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

2006－CSEC－34（1）
2006／7／20

Optimal Normal Basis を経由する同型な拡大体間の基底変換行列の構成法

難波 諒† 野上 保之† 森川 良孝†

† 岡山大学大学院自然科学研究科
〒700-8530 岡山県岡山市津島中 3-1-1
E-mail: †{nanba,nogami,morikawa}@trans.cne.okayama-u.ac.jp

あらまし 楕円曲線暗号や XTR 暗号の定義体として，高速実装に適した拡大体が提案されている．これら拡大体はある特定の既約多項式や基底を採用することで高速実装を図っている．このため，それらの同型な拡大体においては同一元のベクトル表現が異なる．本稿ではこのベクトル表現が異なる元の対応をとる手段として，TypeI Optimal Normal Basis (ONB) を経由して基底を変換する行列を得る手法を提案する．TypeI ONB は正規基底をなす元の集合であり，それらの位数は等しく，加えてそれらの最小多項式は既約 All One Polynomial (AOP) であるという性質をもつため，乗法に関する位数という特徴のみを用いて同型な拡大体間の元と元の対応を与えることができる．この性質により，TypeI ONB が基底変換に適していることを説明し，TypeI ONB を経由して基底変換行列を得る手法を具体例とともに紹介する．最後にシミュレーションを行い，生成時間についても検討する．

キーワード 公開鍵暗号，有限体，TypeI Optimal Normal Basis，基底変換

A Translation Matrix between Two Isomorphic Extension Fields via Optimal Normal Basis Representation

Ryo NAMBA†, Yasuyuki NOGAMI†, and Yoshitaka MORIKAWA†

† Natural Science and Technology, The Graduate School of Okayama University,
3-1-1, Tsushima-naka, Okayama, 700-8530, Japan
E-mail: †{nanba,nogami,morikawa}@trans.cne.okayama-u.ac.jp

Abstract Some extension fields efficient for fast implementation have been proposed. Such extension fields adopt unique modular polynomial and basis. Therefore, an element can have some different vector representations in the isomorphic extension fields. This paper proposes a method for generating a basis translation matrix between two isomorphic extension fields. First, this paper shows that the translation matrix can be obtained via TypeI Optimal Normal Basis (ONB). TypeI ONB plays key role since it has the following properties; TypeI ONB is a set of conjugate elements and of course a normal basis, these conjugates have the same order, they are zeros of a certain irreducible all one polynomial. Then, some examples of translation matrix are shown. From the experimental result, it is shown that the proposed method is enough practical.

Key words public key cryptography, finite field, TypeI Optimal Normal Basis, basis translation

1. まえがき

楕円曲線暗号 [1] や XTR 暗号 [2] は有限体を定義体とする．これらの暗号を高速に実装するには定義体上の演算を高速に実装することが効果的である．ソフトウェア実装の観点からいえば，定義体を拡大体として，その標数をワード長未満として実装するのがよい [3]．近年，ソフトウェア実装に適した拡大体が提案されている．Optimal Extension Field (OEF) は法多項式に既約 2 項式を採用し [4]，All One Polynomial Field (AOPF) は法多項式に既約 All One Polynomial を採用する [5]．

これら拡大体は特定の法多項式・基底を採用し，その効果を活かすために，条件に特化したプログラムライブラリが提供される．ライブラリ内部での元の表現はその拡大体が採用する基底に依存し，同型な拡大体間の同一な元であっても，表現が異

なる．その一方で，同型な定義体間において複数の拡大体をともに用いることが効果的となるアプリケーションもある．例えば，XTR 暗号への電力解析に対して基底を変換し，攻撃を回避する手法が提案されており [6]，このような場合，同型な拡大体間で相互にベクトル表現を変換できなければならない．本稿では TypeI Optimal Normal Basis (ONB) を経由して基底を変換する行列を得る手法を提案する．

まず，第 2 章では拡大体と基底について復習する．とくに TypeI ONB の性質は重要となるので詳しく述べる．TypeI ONB は正規基底をなす元の集合であり，それらの位数は等しく，加えてそれらの最小多項式は既約 All One Polynomial (AOP) であるという性質をもつため，乗法に関する位数という特徴のみを用いて同型な拡大体間の元と元の対応を与えることができる．ゆえに，この性質が基底変換に適している理由について説明する．第 3 章では，TypeI ONB のこれらの性質を使って基底変換行列を得る手法を紹介する．第 4 章では理解を深めるために，基底変換を具体的な例を挙げて説明する．第 5 章では基底変換行列を生成するシミュレーションを行い，生成時間についても検討する．

