Computer Security Symposium 2017
23 - 25 October 2017

BN曲線における効率的な6次ツイスト写像と法多項式の定数の関係

南條　由紀[1]　Md. Al-Amin Khandaker[2]　日下　卓也[2]　野上　保之[2]

概要：BN 曲線において，$\mathbb{F}_{p^2}$ を構成する法多項式の定数を変化させたとき，同じ標数を使用しているにも関わらず，6 次ツイスト写像を行う際に基底元の乗算が必要である場合と必要でない場合があることが分かった．そこで，6 種類の素体上の楕円曲線の位数を調べたところ，基底元をかける必要のない効率的なものとそうでないものでは，それらの位数パターンが異なることが分かった．これより，6 次ツイストの写像元の曲線が効率的なものであるかどうか，これらの位数と法多項式の定数の関係により，判別を行うことが可能となった．

キーワード：ペアリング暗号，計算効率化

The relation between the efficient sextic tiwst and constant of the modular polynomial for BN curve

Yuki Nanjo[1]　Md. Al-Amin Khandaker[2]　Takuya Kusaka[2]　Yasuyuki Nogami[2]

Abstract: In pairing-based cryptography, changing the constant of the $\mathbb{F}_{p^2}$ irreducible polynomial for extension field towering on Barreto-Naehrig curve shows two cases of sextic twist with the same characteristic. One of the cases needs multiplications by the $\mathbb{F}_{p^2}$ basis element but the other doesn't need that. In this paper, we examine the orders of 6 patterns of the elliptic curve in $\mathbb{F}_p$ that yields the two cases. We also show the procedure to identify an efficient and inefficient twist using relations of this difference and constant of the $\mathbb{F}_{p^2}$ irreducible polynomial.

Keywords: Pairing cryptography, efficiency of calculation

1. 序論

楕円曲線暗号は 1985 年に Victor Miller[1] と Neal Koblitz[2] により提案された暗号方式である．楕円曲線暗号は楕円離散対数問題の困難性を安全性の根拠としており，RSA 暗号 [3] の鍵長の 10 分の 1 程度で同程度の安全性が担保されるものとなっている．そして，この楕円曲線上の双線形性写像を利用したペアリング暗号方式 [4]，[5] が提案され，これを用いた ID ベース暗号 [6] では公開鍵に任意のキーワードを選択できるものとなっている．ペアリング暗号では，Miller のアルゴリズムと最終べきの 2 つの過程により，2 つの有理点群 $\mathbb{G}_1$，$\mathbb{G}_2$ を新たな拡大体上の乗法群 $\mathbb{G}_3$ へ双線形写像を行う．しかし，これらは複雑な計算処理を要し，新たな離散対数問題の解法アルゴリズムが発表されたことで，セキュリティパラメータは大きくなりつつある．そこで，これらを効率的に実装するため，計算コストを低減させたアルゴリズムの研究がなされている．効率化の対象としては，Miller のアルゴリズム，最終べきと呼ばれるべき乗算，$\mathbb{G}_1$，$\mathbb{G}_2$ におけるスカラー倍算，$\mathbb{G}_3$ におけるべき乗算などがある．効率的なペアリングとして，ate ペアリング [7]，optimal-ate ペアリング [8]，

[1] 岡山大学工学部電気通信系学科
Department of electrical and communication engineering faculty of engineering, Okayama University, Japan
[2] 岡山大学大学院自然科学研究科
Graduate school of natural science and technology, Okayama University, Japan

χ-ate ペアリング [9] などが提案されている．これらでは，[9] で述べられているように，$\mathbb{G}_2$ についてツイスト写像を行い，真部分体における演算を活用することで，効率的にペアリングを行っている．本研究では，12 次拡大体，18 次拡大体，24 次拡大体を定義体とするペアリング曲線の 6 次ツイスト写像に着目する．このとき，使用する楕円曲線，標数，逐次拡大体 [10] の構成が同じであるにも関わらず，$\mathbb{F}_{p^2}$ における法多項式の定数を変化させることのみで，効率的なものと非効率なものの 2 種類のツイスト写像があることを発見した．効率的な 6 次ツイスト写像の場合では，ベクトルの移動のみでツイストを行うことができるが，非効率な場合は，ベクトルの移動に加えて，$\mathbb{F}_{p^2}$ における基底の乗算が必要となる．本稿では，埋め込み時数 12 の BN(Barreto-Naehrig) 曲線 [11] において，この定数が逐次拡大体にどう影響を与えているのか，数学的に解明をすることが目的である．そして，効率的な 6 次ツイスト写像となる定数と，非効率なツイスト写像となる定数の判別法を提案する．

2. 準備

2.1 BN 曲線 [11]

BN 曲線は以下のように定義される．

$$E : y^2 = x^3 + b,\ b \in \mathbb{F}_p. \tag{1}$$

素数 p，位数 r，トレース t は次式で与えられる．

$$\begin{aligned} p(\chi) &= 36\chi^4 + 36\chi^3 + 24\chi^2 + 6\chi + 1, \\ r(\chi) &= 36\chi^4 + 36\chi^3 + 18\chi^2 + 6\chi + 1, \\ t(\chi) &= 6\chi^2 + 1. \end{aligned}$$

