3 変数 Matsumoto-Imai 中間写像の従順性について

伯田 恵輔 †*　　佐藤 尚宜 †　　高木 剛 ‡

†(株) 日立製作所 横浜研究所
244-0817 神奈川県横浜市戸塚区吉田町 292 番地
keisuke.hakuta.cw@hitachi.com, hisayoshi.sato.th@hitachi.com

*九州大学大学院 数理学府
819-0395 福岡県福岡市西区元岡 744 番地
k-hakuta@math.kyushu-u.ac.jp

‡ 九州大学マス・フォア・インダストリ研究所
819-0395 福岡県福岡市西区元岡 744 番地
takagi@imi.kyushu-u.ac.jp

あらまし 多変数公開鍵暗号の中には, 特殊な性質をもつ多変数連立方程式を利用する方式があり, この特殊な多変数連立方程式から得られる代数構造によって脆弱性が報告されている方式もある. そのような例の一つとして tame 多項式同型写像の分解問題 (Tame 分解問題) の困難性に基づく Tame transformation method (TTM 方式) が知られている. 本稿では, TTM 方式以外の多変数公開鍵暗号に対する tame 分解の可否を検討するための第一歩として, Matsumoto-Imai 暗号に焦点を当て, 標数 2 の素体上定義された 3 変数 Matsumoto-Imai 中間写像が tame 多項式同型写像であることを証明する. また, その分解を具体的に示す.

On Tameness of Matsumoto-Imai Central Maps with Three Variables

Keisuke Hakuta†*　　Hisayoshi Sato†　　Tsuyoshi Takagi‡

†Hitachi, Ltd., Yokohama Research Laboratory
292, Yoshida-cho, Totsuka-ku, Yokohama, 244-0817, JAPAN
keisuke.hakuta.cw@hitachi.com, hisayoshi.sato.th@hitachi.com

*Graduate School of Mathematics, Kyushu University
744, Motooka, Nishi-ku, Fukuoka, 819-0395, JAPAN
k-hakuta@math.kyushu-u.ac.jp

‡Institute of Mathematics for Industry, Kyushu University
744, Motooka, Nishi-ku, Fukuoka, Fukuoka, 819-0395, JAPAN
takagi@imi.kyushu-u.ac.jp

Abstract Many multivariate public key cryptosystems (MPKC) use special polynomial maps. Unfortunatery, several schemes of them were successfully attacked due to unexpected algebraic properties. One such example is tame transformation method (TTM). The security of TTM is based on the intractability of tame decomposition problem. In this paper, as a first step to consider whether or not a public key map can be decomposed as a composition of affine automorphisms and triangular automorphisms for each MPKC, we focus on Matsumoto-Imai cryptosystems. We prove that the Matsumoto-Imai central maps with three variables over $\mathbb{F}_2$ is tame, and we describe the decomposition of each Matsumoto-Imai central map.

1 はじめに

ランダムに選択された多変数連立方程式の求解問題はNP完全であることが知られている (cf. [6, p.251], [14, pp.20–21])). 多変数公開鍵暗号は多変数連立方程式の求解問題に安全性の根拠を置いており (cf. [8]), 量子計算機による攻撃に耐性を持つことが期待される公開鍵暗号である. しかしながら, 多変数公開鍵暗号で利用される多変数連立方程式は一般にはランダムに選択されるとは限らず, なかには特殊な性質をもつ多変数連立方程式を利用する方式もある. そのため, ランダムに選択された多変数連立方程式の求解問題の困難性と多変数公開鍵暗号で利用される多変数連立方程式の求解問題の困難性にはギャップがある. 実際, いくつかの多変数公開鍵暗号方式についてはその脆弱性が指摘されている (cf. [2], [1], [5], [12], [13]). そのため, 安全性評価は重要な課題であり, 多変数公開鍵暗号における中心的な研究テーマのひとつである.

