社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2006－CSEC－34（3）
2006／7／20

# All One Polynomial Field を用いた MNT曲線に対する Pairing 計算の実装

赤根 正剛† 沖本 卓求弥†† 野上 保之† 森川 良孝†

† 岡山大学大学院自然科学研究科
†† 岡山大学工学部通信ネットワーク工学科
†,†† 〒700-8530 岡山県岡山市津島中 3-1-1
E-mail: †,†† {akane,okimoto,nogami,morikawa}@trans.cne.okayama-u.ac.jp

**あらまし** 近年，Tate pairing や Weil paring などの楕円曲線に関する双線形写像を暗号に応用する研究が盛んに行われている．これらの応用では MNT 曲線と呼ばれる非超特異な楕円曲線を用いるものがある．MNT 曲線の埋め込み次数としては 3 次があるが，拡大体の高速実装法として知られる OEF（Optimal Extension Field）では，MNT 曲線に対する標数の条件から 3 次の OEF を構成することはできない．また，4 次および 6 次の場合についても，MNT 曲線のうち，OEF を構成できるものは限られる．そこで本稿では，MNT 曲線を埋め込む拡大体に AOPF（All One Polynomial Field）を用いて Tate pairing を実装し，その計算時間を示す．さらに，AOPF を用いた場合に Tate pairing を効率よく計算できることを紹介する．

**キーワード** 楕円曲線暗号，pairing，MNT 曲線

# Pairing Computation with MNT Curve over All One Polynomial Field

Masataka AKANE†, Takumi OKIMOTO††, Ysuyuki NOGAMI†, and Yoshitaka MORIKAWA†

† Natural Science and Technology, The Graduate School of Okayama University
†† Department of Communication Network Engineering, Faculty of Engineering, Okayama University
†,†† Tsushimanaka 3-1-1, Okayama, 700-8530 Japan
E-mail: †,†† {akane,okimoto,nogami,morikawa}@trans.cne.okayama-u.ac.jp

**Abstract** In recent years, many cryptographic applications with bilinear-pairing over elliptic curves have been proposed. The well-known MNT curves, that are non-supersingular elliptic curves, provide bilinear-pairings over extension fields of degree 3, 4, and 6. When the embedding degree is equal to 3, MNT curves cannot be defined over optimal extension field (OEF). Even when the embedding degree is equal to 4 or 6, MNT curves cannot be always defined over OEF. For some of such cases, it can be defined over all one polynomial field (AOPF). Since Frobenius mapping can be fast carried out in the AOPFs, this paper gives considered some improvements for Tate pairing calculation. Then, some examples and simulation results are shown.

**Key words** Elliptic Curve Cryptography, pairing, MNT curve

## 1. まえがき

公開鍵暗号方式に関する研究の分野で，RSA 暗号に比べ少ない計算リソースで高い安全性を保証でき，暗号化および復号処理が高速であることから，楕円曲線暗号が注目されている．楕円曲線暗号は，楕円曲線上の離散対数問題（ECDLP）を安全性の根拠として構築する暗号である [1]．ECDLP の解読法 [2] として，楕円曲線に対する Tate pairing や Weil paring などの双線形写像を用いるものがある [3]．これらの双線形写像は，ECDLP を構成する楕円曲線上の有理点群 $E(F_q)$ を，定義体の拡大体 $F_{q^k}$（$k$ は $n \mid (q^k-1)$ を満たす最小の自然数）の乗法群に埋め込む写像である．$k$ を楕円曲線の埋め込み次数とよぶ．これらの双線形写像を用いることで楕円曲線上の ECDLP を $F_{q^k}$ の DLP に置き換えることができる．一般の楕円曲線暗

号では，ECDLP が安全であるために大きな埋め込み次数をもつ楕円曲線が用いられる．

近年，Tate pairing や Weil paring などの楕円曲線に関する双線形写像を利用するアプリケーションとして，グループ[4]署名や ID-base[5] 暗号などが提案されている．これらの応用では先に述べた理由から，所望の埋め込み次数をもつ楕円曲線が必要となる．MNT 曲線という埋め込み次数が 6 次以下の楕円曲線について，MNT 曲線が存在するための条件が示されている[10]．埋め込み次数が 3 次の MNT 曲線については，MNT 曲線上の ECDLP を 3 次の拡大体に埋め込むことになる．このとき，拡大体の高速実装法として知られる OEF（Optimal Extension Field）[6] では，MNT 曲線に対する標数の条件から，3 次の OEF を構成することはできない．埋め込み次数が 4 次および 6 次の場合についても，MNT 曲線のうちで OEF を構成できるものは限られる．