ただし，χ は整数であり，素数 p，位数 r，トレース t は以下の関係をもつ．

$$r = p + 1 - t. \tag{2}$$

2.2 逐次拡大体 [10]

既約多項式を用いた効率的な拡大体の構成法は，[12] を参照されたい．具体的に，本研究で用いる BN 曲線における 12 次拡大体 $\mathbb{F}_{((p^2)^2)^3}$ は，$\mathbb{F}_{p^2}$，$\mathbb{F}_{p^4}$，$\mathbb{F}_{p^{12}}$ として以下のように構成する．

$$\begin{cases} \mathbb{F}_{p^2} &= \mathbb{F}_p[\alpha]/(\alpha^2 - c),\ \ c \in \mathbb{F}_p, CNR, QNR, \\ \mathbb{F}_{p^4} &= \mathbb{F}_{p^2}[\beta]/(\beta^2 - \alpha), \\ \mathbb{F}_{p^{12}} &= \mathbb{F}_{p^4}[\gamma]/(\gamma^3 - \beta). \end{cases} \tag{3}$$

ここで，α，β，γ は以下の関係をもつ．

$$\alpha = \beta^2 = \gamma^6. \tag{4}$$

これにより構成される $\mathbb{F}_{((p^2)^2)^3}$ の元の基底は以下のようになる．

$$\{1, \alpha, \beta, \alpha\beta, \gamma, \alpha\gamma, \beta\gamma, \alpha\beta\gamma, \gamma^2, \alpha\gamma^2, \beta\gamma^2, \alpha\beta\gamma^2\}. \tag{5}$$

2.3 Ate ペアリング [7]

BN 曲線における ate ペアリングでは，位数 r をもつ 2 つの有理点群 $\mathbb{G}_1$，$\mathbb{G}_2$ を用いて拡大体上の乗法群 $\mathbb{G}_3$ に写像を行う．ここで，$\mathbb{G}_1$，$\mathbb{G}_2$，$\mathbb{G}_3$ は以下のように定義される．

$$\begin{aligned} \mathbb{G}_1 &= E(\mathbb{F}_{p^{12}})[r] \cap \mathrm{Ker}(\pi_p - [1]), \\ \mathbb{G}_2 &= E(\mathbb{F}_{p^{12}})[r] \cap \mathrm{Ker}(\pi_p - [p]), \\ \mathbb{G}_3 &= \mathbb{F}^*_{p^{12}}/(\mathbb{F}^*_{p^{12}})^r. \end{aligned}$$

ここで，π_p は有理点に対する Frobenius 写像であり，$\pi_p : (x, y) \mapsto (x^p, y^p)$ である．ate ペアリング ate は以下により定義される．

$$ate : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_3. \tag{6}$$

BN 曲線では $\mathbb{G}_1$ は $E(\mathbb{F}_p)$ 上の有理点群となる．ある有理点 $P \in \mathbb{G}_1$，$Q \in \mathbb{G}_2$ を使った ate ペアリング $ate(Q, P)$ は以下により与えられる．

$$ate(Q, P) = f_{(t-1),Q}(P)^{\frac{p^{12}-1}{r}}. \tag{7}$$

ここで，$f_{(t-1),Q}(P)$ は Miller のアルゴリズムの出力を表し，これに対して $\frac{p^{12}-1}{r}$ による最終べき乗算を行って，ate ペアリングの結果 $ate(Q, P)$ が得られる．Algorithm 1 に ate ペアリングのアルゴリズムを示す．ここで，$l_{T,T}(P)$, $l_{T,Q}(P)$ は Miller のアルゴリズムの Line 計算を表す．$P = (x_P, y_P) \in \mathbb{G}_1, Q = (x_Q, y_Q) \in \mathbb{G}_2, T = (x_T, y_T)$ とすれば，$l_{T,T}(P)$，$l_{T,Q}(P)$ は以下により与えられる．

$$l_{T,T}(P) = (y_P - y_T) - \frac{3{x_T}^2}{2y_T}(x_P - x_T) \tag{8}$$

$$l_{T,Q}(P) = (y_P - y_Q) - \frac{y_Q - y_T}{x_Q - y_T}(x_P - x_Q) \tag{9}$$

Algorithm 1 Ate pairing over BN curves

Input: $P \in \mathbb{G}_1$, $Q \in \mathbb{G}_2$
Output: $ate(Q, P) \in \mathbb{G}_3$

```
s ← t − 1;
if s < 0 then
    Q ← −Q;
end if
T ← Q, f ← 1;
for i = ⌊log_2 |s|⌋ − 1 downto 0 do
    f ← f^2 · l_{T,T}(P), T ← 2T;
    if s_i = 1 then
        f ← f · l_{T,Q}(P), T ← T + Q;
    end if
end for
f ← f^{(p^12 − 1)/r};
return f;
```