多変数公開鍵暗号の実現方法のひとつである Tame Transformation Method (TTM 方式) (cf. [9], [10]) では, 逆写像を効率的に計算できる複数個の多項式写像 (後述するアフィン多項式自己同型写像, triangular 多項式自己同型写像) の合成写像を公開鍵とし, 元の複数個の各々の多項式写像を秘密鍵とする. したがって TTM 方式が安全であるための必要条件は合成された多項式写像から元の複数個の多項式写像に分解する問題の困難性である. 本稿ではこの問題を **Tame Decomposition Problem (以下, Tame 分解問題)** と呼ぶことにする. 3 変数以上の多項式環における上述の分解方法は一般には知られておらず, Tame 分解問題は, 上記の複数個の多項式写像をランダムに選択した場合は困難であると考えられている ([10, p.668]).

一般に多変数公開鍵暗号は特殊な性質をもつ多項式写像を利用しており, TTM 方式も特殊な性質をもつ多項式写像が利用されている. そのため, 代数構造のような望まれない性質を持ってしまい, その望まれない性質によって脆弱性が報告されていることがある (cf. [2], [1], [5], [12], [13]).

本稿では, TTM 方式以外の多変数公開鍵暗号方式に対する Tame 分解によって安全性評価にアプローチする. 上述したように, 多変数公開鍵暗号で利用する多項式自己同型写像は特殊な形の多項式である. 仮に, ある多変数公開鍵暗号方式で利用する公開鍵に対して Tame 分解問題を効率的に計算可能であるとするならば, その多変数公開鍵暗号方式は安全性を確保することはできない, と言える. したがって, 多変数公開鍵暗号方式で利用される特殊な多項式自己同型写像に対する Tame 分解問題は多変数公開鍵暗号の安全性評価において重要なアプローチとなり得る. ところが, TTM 方式以外の多変数公開鍵暗号方式では, 公開鍵が Tame 分解可能な写像か否かについては知られていない[1] . 一般に, 与えられた多項式同型写像が Tame 分解可能か否かを決定する問題はアフィン代数幾何の中心的な研究テーマであり, 変数の個数が少ない場合 (e.g., 3) であっても未解決な問題 (またはすでに解決されているが, 長年の間未解決であった問題[2]) がいくつか知られている.

上記の背景を鑑み, 本稿では多変数公開鍵暗号のひとつである Matsumoto-Imai 暗号に対して公開鍵の Tame 分解の可否を考察し, 有限体 $\mathbb{F}_2$ 上定義された 3 変数 Matsumoto-Imai 中間写像が tame 多項式自己同型写像であることを示す. また, その分解を具体的に示す.

2 記号

k を体, $n \in \mathbb{N} := \{1, 2, \ldots, \}$ を自然数, $X_1, \ldots, X_n$ を不定元とし, $A_n := k[X_1, \ldots, X_n]$ を n 変数多項式環とする. $\mathbb{A}_k^n$ を k 上の n 次元アフィン空間とする. また, 可逆な多項式写像全体の集合を $\mathrm{Aut}_k A_n$ とかく.

$\mathbb{F}_q$ を要素数 q の有限体とし, $\{\beta_1, \ldots, \beta_n\}$ を, $\mathbb{F}_{q^n}$ の $\mathbb{F}_q$-線形空間としての基底とする. $\mathbb{A}_k^n$ か

[1] ただし, $\mathbb{A}_{\mathbb{F}_q}^n$ から $\mathbb{A}_{\mathbb{F}_q}^n$ への多項式同型写像を置換とみなすことにすると, この置換がある種の条件を満たす場合に限り, その多項式同型写像が tame 多項式同型写像か否かを判定することができる [7, Theorem 2.3].

[2] このような例の一つとして, Nagata automorphism が知られている [11, Conjecture 3.1, Part 2].

ら $\mathbb{F}_{q^n}$ への $\mathbb{F}_q$-線形空間としての写像を

$$\begin{array}{rccc} \phi: & \mathbb{A}_k^n & \to & \mathbb{F}_{q^n} \\ & \cup & & \cup \\ & (x_1,\ldots,x_n) & \mapsto & x_1\beta_1+\cdots+x_n\beta_n \end{array}$$

とかく. ϕ の逆写像は

$$\begin{array}{rccc} \phi^{-1}: & \mathbb{F}_{q^n} & \to & \mathbb{A}_k^n \\ & \cup & & \cup \\ & x_1\beta_1+\cdots+x_n\beta_n & \mapsto & (x_1,\ldots,x_n) \end{array}$$

である.

