \Psi_i(T,p) \right) (T^{k/6} + p^{k/6} - 1) + h_2.$$

ここで，多項式 h_1, h_2, T は式 *(1)* を満たしている．

定理 6, 7, 8 は，先行研究のように係数 $\lambda_i(x)$ を求めずに hard part を斉次円分多項式を用いて直接，分解している．したがってその計算過程にヒューリスティックを含まず，非常にシンプルな計算過程で最終べきを計算することができる．Algorithm 2 は，埋め込み次数 $k = 2^m 3^n$ の曲線に対する最終べき計算アルゴリズムである．

提案方式 1 と同様の理由により，これら定理も特に BLS 曲線に対して効率的なアルゴリズムを与える．さらに提案方式 1 による最終べき計算よりも提案方式 2 の方が効率的である．

6 応用

この節では，本研究で提案する最終べき計算アルゴリズムを BLS12 曲線に適用し，先行研究との計算量を比較する．計算量比較は素体 $\mathbb{F}_p$ 上の乗算回数をカウントすることで行う．M_k, S_k, I_k, F_n, E_x をそれぞれ $\mathbb{F}_{p^k}$ 上の乗算コスト，2 乗算コスト，逆元算コスト，n フロベニウス乗算コスト，x べき乗算コストとし，I_{cyc} を円分部分群 $\mathbb{G}_{\Phi_k}$ における逆元算コストとする．本研究では簡単のため，加算コストは無視し，$M_2 = 3M_1, M_3 = 6M_1, M_5 = 9M_1$ [18, 9] を用いて拡大体の乗算コストを素体上の乗算コストへと還元する．

Algorithm 2 埋め込み次数 $k = 2^m 3^n$ の最終べき hard part 計算アルゴリズム

Input: $E = (p(x), r(x), t(x), z_0)$, $f \in \mathbb{F}_{p^k}$
Output: $f^{c \cdot \frac{\Phi_k(p(z_0))}{r(z_0)}}$

1: Set $c = \mathrm{lcm}(c_1, c_2)$, where c_1, c_2 are smallest integers such that $c_1 h_1 \in \mathbb{Z}[x], c_2 h_2 \in \mathbb{Z}[x]$ and $\gcd(c, r) = 1$.
2: $h_1 \leftarrow c h_1, h_2 \leftarrow c h_2$
3: $f \leftarrow f^{h_1}, f' \leftarrow f^{h_2}$
4: $f \leftarrow f^{T^{2^{m-1}3^{n-1}}} \cdot f^{p^{2^{m-1}3^{n-1}}} \cdot f^{-1}$
5: $i \leftarrow 2^{m-1}3^{n-1}$
6: **while** $i > 1$ **do**
7: **if** $i \equiv 0 \mod 2$ **then**
8: $f \leftarrow f^{\Psi_i(T,p)}$
9: $i \leftarrow i/2$
10: **end if**
11: **if** $i \equiv 0 \mod 3$ **then**
12: $f \leftarrow f^{\Psi_i(T,p)}$
13: $i \leftarrow i/3$
14: **end if**
15: **end while**
16: $f \leftarrow f \cdot f'$
17: **return** f

6.1 BLS12 曲線

BLS12 曲線の多項式パラメータは，

$$\begin{cases} r(x) = \Phi_{12}(x), \\ p(x) = (x-1)^2 r(x)/3 + x, \\ t(x) = x + 1 \end{cases}$$

で与えられる．最終べきのべき指数は

$$\frac{p^{12}-1}{r} = (p^6 - 1)(p^2 + 1) \cdot \frac{\Phi_{12}(p)}{r}$$

である．BLS12 曲線上の最終べき計算は p 進展開方式と addition-chain 方式の組み合わせにより，[3, 2, 21] などで議論されている．hard part $d = \Phi_{12}(p)/r$ を $\sum \lambda_i(x) p(x)^i$ とおく．[3, 2, 21] によると係数 $\lambda_i(x)$ は，

$$\begin{cases} \lambda_0(x) = x^5 - 2x^4 + 2x^2 - x + 3, \\ \lambda_1(x) = x^4 - 2x^3 + 2x - 1, \\ \lambda_2(x) = x^3 - 2x^2 + x, \\ \lambda_3(x) = x^2 - 2x + 1 \end{cases}$$

である．f^d を計算するために，addition-chain 方式を利用してまず $f^{x^5-2x^4+2x^2}$ を次のように計算していく：

$$f \to f^{-2} \to f^x \to f^{2x} \to f^{x-2} \to f^{x^2-2x} \to f^{x^3-2x^2} \to f^{x^4-2x^3} \to f^{x^4-2x^3+2x} \to f^{x^5-2x^4+2x^2}.$$