2.4 6 次ツイスト

6 次ツイストは BN 曲線において，平方非剰余かつ三乗非剰余である $\mathbb{F}_{p^2}$ 上の元 z を考える [9]．元の曲線 $E(\mathbb{F}_{p^2}) : y^2 = x^3 + b$ の係数 b にこれを乗じた曲線 $E'(\mathbb{F}_{p^2}) : y^2 = x^3 + bz$ は E と同型であり，$E' \to E$ が 6 次ツイスト写像 ψ に相当する．

$$\begin{aligned} E'(\mathbb{F}_{p^2}) : y^2 = x^3 + bz,\ E(\mathbb{F}_{p^{12}}) : y^2 = x^3 + b, \\ \psi : E'(\mathbb{F}_{p^2}) \to E(\mathbb{F}_{p^{12}}), \\ P'(x, y) \mapsto P(z^{-\frac{1}{3}}x, z^{-\frac{1}{2}}y). \end{aligned} \tag{10}$$

6 次ツイスト写像 ψ は同型写像であるため，写像後の有理点に対して楕円加算，楕円二倍算を行った結果は写像前の有理点に対して行った結果と一対一対応となる．ここで，ate ペアリングに用いる $\mathbb{G}_2$ 上の有理点の x 座標，y 座標である $\mathbb{F}_{((p^2)^2)^3}$ の元は，6 つの $\mathbb{F}_{p^2}$ の元でそれぞれあらわされ，そのうち 5 つの元がそれぞれ 0 である．これに対して 6 次ツイストを用いれば，この $\mathbb{F}_{((p^2)^2)^3}$ の元は真部分群である $\mathbb{F}_{p^2}$ の元に写像することができ，効率的に計算を行うことができる．

2.5 7-sparse 乗算 [13]

Algorithm 1 より，BN 曲線の 7-sparse 乗算における Miller の Line 計算では，計算の効率化のため $\mathbb{F}_{p^2}$ 上の乗算や加算を活用する．ペアリングに使用する有理点 $P = (x_P, y_P) \in \mathbb{G}_1$，$Q = (x_Q, y_Q) \in \mathbb{G}_2$ について，Q に対して 6 次ツイストを用いて $Q' \in \mathbb{G}_2'$ へ写像を行い，写像先の有理点 Q' を $Q' = (x'_Q, y'_Q)$ とする．さらに，$T = (x_T, y_T) \in \mathbb{G}_2$，$T + Q' = (x_{T+Q'}, y_{T+Q'})$，$T + T = (x_{T+T}, y_{T+T})$ とする．$\mathbb{F}_{p^2}$ の元 A〜E を用いれば，式 (8) で与えられる $l_{T,T}(P)$ は以下のように計算できる．

$$\begin{aligned} A = \tfrac{1}{2y_T}, B = 3x_T^2, C = AB, D = 2x_T, x_{T+T} = C^2 - D, \\ E = Cx_T - y_T, y_{T+T} = E - Cx_{T+T}, \\ l_{T,T}(P) = y_P - \theta^{-1}Cx_P\upsilon + \theta^{-1}E\omega. \end{aligned} \tag{11}$$

同様に，式 (9) で与えられる $l_{T,Q}(P)$ は，以下のように計算できる．

$$\begin{aligned} A = \tfrac{1}{x'_Q - x_T}, B = y'_Q - y_T, C = AB, D = x_T + x'_Q, \\ x_{T+Q'} = C^2 - D, E = Cx_T - y_T, y_{T+Q'} = E - Cx_{T+Q'}, \\ l_{T,Q}(P) = y_P - \theta^{-1}Cx_P\upsilon + \theta^{-1}E\omega. \end{aligned} \tag{12}$$

このとき，式 (11)，式 (12) の θ^{-1} の計算については，6 次ツイスト写像の際の基底による計算となる．υ，ω は基底であり，β，γ，$\beta\gamma$，γ^2，$\beta\gamma^2$ のいずれかとなる．

ここで，l，$f \in \mathbb{F}_{p^{12}}$ を定義する．l を Line 計算の結果とし，それぞれ以下のように定める．

$$l = a + b\upsilon + c\omega, \tag{13}$$

$$f = f_0 + f_1\beta + f_2\gamma + f_3\beta\gamma + f_4\gamma^2 + f_5\beta\gamma^2. \tag{14}$$

ただし，a は $\mathbb{F}_p$ の元，b，c，f_0〜f_5 は $\mathbb{F}_{p^2}$ の元である．このとき，7-sparse 乗算 $l \cdot f$ はカラツバ法 [14] を用いれば以下の計算コストで求めることができる．ただし，$\bar{m}$，$\bar{m}_u$，$\bar{a}$，$\bar{\theta}$ はそれぞれ $\mathbb{F}_{p^2}$ における乗算，定数倍算，加算，基底計算であり，n は小さな自然数である．

$$10\bar{m} + 6\bar{m}_u + 17\bar{a} + n\bar{\theta}. \tag{15}$$

2.6 擬似 8-sparse 乗算 [9]

