KSS曲線を用いた効率的なペアリング暗号のための18次拡大体構成法の評価

南條 由紀[1]　カンダカル エムディ アルアミン [1]　日下 卓也[1]　野上 保之[1]

概要：近年，ID ベース暗号やグループ署名などの新たな暗号プロトコルが提案されており，それらの実用化に向けて，ペアリング暗号の高速化や計算コスト低減に関する研究が行われている．そこで本稿では，Kachisa-Schaefer-Scott (KSS) 曲線を用いたペアリングを効率的に行うために，そのベースの計算処理となる 18 次拡大体の構成法に着目する．具体的には，3 次拡大体を構成する法多項式に位数 7 の円周等分多項式を用いる新たな 18 次拡大体構成法を提案する．この構成による 18 次拡大体では，3 次拡大体の演算に，効率的な演算手法である，Cyclic Vector Multiplication Algorithm (CVMA) を適用することができる．提案手法の 18 次拡大体を用いてペアリングの実装を行い，評価を行ったところ，特定のパラメータの条件における Miller のアルゴリズムと，$\mathbb{G}_2$，$\mathbb{G}_3$ 上での処理を効率的に行うことができると分かった．

キーワード：ペアリング暗号, Kachisa-Schaefer-Scott (KSS) 曲線, 拡大体構成法

A Study on a Construction Method of Degree 18 Extension Field for Efficient Pairing over KSS Curves

Yuki Nanjo[1]　Md. Al-Amin Khandaker[1]　Takuya Kusaka[1]　Yasuyuki Nogami[1]

Abstract: In recent years, several innovative cryptosystems based on pairing, e.g. ID-based encryption, Group signature, have been proposed. However, pairing requires complex computations. Therefore, finding out efficient techniques is important for the practical implementation of pairing. This paper tries to optimize the pairing by focusing extension field arithmetic, which is basic operations of the pairing. An extension field of degree 18 for the pairing over Kachisa-Schaefer-Scott curves is constructed by using a cyclotomic polynomial of order 7 as a modular polynomial. To employ Cyclic Vector Multiplication Algorithm, which is available in the extension field of degree 3, an efficient Miller's algorithm can be implemented by using the proposed extension field under the specific conditions. Efficient computations on $\mathbb{G}_2$ and $\mathbb{G}_3$ can also be achieved with the proposed towering.

Keywords: Pairing-Based Cryptography, Kachisa-Schaefer-Scott (KSS) Curve, Construction Method of Extension Field.

1. 序論

ペアリング暗号方式 [15,27] は，ID ベース暗号 [9]，検索可能暗号 [8]，属性ベース暗号 [26] などの高機能暗号を実現する次世代の暗号方式として注目されている．ペアリングは，二つの楕円曲線上の有理点群 $\mathbb{G}_1$，$\mathbb{G}_2$ から，拡大体上 $\mathbb{F}_{p^k}$ の乗法群 $\mathbb{G}_3$ への双線形性写像である．ペアリングに用いられる楕円曲線は，ペアリング親和曲線と呼ばれており，Barreto-Naehrig (BN) 曲線 [6]，Barreto-Lynn-Scott (BLS) 曲線 [5]，Kachisa-Schaefer-Scott (KSS) 曲線 [16] などが提案されている．本稿ではとくに，KSS 曲線を用いたペアリングについて議論する．

ペアリングを暗号プロトコルへ応用するためには，実用的な実行速度が求められるが，多くの場合ペアリングは，

[1] 岡山大学大学院自然科学研究科
Graduate school of natural science and technology, Okayama University, Japan

RSA 暗号 [25] や楕円曲線暗号 [22,24] よりも多くの計算量を要する．これに加えて，2016 年に新たな離散対数問題の解法アルゴリズム (exTNFS) [21] が提案されたことにより，ペアリングに用いられる拡大体の標数の bit 長が更新された．[4] によると，KSS 曲線を用いたペアリングにおいて，192-bit セキュリティレベルを担保するためには，少なくとも 676-bit の大きさの素数を用いることが推奨されている．このため，ペアリングを暗号プロトコルに応用するためには，計算量を減らすためのアルゴリズムや，効率的な実装手法が必要とされる．

ペアリングでは主に，Miller のアルゴリズム，最終べき，$\mathbb{G}_1$，$\mathbb{G}_2$ 上でのスカラー倍算，$\mathbb{G}_3$ 上でのべき乗算などの処理が行われる．KSS 曲線を用いたペアリングでは，これらの処理の効率化手法として，Ate [10]，Optimal-ate ペアリング [29] や，最終べきの効率的なアルゴリズム [2] が提案されている．また，$\mathbb{G}_1$，$\mathbb{G}_2$，$\mathbb{G}_3$ 上での計算処理では，GLV 法 [12] を用いて計算量を削減することができる [19]．こういった処理そのものの効率化手法ももちろん重要であるが，これらの処理では拡大体上での演算をベースとしているため，拡大体上の計算効率についても考慮する必要がある．このため，本研究では，拡大体の計算効率を決定づける，拡大体構成法に着目し，ペアリングの効率化を図る．

本研究の先行研究として，Aranha らによる 192-bit セキュリティにおけるペアリングの実装 [2] があげられる．[2] では，BN 曲線，BLS 曲線，KSS 曲線を用いたペアリングに関して，Optimal Extension Field (OEF) [3] を用いた拡大体構成法が提案されており，それを用いたペアリングの実装手法を提案している．本研究では，OEF による拡大体構成よりも高速な演算の実現を模索するため，本研究では部分体の計算効率の改善に着目する．

まず，(i) OEF による拡大体構成法 (Type-I) [3] とは異なる，新たな 18 次拡大体構成法 (Type-II) を提案する．提案手法の 3 次拡大体の法多項式には，位数 7 の円周等分多項式を用いており，3 次拡大体の演算には，Cyclic Vector Multiplication Algorithm (CVMA) [18] を用いることができる．さらに，(ii) Type-I，Type-II の拡大体を構成するためのパラメータの条件を明らかにする．(iii) このパラメータの条件と，KSS 曲線・ツイスト曲線の関係に関する実験結果に基づき，現在の 192-bit セキュリティレベルを担保できる，Type-I，Type-II をそれぞれ構成可能なサンプルパラメータを示す．(iv) Type-I，Type-II を用いたペアリングの実装について，予備実験よりそれぞれのペアリング処理における計算効率を考察する．最後に，(v) サンプルパラメータを用いた実装により，提案する Type-II のペアリングの性能評価を行う．

OEF による Type-I の実装と比較した結果，提案手法の Type-II を用いた実装では，特定のパラメータを用いた Miller のアルゴリズム，$\mathbb{G}_2$ 上におけるスカラー倍算，$\mathbb{G}_3$ 上におけるべき乗算に関して，効率的に計算処理を行うことができることが分かった．また，Miller のアルゴリズムにはパラメータの条件によって効率性が異なってくることも分かったため，効率的な実装を考える際には，パラメータの選び方も考慮する必要があることがわかった．