本稿では，とくに断らない限り，p および，m を素数 (標数) および，正の整数とし，F_p および，F_{p^m} は素体およびその m 次拡大体を表わす．a，A などのアルファベットはそれぞれ素体，拡大体上の元とする．同型な拡大体間の関係を考えるため，$\hat{A} \in \hat{F}_{p^m}$ のようにアクセントを付して表記された元 $\hat{A}$ は $\hat{F}_{p^m}$ が採用する基底によりそのベクトル表現が与えられる元として考える．また，A^T はベクトル A の転置ベクトルを意味し，α のようなギリシャ文字は法多項式の零点を示す．

2. 数学的準備

本節では，拡大体，多項式基底，TypeI Optimal Normal Basis (ONB) について復習する．また，高速実装可能な拡大体として All One Polynomial Field (AOPF)，Optimal Extension Field (OEF) を紹介する．

2.1 拡大体と基底

F_p 上の m 次ベクトル空間である拡大体 F_{p^m} 上の演算は，F_p 上の m 次既約多項式 $f(x)$ を法として定義される．$f(x)$ の零点を α として，次式の基底を与えることができる．

$$\{1, \alpha, \alpha^2, \cdots, \alpha^{m-1}\} \tag{1}$$

この基底を多項式基底と呼び，任意の元 $A \in F_{p^m}$ は式 (1) の基底によるベクトル表現として次のように表すことができる．

$$A = a_1 + a_2\alpha + \cdots + a_m\alpha^{m-1} \tag{2}$$

拡大体上の演算は $f(x)$ の根 α が満たす関係 $f(\alpha) = 0$ を法として定義され，$f(x)$ を法多項式と呼ぶ．

式 (1) の基底をシフトして与えられる式 (3) の元の集合も基底をなし，これを擬多項式基底と呼ぶこととする．

$$\{\alpha, \alpha^2, \alpha^3, \cdots, \alpha^m\} \tag{3}$$

また，式 (4) の零点 α の共役元の集合が基底をなすとき，この基底は正規基底と呼ばれる．正規基底を元の表現に用いた場合，Frobenius 写像 $A \rightarrow A^p$ を高速に行うことができる．

$$\{\alpha, \alpha^p, \alpha^{p^2}, \cdots, \alpha^{p^{m-1}}\} \tag{4}$$

2.2 TypeI Optimal Normal Basis

式 (5) を F_p 上で既約な m 次の All One Polynomial (AOP) とし，その零点を β とする．

$$(x^{m+1} - 1)/(x - 1) = x^m + x^{m-1} + \cdots + x + 1 \tag{5}$$

All One Polynomial の F_p 上の既約性は容易に判別することができる [7]．この AOP の零点 $\beta \in F_{p^m}$ は式 (6) のように正規基底をなし，擬多項式基底と等価となる．

$$\{\beta, \beta^p, \beta^{p^2}, \cdots, \beta^{p^{m-1}}\} = \{\beta, \beta^2, \beta^3, \cdots, \beta^m\} \tag{6}$$

正規基底は Frobenius 写像を用いた逆元演算，擬多項式基底は乗算の高速実装に効果的な基底であるため，その 2 つが等価となるこの基底は拡大体 F_{p^m} の実装に適している．この基底を TypeI Optimal Normal Basis (ONB) と呼ぶ [5]．ただし，次の定理から拡大次数 m は偶数でなければならない．

【定理 1】TypeI ONB が F_{p^m} に存在する必要十分条件は，$m+1$ が素数であり，F_{m+1} 上で p の位数が m となることである．

また，TypeI ONB をなす m 個の元の位数は式 (5) よりすべて $m+1$ となり，定理 1 の条件から位数が $m+1$ となる元は TypeI ONB をなす m 個の元以外に存在しない．この事実から以下に TypeI ONB の性質としてまとめておく．

【性質 1】定理 1 の条件を満たす F_{p^m} 上で位数が $m+1$ となる m 個の元の集合は必ず TypeI ONB である．

TypeI ONB をなす元の集合は，性質 1 より位数という特徴のみを用いて一意に識別することができる．本稿で述べる基底変換は，この TypeI ONB の特徴を同型な拡大体の基底間での対応を得るために利用する．

2.3 TypeI All One Polynomial Field

著者らは，TypeI All One Polynomial Field (AOPF) という拡大体を提案した [5]．TypeI AOPF は All One Polynomal を法多項式に採用し，その零点がなす TypeI ONB を基底として用いる．また，擬多項式基底を考慮した Cyclic Vector Multiplication Algorithm (CVMA) [5] を乗算アルゴリズムとして採用することにより，高速実装を実現している．ただし，基底に TypeI ONB を採用しているため，標数 p と拡大次数 m が定理 1 の条件を満たす必要がある．