また, 次の形の多項式自己同型写像 $J_{a,f}$

$$\begin{aligned} J_{a,f} = (&a_1X_1+f_1(X_2,\ldots,X_n), a_2X_2 \\ &+f_2(X_3,\ldots,X_n),\ldots,a_nX_n+f_n), \\ &a_i\in k\ (i=1,\ldots,n), \\ f_i\in k[X_{i+1},\ldots,X_n]&\ (i=1,\ldots,n-1),\ f_n\in k \end{aligned}$$

は de Jonquières 多項式自己同型写像 (または triangular 多項式自己同型写像) と呼ばれており, 定義から明らかに多項式自己同型写像である. 上で定義した $J_{a,f}$ 全体の集合を $J(k,n)$ とかくことにする:

$$\begin{aligned} J(k,n) := \{&J_{a,f}\in \mathrm{Aut}_k\, A_n | a_i\in k \\ &(i=1,\ldots,n), f_i\in k[X_{i+1},\ldots,X_n] \\ &(i=1,\ldots,n-1),\ f_n\in k\}. \end{aligned}$$

$T(k,n) := \langle \mathrm{Aff}(k,n), J(k,n)\rangle$ とおく. $T(k,n)$ の元は tame 多項式自己同型写像とよばれる. 上記定義より, $J(k,n)$ は $\mathrm{Aut}_k\, A_n$ の部分群であり, また, $J(k,n)$ は $T(k,n)$ の部分群である (cf. [4, p.85]).

以後, 不定元の個数 $n=3$ の場合は, 簡単のため X_1,X_2,X_3 を $X:=X_1$, $Y:=X_2$, $Z:=X_3$ とかくことにする. 不定元 X, Y, Z には $\mathbb{F}_q$ の元のみ代入するため, 各不定元は $X_i^q = X_i$ $(i=1,\ldots,n)$ なる関係を持つとする. すなわち, n 変数多項式環 $\mathbb{F}_q[X_1,\ldots,X_n]$ を直接考えるのではなく, n 変数多項式環のイデアル $I=(X_1^q-X_1,\ldots,X_n^q-X_n)$ による剰余環 $\mathbb{F}_q[X_1,\ldots,X_n]/I$ を考える. そして, 多項式同型写像に関する群は剰余環の元として考えることにする. $\bar{X_i} := X_i \bmod I$ $(i=1,\ldots,n)$ とおくと, $\mathbb{F}_q[X_1,\ldots,X_n]/I \simeq \mathbb{F}_q[\bar{X_1},\ldots,\bar{X_n}]$ である.

3 多変数公開鍵暗号の代表的な方式

本章では, 多変数公開鍵暗号の代表的な方式として, TTM 方式および Matsumoto-Imai 暗号方式の概要を述べる.

3.1 Tame Transformation Method

TTM 方式は Moh によって提案された多変数公開鍵暗号である ([9], [10]). ここでは, TTM 方式の概要を述べる. なお, ここでは概要を述べることを目的としているため, [3, pp.139–140] に沿って TTM 方式を説明する. Moh が提案した実際の TTM 方式 とは異なることに注意されたい.

TTM 方式では, ユーザ A は有限個の de Jonquières 写像 $G_1,\ldots,G_l\in T(k,n)$ を選び, それらの合成写像 $G_1\circ\cdots\circ G_l$ を F とおく. そして, 合成写像 $F=(f_1,\ldots,f_n)$ $(f_i\in A_n,\ i=1,\ldots,n)$ をユーザ A の公開鍵とし, $G_1,\ldots,G_l$ はユーザ A の秘密鍵とする. ユーザ A とは異なるユーザ B が, 平文 $(x_1,\ldots,x_n)\in \mathbb{A}_{\mathbb{F}_q}^n$ をユーザ A の公開鍵 F で暗号化する場合は $(y_1,\ldots,y_n) = (f_1(x_1,\ldots,x_n),\ldots,f_n(x_1,\ldots,x_n))$ を計算し, 計算結果である $(y_1,\ldots,y_n)$ を暗号文とする. そして, 暗号文 $(y_1,\ldots,y_n)$ をユーザ A に送る. ユーザ A が暗号文 $(y_1,\ldots,y_n)$ を復号する場合は自身の秘密鍵 $G_1,\ldots,G_l$ を用いて $(x_1',\ldots,x_n') = ({G_l}^{-1}\circ\cdots\circ{G_1}^{-1})(y_1,\ldots,y_n)$ を計算し, $(x_1',\ldots,x_n')$ を復号文とする.