2. 準備

本節では，ペアリングの基礎となる，KSS 曲線，拡大体，ペアリングとその効率化手法について詳細を示す．

2.1 KSS 曲線

本研究に用いるペアリング親和曲線は，非超特異楕円曲線（通常楕円曲線）である Kachisa-Schaefer-Scott (KSS) 曲線 [16] である．KSS 曲線の埋め込み次数は $k = 16, 18, 38$ などが知られているが，本稿では $k = 18$ の場合について議論する．素数 p に対し，$\mathbb{F}_p$ を素体とする．KSS 曲線は，$E/\mathbb{F}_p : y^2 = x^3 + b$ により定義される．KSS 曲線における標数 p, 位数 r, Frobenius トレース t は $p = p(\chi)$, $r = r(\chi)$, $t = t(\chi)$ として，整数 χ を変数とする，以下の多項式により与えられる．

$$p(\chi) = (\chi^8 + 5\chi^7 + 7\chi^6 + 37\chi^5 + 188\chi^4 + 259\chi^3 + 343\chi^2 + 1763\chi + 2401)/21, \tag{1a}$$

$$r(\chi) = (\chi^6 + 37\chi^3 + 343)/343, \tag{1b}$$

$$t(\chi) = (\chi^4 + 16\chi + 7)/7. \tag{1c}$$

以降では，KSS 曲線に用いられる素数 $p(\chi)$ を KSS 素数，χ を KSS パラメータと呼ぶ．ただし，$p(\chi)$, $r(\chi)$ が素数となるためには，KSS パラメータは少なくとも $\chi \equiv 14 \pmod{42}$ を満たす必要がある．簡単のため，正規化 KSS パラメータ $\chi_0 = (\chi - 14)/42 \in \mathbb{Z}$ を定義する．

2.2 拡大体

以降では，拡大次数 k の拡大体を $\mathbb{F}_{p^k}$ と表す．また，$\mathbb{F}_{p^k}$ が $\mathbb{F}_p$ 上の法多項式 $f(x)$ により構成され，その根が ζ であるとき，$\mathbb{F}_{p^k}$ の構成を $\mathbb{F}_{p^k} = \mathbb{F}_p[\zeta]/f(\zeta)$ のように表現する．k が合成数の場合，逐次拡大体構成法 [7] を用いて，効率的に体を拡大することができ，多くのペアリングの実装において，この手法が用いられている．逐次拡大体構成法を用いると，18 次拡大体 $\mathbb{F}_{p^{18}}$ は，$\mathbb{F}_{((p^3)^3)^2}$ のように構成できる．

$$\begin{cases} \mathbb{F}_{p^3} &= \mathbb{F}_p[\zeta_1]/f_1(\zeta_1), \\ \mathbb{F}_{p^9} &= \mathbb{F}_{p^3}[\zeta_2]/f_2(\zeta_2), \\ \mathbb{F}_{p^{18}} &= \mathbb{F}_{p^9}[\zeta_3]/f_3(\zeta_3). \end{cases} \tag{2}$$

法多項式 $f_1(x), f_2(x), f_3(x)$ は，拡大体上の演算の計算効率を決定づけるため，その選び方はとくに重要である．

なお，Aranha らによる先行研究 [2] では，$\mathbb{F}_{p^{18}}$ を $\mathbb{F}_{((p^3)^2)^3}$

のように構成しているが，本研究では $\mathbb{F}_{((p^3)^3)^2}$ の構成を採用することに注意いただきたい．これについては，Cyclotomic Squaring [13] を適用することを考慮したためである (第 2.3.2 参照).

2.3 ペアリング

本研究で着目するペアリングは，位数 r の 2 つの有理点群 $\mathbb{G}_1$，$\mathbb{G}_2$ を用いて，拡大体上の位数 r の乗法群 $\mathbb{G}_3$ への写像であり，$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_3$ のように表される．KSS 曲線上における Optimal-ate ペアリング [29] では，$\mathbb{G}_1$，$\mathbb{G}_2$，$\mathbb{G}_3$ はそれぞれ，$\mathbb{G}_1 = E(\mathbb{F}_{p^{18}})[r] \cap \mathrm{Ker}(\phi_p - [1])$，$\mathbb{G}_2 = E(\mathbb{F}_{p^{18}})[r] \cap \mathrm{Ker}(\phi_p - [p])$，$\mathbb{G}_3 = \mathbb{F}^*_{p^{18}}/(\mathbb{F}^*_{p^{18}})^r$ により定義される．ただし，$E(\mathbb{F}_{p^{18}})[r]$ は定義体を $\mathbb{F}_{p^{18}}$ とする KSS 曲線の位数 r の有理点の集合，$\mathrm{Ker}(\cdot)$ は写像 $(\cdot)$ により，無限遠点 $\mathcal{O}$ に写像される有理点の集合を意味している．また，ϕ_p は有理点に対する Frobenius 写像であり，$\phi_p : (x, y) \mapsto (x^p, y^p)$ により与えられる．ここで，P，Q をそれぞれ $\mathbb{G}_1$，$\mathbb{G}_2$ 上の有理点とすれば，Optimal-ate ペアリング e_{opt} は以下のように与えられる．

$$e_{opt} : (Q, P) \to \left(f_{\chi,Q}(P) \cdot f^p_{3,Q}(P) \cdot l_{[\chi]Q,[3p]Q}(P)\right)^{(p^{18}-1)/r}.$$

ここで，$f_{\chi,Q}(P)$，$f_{3,Q}(P)$ は Miller のアルゴリズム，$l_{[\chi]Q,[3p]Q}(P)$ は Line 計算を表している．また，$(p^{18}-1)/r$ によるべき乗算は，最終べきと呼ばれている．

2.3.1 Miller のアルゴリズムの効率化手法

KSS 曲線を用いたペアリングでは，6 次ツイスト写像を用いた 11-sparse 乗算や擬似 12-sparse 乗算による効率化手法が提案されている [20]．以降では，$P(x_P, y_P)$ を $\mathbb{G}_1$ 上の有理点とし，$Q(x_Q, y_Q)$，$T(x_T, y_T)$ を $\mathbb{G}_2$ 上の有理点として，それぞれの手法の詳細を示す．

6 次ツイスト: Optimal-ate ペアリングに用いられる $\mathbb{G}_2$ 上の有理点の座標ベクトルは，$\mathbb{F}_{p^{18}}$ 上の元であるが，3 次拡大体 $\mathbb{F}_{p^3}$ 分の情報量しかもたない．このため，$Q, T \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{18}})$ に対して，真部分体を定義体とする楕円曲線上の有理点 $Q', T' \in \mathbb{G}'_2 \subset E'(\mathbb{F}_{p^3})$ へ写像を行うことを考える．このとき，E' は 6 次ツイスト曲線，この写像は 6 次ツイスト写像と呼ばれ，以下のように定義される．

$$\psi_6 : E'(\mathbb{F}_{p^3}) : y^2 = x^3 + bz \to E(\mathbb{F}_{p^{18}}) : y^2 = x^3 + b,$$
$$(x, y) \to (z^{-1/3}x, z^{-1/2}y).$$

ただし，z は $\mathbb{F}_{p^3}$ 上で平方非剰余かつ立方非常余元である．これより, Q, T は, ツイスト曲線上の有理点 $Q'(x_{Q'}, y_{Q'}) = (z^{-1/3}x_{Q'}, z^{-1/2}y_{Q'})$, $T'(x_{T'}, y_{T'}) = (z^{-1/3}x_{T'}, z^{-1/2}y_{T'})$ として扱うことができる．

11-sparse 乗算: T'，Q' の楕円加算 (ECA) の結果を $T' + Q' = R'(x_{R'}, y_{R'})$ とすれば，Miller のアルゴリズムの Line 計算と ECA は，変数 $A, B, C, D, E \in \mathbb{F}_{p^3}$ を用いて，以下のように計算される．

$$A = \frac{1}{x_{Q'} - x_{T'}}, B = y_{Q'} - y_{T'}, C = AB, D = x_{T'} + x_{Q'},$$
$$x_{R'} = C^2 - D, E = Cx_{T'} - y_{T'}, y_{R'} = E - Cx_{R'},$$
$$l_{T',Q'}(P) = y_P - z^{-1/6}Cx_P + z^{-1/2}E. \quad (3)$$