擬似 8-sparse 乗算は 7-sparse 乗算をさらに効率化した計算方法である．式 (11)，式 (12) はどちらも同じような式で表されるため，ここでは $l_{T,T}(P)$ のみを例として説明する．式 (11) の両辺を y_p で割ると以下のようになる．

$$y_p^{-1}l_{T,T}(P) = 1 - \theta^{-1}C(x_p{y_p}^{-1})\upsilon + \theta^{-1}E{y_p}^{-1}\omega. \tag{16}$$

このとき，有理点 $P(x_p, y_p)$ を ${x_p}{y_p}^{-1} = 1$ を満たすような点 $\hat{P}(x_{\hat{p}}, y_{\hat{p}})$ へ写像を行い，この左辺を新たに $\hat{l}_{\hat{T},\hat{T}}(\hat{P})$ とすると，

$$\hat{l}_{\hat{T},\hat{T}}(\hat{P}) = 1 - \theta^{-1}C\upsilon + \theta^{-1}EL\omega. \tag{17}$$

ただし，L は $L = {x_p}^{-3}{y_p}^2$ を満たす．ここで，$\hat{l}$，$f \in \mathbb{F}_{p^{12}}$ を式 (13)，式 (14) のように定義すれば，擬似 8-sparse 乗算 $\hat{l} \cdot f$ は以下の計算コストで求めることができる．

$$10\bar{m} + 17\bar{a} + n\bar{\theta}. \tag{18}$$

3. 2 種類の 6 次ツイスト

3.1 6 次ツイスト曲線

2.1 節で述べた逐次拡大体を使用したとき，$\mathbb{G}_2'$ を含む 6 次ツイスト曲線は $\mathbb{F}_{p^2}$ 上の元 z の選び方によって，以下の 2 種類の曲線のいずれかになる．

$$\bar{E}' : y^2 = x^3 + b\alpha\ (z = \alpha), \tag{19a}$$

$$\bar{E}'' : y^2 = x^3 + b\alpha^5\ (z = \alpha^5). \tag{19b}$$

ここで，α は $\mathbb{F}_{p^2}$ を構成するための既約多項式の根である．それぞれの曲線に対応するツイスト写像先の有理点 $P \in \mathbb{G}_2$ のベクトルは以下のようになる．

$$\bar{P}'(x, y) \mapsto P((0, 0, 0, x_3, 0, 0), (0, y_1, 0, 0, 0, 0)), \tag{20a}$$

$$\bar{P}''(x, y) \mapsto P((0, 0, 0, 0, x_4, 0), (0, y_1, 0, 0, 0, 0)). \tag{20b}$$

ただし，有理点の x 座標，y 座標における $\mathbb{F}_{p^2}$ ベクトルの基底の並びは $\{1, \beta, \gamma, \beta\gamma, \gamma^2, \beta\gamma^2\}$ であり，式 (20a)，式 (20b) の x_3，x_4，y_1 は $\mathbb{F}_{p^2}$ の元である．

3.2 効率的なツイスト曲線と非効率なツイスト曲線

それぞれの 6 次ツイストにかかる計算コストから，どちらがより効率的な 6 次ツイスト曲線なのかを調べる．

3.2.1 $\bar{E}'$ の場合

$\bar{E}'$ をツイスト曲線とする 6 次ツイスト写像を ψ_1 とすると，2.4 節より，ψ_1 は以下のようになる．

$$\psi_1 : \bar{P}'(x, y) \mapsto P(\alpha^{-\frac{1}{3}}x, \alpha^{-\frac{1}{2}}y). \tag{21}$$

P のベクトルについて，これを式 (4) を用いて，以下のように式変形を行う．

$$\begin{aligned} P(\alpha^{-\frac{1}{3}}x, \alpha^{-\frac{1}{2}}y) &= P(\alpha^{-1}\alpha^{\frac{2}{3}}x, \alpha^{-1}\alpha^{\frac{1}{2}}y), \\ &= P((\alpha^{-1}x)\beta\gamma, (\alpha^{-1}y)\beta). \end{aligned} \tag{22}$$

ここで，ツイスト写像先の有理点 $P \in \mathbb{G}_2$ のベクトルは式 (20a) であるから，x 座標の $\beta\gamma$，y 座標の β は写像先の基底であることが分かる．これより，実装上で 6 次ツイストを行う際は，基底を移動させる操作の他に，x ベクトル，y ベクトルに α^{-1} の乗算を行う必要がある．また，このときの Miller のアルゴリズムの Line 計算 $\hat{l}_{\hat{T},\hat{T}}(\hat{P})$ は，式 (17) 以下により与えられる．

$$\hat{l}_{\hat{T},\hat{T}}(\hat{P}) = 1 - (\alpha^{-1})C\beta\gamma^2 + (\alpha^{-1})EL\beta. \tag{23}$$