この計算結果を用いると，f^d は次のように計算できる．

$$\begin{aligned} f^d =& f^{x^5-2x^4+2x^2} \cdot (f^{x-2})^{-1} \cdot f \cdot (f^{x^4-2x^3+2x} \cdot f^{-1})^p \\ & \cdot (f^{x^3-2x^2} \cdot f^x)^{p^2} \cdot (f^{x^2-2x} \cdot f)^{p^3}. \end{aligned}$$

この計算手順における最終べきの計算量は

$$I_{12} + 1135M_1 + 28890S_1 \tag{4}$$

である．詳細な計算量評価については [2] を参照されたい．

次に，提案方式 2 における定理 8 を用いて BLS12 曲線の最終べき計算アルゴリズムを与える．式 (1) における多項式 h_1, h_2, T は

$$\begin{cases} h_1(x) = (x-1)^2/3 \\ h_2(x) = 1 \\ T(x) = x \end{cases}$$

であるので，Algorithm 2 のステップ 1,2 で $c = 3$ となるため，hard part を $3 \cdot \Phi_{12}(p)/r$ として分解する．定理 8 を用いると，

$$\begin{aligned} 3 \cdot \frac{\Phi_{12}(p(x))}{r(x)} &= (x-1)^2 \cdot \Psi_1(x,p)\Psi_2(x,p) \cdot (x^2+p^2 \\ &\quad -1)+3 \\ &= (x-1)^2 \cdot (x+p) \cdot (x^2+p^2-1)+3 \end{aligned}$$

を得ることができる．この分解に対して，Algorithm 2 を適用しても十分高速な計算が可能であるが，パラメータによってはさらに最適化することができる．

パラメータ x のビット長を n，ハミング重みを w とすると，通常 E_{x-1} の計算コストは $(n-1)S_k + (w-1)M_k$ である．x が偶数であるとき，$x-1$ べき乗算をする代わりに，$x/2$ べき乗算を組み合わせることでさらに効率的に計算できることが報告されている [13]．$f^{(x-1)^2}$ を

$$f \to f^{2x} \to (f^{2x})^{x/2}$$

と計算する．なお，ここで f^2 が必要であるが，それは Algorithm 2 のステップ 3 で計算済みである．したがって，この場合の該当箇所の計算量は $(n-2)S_k + (w-1)M_k$ となる．一方，パラメータ x が奇数であるときでも，Algorithm 2 はさらに改良することができる．具体的には，Algorithm 2 のステップ 4 を最適化することができる．$f^{x^2+p^2-1}$ を計算するには通常，

$$2E_x + M_k + F_2 = 2(n-1)S_k + (2w-1)M_k + F_2$$

の計算が必要である．ところが，$x^2+p^2-1 = (x-1)(x+1)+p^2$ と変形することで，

$$E_{x-1} + E_{x+1} + M_k + F_2 = 2(n-1)S_k + (2w-2)M_k + F_2$$

とできるので乗算計算を 1 回減らすことができる．さらに，パラメータ x が $x = \cdots \pm 2 \pm 1$ という形をしている場合は，乗算回数を最大 3 回削減することができる．

ここでは，計算量評価に必要となるパラメータは公平を期すために [2] で採用されている $x = -2^{107} + 2^{84} + 2^{19}$ を適用する．このとき，最終べきの計算量は，

$$\begin{aligned} & (I_{12} + F_2 + 2M_{12}) + (4E_x + E_{x/2} + 7M_{12} + S_{12} + F_1 \\ & \quad + F_2) \\ =& I_{12} + 19M_{12} + 535S_{12} + F_1 + 2F_2 \\ =& I_{12} + 1066M_1 + 28890S_1 \end{aligned}$$

である．従来法による最終べきの計算量 (4) に比べて，乗算回数を 69 回削減できている．

7 結論

本論文では，任意の楕円曲線族に適用可能な，ヒューリスティックが存在しない効率的な最終べき計算アルゴリズムを二つ提案した．一つ目は，円分多項式の構造を利用した，任意の埋め込み次数に適用可能な，p 進展開方式を一般化した最終べき計算アルゴリズムである．この方式により，全ての BLS 曲線に対して効率的な最終べき計算アルゴリズムの存在が保証される．二つ目は，斉次円分多項式を利用した，埋め込み次数が $2^m, 3^n, 2^m3^n$ $(m, n \geq 1)$ の楕円曲線族に適用可能な方式である．この方式により，対応する全ての BLS 曲線に対して既存のアルゴリズムよりも効率的な計算アルゴリズムを与える．

8 謝辞

本研究（の一部）は，内閣府が進める戦略的イノベーション創造プログラム（SIP）「IoT 社会に対応したサイバー・フィジカル・セキュリティ」（JPNP18015）（管理法人：NEDO）によって実施されたものである。

参考文献

[1] Aranha, D.F., Barreto, P.S.L.M., Longa, P., Ricardini, J.E.: The realm of the pairings. In: SAC 2013 Proceedings. pp. 3–25 (2013)