そこで本稿では，MNT 曲線を埋め込む拡大体に AOPF（All One Polynomial Field）[7] を用いる．AOPF は，既約な All One Polynomial（AOP）を法多項式とする拡大体である．AOPF のフロベニアス写像は，AOPF の元が正規基底で表されることを利用して，ベクトル要素の並び替えのみで求めることができる．また，乗算に Cyclic Vector Multiplication Algorithm（CVMA）[7] という高速な演算手法を用いている．本稿では，MNT 曲線を埋め込む拡大体に OEF を構成できない場合でも，AOPF を構成できる場合があることを示す．AOPF を用いた場合に Tate pairing のべき乗計算にフロベニアス写像を適用することで，効率よく計算できることを紹介する．また，埋め込み次数が 4 次および 6 次の MNT 曲線に対して，AOPF を用いて Tate pairing の実装を行い，Tate pairing に要する計算時間を示す．

## 2. 数学的準備

本稿ではとくに説明のない限り，$p$ は素数を表すこととする．$q$ は素数 $p$ のべき乗を表す．$F_p$，$F_{p^k}$ は標数 $p$ の素体とその $k$ 次拡大体を表す．$F_p^*$，$F_{p^k}^*$ はそれぞれ $F_p$，$F_{p^k}$ の乗法群を表す．$a \mid b$ は $a$ が $b$ を割り切ることを表す．

### 2.1 All One Polynomial Field (AOPF)

AOPF は，既約な All One Polynomial（AOP）を法多項式とする拡大体である[7]．AOPF による拡大体の構成は，標数 $p$ と拡大次数 $k$ の条件により，TypeI と TypeII の 2 つに分かれる．それぞれの場合について，AOPF を構成するための要件と，用いる法多項式および基底表現を示す．

**【AOPF TypeI の条件】**

- $k+1$ が素数となる．
- $F_{k+1}$ で $p$ が原始元となる．

**法多項式**

$$\frac{x^{k+1}-1}{x-1} = x^k + x^{k-1} + \cdots + x + 1 \qquad (1)$$

**基底**

法多項式の零点 $\omega$ 用いて，次式で表される基底 TypeI Optimal Normal Basis（ONB）を用いる．

$$\{\omega, \omega^2, \omega^3, \cdots, \omega^m\} \qquad (2a)$$

$$\{\omega, \omega^p, \omega^{p^2}, \cdots, \omega^{p^{k-1}}\} \qquad (2b)$$

式 (2a) と式 (2b) は等価であり，式 (2a) を擬多項式基底，式 (2b) を正規基底とよぶ．

**【AOPF TypeII の条件】**

- $2k+1$ が素数となる．
- 上の条件に加えて，以下の条件のいずれかを満たす．
  - $F_{2k+1}$ で $p$ が原始元となる．
  - $2 \mid (m-1)$ かつ $F_{2k+1}$ で $p$ の位数が $k$ となる．

**法多項式**

$$\frac{x^{2k+1}-1}{x-1} = x^{2k} + x^{2k-1} + \cdots + x^2 + x + 1 \qquad (3)$$

**基底**

$2k$ 次 AOP の零点 $\omega$ を用いて次式で表される基底：TypeII ONB を用いる[8]．

$$\{\omega+\omega^{-1}, \omega^2+\omega^{-2}, \cdots, \omega^k+\omega^{-k}\} \qquad (4a)$$

$$\{\omega+\omega^{-1}, \omega^p+\omega^{-p}, \cdots, \omega^{p^{k-1}}+\omega^{-p^{k-1}}\} \qquad (4b)$$

式 (4a) と式 (4b) は等価である．AOPF TypeII は，$2k$ 次の AOPF TypeI をイメージし，その部分体を利用することで $F_{p^k}$ を構成している．AOPF TypeII は $F_p^k$ での乗算コストを，$k$ に依存する計算オーダーに抑えられる特徴ある．

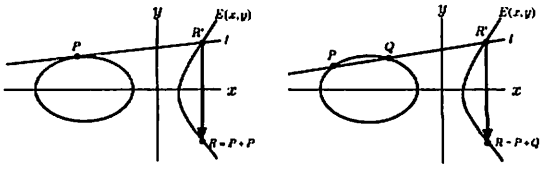
AOPF では，乗算に Cyclic Vector Multiplication Algorithm（CVMA）[7] という高速な演算手法を用い，逆元導出では伊東-辻井 Algorithm（ITA）[9] を用いる．またフロベニアス写像は，AOPF の元が正規基底で表されることを利用して，ベクトル要素の並び替えのみで求めることができる．