2.4 Optimal Extension Field

Bailey らは Optimal Extension Field (OEF) と呼ばれる拡大体を提案した [4]．OEF は既約 2 項式 $f(x) = x^m - c$ を法多項式として採用し，その多項式基底を用いる．これは高速実装に効果的であるが，このような既約 2 項式が F_p 上に存在するためには定理 2 を満たす必要がある．

表 1　OEF と TypeI AOPF の比較

	OEF	TypeI AOPF
既約多項式	既約 2 項式 $x^m - c$	All One Polynomial $(x^{m+1}-1)/(x-1)$
基底	多項式基底 $\{1, \alpha, \alpha^2, \cdots, \alpha^{m-1}\}$	TypeI ONB $\{\beta, \beta^p, \beta^{p^2}, \cdots, \beta^{p^m-1}\}$ $= \{\beta, \beta^2, \beta^3, \cdots, \beta^m\}$
条件	定理 2	定理 1

【定理 2】F_p 上で既約な 2 項式 $f(x) = x^m - c$ が存在するための必要十分条件は m の任意の素因数が $p-1$ を割り切ることである．ただし，m を 4 が割り切るときには，$p-1$ が 4 が割り切れなければならない．[8].

OEF は高速実装に効果的であり，基底変換の対象として有用である．また，後述する基底変換の具体例においても法多項式が 2 項式であるため，検算が容易である．表 1 に OEF，TypeI AOPF の相違点を示す．

本稿で示す基底変換は，TypeI ONB の性質 1 を利用するため，TypeI ONB が存在する拡大体と同型な拡大体間の元の変換を対象とする．つまり，定理 1 を満たす拡大体 F_{p^m} が基底変換の対象となる．

本稿の手法は TypeI AOPF と同型な拡大体間での基底変換を実現するが，定理 1 の条件は OEF の構成条件である定理 2 と異なるため，TypeI ONB が存在しない OEF に対しては基底変換を実現できない．しかし，定理 1，定理 2 を同時に満たす標数 p，拡大次数 m の組も存在し，その条件を満たす同型な OEF，TypeI AOPF 間での基底変換は可能である．

2.5　拡大体の表記法と元の区別

素体 F_p 上の元は扱いを簡単にするため，通常 0 から $p-1$ の整数を用いて式 (7) のように表記する．

$$F_p = \{0, 1, 2, \cdots, p-1\} \tag{7}$$

この表記は元の加法による情報も記述している．理解を簡単にするために，例として F_7 を考えれば，F_7 の原始元 (乗法群の生成元) を g とすれば F_7 は式 (8) のようにも表記できる．

$$F_7 = \{0, g, g^2, \cdots, g^6 = 1\} \tag{8}$$

式 (7) の表記では F_7 の原始元は 3，5 であり，単位元 1 の和の個数により $3 = 1+1+1$，$5 = 1+1+1+1+1$ というように区別され，表記に加法的な元の特徴が含まれていると言える．一方，式 (8) の表記では $g = 3$ であるか，$g = 5$ であるか記述できず，加法に関する特徴が損なわれていると言える．

一方，拡大体 F_{p^m} の元すべてを列挙しようとしたとき，式 (7) のように加法の情報も記述することはできない．また，加法の情報によりすべての元を列挙することはできず，乗法に関する情報を用いて式 (8) のように原始元 g を用いて記述することになる．

$$F_{p^m} = \{0, g, g^2, \cdots, g^{p^m-1} = 1\} \tag{9}$$

したがって，加法による情報から同型な拡大体間の元の対応を考えることはむずかしく，乗法の特徴 (位数) から対応を与えることが現実的である．しかし，TypeI ONB をなす元以外の元から対応を得ることは困難である．なぜなら，TypeI ONB をなすは乗法に関する位数という特徴のみを用いて同型な拡大体間の元と元の対応を与えることができるからである．

例として，法多項式 x^2+1，その零点 α がなす多項式基底 $\{1, \alpha\}$ を採用する $\hat{F}_{3^2}$，法多項式 x^2+2x+2，その零点 β がなす多項式基底 $\{1, \beta\}$ を採用する $\hat{F}_{3^2}$ を考える．このとき β の位数は 8 であるが，$\hat{F}_{3^2}$ 上に位数 8 となる元は複数存在する．β を $\hat{F}_{3^2}$ 上の位数 8 の元 $\alpha+1$ との対応をとり，$\beta = \alpha+1$ とするとこれは誤りである．なぜなら，$\alpha+1$ の最小多項式は $M_{\alpha+1}(x) = x^2+x+2$ であり，$\beta \neq \alpha+1$ であることがわかる．正しくは $\beta = \alpha+2$，もしくは $\beta = 2\alpha+2$ のように対応をとらなければならない．