TTM 方式の鍵ペア生成, 暗号化, 復号化をアルゴリズムとして以下に記述する.

Algorithm 1 TTM 方式の鍵ペア生成

Input: l

Output: (pk, sk)

1: Select l tame automorphisms $G_1,\ldots,G_l\in T(\mathbb{F}_q,n)$
2: Compute $F\leftarrow G_1\circ\cdots\circ G_l\in T(\mathbb{F}_q,n)$
3: $pk\leftarrow F$, $sk\leftarrow\{G_1,\ldots,G_l\}$
4: **return** (pk,sk)

Algorithm 2 TTM 方式の暗号化

Input: 平文 $(x_1, \ldots, x_n)$,
公開鍵 $pk = F = (f_1, \ldots, f_n)$
Output: 暗号文 $(y_1, \ldots, y_n)$
1: Compute $(y_1, \ldots, y_n)$
$= (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n))$
2: **return** $(y_1, \ldots, y_n)$

Algorithm 3 TTM 方式の復号

Input: 暗号文 $(y_1, \ldots, y_n)$,
秘密鍵 $sk = \{G_1, \ldots, G_l\}$
Output: 平文 $(x_1, \ldots, x_n)$
1: Compute $(x_1, \ldots, x_n)$
$= ({G_l}^{-1} \circ \cdots \circ {G_1}^{-1})(y_1, \ldots, y_n)$
2: **return** $(x'_1, \ldots, x'_n)$

ユーザ B が通信路経由でユーザ A に送信する際に暗号文が第三者によって改ざんされていなければユーザ A は正しい平文を得ることができる (すなわち, $(x'_1, \ldots, x'_n) = (x_1, \ldots, x_n)$ が成り立つ). また, ユーザ A が復号処理を行えるのは, $G_1, \ldots, G_l \in T(k, n)$ であることによる. TTM 方式は, 合成写像 F が与えられたときに, その逆写像 F^{-1} を効率的に計算することが困難であること, および合成写像 F を tame 自己同型多項式写像 $G_1, \ldots, G_l$ に分解することが困難であること, を安全性の根拠においている. したがって, 一般に, 多項式自己同型写像 F から tame 多項式自己同型写像 $G_1, \ldots, G_l$ に分解する効率的なアルゴリズムが存在すると, TTM 方式は効率的に解読される.

3.2 Matsumoto-Imai 暗号方式

Matsumoto-Imai 暗号方式 [8] の概要を述べる. なお, 前節と同様, ここでは概要を述べることを目的としているため, Matsumoto-Imai が提案した multiple-branch Matsumoto-Imai 方式ではなく, single-branch Matsumoto-Imai 方式を用いて説明する.