### 2.2 楕円曲線

本稿で扱う楕円曲線 $E(x, y)$ は，$F_q$ 上 $(p > 3)$ で定義され，次式で表される．

$$E(x, y) = x^3 + ax + b - y^2 = 0, \quad a, b \in F_q \qquad (5)$$

式 (5) を満足する $(x, y)$ の組と唯一の無限遠点 $\mathcal{O}$ を合わせて，楕円曲線 $E(x, y)$ 上の有理点と呼ぶ．ここで，曲線上のすべての有理点の集合を考え，任意の有理点 $P$，$Q$，$R$ に対して 楕円加算と呼ばれる内部演算 $P+Q=R$ を図 2 のように定義すると，この有理点の集合は可換群をなす．無限遠点 $\mathcal{O}$ は楕円加算の単位元として機能する．有理点 $P$ を $k$ 回足した点 $kP$ を求める計算を楕円スカラー倍算と呼ぶ．この有理点の成す群を利




(a) $P=Q$ の場合　　(b) $P \neq Q$ の場合

図 1 楕円加算

用して構築する暗号が楕円曲線暗号である [1]．楕円曲線暗号では，安全性の観点から素数位数の有理点群が用いられることが多い．素数位数の有理点群では，無限遠点を除く任意の有理点が生成元となる．

### 2.3 楕円曲線の pairing

楕円曲線の定義体を $F_q$ とする．$E_1[n]$ および $E_2[n]$ を，楕円曲線上の素数位数 $n$ の有理点群とする．$^\forall P \in E_1[n]$ および $^\forall Q \in E_2[n]$ は，それぞれ $nP = \mathcal{O}$ および $nQ = \mathcal{O}$ を満たす．$E_1[n] \times E_2[n]$ から，位数 $n$ の乗法に関する巡回群 $K[n]$ への非退化な双線形写像 $\phi$ が存在し，この写像 $\phi$ を pairing とよぶ [3]．

$$e : E_1[n] \times E_2[n] \longrightarrow K[n] \tag{6}$$

また，非退化および双線形であるとは，以下の性質を指す．

- **非退化**

$\mathcal{O}$ を除く $^\forall P \in E_1[n]$ に対して，$\phi(P,Q) \neq 1$ となる $Q \in E_2[n]$ が存在する．また，$\mathcal{O}$ を除く $^\forall Q \in E_2[n]$ に対して，$\phi(P,Q) \neq 1$ となる $P \in E_1[n]$ が存在する．

- **双線形**

$^\forall P, P' \in E_1[n]$ および $^\forall Q, Q' \in E_2[n]$ に対して，次式が成立．

$$\begin{aligned} \phi(P+P',Q) &= \phi(P,Q)\phi(P',Q) \\ \phi(P,Q+Q') &= \phi(P,Q)\phi(P,Q') \end{aligned} \tag{7}$$

### 2.4 因子と有理関数

本節では，pairing の計算に必要となる因子と有理関数について述べる．関数 $f(x,y)=0$ が，楕円曲線 $E(x,y)$ と，$m$ 個の有理点 $P$，$P'$，$P''\cdots$ で交わるとき，関数 $f(x,y)$（以降では $f$ と書く）の因子 $div(f)$ を次のように表す．

$$div(f) = (P) + (P') + (P'') \cdots - m(\mathcal{O}) \tag{8}$$

関数 $f$ をとくに有理関数とよぶ．有理関数 $f$ が定数関数のときは，$div(f)$ を式 (8) の因子の加算法則における零元とする．図 2 に示すように，直線 $l(x,y)=0$ を有理点 $P_1$，$P_2$，$-P_3$ を通る直線とし，直線 $v(x,y)=0$ を有理点 $P_3$，$-P_3$ を通る直線とする．このとき，直線 $l$，$v$ の因子 $div(l)$，$div(v)$ は，次のように表される．

$$\begin{aligned} div(l) &= (P_1) + (P_2) + (-P_3) - 3(\mathcal{O}) \\ div(v) &= (P_3) + (-P_3) - 2(\mathcal{O}) \end{aligned} \tag{9}$$