ここで，$\hat{l}$，$f \in \mathbb{F}_{p^{12}}$ を以下のように定める．

$$\begin{aligned} \hat{l} &= \hat{l}_{\hat{T},\hat{T}}(\hat{P}) = 1 + a\beta + b\beta\gamma^2, \\ f &= f_0 + f_1\beta + f_2\gamma + f_3\beta\gamma + f_4\gamma^2 + f_5\beta\gamma^2. \end{aligned}$$

ただし，a，b，f_0〜f_5 は $\mathbb{F}_{p^2}$ の元である．このとき，これらの擬似 8-sparse 乗算 $\hat{l} \cdot f$ は以下により与えられる．

$$\begin{aligned} \hat{l} \cdot f = &\{f_0 + \alpha(af_1 + bf_2)\} \\ &+ \{f_1 + af_0 + \alpha bf_3\}\beta \\ &+ \{f_2 + \alpha(af_3 + bf_4)\}\gamma \\ &+ \{f_3 + af_2 + \alpha bf_5\}\beta\gamma \\ &+ \{f_4 + \alpha(af_5 + bf_1)\}\gamma^2 \\ &+ \{f_5 + af_4 + bf_0\}\beta\gamma^2. \end{aligned} \tag{24}$$

6 次ツイスト写像に ψ_1 を用いた場合，この計算コストは以下のようになり，式 (18) における n は $n = 5$ となる．

$$10\bar{m} + 17\bar{a} + 5\bar{\alpha}. \tag{25}$$

ただし，$\bar{m}$，$\bar{a}$ は 2.6 節で示したものであり，$\bar{\alpha}$ は $\mathbb{F}_{p^2}$ における基底計算である．

3.2.2 $\bar{E}''$ の場合

$\bar{E}''$ をツイスト曲線とする 6 次ツイスト写像を ψ_2 とすると，2.4 節より，ψ_2 は以下のようになる．

$$\psi_2 : \bar{P}''(x, y) \mapsto P(\alpha^{-\frac{5}{3}}x, \alpha^{-\frac{5}{2}}y). \tag{26}$$

P のベクトルについて，式 (4) を用いて，以下のように式変形を行う．

$$\begin{aligned} P(\alpha^{-\frac{5}{3}}x, \alpha^{-\frac{5}{2}}y) &= P(\alpha^{-2}\alpha^{\frac{1}{3}}x, \alpha^{-3}\alpha^{\frac{1}{2}}y), \\ &= P((\alpha^{-2}x)\gamma^2, (\alpha^{-3}y)\beta). \end{aligned} \tag{27}$$

ここで，ツイスト写像先の有理点 $P \in \mathbb{G}_2$ のベクトルは式 (20b) であるから，x 座標の γ^2，y 座標の β については写像先の基底であることが分かる．さらに，x ベクトルにかかる α^{-2}，y ベクトルにかかる α^{-3} については，楕円加算，楕円二倍算などの結果に影響を与えない．これより，$P((\alpha^{-2}x)\gamma^2, (\alpha^{-3}y)\beta)$ による 6 次ツイストは $P(x\gamma^2, y\beta)$ のようにツイストをしたと考えても影響がないため，6 次ツイスト写像の同型性が保たれる（証明は略す）．このため，実装上では基底を移動させる操作のみで 6 次ツイストを行うことができる．$\bar{E}'$ を使った 6 次ツイスト写像 ψ_1 の場合は基底計算が必要であったが，今回の場合はこれを必要としないため，ψ_2 を用いた 6 次ツイスト写像の方がより効率的である．さらに，このときの Miller のアルゴリズムの Line 計算は以下により与えられる．

$$\hat{l}_{\hat{T},\hat{Q}}(\hat{P}) = 1 - C\gamma + EL\beta. \tag{28}$$

これと式 (23) を比較すれば，基底計算なしで計算を行うことができるため，効率的に Line 計算を行うことができる．ここで，$\hat{l}$，$f \in \mathbb{F}_{p^{12}}$ を以下のように定める．

$$\hat{l} = \hat{l}_{\hat{T},\hat{Q}}(\hat{P}) = 1 + a\beta + b\gamma, \tag{29}$$

$$f = f_0 + f_1\beta + f_2\gamma + f_3\beta\gamma + f_4\gamma^2 + f_5\beta\gamma^2 \tag{30}$$

ただし，a，b，f_0〜f_5 は $\mathbb{F}_{p^2}$ の元である．このとき，擬似 8-sparse 乗算 $\hat{l} \cdot f$ は以下のような式により与えられる．

$$\begin{aligned} \hat{l} \cdot f = &\{f_0 + \alpha(af_1 + bf_5)\} \\ &+ \{f_1 + af_0 + bf_4\}\beta \\ &+ \{f_2 + \alpha af_3 + bf_0\}\gamma \\ &+ \{f_3 + af_2 + bf_1\}\beta\gamma \\ &+ \{f_4 + \alpha af_5 + bf_2)\}\gamma^2 \\ &+ \{f_5 + af_4 + bf_3\}\beta\gamma^2. \end{aligned} \tag{31}$$