Matsumoto-Imai 方式では, ユーザ A は 2 つのアフィン多項式自己同型写像 L_1, L_2 を選び, $\mathbb{F}_{q^n}$ の $\mathbb{F}_q$-線形空間としての基底 $\{\beta_1, \ldots, \beta_n\}$ を一つとって固定する. また, $\gcd(q^n - 1, q^\theta + 1) = 1$ かつ $0 < \theta < n$ を満たす θ を選び, $\mathbb{F}_q^n$ から $\mathbb{F}_q^n$ への写像 $\bar{F}^{(\theta)}$ を $\bar{F}^{(\theta)} : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n},\ m \mapsto m^{q^\theta+1}$ によって定義する. 上記の θ に関する条件は $\bar{F}^{(\theta)}$ が全単射であるための必要十分条件であることに注意されたい. ユーザ A は合成写像 $L_1 \circ \phi^{-1} \circ \bar{F}^{(\theta)} \circ \phi \circ L_2$ を $F^{(\theta)}$ とおく. そして, 合成写像 $F^{(\theta)}$ を公開鍵とし, 2 つのアフィン多項式自己同型写像 L_1, L_2 を秘密鍵とする. なお, 写像 $\bar{F}^{(\theta)}$ は剰余環 $\mathbb{F}_q[X_1, \ldots, X_n]/I$ で考えると, 2 次の多項式自己同型写像[3] であることに注意されたい. ここでは, $F^{(\theta)} := (f_1, \ldots, f_n)$ とおくことにする. ユーザ A とは異なるユーザ B が, 平文 $(x_1, \ldots, x_n) \in \mathbb{A}^n_{\mathbb{F}_q}$ をユーザ A の公開鍵 F で暗号化する場合は $(y_1, \ldots, y_n) = (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n))$ を計算し, 計算結果である $(y_1, \ldots, y_n)$ を暗号文とする. そして, 暗号文 $(y_1, \ldots, y_n)$ をユーザ A に送る. ユーザ A が暗号文 $(y_1, \ldots, y_n)$ を復号する場合は自身の秘密鍵 L_1, L_2 を用いて $(x'_1, \ldots, x'_n) = ({L_2}^{-1} \circ \bar{F}^{(\theta)\ -1} \circ {L_1}^{-1})(y_1, \ldots, y_n)$ を計算し, $(x'_1, \ldots, x'_n)$ を復号文とする.

本稿では, 写像 $\bar{F}^{(\theta)}$ を **Matsumoto-Imai 中間写像**[4] とよび, 写像 $F^{(\theta)}$ を **Matsumoto-Imai 公開鍵写像**とよぶ.

4 主定理

本章では主定理を述べ, 主定理を証明する.

Main Theorem.

$\bar{F}^{(\theta)}$ を Matsumoto-Imai 中間写像とする. $q = 2$, $n = 3$ のとき, $\bar{F}^{(\theta)} \in \mathrm{Aut}_{\mathbb{F}_2}\, \mathbb{F}_2[\bar{X}, \bar{Y}, \bar{Z}]$ は tame 多項式自己同型写像である.

Proof.

$q = 2$, $n = 3$ とする. $\gcd(2^3 - 1, 2^\theta + 1) = 1$, $0 < \theta < n$ を満たす θ は $\theta = 1, 2$ である. 主張を示す前に, 証明の方針を述べる. まず, 主張は

[3] 2 次の多項式自己同型写像については, Rusek Conjecture と呼ばれている以下の予想がある [15, Conjecture 5.5]:
k を体, かつ $\mathbb{Q}$-代数とし, $n \geq 3$, $F \in \mathrm{Aut}_k\, A_n$ とする. このとき, $\deg F \leq 2$ ならば $F \in T(k, n)$ が成り立つ.

[4] 隠れ単項式とも呼ばれているが, 本稿では [3] に従い, Matsumoto-Imai 中間写像とよぶことにする.

$\theta = 1$ の場合と $\theta = 2$ の場合に分け, それぞれの場合について $\bar{F}^{(\theta)}$ が tame であることを示す.

$\mathbb{F}_{2^3}$ を表現する既約多項式を任意に一つとって固定しても一般性を失わない. なぜなら, Matsumoto-Imai 中間写像 $\bar{F}^{(\theta)}$ は, $\mathbb{F}_{q^n}$ の $\mathbb{F}_q$-線形空間としての基底に依存するが, $\{\beta_1, \ldots, \beta_n\}$ とは異なる基底 $\{\beta'_1, \ldots, \beta'_n\}$ を取った場合, 基底 $\{\beta_1, \ldots, \beta_n\}$ から基底 $\{\beta'_1, \ldots, \beta'_n\}$ への基底取り換え行列 M は一般線型群 $GL(n, \mathbb{F}_q)$ の元となる. したがって, $M \in GL(n, \mathbb{F}_q)$ から誘導されるアフィン多項式自己同型写像を $\widetilde{M}$ とすると, Matsumoto-Imai 中間写像 $\bar{F}^{(\theta)}$ が tame 自己同型多項式写像ならば, 上記とは異なる Matsumoto-Imai 中間写像 $\widetilde{M} \circ \bar{F}^{(\theta)} \circ \widetilde{M}^{-1}$ もまた tame 自己同型多項式写像となるからである.