さらに $div(l/v)$ は，次式で定義される．

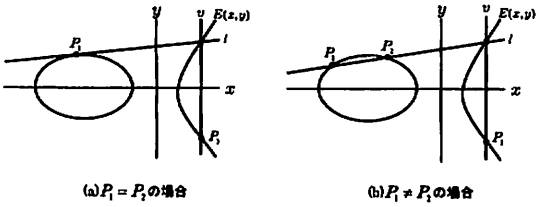



図 2 直線 $l$ と $v$ のイメージ

$$div\left(\frac{l}{v}\right) = div(l) - div(v) = (P_1) + (P_2) - (P_3) - (\mathcal{O}) \tag{10}$$

ここで，2 点 $P_1$，$P_2 \in E[n]$ に対して，ある因子 $D_1$ および $D_2$ が，有理関数 $f_1$ および $f_2$ を用いて次式で表されるとする．

$$\begin{aligned} D_1 &= (P_1) - (\mathcal{O}) + div(f_1) \\ D_2 &= (P_2) - (\mathcal{O}) + div(f_2) \end{aligned} \tag{11}$$

このとき式 (10) から，$D_1 + D_2$ は楕円加算 $P_1 + P_2 = P_3$ を用いて，次のように計算できる．

$$D_1 + D_2 = (P_3) - (\mathcal{O}) + div\left(f_1 f_2 \frac{l}{v}\right) \tag{12}$$

$P_3 = \mathcal{O}$ のときは $v(x,y) = 1$ とする．また，ある因子 $D$ が，有理点 $P \in E[n]$ に対して

$$D = (P) - (\mathcal{O}) = (P) - (\mathcal{O}) + div(1) \tag{13}$$

の形で表されるとき，式 (12) から，

$$nD = (nP) - (\mathcal{O}) + div(f_P) = div(f_P) \tag{14}$$

となる．$nD = div(f_P)$ を，有理点 $P$ の主因子といい，Tate pairing は主因子の有理関数 $f_P$ を用いて定義される．

### 2.5 Tate pairing

$E(F_q)[n]$ は，$F_q$ を定義体とする楕円曲線上の素数位数 $n$ の有理点群とする．$n \mid (q^k - 1)$ を満たす最小の自然数 $k$ を，楕円曲線の埋め込み次数とよぶ．MNT 曲線という埋め込み次数が 6 次以下の楕円曲線について，条件が示されている [10]．$k$ 次埋め込み次数をもつ楕円曲線 $E(F_q)$ の元の個数を $\#E(F_q)$ と書くと，$n^2 \mid \#E(F_{q^k})$ を満たし，$E(F_q)$ は $n$-ねじれ群となる [11]．

Tate pairing は，式 (15) で表される楕円曲線上の有理点群に対する，非退化な双線形写像 $\phi$ で表され，次式で定義される．

$$E_1[n] = E(F_q)[n]\ ,\ E_2[n] = \left(\frac{\#E(F_{q^k})}{n^2}\right) E(F_{q^k}) \tag{15}$$

$$\phi : E_1[n] \times E_2[n] \longrightarrow (F_{q^k}^*)^{(q^k-1)/n} \tag{16}$$

以上のように，楕円曲線 $E(F_q)$ 上の部分群を，Tate pairing を用いて拡大体 $F_{q^k}$ の乗法群へ埋め込むことができる．したがって，楕円曲線 $E(F_q)$ 上の離散対数問題（ECDLP）を，$F_{q^k}^*$ 上の離散対数問題（DLP）に帰着させることができる．これを FR-帰着 [2] といい，ECDLP が安全であるためには，大きな埋め込み次数 $k$ が必要となる．その一方で，Tate pairing などの双線形写像に対して，暗号の安全性の根拠となる楕円双曲線問題（BDHP）が定義される．BDHP に基づく暗号として，グループ署名 [4] や ID-base 暗号 [5] などが考えられている．

## 3. MNT 曲線

埋め込み次数 $k$ をもつ MNT 曲線が存在するためには，$l$ を整数として，定義体の標数 $p$ が表 1 に示す条件を満たさなければならない [10]．

表 1 より，埋め込み次数 $k=3$ のときは，拡大体の高速演

表 1　埋め込み次数 $k$ をもつための標数 $p$ の条件

| 埋め込み次数 $k$ | 標数 $p$ |
|---|---|
| 3 | $12l^2-1$ |
| 4 | $l^2+l+1$ |
| 6 | $4l^2+1$ |