6 次ツイスト写像に ψ_1 を用いた場合，この計算コストは以下のようになり，式 (18) における n は $n = 3$ となる．

$$10\bar{m} + 17\bar{a} + 3\bar{\alpha}. \tag{32}$$

式 (25) より，ψ_1 を用いた場合は 5 回の基底計算が必要であったが，ψ_2 の場合では 3 回のみ要する．これより，擬似 8-sparse 乗算においても，ψ_2 を用いた場合の方が効率的に計算を行うことができる．

表 1　ψ_1 と ψ_2 における $\mathbb{F}_{p^2}$ の 6 種類の楕円曲線の位数
Table 1　Comparison the orders of 6 patterns of $\mathbb{F}_{p^2}$ elliptic curves in the case of ψ_1 and ψ_2

	ψ_1(inefficient)	ψ_2(efficient)
$\#E(\mathbb{F}_{p^2})$	p^2+1-t_2	p^2+1-t_2
$\#E'(\mathbb{F}_{p^2})$	$p^2+1+(3f-t_2)/2$	$p^2+1-(3f+t_2)/2$
$\#E''(\mathbb{F}_{p^2})$	$p^2+1+(3f+t_2)/2$	$p^2+1-(3f-t_2)/2$
$\#\acute{E}(\mathbb{F}_{p^2})$	p^2+1+t_2	p^2+1+t_2
$\#\acute{E}'(\mathbb{F}_{p^2})$	$p^2+1-(3f-t_2)/2$	$p^2+1+(3f+t_2)/2$
$\#\acute{E}''(\mathbb{F}_{p^2})$	$p^2+1-(3f+t_2)/2$	$p^2+1+(3f-t_2)/2$

表 2　ψ_1 と ψ_2 における $\mathbb{F}_p$ の 6 種類の楕円曲線の位数
Table 2　Comparison the orders of 6 patterns of $\mathbb{F}_p$ elliptic curves in the case of ψ_1 and ψ_2

	ψ_1(inefficient)	ψ_2(efficient)
$\#E(\mathbb{F}_p)$	$p+1-t$	$p+1-t$
$\#E'(\mathbb{F}_p)$	$p+1+\sqrt{\frac{-3f-t_2+4p}{2}}$	$p+1-\sqrt{\frac{3f-t_2+4p}{2}}$
$\#E''(\mathbb{F}_p)$	$p+1+\sqrt{\frac{3f-t_2+4p}{2}}$	$p+1-\sqrt{\frac{-3f-t_2+4p}{2}}$
$\#\acute{E}(\mathbb{F}_p)$	$p+1+t$	$p+1+t$
$\#\acute{E}'(\mathbb{F}_p)$	$p+1-\sqrt{\frac{-3f-t_2+4p}{2}}$	$p+1+\sqrt{\frac{3f-t_2+4p}{2}}$
$\#\acute{E}''(\mathbb{F}_p)$	$p+1-\sqrt{\frac{3f-t_2+4p}{2}}$	$p+1+\sqrt{\frac{-3f-t_2+4p}{2}}$

3.3　6 次ツイスト写像と曲線の位数の関係

BN 曲線の 6 次ツイスト曲線 E' の位数は以下のいずれかであることが分かっている [7].

$$\#E'(\mathbb{F}_{p^2}) = p^2+1-(-3f+t_2)/2, \tag{33}$$
$$\#E'(\mathbb{F}_{p^2}) = p^2+1-(3f+t_2)/2. \tag{34}$$

ただし，t_2 は $E(\mathbb{F}_{p^2})$ におけるトレースであり，$t_2 = t^2-2p$ を満たす．さらに，f は ${t_2}^2-4p=-3f^2$ を満たす整数である．6 次ツイストによる効率的なペアリングを可能とするツイスト曲線 $E'(\mathbb{F}_{p^2})$ には位数 r の部分群が含まれる必要があるため，$\#E'(\mathbb{F}_{p^2})$ は r で割り切れる必要がある．本稿では f が正の場合についてのみ考える．f が正整数のとき，位数 r は式 (34) を割り切る．これより，このときの 6 次ツイスト曲線の位数は $p^2+1-(3f+t_2)/2$ である．これを元に $\mathbb{F}_{p^2}$ における α を用いた 6 種類の楕円曲線について，ψ_1，ψ_2 それぞれの場合どのような位数パターンをもつか調べた．この 6 種類の曲線を $E(\mathbb{F}_{p^2})$，$E'(\mathbb{F}_{p^2})$，$E''(\mathbb{F}_{p^2})$，$\acute{E}(\mathbb{F}_{p^2})$，$\acute{E}'(\mathbb{F}_{p^2})$，$\acute{E}''(\mathbb{F}_{p^2})$ とし，それぞれ以下のように定義する．

$$E(\mathbb{F}_{p^2}) : y^2 = x^3+b, \tag{35}$$
$$E'(\mathbb{F}_{p^2}) : y^2 = x^3+b\alpha, \tag{36}$$
$$E''(\mathbb{F}_{p^2}) : y^2 = x^3+b\alpha^2, \tag{37}$$
$$\acute{E}(\mathbb{F}_{p^2}) : y^2 = x^3+b\alpha^3, \tag{38}$$
$$\acute{E}'(\mathbb{F}_{p^2}) : y^2 = x^3+b\alpha^4, \tag{39}$$
$$\acute{E}''(\mathbb{F}_{p^2}) : y^2 = x^3+b\alpha^5. \tag{40}$$