このように加法的な元の特徴を記述できる素体 F_p 上の元を係数にもつ最小多項式を確認しなければ，同型な拡大体上の元の対応を得ることはできない．すなわち，"位数 8 である元は区別がつく" のである．

これに対して TypeI ONB をなす元はすべて位数が $m+1$ であり，その最小多項式は既約 AOP となるため，区別がつかない．この特徴は位数 $m+1$ の元と他の元との対応に位数という特徴のみを用いればよいことを意味する．

3.　基底変換行列の生成法

標数 p，拡大次数 m が定理 1 の条件を満たす同型な拡大体 $\hat{F}_{p^m}$ と $\hat{F}_{p^m}$ 関係を考える．このとき，式 (6) の TypeI ONB を基底として用いた拡大体 F_{p^m} も構成することができる．m 次既約 AOP の零点 β は性質 1 より位数が $m+1$ であり，$\beta^{m+1} = 1$ を満たす(注1)．また，F_{p^m} と同型である $\hat{F}_{p^m}$，$\hat{F}_{p^m}$ にも位数 $m+1$ となる m 個の元が存在する．

非零元 $\hat{B} \in \hat{F}_{p^m}$ が式 (10) を満たすとき，

$$\hat{B}^{(p^m-1)/(m+1)} \neq 1 \tag{10}$$

$$\left(\hat{B}^{(p^m-1)/(m+1)}\right)^{m+1} = \hat{B}^{p^m-1} = 1 \tag{11}$$

式 (11) より，$\hat{B}^{(p^m-1)/(m+1)}$ は位数が $m+1$ となり(注2)，2.5 節の議論より，これは TypeI ONB をなす元 β の $\hat{F}_{p^m}$ における表現 $\hat{\beta}$ を得たことになる．任意の非零元 $\hat{B}$ が式 (10) を満たす確率はほぼ $m/(m+1)$ で与えられるため，容易に $\hat{F}_{p^m}$ 上の $\hat{B}^{(p^m-1)/(m+1)}$ を β として与えることができる．したがって，式 (12) の m 個の 1 対 1 対応の関係として，TypeI ONB $\{\beta, \beta^2, \cdots, \beta^m\}$ の $\hat{F}_{p^m}$ の基底による表現を導くことができる．ただし，議論を簡単にするために $\hat{F}_{p^m}$ は多項式基底を採用しているものとする．

(注1)：定理 1 を満たす場合，F_{p^m} の乗法群の位数 p^m-1 は $m+1$ で割り切れる [8].

(注2)：定理 1 より $m+1$ は素数であり，位数が $m+1$ の約数となることはない．

$$\hat{\beta} = \hat{B}^{(p^m-1)/(m+1)}$$
$$= b_{11} + b_{12}\alpha + \cdots + b_{1m}\alpha^{m-1} \quad (12a)$$
$$\hat{\beta}^2 = \left(\hat{B}^{(p^m-1)/(m+1)}\right)^2$$
$$= b_{21} + b_{22}\alpha + \cdots + b_{2m}\alpha^{m-1} \quad (12b)$$
$$\vdots$$
$$\hat{\beta}^m = \left(\hat{B}^{(p^m-1)/(m+1)}\right)^m$$
$$= b_{m1} + b_{m2}\alpha + \cdots + b_{mm}\alpha^{m-1} \quad (12c)$$

$\{\hat{\beta}, \hat{\beta}^2, \cdots, \hat{\beta}^m\}$ は F_{p^m} が採用する TypeI ONB と一致するため，式(12)の等式から $\hat{C} \in \hat{F}_{p^m}$ と $A \in F_{p^m}$ に対して $\hat{C}^T = \hat{M}A^T$ を満たすベクトル表現を変換する式(13b)の行列 $\hat{M}$ が与えられる．また，逆変換行列 $\hat{M}^{-1}$ も与えられる．

$$\hat{F}_{p^m} \underset{\hat{M}}{\overset{\hat{M}^{-1}}{\rightleftharpoons}} F_{p^m} \quad (13a)$$

$$\hat{M} = \begin{pmatrix} b_{11} & b_{21} & \cdots & b_{m1} \\ b_{12} & b_{22} & \cdots & b_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ b_{1m} & b_{2m} & \cdots & b_{mm} \end{pmatrix} \quad (13b)$$

$$\hat{M}^{-1} = \begin{pmatrix} b_{11} & b_{21} & \cdots & b_{m1} \\ b_{12} & b_{22} & \cdots & b_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ b_{1m} & b_{2m} & \cdots & b_{mm} \end{pmatrix}^{-1} \quad (13c)$$