算法として知られている Optimal Extension Field (OEF) [6] を用いて，3 次拡大体 $F_{q^3}$ を構成することはできない(注1)．また，MNT 曲線などの $k \leqq 6$ の小さな埋め込み次数をもつ楕円曲線は，ECDLP の安全性を評価する場合に，写像先の $k$ 次拡大体 $F_{q^k}^*$ 上の DLP についても評価する必要がある．現状，1024 ビットの DLP が安全であるとすれば，例えば $p \simeq 2^{160}$ のとき，埋め込み次数 $k$ が 6 次以上であることが望ましい．しかしながら，例えば，埋め込み次数 $k$ が 6 次の MNT 曲線で，MNT 曲線を埋め込む 6 次拡大体の構成を OEF に限った場合は，標数 $p=36l^2+1$ の条件を満たさなければならず，MNT 曲線を pairing に利用できない場合がある．pairing に利用できる MNT 曲線の数が減ることは大きな問題となる．

そこで本稿では，$k$ 次拡大体 $F_{q^k}$ を OEF を用いて構成できない場合に，拡大体の構成法に AOPF を用いることについて議論する．AOPF では，2.1 章で示した条件を満たすとき，拡大体を構成することができる．また，3 次，4 次，および 6 次拡大体では，AOPF を用いる方が OEF を用いる場合よりも高速に演算が可能である．以降は，4. で AOPF を用いて構成した拡大体上の Tate pairing 計算の高速化を示す．さらに 5. ではシミュレーションを行い，Tate pairing に必要な計算時間の詳細を示す．

## 4. Tate pairing 計算の高速化

本章では，Tate pairing を計算する手順を紹介し，楕円曲線 $E(F_q)$ を埋め込む拡大体に AOPF を用いた場合の，Tate pairing の高速実装について議論する．

### 4.1 Tate pairing の計算

式 (15) で定義した $E_1[n]$ と $E_2[n]$ について，$P \in E_1[n]$, $Q \in E_2[n]$ および $S \in E(F_{q^k})$ とする．Tate pairing $\phi$ は，節 2.4 で述べた主因子の有理関数 $f_P$ を用いて，次式で与えられる．

$$\phi(P,Q)=\left(\frac{f_P(Q+S)}{f_P(S)}\right)^{(q^k-1)/n} \tag{17}$$

式 (17) から，Tate pairing の計算は $f_P(Q+S)/f_P(S)$ の値を計算する部分と，その値を $F_{q^k}$ 上で $(q^k-1)/n$ 乗する部分の大きく 2 つに分けて考えることができる．$f_P(Q+S)/f_P(S)$ の値を計算する代表的なアルゴリズムとして，以下に示す Miller のアルゴリズムが知られている [12]．

上記の Miller のアルゴリズムは，有理点 $P$ に対する楕円曲線上の $n$ 倍算を，バイナリ法を用いて計算する処理に加えて，その過程で得られる直線 $l$ および $v$（もしくはその逆元）を $f$ に掛け込んでいく処理と考えることができる．以降では，NAF

(注1)：OEF で $k$ 次拡大体を構成するための条件は，$k$ の各素因数が $k$ を割り切り，$4 \mid k$ の場合には $4 \mid (p-1)$ でなければならない．

**Miller のアルゴリズム**

入力：位数 $n$，$P \in E_1[n]$, $Q \in E_2[n]$, $S \in E(F_{q^k})$
出力：$f_P(Q+S)/f_P(S)$

1. $T \leftarrow P$.
2. $f \leftarrow 1$.
3. For $i = \lfloor \log_2(n) \rfloor - 1$ to 0:
4. 　$l = (T$ を通る接線$)$ を求める.
5. 　$v = (2T$ を通る垂線$)$ を求める.
6. 　$f \leftarrow f^2 \frac{l(Q+S)v(S)}{v(Q+S)l(S)}$.
7. 　$T \leftarrow 2T$.
8. 　If $(n$ の $i$ ビット目$) == 1$, then:
9. 　　$l = (T$ と $P$ を通る直線$)$ を求める.
10. 　　$v = ((T+P)$ を通る垂線$)$ を求める.
11. 　　$f \leftarrow f \frac{l(Q+S)v(S)}{v(Q+S)l(S)}$.
12. 　　$T \leftarrow T+P$.
13. $f$ を出力.