この結果を表 1 に示す．この結果より，6 次ツイスト写像が異なれば，その位数パターンは異なることが分かる．　このように，$\mathbb{F}_{p^2}$ においてその楕円曲線の性質が変化するのは，α の性質の違いによるものであると考えられる．ここで，α は $\alpha^2=c$ という関係をもち，c は $\mathbb{F}_{p^2}$ の既約多項式の定数であるため，α の性質の違いはこの c によるものであると考えられる．そこで $\mathbb{F}_p$ において，c を用いた 6 種類の楕円曲線について，同様にどのような位数パターンをもつか調べた．この 6 種類の曲線を $E(\mathbb{F}_p)$，$E'(\mathbb{F}_p)$，$E''(\mathbb{F}_p)$，$\acute{E}(\mathbb{F}_p)$，$\acute{E}'(\mathbb{F}_p)$，$\acute{E}''(\mathbb{F}_p)$ とし，それぞれ以下のように定義する．

$$E(\mathbb{F}_p) : y^2 = x^3+b, \tag{41}$$
$$E'(\mathbb{F}_p) : y^2 = x^3+bc, \tag{42}$$
$$E''(\mathbb{F}_p) : y^2 = x^3+bc^2, \tag{43}$$
$$\acute{E}(\mathbb{F}_p) : y^2 = x^3+bc^3, \tag{44}$$
$$\acute{E}'(\mathbb{F}_p) : y^2 = x^3+bc^4, \tag{45}$$
$$\acute{E}''(\mathbb{F}_p) : y^2 = x^3+bc^5. \tag{46}$$

この結果を表 2 に示す．これについても ψ_1，ψ_2 それぞれで別の位数をパターンをもつことが分かった．曲線 $E'(\mathbb{F}_p)$ の位数に着目すれば，効率的な 6 次ツイスト写像 ψ_2 の場合，その位数 $\#E'(\mathbb{F}_p)$ は $p+1+\sqrt{\frac{-3f-t_2+4p}{2}}$ となるが，非効率な場合では $p+1-\sqrt{\frac{3f-t_2+4p}{2}}$ となる．この結果より，効率的な 6 次ツイストを行うための既約多項式の定数 c が満たすべき条件は，$\#E'(\mathbb{F}_p)$ が $p+1+\sqrt{\frac{-3f-t_2+4p}{2}}$ となることであり，以下で与えられる．

$$E'(\mathbb{F}_p) : y^2 = x^3+bc, \quad P \in E'(\mathbb{F}_p),$$
$$\left[p+1+\sqrt{\frac{-3f-t_2+4p}{2}}\right] P = \mathcal{O}. \tag{47}$$

これより，ある定数 c による 6 次ツイストが効率的なものかどうかの判別は，12 次拡大体 $\mathbb{F}_{((p^2)^2)^3}$ を構成する前に行うことができる．

4.　計算コストの比較

効率的な 6 次ツイストを行った場合と非効率な場合の Miller のアルゴリズムの Line 計算，擬似 8-sparse 乗算の比較を行うため，Line 計算については式 (23)，式 (28)，擬似 8-sparse 乗算については式 (24)，式 (31) について，実際に実装したものを用いて計算コストの比較を行った．効率的な場合と非効率な場合について，いずれについても以下の曲線とパラメータを使用した．なお，χ により生成される素数 p は 462bit である．

$$E : y^2 = x^3+2,$$
$$\chi = 2077172273533976697292497872329739 0.$$

逐次拡大体はセクション 2.2 で述べたものを使用し，効率

表 3　$\mathbb{F}_{p^4}$ と $\mathbb{F}_{p^{12}}$ における乗算と二乗算の計算コスト

Table 3　The multiplication and squaring costs in $\mathbb{F}_{p^4}$ and $\mathbb{F}_{p^{12}}$

	$\mathbb{F}_{p^4}$	$\mathbb{F}_{p^{12}}$
乗算	$3\bar{m}+5\bar{a}+\bar{\alpha}$	$18\bar{m}+60\bar{a}+6\bar{\alpha}$
二乗算	$2\bar{m}+5\bar{a}+2\bar{\alpha}$	$12\bar{m}+43\bar{a}+8\bar{\alpha}$