式(1)の多項式基底をなす元の位数はそれぞれ異なり得る．同型な拡大体上で $\alpha^i|_{i=1,2,\cdots,m-1}$ と同じ位数をもつ元は複数存在し，2.5 節の議論から同じ位数の元の区別がつくため 1 対 1 の対応を得ることができない．一方，TypeI ONB をなす元は位数がともに $m+1$ と等しく，その位数をもつ拡大体の元は m 個のみであり，正規基底をなす共役元として存在する．したがって，必ず同型な拡大体上の位数が $m+1$ となる元との対応を m 個の元の組として一意に定めることが可能となる(注3)．このため，変換行列生成に TypeI ONB をなす元の対応を利用する．$\hat{M}$ を得るアルゴリズムは図 1 となる．ただし，$\hat{B} = [b_i]$, $\hat{C} = [c_i]$, $\hat{M} = [b_{ij}]$ のようにベクトル，行列の要素は小文字と添字により表記する．

同様にすれば，$\tilde{F}_{p^m}$ 上の元のベクトル表現を F_{p^m} 上のベクトル表現に変換する変換行列 $\tilde{M}$ とその逆変換行列 $\tilde{M}^{-1}$ も与えられる．

$$\tilde{F}_{p^m} \underset{\tilde{M}}{\overset{\tilde{M}^{-1}}{\rightleftharpoons}} F_{p^m} \quad (14)$$

(注3)：式(10)により得られる β によって TypeI AOPF 上のベクトルの要素の順が異なることがあるが，2.5 節の議論から β に区別はないため，TypeI AOPF の構成に問題はなく 1 対 1 の対応を得ることができる．

基底変換行列導出アルゴリズム

入力：m 次既約多項式 $f(x)$
出力：法多項式 $f(x)$，多項式基底による拡大体を $\hat{F}_{p^m}$ として，TypeI AOPF 上の元を $\hat{F}_{p^m}$ 上の元に写像する行列 $\hat{M}$

1. $\hat{B} \in \hat{F}_{p^m}$ をランダムな非零元とする．
2. $\hat{B} \leftarrow \hat{B}^{(p^m-1)/(m+1)}$ とし，$\hat{B}$ が 1 ならば 1. へ戻る．
3. $\hat{C} \leftarrow \hat{B}$, $i \leftarrow 1$ とする．
4. $i = m+1$ ならば終了．
5. $j \leftarrow 1$ とする．
6. $j = m+1$ ならば 9. へ進む．
7. $b_{ji} \leftarrow b_j$.
8. $j \leftarrow j+1$ として 6. へ戻る．
9. $\hat{B} \leftarrow \hat{B}\hat{C}$.
10. $i \leftarrow i+1$ として 4. へ戻る．

図 1　基底変換行列導出アルゴリズム

その結果，TypeI ONB を経由することで，任意の多項式基底による拡大体 $\hat{F}_{p^m}$, $\tilde{F}_{p^m}$ のベクトル表現を変換する行列 $\tilde{M}\hat{M}^{-1}$, $\hat{M}\tilde{M}^{-1}$ を得ることができる．

$$\hat{F}_{p^m} \underset{\hat{M}\tilde{M}^{-1}}{\overset{\tilde{M}\hat{M}^{-1}}{\rightleftharpoons}} \tilde{F}_{p^m} \quad (15)$$

これら $\tilde{M}\hat{M}^{-1}$, $\hat{M}\tilde{M}^{-1}$ を乗じる写像は同型写像となる．

4. 基底変換の例

本節では基底変換の具体的な例を与える．$p = 13$, $m = 4$ として 2 つの同型な拡大体 F_{13^4} と $\hat{F}_{13^4}$ を考える．F_{13^4} は法多項式に 2 次既約 AOP $x^4 + x^3 + x^2 + x + 1$，基底として以下の TypeI ONB を採用する．

$$\{\beta, \beta^2, \beta^3, \beta^4\} = \{\beta, \beta^7, \beta^{7^3}, \beta^{7^2}\} \quad (16)$$

β は法多項式 $x^4 + x^3 + x^2 + x + 1$ の零点であり，位数は 5 である．また，$\hat{F}_{13^4}$ は既約 2 項式 $\hat{f}(x) = x^4 - 2$ を法多項式とし，その零点 α による多項式基底 $\{1, \alpha, \alpha^2, \alpha^3\}$ を採用する(注4)．α は $\alpha^4 = 2$ を満たすため，α の位数は 48 となる．

$$\alpha^{48} = 2^{12} = 1 \quad (17)$$

このとき，式(18)を用いて，式(10)を満たす非零元 $\hat{B}$ を探さなければならない．

$$(p^m - 1)/(m+1) = (13^4 - 1)/5 = 5712 \quad (18)$$

式(17)と $48 \mid 5712$ から，零点 α は式(10)を満たさない．しかし，$1+\alpha$ は式(10)の条件を満たし，以下の関係式が得られる．