以下, $\mathbb{F}_{2^3}$ を表現する既約多項式を $X^3 + X + 1$ とする. 主張の示し方は, Matsumoto-Imai central map $\bar{F}^{(\theta)}$ を, 実際にアフィン多項式自己同型写像と基本多項式自己同型写像の合成の形に分解する. そのため, 以下の多項式写像を準備する:

$$
\begin{aligned}
\tau_1 &= (\bar{X} + \bar{Y} + \bar{Z} + \bar{Y}\bar{Z}, \bar{Y}, \bar{Z}),\\
\tau_2 &= (\bar{X} + \bar{Z} + \bar{Y}\bar{Z}, \bar{Y} + \bar{Z}, \bar{Z}),\\
\tau_3 &= (\bar{X} + \bar{Y} + \bar{Y}\bar{Z}, \bar{Y}, \bar{Z}),\\
\lambda_1 &= (\bar{Y} + \bar{Z}, \bar{X} + \bar{Y}, \bar{X}),\\
\lambda_2 &= (\bar{Y}, \bar{X}, \bar{Z}),\\
\lambda_3 &= (\bar{Z}, \bar{X}, \bar{Y}),\\
\hat{\lambda_3} &= (\bar{X}, \bar{Y} + \bar{Z}, \bar{Y}).
\end{aligned}
$$

このとき, $\tau_i \in J(k, n)$ $(i = 1, 2, 3)$ が成り立つ. さらに, ${\tau_i}^{-1} = \tau_i$ $(i = 1, 2, 3)$ である. また, $\lambda_i \in \mathrm{Aff}(k, n)$ $(i = 1, 2, 3)$, $\hat{\lambda_3} \in \mathrm{Aff}(k, n)$ が成り立つ. 実際, ${\lambda_1}^{-1} = (\bar{Z}, \bar{Y} + \bar{Z}, \bar{X} + \bar{Y} + \bar{Z})$, ${\lambda_2}^{-1} = (\bar{Y}, \bar{X}, \bar{Z}) = \lambda_2$, ${\lambda_3}^{-1} = (\bar{Y}, \bar{Z}, \bar{X})$, ${\hat{\lambda_3}}^{-1} = (\bar{Y}, \bar{X}, \bar{Z})$ とかける.

(Case 1) $\theta = 1$.

簡単な計算により, $\bar{F}^{(1)} = (\bar{X} + \bar{Y} + \bar{Z} + \bar{Y}\bar{Z}, \bar{Y} + \bar{X}\bar{Y} + \bar{X}\bar{Z}, \bar{Z} + \bar{X}\bar{Y})$ が成り立つことがわかる. $\bar{F}^{(1)} = \lambda_3 \circ \tau_3 \circ \lambda_2 \circ \tau_2 \circ \lambda_1 \circ \tau_1$ であることを示すことにより, $\theta = 1$ の場合に主張が成り立つことを示す.