表現を用いた Miller のアルゴリズムについて示し，$F_{q^k}$ 上での $(q^k-1)/n$ 乗の計算の効率化を行い，AOPF 上で Tate pairing を高速に計算できることを示す．

### 4.2 NAF 表現を用いた Miller のアルゴリズムの実装

本節で示す NAF 表現を用いた Miller のアルゴリズムは，拡大体の構成法に関係なく適用することができる．楕円スカラー倍算の高速化手法として知られている NAF 表現を用いる手法を Miller のアルゴリズムに応用して，$f_P(Q+S)/f_P(S)$ の計算を行った．$n$ に NAF 表現（$n_{(\mathrm{NAF})}$ とする）を応用した Miller のアルゴリズムを以下に示す．

**Miller のアルゴリズム（NAF）**

入力：位数 $n_{(\mathrm{NAF})}$, $P \in E_1[n]$, $Q \in E_2[n]$, $S \in (F_{q^k})$
出力：$f_P(Q+S)/f_P(S)$

1. $T \leftarrow P$.
2. $f \leftarrow 1$.
3. For $i = \lfloor \log_2(n) \rfloor - 1$ to 0:
4. 　$l = (T$ を通る接線$)$ を求める.
5. 　$v = (2T$ を通る垂線$)$ を求める.
6. 　$f \leftarrow f^2 \frac{l(Q+S)v(S)}{v(Q-S)l(S)}$.
7. 　$T \leftarrow 2T$.
8. 　If $(n$ の $i$ ビット目$) == 1$, then:
9. 　　$l = (T$ と $P$ を通る直線$)$ を求める.
10. 　　$v = ((T+P)$ を通る垂線$)$ を求める.
11. 　　$f \leftarrow f \frac{l(Q+S)v(S)}{v(Q+S)l(S)}$.
12. 　　$T \leftarrow T+P$.
13. 　Else If $(n$ の $i$ ビット目$) == -1$, then:
14. 　　$l = (-T$ と $P$ を通る直線$)$ を求める.
15. 　　$v = ((-T+P)$ を通る垂線$)$ を求める.
16. 　　$f \leftarrow f \left(\frac{l(Q+S)v(S)}{v(Q+S)l(S)}\right)^{-1}$.
17. 　　$T \leftarrow -(-T+P)$.
18. $f$ を出力.

$n$ に NAF 表現を用いることで、アルゴリズム中の楕円加算および直線 $l$，$v$ の計算回数を削減することができる．

### 4.3 べき乗計算の高速化

この節では，AOPFにより構成した$k$次拡大体$F_{q^k}$上では，フロベニアス写像を用いることで$(q^k-1)/n$乗を高速に計算できることを示す．

#### 4.3.1 べき数$(q^k-1)/n$の分割

$k=3$，4，6のそれぞれの場合について，$q^k-1$は，円周等分多項式$\Phi_i(x)$（$i$は$k$の約数）の考え方を用いて次のように因数分解できる．$\Phi_i$は$\Phi_i(q)$を表すものとする．

表2 $q^k-1$の因数分解

| $k$ | $q^k-1$ |
|---|---|
| 3 | $\Phi_1\Phi_3=(q-1)(q^2+q+1)$ |
| 4 | $\Phi_1\Phi_2\Phi_4=(q-1)(q+1)(q^2+1)$ |
| 6 | $\Phi_1\Phi_2\Phi_3\Phi_6=(q-1)(q+1)(q^2+q+1)(q^2-q+1)$ |

円周等分多項式$\Phi_i(x)$とは，1の原始$i$乗根を根にもつ多項式である．$k$は2.5節で述べたように，$n \mid (q^k-1)$を満たす最小の自然数であるので，$k$未満の$i$に対して$n \nmid \Phi_i$である．$n \mid \Phi_k$となることを踏まえ，$(q^k-1)/n$は次のように分割して表すことができる．

表3 べき数$(q^k-1)/n$の分割

| $k$ | $(q^k-1)/n$ |
|---|---|
| 3 | $\Phi_1(\Phi_3/n)$ |
| 4 | $\Phi_1\Phi_2(\Phi_4/n)$ |
| 6 | $\Phi_1\Phi_2\Phi_3(\Phi_6/n)$ |