[2] Aranha, D.F., Fuentes-Castañeda, L., Knapp, E., Menezes, A., Rodríguez-Henríquez, F.: Implementing pairings at the 192-bit security level. In: Pairing 2012 Proceedings. pp. 177–195 (2012)

[3] Aranha, D.F., Karabina, K., Longa, P., Gebotys, C.H., Hernandez, J.L.: Faster explicit formulas for computing pairings over ordinary curves. In: EUROCRYPT 2011 Proceedings. pp. 48–68 (2011)

[4] Barbulescu, R., El Mrabet, N., Ghammam, L.: A taxonomy of pairings, their security, their complexity. Cryptol. ePrint Arch. Report 2019/485 (2019)

[5] Barreto, P.S.L.M., Lynn, B., Scott, M.: Constructing elliptic curves with prescribed embedding degrees. In: SCN 2002 Proceedings. pp. 257–267 (2002)

[6] Benger, N.: Cryptographic pairings: Efficiency and DLP security. Dublin City Univ. Ph.D.thesis (2010)

[7] Boneh, D., Franklin, M.K.: Identity-based encryption from the weil pairing. In: Advances in Cryptology - CRYPTO 2001 Proceedings. LNCS, vol. 2139, pp. 213–229. Springer (2001)

[8] Boneh, D., Lynn, B., Shacham, H.: Short signatures from the weil pairing. J. Cryptol. **17**(4), 297–319 (2004)

[9] El Mrabet, N., Guillevic, A., Ionica, S.: Efficient multiplication in finite field extensions of degree 5. In: AFRICACRYPT 2011 Proceedings. pp. 188–205 (2011)

[10] Fouotsa, E., El Mrabet, N., Pecha, A.: Computing optimal ate pairings on elliptic curves with embedding degree $9, 15$ and 27. Cryptology ePrint Archive, Report 2016/1187 (2016)

[11] Freeman, D., Scott, M., Teske, E.: A taxonomy of pairing-friendly elliptic curves. J. Cryptology **23**(2), 224–280 (2010)

[12] Fuentes-Castañeda, L., Knapp, E., Rodríguez-Henríquez, F.: Faster hashing to $\mathbb{G}_2$. In: SAC 2011 Proceedings. pp. 412–430 (2011)

[13] Ghammam, L., Fouotsa, E.: Improving the computation of the optimal ate pairing for a high security level. J. Appl. Math. Comput. **59**, 21–36 (2019)

[14] Guillevic, A.: A short-list of pairing-friendly curves resistant to special TNFS at the 128-bit security level. In: PKC 2020 Proceedings Part II. pp. 535–564 (2020)

[15] Hayashida, D., Hayasaka, K., Teruya, T.: Efficient final exponentiation via cyclotomic structure for pairings over families of elliptic curves. IACR Cryptol. ePrint Arch. **2020**, 875 (2020)

[16] Kim, T., Barbulescu, R.: Extended tower number field sieve: A new complexity for the medium prime case. In: CRYPTO 2016 Proceedings Part I. pp. 543–571 (2016)

[17] Kim, T., Jeong, J.: Extended tower number field sieve with application to finite fields of arbitrary composite extension degree. In: PKC 2017 Proceedings Part I. pp. 388–408 (2017)

[18] Knuth, D.E.: The art of computer programming, Volume II: Seminumerical Algorithms. Addison-Wesley, 3rd edn. (1998)

[19] Mbang, N.B., Aranha, D., Fouotsa, E.: Computing the optimal ate pairing over elliptic curves with embedding degrees 54 and 48 at the 256-bit security level. IJACT **4**(1), 45–59 (2020)

[20] Okamoto, T., Takashima, K.: Fully secure functional encryption with general relations from the decisional linear assumption. In: CRYPTO 2010 Proceedings. LNCS, vol. 6223, pp. 191–208. Springer (2010)

[21] Scott, M., Benger, N., Charlemagne, M., Perez, L.J.D., Kachisa, E.J.: On the final exponentiation for calculating pairings on ordinary elliptic curves. In: Pairing 2009 Proceedings. pp. 78–88 (2009)

[22] Toure, M.A., Samake, K., Traore, S.: Optimal ate pairing on elliptic curves with embedding degree 21. IJSR (2018)

[23] Zhang, X., Lin, D.: Analysis of optimum pairing products at high security levels. In: INDOCRYPT 2012 Proceedings. pp. 412–430 (2012)

[24] 林田大輝, 早坂健一郎: BLS-21 曲線を用いた効率的なペアリング計算. 2020 Symposium on Cryptography and Infomation Security (2020)

[25] 白勢政明, 南條由紀: 任意の BLS 曲線の最終べきの hard part について. IEICE Technical Report, ISEC2020-30 (2020)