ただし，z は $\mathbb{F}_{p^3}$ 上で平方非常余かつ立方非常余元である．式 (3) による Line 計算のベクトルは，11 個のゼロ元と 7 個の非ゼロ元により表される．この形式の Line 計算による 18 次拡大体上の乗算は，11-sprase 乗算と呼ばれる．

擬似 12-sparse 乗算: 式 (3) の両辺に y_P^{-1} を乗じれば，$y_P^{-1}l_{T',Q'}(P) = 1 - z^{-1/6}Cy_P^{-1}x_P + z^{-1/2}Ey_P^{-1}$ が得られ，1 つの非ゼロ元が 1 となり，さらなる効率化を図ることができる．y_P^{-1} による乗算コストを抑えるため，P，Q'，T' について，$\hat{z} = (x_P y_P^{-1})^6 \in \mathbb{F}_p$ を用いた，以下により与えられる同型写像を適用する．

$$\hat{\psi}_1 : \hat{E}(\mathbb{F}_p) : y^2 = x^3 + b\hat{z} \to E(\mathbb{F}_p) : y^2 = x^3 + b,$$
$$(x, y) \mapsto (\hat{z}^{-1/3}x, \hat{z}^{-1/2}y),$$
$$\hat{\psi}'_1 : \hat{E}'(\mathbb{F}_{p^3}) : y^2 = x^3 + bz\hat{z} \to E'(\mathbb{F}_{p^3}) : y^2 = x^3 + bz,$$
$$(x, y) \mapsto (\hat{z}^{-1/3}x, \hat{z}^{-1/2}y).$$

これより，P は，$\hat{P}(x_{\hat{P}}, y_{\hat{P}}) = (x_P^3 y_P^{-2}, x_P^3 y_P^{-2})$，$Q$，$T$ はそれぞれ，$\hat{Q}'(x_{\hat{Q}'}, y_{\hat{Q}'}) = (x_P^2 y_P^{-2} x_{Q'}, x_P^3 y_P^{-3} y_{Q'})$，$\hat{T}'(x_{\hat{T}'}, y_{\hat{T}'}) = (x_P^2 y_P^{-2} x_{T'}, x_P^3 y_P^{-3} y_{T'})$ へ写像が行われる．これらの有理点を用いれば，$y_P^{-1}x_P$ は 1 となり，y_P^{-1} による乗算コストを抑えることができる．これらの有理点を用いた Line 計算を $y_P^{-1}l_{T',Q'}(P) = \hat{l}_{\hat{T}',\hat{Q}'}(\hat{P})$ とすれば，以下のように計算される．

$$\hat{l}_{\hat{T}',\hat{Q}'}(\hat{P}) = 1 - z^{-1/6}C + z^{-1/2}Ey_{\hat{P}}^{-1}. \quad (4)$$

式 (4) による Line 計算のベクトルは，式 (3) の非ゼロ元の 1 つが 1 になったため，この形式によるベクトルの乗算は，擬似 12-sprase 乗算と呼ばれる．

2.3.2 最終べきの効率化手法

最終べきの指数部は，$(p^{18} - 1)/r = (p^9 - 1) \cdot (p^3 + 1) \cdot (p^6 - p^3 + 1)/r$ のように表される．$(p^9 - 1) \cdot (p^3 + 1)$ 部分のべき乗算は，Frobenius 写像を利用して簡単に計算できるため，Easy part と呼ばれる．それ以外の $(p^6 - p^3 + 1)/r$ のべき乗算計算は Hard part と呼ばれ，最終べきの性能は主に Hard part の処理効率に決定づけられる．[2] には，Hard Part の効率的なアルゴリズムが提案されており，8 回の二乗算，54 回の乗算，29 回の Frobenius 写像，7 回の χ によるべき乗算により計算することができる．また，Hard part での処理や，$\mathbb{G}_3$ 上のべき乗算における二乗算は，Cyclotomic squaring [13] を適用することができる．

Cyclotomic Squaring: $A_c = a_{c0} + a_{c1}\gamma$ を $\mathbb{G}_3$ 上の元とする．ただし，a_{c0}, a_{c1} は $\mathbb{F}_{p^9}$ 上の元である．このとき，A_c は $A_c^{p^9+1} = 1$ を満たすため，$(a_{c0} + a_{c1}\gamma)(a_{c0} - a_{c1}\gamma) = 1$

が成り立ち，$a_{c0}^2 = 1 + a_{c1}^2\gamma^2$ が得られる．これを適用すれば，$\mathbb{G}_3$ 上の二乗算は，$A_c^2 = (1+2a_{c1}^2\gamma^2) + ((a_{c0}+a_{c1})^2 - 1 - a_{c1}^2(1+\gamma^2))\gamma$ のように計算できる．

Cyclotomic squaring よりもさらに低コストな二乗算を実現する Complex squaring [17] も存在するが，本研究では議論しない．このため，本研究の最終べきと $\mathbb{G}_3$ 上のべき乗算に関しては，最効率の実装ではない．

2.3.3 $\mathbb{G}_1$・$\mathbb{G}_2$・$\mathbb{G}_3$ 上の処理の効率化手法

KSS 曲線を用いたペアリングでは，$\mathbb{G}_1$ 上のスカラー倍算に関しては 2-GLV 法，$\mathbb{G}_2$ 上のスカラー倍算，$\mathbb{G}_3$ 上のべき乗算に関しては，それぞれ 2-GLV 法に加えて，3-GLV 法，6-GLV 法が適用できる [19]．

例として，2-GLV 法を用いた $\mathbb{G}_2$ 上のスカラー倍算を紹介する．[19] によると，$\mathbb{G}_2$ 上でのスカラー倍算は，6 次ツイスト写像を用いることで，$\mathbb{G}_2'$ 上において計算される．このため，以降では，$\mathbb{G}_2'$ 上の有理点を Q' として考える．また，s を r と同程度の大きさのスカラー値とすると，スカラー倍算 $[s]Q'$ は，以下のように計算することができる．

2-GLV 法を用いたスカラー倍算: KSS 曲線の有理点の総数は $\#E = p+1-t$ により表され，$r|\#E$ を満たす．これより，$p \equiv t-1 \pmod r$ が成り立つ．s を $t-1$ で割ったときの商とあまりのスカラー値をそれぞれ s_0, s_1 とすれば，スカラー倍算は $[s]Q' = [s_0 \cdot (t-1)]Q' + [s_1]Q'$ として考えることができる．このとき，$p \equiv t-1 \pmod r$ より，$[t-1]Q'$ は Skew Frobenius 写像 $\tilde{\phi}_p$ [19] を用いることによって，簡単に計算することができる．これより，$[s]Q'$ によるスカラー倍算は，$[s]Q' = [s_0]\tilde{\phi}_p(Q') + [s_1]Q'$ のように表せる．これに対して，2-GLV 法を適用すれば，効率的にスカラー倍算を行うことができる．また，s_0, s_1 を符号付き二進数形式の Joint sparse form [1] に変換すれば，さらなる高速化が期待できる．

3. 18 次拡大体の構成法とペアリングの実装

本節では，提案する 18 次拡大体構成法と，それを用いたペアリングの実装について議論する．

3.1 拡大体構成法

本研究で着目する，OEF による 18 次拡大体構成法 (Type-I) と，円周等分多項式を用いた新たな拡大体構成 (Type-II) の詳細を示す．

Type-I: OEF を用いて逐次的に拡大体を構成する手法は，現在広くペアリングに用いられている拡大体構成である．本研究では，以下のように構成する 18 次拡大体を，Type-I と定義する．

$$T : \begin{cases} \mathbb{F}_{p^3} &= \mathbb{F}_p[\alpha]/(\alpha^3 - c), \\ \mathbb{F}_{p^9} &= \mathbb{F}_{p^3}[\beta]/(\beta^3 - \alpha), \\ \mathbb{F}_{p^{18}} &= \mathbb{F}_{p^9}[\gamma]/(\gamma^2 - \beta). \end{cases} \tag{5}$$