表 4　ψ_1 と ψ_2 における Line 計算と擬似 8-sparse 乗算の計算コスト

Table 4　The costs of the Line calculation and 8-sparse multiplication in the case of ψ_1 and ψ_2

	efficient	inefficient
$\hat{l}_{\hat{T},\hat{T}}$	$4\bar{m}+2\bar{m}_u+2\bar{s}+5\bar{a}$	$4\bar{m}+2\bar{m}_u+2\bar{s}+5\bar{a}+2\bar{\boldsymbol{\alpha}}$
$\hat{l}_{\hat{T},\hat{Q}}$	$4\bar{m}+2\bar{m}_u+\bar{s}+6\bar{a}$	$4\bar{m}+2\bar{m}_u+\bar{s}+6\bar{a}+2\bar{\boldsymbol{\alpha}}$
8-sparse	$10\bar{m}+17\bar{a}+3\bar{\boldsymbol{\alpha}}$	$10\bar{m}+17\bar{a}+5\bar{\boldsymbol{\alpha}}$

的な場合の c として，式 (47) を満たす $c=2$，非効率な場合にはこれを満たさない $c=23$ を用いた．$\mathbb{F}_{p^4}$，$\mathbb{F}_{p^{12}}$ それぞれにおける乗算，二乗算に要する $\mathbb{F}_{p^2}$ 上の計算コストを表 3 に示す．さらに，効率的な 6 次ツイストを行った場合と非効率な場合の Line 計算 $\hat{l}_{\hat{T},\hat{T}}$，$\hat{l}_{\hat{T},\hat{Q}}$ と，それぞれの擬似 8-sparse 乗算に要する $\mathbb{F}_{p^2}$ 上の計算コストの結果を表 4 に示す．$\bar{m}$ は $\mathbb{F}_{p^2}$ における乗算，$\bar{m}_u$ は定数倍算，$\bar{s}$ は二乗算，$\bar{a}$ は加減算，$\bar{\alpha}$ はそれぞれ基底計算を表す．ここで，基底の乗算 $\bar{\alpha}$ と逆元乗算 $\bar{\alpha}^{-1}$ の計算コストは同じであるため，いずれの計算コストも $\bar{\alpha}$ と表す．また，$\bar{\alpha}$ は $\mathbb{F}_p$ における乗算に相当するものであるため，これを考慮すると，効率的な 6 次ツイストを用いた ate ペアリングの Miller のアルゴリズムでは，およそ 3%の計算効率化を実現することができる．

5. 結論

BN 曲線において，法多項式の定数 c が逐次拡大体にどう影響を与えているのか，数学的な解明を行うことができた．これらを理解することは，最適で効率的な実装を行う上で重要な部分であると考える．また，本稿では BN 曲線のみに着目したが，6 次ツイストを用いるすべての曲線について同様なことが言えると予想される．また，今回は法多項式の定数 c が満たすべき条件として，曲線の位数についての関係式を導出した．しかし，この c の性質を決定づける素数の条件によっても，その判別が可能であると考えている．

参考文献

[1] V. S. Miller. : *Use of elliptic curves in cryptography*, Conference on the Theory and Application of Cryptographic Techniques, pages 417-426. Springer, 1985.

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

[3] R. L. Rivest, A. Shamir, and L. Adlema. : *A method for obtaining digital signatures and public-key cryptosystems*, Communication of the ACM, 21(2) : 120-126, 1978.

[4] R. Sakai. : *Cryptosystems based on pairing*, The 2000 Symposium on Cryptography and Information Security, Okinawa, Japan, Jan, oages 26-28, 2000.

[5] A. Joux. : *A one round protocol for triparite diffie-helman*, International Algorithmic Number Theory Symposium, pages 385-393. Springer, 2000.

[6] D. Boneh, B. Lynn, and H. Shacham. : *Short signatures from the weil pairing*, Cryptologyâ ĂŤASIACRYRT 2001, pages 514-532. Springer, 2001.

[7] F. Hess, N. P. Smart, and F. Vercauteren. : *The Eta-pairing revisited*, IEEE Transactions on Information Theory, 52(10) : 4595-4602, 2006.

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

[9] Y. Nogami, M. Akane, Y. Sakemi, H. Kato, and Y. Morikawa. : *Integer viriable χ-based ate pairing*, International Congerence on Pairing-Based Cryptography, pages 178-191. Springer, 2008.

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

[11] P. S. Barreto and M. Naehrig. : *Pairing-friendly elliptic curves of prime order*, International Workshop pm Selected Areas in Cryptography SAC 2005, pages 319-331. Springer, 2005.

[12] L. C. Washington. : *Elliptic curves: number theory and cryptography*, CRC press, 2008.

[13] D. F. Aranha, K. Karabina, P. Longa, C. H. Gebotys, and J. Lo'pez. : *Faster explicit formulas for computing pairings over ordinary curves*, Eurocrypt, volume 6632, pages 48-68. Springer, 2011.

[14] A. Karatsuba and Y. Ofman. : *Multiplication of many-digital numbers by automatic computers*, DOKLADY AKADEMII NAUK SSSR, vol. 145, no. 2, p. 293, 1962.