$k$未満の$i$に対して，$\Phi_i$乗の計算は，フロベニアス写像を用いてより高速に求めることができる．したがって，$\Phi_k/n$乗のみバイナリ法で計算する．以上で示したべき数$(q^k-1)/n$の分割により，$(q^k-1)/n$乗のべき乗算は，$k=3$，4，6で$\log_2 n \simeq \log_2 q$の場合，乗算回数をおよそ$1/(k-1)$に削減できる．また，$\Phi_k/n \gg p$の場合は，残りの$\Phi_k/n$乗の計算もべき数$\Phi_k/n$を$p$進数展開することで，フロベニアス写像を用いて効率よく求めることができる(注2)．

#### 4.3.2 べき数の$p$進数展開

べき数の$p$進数展開によるべき乗算の高速化は，$\Phi_k/n \gg p$の場合に適用できる．したがって$\Phi_k$が高次の場合，すなわち$k>6$の場合に効果が大きい．本稿では，主に埋め込み次数$k \leq 6$をもつ楕円曲線を扱ってきたが，このときは逆にべき数の$p$進数展開によるべき乗算の高速化は期待できない．

べき数の$p$進数展開によるべき乗算の高速化が有効な具体例を挙げると，例えば標数が素数$p$で埋め込み次数$k=10$のとき，$\Phi_{10}=p^5+1$となり，べき数$(p^5+1)/n$に$p$進数展開を用いると，$F_{p^{10}}$上の乗算回数は，およそ$\log_2(p^5/n)+(1/2)\log_2(p^5/n)$から$\log_2(p)+(1/2)\log_2(p^5/n)$に削減できる．よって$\log_2 n \simeq \log_2 p$の場合，べき数の$p$進数展開を用いることで，乗算回数はおよそ以下のようになる．

$$\frac{\log_2 p+(1/2)\log_2 p^4}{\log_2 p^4+(1/2)\log_2 p^4}=\frac{1}{2} \tag{18}$$

(注2)：OEFの場合は，フロベニアス写像に$k-1$回の素体上乗算が必要となる．

## 5. Tate pairingの計算時間の比較

本章では，AOPFを用いたTate pairing計算について，前章までに示した高速化手法を計算機上でシミュレーションし，計算速度を比較する．埋め込み次数$k=4$および6をもつ楕円曲線について，C++言語および多倍長精度整数ライブラリNTL[13]を用いてシミュレーションを行った．それぞれの場合について，素体および$E(F_q)[n]$を埋め込む拡大体での，乗算，逆元導出，楕円二倍算，楕円加算にかかる計算時間と，Tate pairing計算の各処理にかかる計算時間の比較を表4および表5に示す．

表4 埋め込み次数$k=4$のpairing計算時間[ms]と改善率

| $p=10933556345464879933385093918889135651143077946340745101826820311753$ (223bit)<br>$n=201525155822534945453377050718944 17$ (114bit)<br>$y^2=x^3+5x+4813872554411403340911170262491796550812896720816470940343015274537$ | | |
|---|---|---|
| $\{F_p$ / $F_{p^4}\}$上の乗算（1回の時間） | | .00095 / .0202 |
| $\{F_p$ / $F_{p^4}\}$上の逆元導出 | | .00775 / .292 |
| $\{F_p$ / $F_{p^4}\}$上の楕円二倍算 | | .0276 / .448 |
| $\{F_p$ / $F_{p^4}\}$上の楕円加算 | | .0243 / .397 |
| STEP1 | Millerのアルゴリズム | 22.6 |
| | Millerのアルゴリズム（NAF） | 20.4 |
| | 改善率 | 9.7 % |
| STEP2 | $(q^4-1)/n$乗の計算 | 24.5 |
| | $(q^4-1)/n$乗を分割して計算 | 10.5 |
| | 改善率 | 57.1 % |
| TOTAL | Tate pairingの計算時間（改善前） | 47.1 |
| | Tate pairingの計算時間（改善後） | 30.9 |
| | 改善率 | 34.4 % |

表5 埋め込み次数$k=6$のpairing計算時間[ms]と改善率

| $p=53956142377615320457340076010631315$<br>$18176979226056449333636374498577$ (216bit)<br>$n=83100839305506782443$ (67bit)<br>$y^2=x^3+x+4089434746397824212251439024848984821143404203093761965873012641 6$ | | |
|---|---|---|
| $\{F_p$ / $F_{p^6}\}$上の乗算（1回の時間） | | .00105 / .0433 |
| $\{F_p$ / $F_{p^6}\}$上の逆元導出 | | .00755 / .415 |
| $\{F_p$ / $F_{p^6}\}$上の楕円二倍算 | | .0328 / .669 |
| $\{F_p$ / $F_{p^6}\}$上の楕円加算 | | .0290 / .566 |
| STEP1 | Millerのアルゴリズム | 23.1 |
| | Millerのアルゴリズム（NAF） | 20.3 |
| | 改善率 | 12.1 % |
| STEP2 | $(q^6-1)/n$乗の計算 | 80.1 |
| | $(q^6-1)/n$乗を分割して計算 | 24.1 |
| | 改善率 | 69.9 % |
| TOTAL | Tate pairingの計算時間（改善前） | 103.2 |
| | Tate pairingの計算時間（改善後） | 44.4 |
| | 改善率 | 57.0 % |