$$\begin{aligned} \hat{\beta} &= (1+\alpha)^{5712} = 3 + 11\alpha + 9\alpha^2 + 8\alpha^3 \\ \hat{\beta}^2 &= \{(1+\alpha)^{5712}\}^2 = 3 + 3\alpha + 4\alpha^2 + 12\alpha^3 \\ \hat{\beta}^3 &= \{(1+\alpha)^{5712}\}^3 = 3 + 10\alpha + 4\alpha^2 + \alpha^3 \\ \hat{\beta}^4 &= \{(1+\alpha)^{5712}\}^4 = 3 + 2\alpha + 9\alpha^2 + 5\alpha^3 \end{aligned} \quad (19)$$

(注4)：この拡大体は OEF の一例である．

式(19)から，基底変換行列 $\hat{M}$ とその逆変換行列 $\hat{M}^{-1}$ を以下のように得る．

$$\hat{M} = \begin{pmatrix} 3 & 3 & 3 & 3 \\ 11 & 3 & 10 & 2 \\ 9 & 4 & 4 & 9 \\ 8 & 12 & 1 & 5 \end{pmatrix} \tag{20a}$$

$$\hat{M}^{-1} = \begin{pmatrix} 12 & 8 & 4 & 11 \\ 12 & 12 & 9 & 3 \\ 12 & 1 & 9 & 10 \\ 12 & 5 & 4 & 2 \end{pmatrix} \tag{20b}$$

さらに，もう一つの同型な拡大体 $\tilde{F}_{13^4}$ を考える．$\tilde{F}_{13^4}$ には法多項式として既約2項式 $\tilde{f}(x) = x^4 - 6$ を採用し，その零点 α' による多項式基底を用いる．式(19)と同様に考え，次式を得る．

$$\begin{aligned} \tilde{\beta} &= (1+\alpha')^{5712} = 3 + 5\alpha' + \alpha'^2 + 5\alpha'^3 \\ \tilde{\beta}^2 &= \{(1+\alpha')^{5712}\}^2 = 3 + 12\alpha' + 12\alpha'^2 + \alpha'^3 \\ \tilde{\beta}^3 &= \{(1+\alpha')^{5712}\}^3 = 3 + \alpha' + 12\alpha'^2 + 12\alpha'^3 \\ \tilde{\beta}^4 &= \{(1+\alpha')^{5712}\}^4 = 3 + 8\alpha' + \alpha'^2 + 8\alpha'^3 \end{aligned} \tag{21}$$

F_{13^4} と $\tilde{F}_{13^4}$ の基底変換行列 $\tilde{M}$ とその逆変換行列 $\tilde{M}^{-1}$ は以下のようになる．

$$\tilde{M} = \begin{pmatrix} 3 & 3 & 3 & 3 \\ 5 & 12 & 1 & 8 \\ 1 & 12 & 12 & 1 \\ 5 & 1 & 12 & 8 \end{pmatrix} \tag{22a}$$

$$\tilde{M}^{-1} = \begin{pmatrix} 12 & 2 & 10 & 2 \\ 12 & 3 & 3 & 10 \\ 12 & 10 & 3 & 3 \\ 12 & 11 & 10 & 11 \end{pmatrix} \tag{22b}$$

これらの結果から $\hat{F}_{13^4}$ と $\tilde{F}_{13^4}$ の基底を変換する行列 $\tilde{M}\hat{M}^{-1}$, $\hat{M}\tilde{M}^{-1}$ が与えられる．

$$\tilde{M}\hat{M}^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 12 \end{pmatrix} \tag{23a}$$

$$\hat{M}\tilde{M}^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 10 & 0 & 0 \\ 0 & 0 & 9 & 0 \\ 0 & 0 & 0 & 12 \end{pmatrix} \tag{23b}$$

また，β が式(24)のように与えられても基底変換行列とそれに対応する逆変換行列を用いれば，$\hat{F}_{13^4}$, $\tilde{F}_{13^4}$ の拡大体の基底は相互に変換できる．なぜなら，β の共役元はそれぞれを区別することはできないからである[注3]．このことから TypeI AOPF 上のベクトルの要素の順番を問題にしなければ基底変換行列を生成できる．

$$\begin{aligned} \tilde{\beta} &= (2+\alpha')^{5712} = 3 + 12\alpha' + 12\alpha'^2 + \alpha'^3 \\ \tilde{\beta}^2 &= \{(2+\alpha')^{5712}\}^2 = 3 + 8\alpha' + \alpha'^2 + 8\alpha'^3 \\ \tilde{\beta}^3 &= \{(2+\alpha')^{5712}\}^3 = 3 + 5\alpha' + \alpha'^2 + 5\alpha'^3 \\ \tilde{\beta}^4 &= \{(2+\alpha')^{5712}\}^4 = 3 + \alpha' + 12\alpha'^2 + 12\alpha'^3 \end{aligned} \tag{24}$$