このとき，α, β, γ は，それぞれの拡大体を構成する法多項式の根である．また，c は $\mathbb{F}_p$ 上の平方非剰余かつ立方非剰余元であり，本研究では，$c = 2$ の場合を議論する．この構成による 18 次拡大体の元の基底は，$\{1, \alpha, \alpha^2,\ \beta, \alpha\beta, \alpha^2\beta,\ \beta^2, \alpha\beta^2, \alpha^2\beta^2,\ \gamma, \alpha\gamma, \alpha^2\gamma, \beta\gamma, \alpha\beta\gamma, \alpha^2\beta\gamma,\ \beta^2\gamma, \alpha\beta^2\gamma, \alpha^2\beta^2\gamma\}$ により与えられる．

Type-II (New construction): Type-I より良い計算効率をもつ 18 次拡大体を構成するために，3 次拡大体を構成する法多項式に位数 7 の円周等分多項式 $\Phi_7(x)$ を用いて，新たな拡大体構成法 (Type-II) を以下のように定義する．

$$T' : \begin{cases} \mathbb{F}_{p^3} &= \mathbb{F}_p[\omega]/\Phi_7(\omega), \\ \mathbb{F}_{p^9} &= \mathbb{F}_{p^3}[\beta]/(\beta^3 - (\tau_1 - c')), \\ \mathbb{F}_{p^{18}} &= \mathbb{F}_{p^9}[\gamma]/(\gamma^2 - \beta). \end{cases} \tag{6}$$

ω, β, γ は，それぞれの拡大体を構成する既約多項式の根である．ただし，c' は $\mathbb{F}_p$ 上の元であり，本稿では，$c' = 2$ とする．なお，τ_1, τ_2, τ_3 は $\tau_1 = \omega + \omega^6$, $\tau_2 = \omega^2 + \omega^5$, $\tau_3 = \omega^3 + \omega^4$ により与えられる．18 次拡大体の元の基底は，$\{\tau_1, \tau_2, \tau_3, \tau_1\beta, \tau_2\beta, \tau_3\beta, \tau_1\beta^2, \tau_2\beta^2, \tau_3\beta^2, \tau_1\gamma, \tau_2\gamma, \tau_3\gamma, \tau_1\beta\gamma, \tau_2\beta\gamma, \tau_3\beta\gamma, \tau_1\beta^2\gamma, \tau_2\beta^2\gamma, \tau_3\beta^2\gamma\}$ により与えられる．このとき，部分体となる 3 次拡大体 $\mathbb{F}_{p^3}$ の演算には，効率的な演算手法である CVMA を用いることができる．

注意 1. Type-II の構成の基底 τ_1, τ_2, τ_3 について，$\Phi_7(\omega) = 0$ より，$\tau_1+\tau_2+\tau_3 = -1$, $\tau_1\tau_2+\tau_2\tau_3+\tau_3\tau_1 = -2$, $\tau_1\tau_2\tau_3 = 1$ がそれぞれ成り立つ．

3.2 拡大体の構成条件

Type-I，Type-II による 18 次拡大体の構成条件を明らかにするために，KSS 素数を標数とする素体上の平方剰余・立方剰余性に関する補題を示す．

補題 1. p が KSS 素数であるとき，$2, 7 \in \mathbb{F}_p$ の平方剰余，立方剰余性は，正規化 KSS パラメータ χ_0 の条件によって以下のように与えられる．

(a) $$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } \chi_0 \equiv 2, 3 \pmod 4, \\ -1 & \text{if } \chi_0 \equiv 0, 1 \pmod 4. \end{cases}$$

(b) $$\left(\frac{-7}{p}\right) = \begin{cases} 1 & \text{if } \chi_0 \equiv 0, 1, 5 \pmod 7, \\ -1 & \text{if } \chi_0 \equiv 2, 3, 4, 6 \pmod 7. \end{cases}$$

(c) $$\left(\frac{2}{p}\right)_3 \begin{cases} = 1 & \text{if } \chi_0 \equiv 0 \pmod 3, \\ \neq 1 & \text{if } \chi_0 \equiv 1, 2 \pmod 3. \end{cases}$$

(d) $$\left(\frac{-7}{p}\right)_3 \begin{cases} = 1 & \text{if } \chi_0 \equiv 3, 11, 13, 14, 15, 19 \pmod{21}, \\ \neq 1 & \text{otherwise.} \end{cases}$$

Proof. (a) Legendre 記号の性質は，[23] に示されている．まず，Legendre 記号は，$\left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \pmod 8$ が成り立つ性質をもつ．KSS 素数 p に対してこれを適用すれば，(a) が得られる．(b) さらに，Legendre 記号では，

$p' \neq p$ を素数とすると，$p \equiv p' \equiv 3 \pmod 4$ を満たすとき $\left(\frac{p'}{p}\right) = -\left(\frac{p}{p'}\right)$，満たさないとき $\left(\frac{p'}{p}\right) = \left(\frac{p}{p'}\right)$ が成り立つ．p を KSS 素数，p' を 7 とすれば，7 の平方剰余性の条件が得られる．また，$\left(\frac{-1}{p}\right) = 1 \Leftrightarrow p \equiv 1 \pmod 4$ が成り立つため，-1 の平方剰余性の条件も得られる．$\left(\frac{-1}{p}\right)\left(\frac{7}{p}\right) = \left(\frac{-7}{p}\right)$ より，-7 の剰余性の条件 (b) が導出される．

(c)(d) U, V を $p = U^2 + 3V^2$ を満たす整数とする．このとき，Euler の予想 [24] より，$\left(\frac{2}{p}\right)_3 = 1 \Leftrightarrow 3|V$，$\left(\frac{7}{p}\right)_3 = 1 \Leftrightarrow (3|V$ and $7|U)$ or $21|(V \pm U)$ or $7|(4V \pm U)$ or $21|V$or $7|(V \pm 2U)$ が成り立つ．p が KSS 素数であるとき，$4p = t^2 + 3f^2$ を満たす整数 f が存在し，$f = (5\chi^4+14\chi^3+94\chi+259)/21$ により表される．このとき，$4p = t^2+3f^2$ を式変形すると，$U = (3f-t)/4, V = (f+t)/4$ が与えられ，これに対して Euler の予想を適用すれば，(c), (d) が得られる． □

補題 2. (i) 正規化 KSS パラメータ χ_0 が $\chi_0 \equiv 1, 4, 5, \text{or } 8 \pmod{12}$ を満たすとき，Type-I による 18 次拡大体が構成できる．(ii) $\chi_0 \equiv 4, 10, 17, \text{or } 18 \pmod{21}$ を満たすとき，Type-II による 18 次拡大体が構成できる．

Proof. (i) Type-I について，$\mathbb{F}_p \xrightarrow{\alpha^3-c} \mathbb{F}_{p^3}$ を構成するとき，法多項式は既約である必要があり，c は $\mathbb{F}_p$ 上で立方非剰余元となる必要がある．さらに，$\mathbb{F}_{p^3} \xrightarrow{\beta^3-\alpha} \mathbb{F}_{p^9}$ を構成するときは，α は $\mathbb{F}_{p^3}$ 上で立方非剰余元である必要がある．ここで，$\alpha^{(p^3-1)/3} = \alpha^{(p^2+p+1)\cdot(p-1)/3} = (-\alpha^3)^{(p-1)/3} = (-c)^{(p-1)/3}$ であるから，α が立方非常余元になるためには，$-c$ が $\mathbb{F}_p$ 上で立方非剰余元となる必要がある．本稿では $c = 2$ であるため，これらの条件を考慮すると，KSS パラメータは $\chi_0 \equiv 1, 2 \pmod 3$ を満たす必要がある (補題 1 (c) 参照)．$\mathbb{F}_{p^9} \xrightarrow{\gamma^2-\beta} \mathbb{F}_{p^{18}}$ についても同様に考えると，$c = 2$ は $\mathbb{F}_p$ 上で平方非剰余元である必要があり，$\chi_0 \equiv 0, 1 \pmod 4$ を満たす必要がある (補題 1 (a) 参照)．以上より，Type-I における 18 次拡大体は，$\chi_0 \equiv 1, 4, 5, 8 \pmod{12}$ を満たすとき構成可能である．