C++言語，NTL，Pentium4 (3.8GHz)

STEP2 のべき数を分割して計算した場合に，STEP2 の処理時間が $k=4$ の場合は約 57%，$k=6$ の場合は約 70%改善された．すなわち，AOPF を用いることで Tate pairing を効率よく計算することができる．また，今回シミュレーションに利用した楕円曲線は，定義体の標数 $p$ に対し $n$ のビット数が小さいため，Tate pairing 計算全体のうちで STEP1（Miller のアルゴリズム）の占める割合が小さいが，$\log_2 n \simeq \log_2 p$ の場合は，STEP1 の割合が大きくなり，NAF 表現を用いる高速化の効果がより大きくなると考えられる．今後は定義体の標数 $p$ に対して，$n$ が同じぐらいのビット数となる MNT 曲線を，効率よく生成することが課題であると言える．

## 6. ま と め

本稿では，MNT 曲線を埋め込む拡大体に All One Polynomial Field（AOPF）を用いることを提案した．また，AOPF を用いて MNT 曲線に対する Tate pairing 計算の実装を行い，処理時間の比較を示した．さらに，AOPF を用いた場合，Tate pairing を効率よく計算できることを示した．

## 文　献


[1] I.Blake, G.Seroussi, and N.Smart, Elliptic Curve in Cryptography, LNS 265, Cambridge University Press, 1999.

[2] G. Frey and H. G.Ruck, "A remark concerning $m$-divisibility and the discrete logarithm in the divisor class group of curves", Mathmatics of computation, 62(1994), pp.865-874.

[3] Henri Cohen, Gerhard Frey, Roberto Avanzi, "Handbook of Elliptic and Hyperelliptic Curve Crytography: Theory and Practice (Discrete Mathematics and Its Applications)", 2004.

[4] T.Nakanishi and N.Funabiki "Verifier-Local Revocation Group Signature Schemes with Backward Unlinkability from Bilinear Maps", In ASIACRYPT 2005, LNCS 3788, Springer Verlag, pp.533-548, December 2005.

[5] D.Boneh and M.Franklin "Identity based encryption from the Weil Pairing, "Proc. of Crypto2001, LNCS 2139, Springer-Verlag, pp.213-229, 2001.

[6] D.Bailey and C.paar, "Optimal Extension Fields for Fast Arithmetic on Public-Key Algorithms," Proc.Crypto'98, Springer LNCS, vol.1462, pp.472-485, 1998.

[7] Y.Nogami, A.Saito, and Y.Morikawa, "Finite Extension Field with Modulus of All-One Polynomial and Representation of Its Elements for Fast Arithmetic Operations," Trans. IEICE, vol.E86-A, no.9, p.2376-2387, 2003.

[8] Y.Nogami, S.Shinonaga, Y.Morikawa, "Fast Implementation of Extension Fields with TypeII ONB and Cyclic Vector Multiplication Algorithm," Trans. IEICE, vol.E88-A, no.5, p.1200-1208, 2005.

[9] 伊東利哉，辻井重男，"正規基底を用いた有限体における高速逆元算出アルゴリズム"，信学論 (A), vol.J70-A, no11, pp.1637-1645, 1987.

[10] A.Miyaji, M.Nakabayashi and S.Takano, "New explicit conditions of Elliptic Curve Traces under FR-reduction", IEICE Trans., Fundamentals. vol. E84-A, No.5(2001), pp.1234-1243.

[11] R.Balasubramanian and N.Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm. Journal of Cryptology, 11(2):pp.141-145,1998.

[12] S.D.Galbraith, K.Harrison, and D.Soldera, "Implemeting the Tate pairing", ANTS V, LNCS 2369, pp.324-337, Springer-Verlag, 2002.

[13] A Library for doing Number Theory. http://www.shoup.net/ntl/