式(24)を採用すれば，$\tilde{M}, \tilde{M}^{-1}$ は以下のように与えられる．

$$\tilde{M} = \begin{pmatrix} 3 & 3 & 3 & 3 \\ 12 & 8 & 5 & 1 \\ 12 & 1 & 1 & 12 \\ 1 & 8 & 5 & 12 \end{pmatrix} \tag{25a}$$

$$\tilde{M}^{-1} = \begin{pmatrix} 12 & 3 & 3 & 10 \\ 12 & 11 & 10 & 11 \\ 12 & 2 & 10 & 2 \\ 12 & 10 & 3 & 3 \end{pmatrix} \tag{25b}$$

この場合の $\tilde{M}\hat{M}^{-1}$, $\hat{M}\tilde{M}^{-1}$ は以下のように与えられる．

$$\tilde{M}\hat{M}^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 7 & 0 & 0 \\ 0 & 0 & 10 & 0 \\ 0 & 0 & 0 & 5 \end{pmatrix} \tag{26a}$$

$$\hat{M}\tilde{M}^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 8 \end{pmatrix} \tag{26b}$$

これらの $\tilde{M}\hat{M}^{-1}$, $\hat{M}\tilde{M}^{-1}$ を用いて，$\hat{F}_{13^4}$ 上の元と $\tilde{F}_{13^4}$ 上の元のベクトル表現を相互に変換できる．これらの行列を乗ずる写像は同型写像である．以下の $\hat{F}_{13^4}$ 上の元に対して，式(26)の基底変換を考える．

$$\hat{X} = 1 + \alpha + \alpha^2 + \alpha^3 \tag{27a}$$

$$\hat{Y} = 2 + 2\alpha + 2\alpha^2 + 2\alpha^3 \tag{27b}$$

$$\hat{X} \cdot \hat{Y} = \hat{Z} = 1 + 12\alpha + 10\alpha^2 + 8\alpha^3 \tag{27c}$$

式(26)の行列を乗じて，$\tilde{F}_{13^4}$ 上の表現を得る．

$$\tilde{X} = \{\tilde{M}\hat{M}^{-1}\hat{X}^T\}^T = 1 + 7\alpha' + 10\alpha'^2 + 5\alpha'^3 \tag{28a}$$

$$\tilde{Y} = \{\tilde{M}\hat{M}^{-1}\hat{X}^T\}^T = 2 + \alpha' + 7\alpha'^2 + 10\alpha'^3 \tag{28b}$$

$$\tilde{X} \cdot \tilde{Y} = \tilde{Z} = 1 + 6\alpha' + 9\alpha'^2 + \alpha'^3 \tag{28c}$$

この $\tilde{Z}$ に $\hat{M}\tilde{M}^{-1}$ を乗じたものは式(29)のように $\hat{Z}$ となり，同型写像であることが確認できた．式(23)を用いても同様に同型写像となる．

$$\hat{Z} = \{\hat{M}\tilde{M}^{-1}\tilde{Z}^T\}^T = 1 + 12\alpha + 10\alpha^2 + 8\alpha^3 \tag{29}$$

また，式(23a)，式(26a)から零点 α，α' の関係が導ける．

$$\alpha = 4\alpha' \quad \text{or} \quad \alpha = 7\alpha' \tag{30}$$

これは以下の既約多項式の関係からも類推できるが，$\hat{f}(x)$, $\tilde{f}(x)$

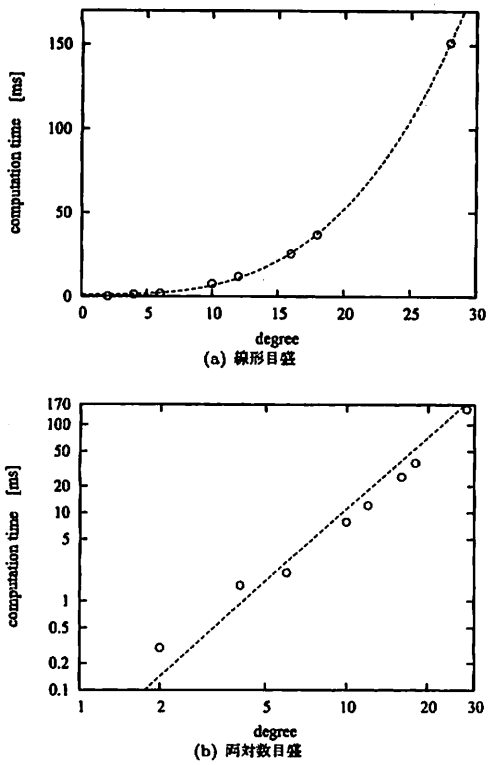

図 2 基底変換行列の生成処理時間
($\log_2 p \fallingdotseq 32$, Pentium4 3.6GHz)