(ii) Type-II について，$\mathbb{F}_p \xrightarrow{\Phi_7(\omega)} \mathbb{F}_{p^3}$ を構成する際，$\Phi_7(x)$ が既約になる条件は $p \not\equiv 1, 6 \pmod 7$ である [18]．さらに，$\mathbb{F}_{p^3} \xrightarrow{\beta^3-(\tau_1-c')} \mathbb{F}_{p^9} \xrightarrow{\gamma^2-\beta} \mathbb{F}_{p^{18}}$ を構成するときは，$(\tau_1 - c')$ は $\mathbb{F}_{p^3}$ 上で平方非剰余かつ立方非剰余元である必要がある．ここで，$c' = 2$ であるため，$(\tau_1 - c')^{(p^3-1)}$ は，$(\tau_1 - 2)^{(p^2+p+1)\cdot(p-1)} = (\tau_1\tau_2\tau_3 - 2(\tau_1\tau_2 + \tau_2\tau_3 + \tau_3\tau_1) + 4(\tau_1 + \tau_2 + \tau_3) - 8)^{p-1}$ のように変形することができる．注意 1 に示す関係式を適用すれば，$(\tau_1-2)^{(p^3-1)} = (-7)^{p-1}$ が得られる．これより，$(\tau_1 - 2)$ が $\mathbb{F}_{p^3}$ 上で平方非剰余かつ立方非剰余元になるためには，-7 が $\mathbb{F}_p$ 上で平方非剰余かつ立方非剰余元となる必要がある．補題 1 (b), (d) に示される条件を考慮すれば，Type-II による拡大体を構成するための条件は，$\chi_0 \equiv 4, 10, 17, 18 \pmod{21}$ である． □

表 1 KSS パラメータの条件と KSS 曲線・ツイスト曲線

分類	*Class 1*	*Class 2*
χ_0 の条件	$\chi_0 \equiv 5, 8 \pmod{12}$	$\chi_0 \equiv 1, 4 \pmod{12}$
拡大体	Type-I	Type-I
$E/\mathbb{F}_p$	$y^2 = x^3 + 2^5$	$y^2 = x^3 + 2$
$E'/\mathbb{F}_{p^3}$	$y^2 = x^3 + 2^5\alpha$	$y^2 = x^3 + 2\alpha^{-1}$
χ_0 の条件	$\chi_0 \equiv 4, 17 \pmod{21}$	$\chi_0 \equiv 10, 18 \pmod{21}$
拡大体	Type-II	Type-II
$E/\mathbb{F}_p$	$y^2 = x^3 + 7^5$	$y^2 = x^3 + 7$
$E'/\mathbb{F}_{p^3}$	$y^2 = x^3 + 7^5(\tau_1 - 2)$	$y^2 = x^3 + 7(\tau_1 - 2)^{-1}$

表 2 サンプルパラメータ

	KSS パラメータ χ
[*I*]-1 Type-I (*Class 1*)	$\chi = 2^{85} - 2^{74} - 2^{71} + 2^{45} - 2^1$
[*II*]-1 Type-II (*Class 1*)	$\chi = 2^{85} + 2^{49} + 2^{42} - 2^{39} - 2^2$
[*I*]-2 Type-I (*Class 2*)	$\chi = 2^{85} + 2^{76} + 2^{71} + 2^{45} - 2^1$
[*II*]-2 Type-II (*Class 2*)	$\chi = 2^{85} - 2^{70} + 2^{68} + 2^{11} - 2^3$

3.3 KSS 曲線・ツイスト曲線とサンプルパラメータ

第 3.2 節で明らかにした 18 次拡大体の構成条件に関する予備実験の結果を表 1 に示す．予備実験の結果では，Type-I，Type-II それぞれの構成条件は，表 1 に示すような二つのパラメータクラス *Class 1*，*Class 2* に分類可能であり，それぞれの正規化 KSS パラメータの条件において，KSS 曲線 $E/\mathbb{F}_p$ とそのツイスト曲線 $E/\mathbb{F}_{p^3}$ が一意に決定できた．表 2 には，表 1 に基づいて探索した，Type-I，Type-II を構成可能な *Class 1*，*Class 2* の KSS パラメータがそれぞれ示されている．これらのパラメータにより生成される素数の大きさはいずれも 676-bit であり，192-bit セキュリティレベルの安全性を担保することができる [4]．

パラメータクラスの分類条件と曲線の一意性が一般の場合に成立するかどうかは明らかでないが，BN 曲線や BLS 曲線の係数決定に関する先行研究 [11, 28] を利用すれば，証明可能であると期待できる．

3.4 ペアリングの実装とそれぞれの処理の考察

表 2 による KSS パラメータを利用した，Type-I，Type-II によるペアリングの実装の詳細を示す．なお，表 3 には $\mathbb{F}_{p^3}$ と $\mathbb{F}_{p^{18}}$ 上での演算コスト，表 4 にはツイスト曲線上での演算コストの詳細が示されている．ただし，表中の $\mathcal{M}$，$\mathcal{S}$，$\mathcal{A}$，$\mathcal{A}_u$，$\mathcal{I}$ はそれぞれ，$\mathbb{F}_p$ 上の乗算，二乗算，加減算・符号反転，定数加減算，逆元計算を表している．

Miller のアルゴリズム: Miller のアルゴリズムでは，擬似 12-sparse 乗算を用いた Optimal-ate ペアリングを実装する．Type-I と Type-II による拡大体をペアリングに用いた場合，擬似 12-sparse 乗算を用いた Miller のアルゴリズムの Line 計算は，表 5 により与えられる．

Class 1 と *Class 2* のパラメータによる Line 計算の式を比較すると，明らかに *Class 1* を用いた場合は，α^{-1}，$(\tau_1 - 2)^{-1}(= \beta^3)$ による $\mathbb{F}_{p^3}$ 上の乗算が 2 回ずつ余分に必

要となることが分かる．これより，*Class 2* のパラメータを用いた実装の方が，*Class 1* よりも効率的な Miller のアルゴリズムが実現できると考えられる．また，Miller のアルゴリズムでは，$\mathbb{F}_{p^3}$ 上の演算が用いられる．表 3 より，$\mathbb{F}_{p^3}$ の演算に CVMA が用いられている Type-II では，逆元計算にかかる $\mathcal{A}$ は 3 回多いが，乗算にかかる $\mathcal{A}$ は 5 回少ない．これより，Type-II を用いた方が，Type-I よりも効率的な実装が可能であると言える．ただし，*Class 1* のパラメータを用いた場合，$(\tau_1-2)^{-1}$，$\alpha^{-1}(=\beta^{-3})$ による乗算コストは Type-I の方が低コストであるため，CVMA による演算の効果が相殺される可能性がある．

最終べき: 最終べきでは，[2] による効率的なアルゴリズムと，Cyclotomic squaring を実装に用いる．ただし，Complex squaring は実装していないため，最終べきに関しては最効率の実装ではない．