が 2 項式でない場合，類推することは難しい．

$$\hat{f}(4x) = (4x)^4 - 2 = 9x^4 - 2 = 9(x^4 - 6) = 9\tilde{f}(x) \quad (31a)$$

$$\hat{f}(7x) = (7x)^4 - 2 = 9x^4 - 2 = 9(x^4 - 6) = 9\tilde{f}(x) \quad (31b)$$

実際に $\hat{F}_{13^4}$, $\tilde{F}_{13^4}$ が採用する法多項式を $x^4 + 9x^3 + 11x^2 + 10x + 12$, $x^4 + x^3 + 7x^2 + 7x + 6$ とすると基底変換行列は以下のようになる．

$$\tilde{M}\hat{M}^{-1} = \begin{pmatrix} 1 & 2 & 2 & 3 \\ 0 & 0 & 2 & 3 \\ 0 & 2 & 5 & 2 \\ 0 & 4 & 12 & 3 \end{pmatrix} \quad (32a)$$

$$\hat{M}\tilde{M}^{-1} = \begin{pmatrix} 1 & 5 & 6 & 3 \\ 0 & 10 & 10 & 5 \\ 0 & 5 & 9 & 2 \\ 0 & 10 & 7 & 3 \end{pmatrix} \quad (32b)$$

5. 計算機シミュレーション

基底変換行列を実際に計算機で生成する際の計算時間を図 2 に示す．図 2 での基底変換行列の生成時間とは TypeI AOPF F_{p^m} と同型な拡大体 $\hat{F}_{p^m}$ の基底変換行列の組 $\hat{M}$, $\hat{M}^{-1}$ の生成に要する時間を表す．標数 p は 32 ビットのランダムな素数，拡大体 $\hat{F}_{p^m}$ が採用する法多項式もランダムとして，各次数に対し 100 回の基底変換行列の生成を行い，処理時間の平均値をグラフに示したものである．ただし，標数 p と拡大次数 m は定理 1 を満たす必要がある．シミュレーションプログラムは，Linux 上で C++言語，多倍長演算ライブラリ NTL [9] を用いて作成した．シミュレーションを行った計算機の CPU は Pentium4 3.6GHz である．図 2 から，基底変換の計算量は m^3 に比例するといえる．

公開鍵暗号の定義体として位数が 1000 ビット程度となる拡大体は標数 p が 32 ビットであれば 30 次程度となる．この結果から，30 次程度の拡大体に対して，ほぼ 200 ms で基底変換行列を生成可能であり，実際に基底変換行列と既約多項式の組をアプリケーションの前計算として用いることは可能である．

6. むすび

本稿では TypeI ONB を経由することで，2 つの同型な拡大体間の異なる基底で表現された元を相互に変換する行列を得る手法を提案した．まず，拡大体と基底について復習した．その後，TypeI ONB の特徴が基底変換行列の生成に必要な m 個の対応関係を得る点で適した基底であることを用い，基底変換行列を生成する手法を示した．その特徴とは Type I ONB をなす元がすべて位数 $m+1$ であり，位数 $m+1$ となる元は拡大体 F_{p^m} 上に m 個のみ存在するというものであった．また，基底変換行列の生成法とともにその具体例とシミュレーション結果も示した．

文献

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

[2] A.Lenstra, E.Verheul, "The XTR public key system," Advances in Cryptology - Proc.Crypto'00 , pp.1-19, Springer, 2000.

[3] K.Aoki, K.Okeya, T.Kobayashi, Y.Sakai, K.Takashima, T.Tsurumaru, G.Yamamoto, H.Yoshida, and D.Watanabe, "Optimaization of prime field mutiplication using redundant representation", SCIS 2004, 3A3-5, 2004.

[4] 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.

[5] 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, pp.2376-2387, 2003.

[6] D.G.Han, T.Izu, J.Lim, K.Sakurai, "Side Channel Cryptoanalysis on XTR Public Key Cryptosystem," Trans. IEICE, vol.E88-A, no.5, pp.1214-1223, 2005.

[7] T.Sugimura and Y.Suetsugu, "Consideration on cyclotomic Plynomials," Trans. IEICE, vol.J73-A, no.12, pp.1929-1935, 1990.

[8] R.Lidl and H.Niederreiter, Finite Fields, Encyclopedia of Mathematics and Its Applications, Cambridge University Press, 1984.

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