最終べきの処理は，$\mathbb{F}_{p^{18}}$ 上の演算が用いられる．いずれのパラメータクラスを用いても，$\mathbb{F}_{p^{18}}$ 上の演算コストは表 3 に示されるものとなる．Type-I と比較して，$\mathbb{F}_{p^3}$ 上の乗算が効率的に行われる Type-II では，$\mathbb{F}_{p^{18}}$ 上の乗算，二乗算，逆元計算にかかる $\mathcal{A}$ が削減されている．しかし，最終べきでとくに用いられる，Cyclotomic Squaring や Frobneius 写像の計算量は増大している．Cyclotomic Squaring に関しては，演算内で呼び出される $\mathbb{F}_{p^9}$ 上の二乗算のコストが，Type-II の β^3 による乗算コストの大きさにより，増大したためであると考えられる．また，Frobenius 写像については，$\mathbb{F}_{p^3}$ の基底の複雑さにより，基底の p 乗算にかかる計算が複雑になってしまったと考えられる．例えば，基底元 β の p 乗算は，$\beta^p=(\beta^3)^{(p-1)/3}\beta$ のように計算でき，Type-I の場合では，さらに $(\beta^3)^{(p-1)/3}=(\alpha^2)^{(p-1)/6}=2^{(p-1)/6}\in\mathbb{F}_p$ のように変形できる．しかし，Type-II では，$(\beta^3)^{(p-1)/3}=(\tau_1-2)^{(p-1)/6}\in\mathbb{F}_{p^3}$ となり，β^p の計算のためには $\mathbb{F}_{p^3}$ 上の乗算が必要となる．これより，最終べきに関しては，Type-II よりも Type-I の方が効率的に計算処理ができると考えられる．

$\mathbb{G}_1$，$\mathbb{G}_2$ 上のスカラー倍算: $\mathbb{G}_1$ 上のスカラー倍算には，Joint sparse form を利用した 2-GLV 法，$\mathbb{G}_2$ 上のスカラー倍算に関しては，6-GLV 法を用いた実装を行う．

$\mathbb{G}_1$ 上のスカラー倍算では，$\mathbb{F}_p$ を定義体とする KSS 曲線上における演算が用いられる．$\mathbb{F}_p$ の構成は同一であり，KSS 曲線上の楕円加算，楕円二倍算の計算コストはパラメータクラスに関わらず，Type-I，Type-II いずれも同じであるため，その性能に差はないと言える．

$\mathbb{G}_2$ 上のスカラー倍算では，$\mathbb{F}_{p^3}$ を定義体とするツイスト曲線 E' 上で処理が行われる．表 4 によると，楕円加算，楕円二倍算の計算コストは部分体に CVMA を用いている Type-II の方が低コストである．Skew Frobenius 写像は $\mathbb{F}_{p^{18}}$ 上の Frobenius 写像と同様の理由で，Type-I を用いた方が低コストである．これに加えて，Skew Frobenius 写像は，6 次ツイスト写像の効率性により，*Class 1* よりも *Class 2* を用いた方が効率的である．しかし，$\mathbb{G}_2$ 上のスカ

表 3 3 次拡大体と 18 次拡大体上の演算コスト

$\mathbb{F}_{p^3}$ 上の演算		Type-I	Type-II
加減算/符号反転		$3\mathcal{A}$	$3\mathcal{A}$
乗算		$6\mathcal{M}+17\mathcal{A}$	$6\mathcal{M}+\boldsymbol{12\mathcal{A}}$
二乗算		$2\mathcal{M}+3\mathcal{S}+11\mathcal{A}$	$2\mathcal{M}+3\mathcal{S}+11\mathcal{A}$
逆元計算		$9\mathcal{M}+3\mathcal{S}$ $+\boldsymbol{8\mathcal{A}}+\mathcal{I}$	$9\mathcal{M}+3\mathcal{S}$ $+11\mathcal{A}+\mathcal{I}$
β^3 による乗算		$\boldsymbol{\mathcal{A}}$	$9\mathcal{A}$
β^{-3} による乗算		$3\mathcal{M}+\boldsymbol{2\mathcal{A}}$	$3\mathcal{M}+15\mathcal{A}$
Frobenius 写像		$2\mathcal{A}$	$\mathbf{0}$
$\mathbb{F}_{p^{18}}$ 上の演算		Type-I	Type-II
加減算/符号反転		$18\mathcal{A}$	$18\mathcal{A}$
乗算		$108\mathcal{M}+493\mathcal{A}$	$108\mathcal{M}+\boldsymbol{459\mathcal{A}}$
二乗算		$72\mathcal{M}+345\mathcal{A}$	$72\mathcal{M}+\boldsymbol{333\mathcal{A}}$
Cyc. Squaring		$5\mathcal{M}+49\mathcal{S}$ $+\boldsymbol{229\mathcal{A}}+2\mathcal{A}_u$	$5\mathcal{M}+49\mathcal{S}$ $+249\mathcal{A}+6\mathcal{A}_u$
逆元計算		$177\mathcal{M}+48\mathcal{S}$ $+827\mathcal{A}+\mathcal{I}$	$177\mathcal{M}+48\mathcal{S}$ $+\boldsymbol{761\mathcal{A}}+\mathcal{I}$
Frobenius 写像	p	$\boldsymbol{16\mathcal{M}+7\mathcal{A}}$	$24\mathcal{M}+52\mathcal{A}$
	p^2	$\boldsymbol{16\mathcal{M}+6\mathcal{A}}$	$24\mathcal{M}+52\mathcal{A}$
	p^3	$\boldsymbol{12\mathcal{M}}+3\mathcal{A}$	$12\mathcal{M}+3\mathcal{A}$
	p^4	$\boldsymbol{16\mathcal{M}+6\mathcal{A}}$	$24\mathcal{M}+52\mathcal{A}$
	p^5	$\boldsymbol{16\mathcal{M}+7\mathcal{A}}$	$24\mathcal{M}+52\mathcal{A}$
	p^9	$9\mathcal{A}$	$9\mathcal{A}$

表 4 ツイスト曲線上の演算コスト

$E'(\mathbb{F}_{p^3})$ 上の演算		Type-I	Type-II
楕円加算 (ECA)		$23\mathcal{M}+6\mathcal{S}$ $+71\mathcal{A}+\mathcal{I}$	$23\mathcal{M}+6\mathcal{S}$ $+\boldsymbol{64\mathcal{A}}+\mathcal{I}$
楕円二倍算 (ECD)		$25\mathcal{M}+9\mathcal{S}$ $+85\mathcal{A}+\mathcal{I}$	$25\mathcal{M}+9\mathcal{S}$ $+\boldsymbol{78\mathcal{A}}+\mathcal{I}$
逆元計算		$3\mathcal{A}$	$3\mathcal{A}$
Skew Frobenius 写像 (*Class 1*)	p	$\boldsymbol{11\mathcal{M}}+8\mathcal{S}$	$12\mathcal{M}+64\mathcal{S}$
	p^2	$12\mathcal{M}+\boldsymbol{8\mathcal{S}}$	$12\mathcal{M}+64\mathcal{S}$
	p^3	$3\mathcal{M}+\boldsymbol{3\mathcal{S}}$	$3\mathcal{M}+6\mathcal{S}$
Skew Frobenius 写像 (*Class 2*)	p	$\boldsymbol{5\mathcal{M}+2\mathcal{S}}$	$6\mathcal{M}+16\mathcal{S}$
	p^2	$6\mathcal{M}+\boldsymbol{2\mathcal{S}}$	$6\mathcal{M}+16\mathcal{S}$
	p^3	$3\mathcal{M}+3\mathcal{S}$	$3\mathcal{M}+3\mathcal{S}$

表 5 擬似 12-sprase 乗算を用いた Line 計算

	Line 計算 $\hat{l}_{\hat{T}',\hat{Q}'}(\hat{P})$
Type-I (*Class 1*)	$1-\alpha^{-1}C\beta^2\gamma+\alpha^{-1}Ey_{\hat{P}}{}^{-1}\beta\gamma$ $=(\underbrace{1}_{1},0,0,0,\underbrace{\alpha^{-1}Ey_{\hat{P}}{}^{-1}}_{\beta\gamma},\underbrace{-\alpha^{-1}C}_{\beta^2\gamma})$
Type-II (*Class 1*)	$1-(\tau_1-2)^{-1}C\beta^2\gamma+(\tau_1-2)^{-1}Ey_{\hat{P}}{}^{-1}\beta\gamma$ $=(\underbrace{1}_{1},0,0,0,\underbrace{(\tau_1-2)^{-1}Ey_{\hat{P}}{}^{-1}}_{\beta\gamma},\underbrace{-(\tau_1-2)^{-1}C}_{\beta^2\gamma})$
Type-I (*Class 2*)	$1-C\gamma+Ey_{\hat{P}}{}^{-1}\beta\gamma$ $=(\underbrace{1}_{1},0,0,\underbrace{-C}_{\gamma},\underbrace{Ey_{\hat{P}}{}^{-1}}_{\beta\gamma},0)$
Type-II (*Class 2*)	$1-C\gamma+Ey_{\hat{P}}{}^{-1}\beta\gamma$ $=(\underbrace{1}_{1},0,0,\underbrace{-C}_{\gamma},\underbrace{Ey_{\hat{P}}{}^{-1}}_{\beta\gamma},0)$

ラー倍算において，Skew Frobenius 写像は数回しか用いられないため，ほとんど影響を与えないと考えられる．これより，$\mathbb{G}_2$ 上のスカラー倍算では，Type-II を用いた方が効率的であると考えられる．

$\mathbb{G}_3$ 上でのべき乗算: $\mathbb{G}_3$ 上のべき乗算については，$\mathbb{G}_2$ と同様に，6-GLV 法を用いた実装を行う．

$\mathbb{G}_3$ 上のべき乗算では，最終べきと同様に，$\mathbb{F}_{p^{18}}$ 上の演算が用いられる．最終べきの実装で述べたように，Type-II では，$\mathbb{F}_{p^{18}}$ 上の Cyclotomic squaring や Frobenius 写像は効率的でない．しかし，$\mathbb{G}_3$ 上のべき乗算においては，$\mathbb{F}_{p^{18}}$ 上の乗算が最終べきよりも多用され，Frobenius 写像は数回しか用いられない．これより，Cyclotomic squaring は非効率であるものの，Type-II による $\mathbb{G}_3$ 上のべき乗算は，Type-I と同等以上の性能を持つと考えられる．

4. 実験結果

多倍長整数演算ライブラリ GMP [14] を用いて，パラメータクラス別に Type-I，Type-II の構成を用いたペアリングの実装を行い，計算コストと実行速度の比較を行った結果を示す．実験に用いたサンプルコードは，GitHub[*1]を参照されたい．実験では，表 6 に示す実験環境を用いており，計算コストの評価に関しては，プログラム内のカウンタに基づいて，$\mathbb{F}_p$ 上の演算 $\mathcal{M}$，$\mathcal{S}$，$\mathcal{A}$，$\mathcal{A}_u$，$\mathcal{I}$ の呼び出し回数のカウントを行った．ペアリングのコスト評価の際には，これらの演算の比率を $\mathcal{M}=5\mathcal{A}$，$\mathcal{S}=4.5\mathcal{A}$，$\mathcal{A}_u=0.3\mathcal{A}$，$\mathcal{I}=30\mathcal{A}$ と仮定している．この比率に関しては，676-bit の標数を用いた $\mathbb{F}_p$ 上におけるそれぞれの演算の 100 万回試行時に得られた実行速度に基づいて算出したものである．

表 7 には，Miller のアルゴリズム (ML) と最終べき (FE) の 1 回試行にかかる $\mathbb{F}_p$ 上の演算量と，スカラー値をランダムに設定した $\mathbb{G}_1$，$\mathbb{G}_2$，$\mathbb{G}_3$ 上の計算における，100 回試行の平均演算量が示されている．また，表 7 には，100 回試行時に得られた実行速度の平均値も併せて示されている．表 8 は，表 7 の結果よりコスト評価を行い，実装効率の順序付けを行った結果を表したものである．ただし，記号 $=$，$\approx$ は，両辺の実装結果を比較したときに，それぞれの計算コストが同じもしくは，その比率が 0.5%未満であることを表している．記号 $\overset{\delta\%}{<}$ は右辺の実装結果の方が，左辺の結果よりも $\delta\%$ 効率的であることを表している．

実験結果により得られたコスト評価の結果は，おおむね第 3.4 節で考察した内容に準じている．本研究で提案した Type-II による拡大体構成では，Type-I を用いた結果と比較して，*Class 2* のパラメータを用いた場合の Miller のアルゴリズムを 3.3%，$\mathbb{G}_2$ 上のスカラー倍算を 2.0%，$\mathbb{G}_3$ 上のべき乗算を 1.9%効率化することができた．しかし，ペアリング処理の中で最も計算コストがかかる最終べきに関

[*1] `http://github.com/YukiNanjo/KSS18_towering`

表 6 実験環境

CPU	Intel(R) Core(TM) i7-7567U CPU @ 3.50GHz
Memory	8GB
Compiler	GCC 4.2.1
OS	macOS High Sierra 10.13.6
Language	C
Library	GMP ver 6.1.2 [14]

表 7 ペアリングの計算量と実行時間

Pairing	[*I*]-1 Type-I *(Class 1)*					Time
Operations	$\mathcal{M}$	$\mathcal{S}$	$\mathcal{A}$	$\mathcal{A}_u$	$\mathcal{I}$	[ms]
ML	1905	14544	61412	0	93	9.43
FE (Easy)	38	415	1825	0	1	0.27
FE (Hard)	3445	38197	177953	1202	0	24.09
$\mathbb{G}_1$ SCM	780	647	2598	0	389	3.05
$\mathbb{G}_2$ SCM	6443	1914	20555	0	269	5.61
$\mathbb{G}_3$ Exp.	618	25860	119264	173	0	14.80
Pairing	[*II*]-1 Type-II *(Class 1)*					Time
Operations	$\mathcal{M}$	$\mathcal{S}$	$\mathcal{A}$	$\mathcal{A}_u$	$\mathcal{I}$	[ms]
ML	1988	14470	60799	0	93	9.19
FE (Easy)	39	414	1691	0	1	0.26
FE (Hard)	3629	38197	188267	3606	0	24.19
$\mathbb{G}_1$ SCM	779	646	2600	0	389	3.07
$\mathbb{G}_2$ SCM	6449	1915	18949	0	269	5.42
$\mathbb{G}_3$ Exp.	650	25852	114446	521	0	14.16
Pairing	[*I*]-2 Type-I *(Class 2)*					Time
Operations	$\mathcal{M}$	$\mathcal{S}$	$\mathcal{A}$	$\mathcal{A}_u$	$\mathcal{I}$	[ms]
ML	1347	14544	60852	0	93	9.21
FE (Easy)	38	415	1825	0	1	0.27
FE (Hard)	3445	38197	177953	1202	0	24.12
$\mathbb{G}_1$ SCM	779	646	2594	0	389	3.06
$\mathbb{G}_2$ SCM	6411	1913	20518	0	269	5.65
$\mathbb{G}_3$ Exp.	619	25863	119277	174	0	14.87
Pairing	[*II*]-2 Type-II *(Class 2)*					Time
Operations	$\mathcal{M}$	$\mathcal{S}$	$\mathcal{A}$	$\mathcal{A}_u$	$\mathcal{I}$	[ms]
ML	1430	14470	56317	0	93	8.70
FE (Easy)	39	414	1691	0	1	0.26
FE (Hard)	3629	38197	188267	3606	0	24.21
$\mathbb{G}_1$ SCM	780	647	2602	0	389	3.09
$\mathbb{G}_2$ SCM	6435	1919	18752	0	270	5.40
$\mathbb{G}_3$ Exp.	650	25860	114481	521	0	14.05

表 8 ペアリングの処理効率の比較

Pairing	処理効率の優劣						
Operations	低効率 $\longleftarrow\!\!\longrightarrow$ 高効率						
ML	[*I*]-1	$\approx$	[*II*]-1	$\overset{2.0\%}{<}$	[*I*]-2	$\overset{3.3\%}{<}$	[*II*]-2
FE	[*II*]-1	$=$	[*II*]-2	$\overset{3.1\%}{<}$	[*I*]-1	$=$	[*I*]-2
$\mathbb{G}_1$ SCM	[*I*]-1	$\approx$	[*I*]-2	$\approx$	[*II*]-1	$\approx$	[*II*]-2
$\mathbb{G}_2$ SCM	[*I*]-1	$\approx$	[*I*]-2	$\overset{2.0\%}{<}$	[*II*]-1	$\approx$	[*II*]-2
$\mathbb{G}_3$ Exp.	[*I*]-1	$\approx$	[*I*]-2	$\overset{1.9\%}{<}$	[*II*]-1	$\approx$	[*II*]-2

しては，Frobenius 写像や Cyclotomic squaring のコストにより，Type-I よりも 3.1%性能が低下した．また，Miller のアルゴリズムに関しては，Type-II の構成を用いても，*Class 1* のパラメータを選んだ場合，その性能は Type-I を用いた場合とほぼ同じであるため，Type-II の構成を用いる場合は，とくにパラメータの選び方に注意が必要である．

5. 結論

本稿では，3 次拡大体の法多項式に位数 7 の円周等分多項式を用いた拡大体構成法 (Type-II) を提案し，その評価を行った．その結果，*Class 2* のパラメータを用いた Miller のアルゴリズムと，$\mathbb{G}_2$，$\mathbb{G}_3$ 上の処理を効率化することができたが，最終べきの計算コストは増大した．このため，Type-II の拡大体構成の見直しを行い，Frobenius 写像や Cyclotomic squaring の効率化を行う必要がある．また，いずれの拡大体構成を用いても，Miller のアルゴリズムには *Class 1* よりも *Class 2* によるパラメータを用いた方が効率的である結果が得られた．このため，パラメータクラスの分類条件と曲線の一意性の一般化が今後の課題である．

6. 謝辞

本研究を進めるにあたりご協力をいただいた，公立はこだて未来大学の白勢政明准教授に深謝する．

参考文献

[1] Adikari, J., Dimitrov, V., Imbert, L.: Hybrid binary-ternary joint sparse form and its application in elliptic curve cryptography (2008)

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

[3] Bailey, D.V., Paar, C.: Efficient arithmetic in finite field extensions with application in elliptic curve cryptography. Journal of cryptology 14(3), 153–176 (2001)

[4] Barbulescu, R., Duquesne, S.: Updating key size estimations for pairings. Cryptology ePrint Archive, Report 2017/334 (2017), `http://eprint.iacr.org/2017/334`

[5] Barreto, P.S., Lynn, B., Scott, M.: Constructing elliptic curves with prescribed embedding degrees. In: International Conference on Security in Communication Networks. pp. 257–267. Springer (2002)

[6] Barreto, P.S., Naehrig, M.: Pairing-friendly elliptic curves of prime order. In: International Workshop on Selected Areas in Cryptography. pp. 319–331. Springer (2005)

[7] Benger, N., Scott, M.: Constructing tower extensions of finite fields for implementation of pairing-based cryptography. In: International Workshop on the Arithmetic of Finite Fields. pp. 180–195. Springer (2010)

[8] Boneh, D., Di Crescenzo, G., Ostrovsky, R., Persiano, G.: Public key encryption with keyword search. In: International conference on the theory and applications of cryptographic techniques. pp. 506–522. Springer (2004)

[9] Boneh, D., Lynn, B., Shacham, H.: Short signatures from the weil pairing. Advances in Cryptology-ASIACRYPT 2001 pp. 514–532 (2001)

[10] Cohen, H., Frey, G., Avanzi, R., Doche, C., Lange, T., Nguyen, K., Vercauteren, F.: Handbook of elliptic and hyperelliptic curve cryptography. CRC press (2005)

[11] Costello, C., Lauter, K., Naehrig, M.: Attractive subfamilies of bls curves for implementing high-security pairings. In: International Conference on Cryptology in India. pp. 320–342. Springer (2011)

[12] Gallant, R.P., Lambert, R.J., Vanstone, S.A.: Faster point multiplication on elliptic curves with efficient endomorphisms. In: Annual International Cryptology Conference. pp. 190–200. Springer (2001)

[13] Granger, R., Scott, M.: Faster squaring in the cyclotomic subgroup of sixth degree extensions. In: International Workshop on Public Key Cryptography. pp. 209–223. Springer (2010)

[14] Granlund, T.: the gmp development team: Gnu mp: the gnu multiple precision arithmetic library, 6.1. 0 edn.(2015)

[15] Joux, A.: A one round protocol for tripartite diffie–hellman. In: International algorithmic number theory symposium. pp. 385–393. Springer (2000)

[16] Kachisa, E.J., Schaefer, E.F., Scott, M.: Constructing brezing-weng pairing-friendly elliptic curves using elements in the cyclotomic field. Pairing 8, 126–135 (2008)

[17] Karabina, K.: Squaring in cyclotomic subgroups. Mathematics of Computation 82(281), 555–579 (2013)

[18] Kato, H., Nogami, Y., Yoshida, T., Morikawa, Y.: Cyclic vector multiplication algorithm based on a special class of gauss period normal basis. ETRI journal 29(6), 769–778 (2007)

[19] Khandaker, M.A.A., Nogami, Y.: An improvement of scalar multiplication by skew frobenius map with multi-scalar multiplication for kss curve. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 100(9), 1838–1845 (2017)

[20] Khandaker, M.A.A., Ono, H., Nogami, Y., Shirase, M., Duquesne, S.: An improvement of optimal ate pairing on kss curve with pseudo 12-sparse multiplication. In: International Conference on Information Security and Cryptology. pp. 208–219. Springer (2016)

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

[22] Koblitz, N.: Elliptic curve cryptosystems. Mathematics of computation 48(177), 203–209 (1987)

[23] Koblitz, N.: A course in number theory and cryptography, vol. 114. Springer Science & Business Media (1994)

[24] Lemmermeyer, F.: Reciprocity laws: from Euler to Eisenstein. Springer Science & Business Media (2013)

[25] Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM 21(2), 120–126 (1978)

[26] Sahai, A., Waters, B., et al.: Fuzzy identity-based encryption. In: Eurocrypt. vol. 3494, pp. 457–473. Springer (2005)

[27] Sakai, R.: Cryptosystems based on pairing. In: The 2000 Symposium on Cryptography and Information Security, Okinawa, Japan, Jan. pp. 26–28 (2000)

[28] Shirase, M.: Barreto-naehrig curve with fixed coefficient-efficiently constructing pairing-friendly curves- (2010)

[29] Vercauteren, F.: Optimal pairings. IEEE Transactions on Information Theory 56(1), 455–461 (2010)