$$
\begin{aligned}
& \lambda_3 \circ \tau_3 \circ \lambda_2 \circ \tau_2 \circ \lambda_1 \circ \tau_1\\
=\ & \lambda_3 \circ \tau_3 \circ \lambda_2 \circ \tau_2\\
& (\bar{Y} + \bar{Z}, \bar{X} + \bar{Y}, \bar{X}) \circ (\bar{X} + \bar{Y} + \bar{Z} + \bar{Y}\bar{Z},\\
& \bar{Y}, \bar{Z})\\
=\ & \lambda_3 \circ \tau_3 \circ \lambda_2 \circ (\bar{X} + \bar{Z} + \bar{Y}\bar{Z}, \bar{Y} + \bar{Z}, \bar{Z})\\
& \circ(\bar{Y} + \bar{Z}, \bar{X} + \bar{Z} + \bar{Y}\bar{Z}, \bar{X} + \bar{Y} + \bar{Z} + \bar{Y}\bar{Z})\\
=\ & \lambda_3 \circ \tau_3 \circ (\bar{Y}, \bar{X}, \bar{Z})\\
& \circ(\bar{Z} + \bar{X}\bar{Y}, \bar{Y}, \bar{X} + \bar{Y} + \bar{Z} + \bar{Y}\bar{Z})\\
=\ & \lambda_3 \circ (\bar{X} + \bar{Y} + \bar{Y}\bar{Z}, \bar{Y}, \bar{Z})\\
& \circ(\bar{Y}, \bar{Z} + \bar{X}\bar{Y}, \bar{X} + \bar{Y} + \bar{Z} + \bar{Y}\bar{Z})\\
=\ & (\bar{Z}, \bar{X}, \bar{Y}) \circ (\bar{Y} + \bar{X}\bar{Y} + \bar{X}\bar{Z}, \bar{Z} + \bar{X}\bar{Y},\\
& \bar{X} + \bar{Y} + \bar{Z} + \bar{Y}\bar{Z})\\
=\ & (\bar{X} + \bar{Y} + \bar{Z} + \bar{Y}\bar{Z}, \bar{Y} + \bar{X}\bar{Y} + \bar{X}\bar{Z}, \bar{Z}\\
& +\bar{X}\bar{Y})\\
=\ & \bar{F}^{(1)}
\end{aligned}
$$

(Case 2) $\theta = 2$.

簡単な計算により, $\bar{F}^{(2)} = (\bar{X} + \bar{Y} + \bar{Z} + \bar{Y}\bar{Z}, \bar{Y} + \bar{Z} + \bar{X}\bar{Z}, \bar{Y} + \bar{X}\bar{Y} + \bar{X}\bar{Z})$ が成り立つことがわかる. $\bar{F}^{(2)} = \hat{\lambda_3} \circ \tau_3 \circ \lambda_2 \circ \tau_2 \circ \lambda_1 \circ \tau_1$ であることを示すことにより, $\theta = 2$ の場合に主張が成り立つことを示す. (Case 1) の場合の議論により, $\bar{F}^{(2)} = \hat{\lambda_3} \circ (\bar{Y} + \bar{X}\bar{Y} + \bar{X}\bar{Z}, \bar{Z} + \bar{X}\bar{Y}, \bar{X} + \bar{Y} + \bar{Z} + \bar{Y}\bar{Z})$ である.

$$
\begin{aligned}
& \hat{\lambda_3} \circ \tau_3 \circ \lambda_2 \circ \tau_2 \circ \lambda_1 \circ \tau_1\\
=\ & (\bar{X}, \bar{Y} + \bar{Z}, \bar{Y})\\
& \circ(\bar{Y} + \bar{X}\bar{Y} + \bar{X}\bar{Z}, \bar{Z} + \bar{X}\bar{Y},\\
& \bar{X} + \bar{Y} + \bar{Z} + \bar{Y}\bar{Z})\\
=\ & (\bar{X} + \bar{Y} + \bar{Z} + \bar{Y}\bar{Z}, \bar{Y} + \bar{Z} + \bar{X}\bar{Z}, \bar{Y} + \bar{X}\bar{Y} + \bar{X}\bar{Z})\\
=\ & \bar{F}^{(2)}
\end{aligned}
$$

ゆえに, $q = 2$, $n = 3$ のとき, Matsumoto-Imai central map $\bar{F}^{(\theta)} \in \mathrm{Aut}_{\mathbb{F}_2} \mathbb{F}_2[\bar{X}, \bar{Y}, \bar{Z}]$ は tame 多項式自己同型写像である. □

Matsumoto-Imai 公開鍵写像は, Matsumoto-Imai 中間写像の右側と左側にそれぞれアフィン多項式自己同型写像を合成する. したがって, 以下の Corollary を得る.

Corollary.

$F^{(\theta)}$ を Matsumoto-Imai 公開鍵写像とする. $q = 2$, $n = 3$ のとき, $F^{(\theta)} \in \mathrm{Aut}_{\mathbb{F}_2} \mathbb{F}_2[\bar{X}, \bar{Y}, \bar{Z}]$ は tame 多項式自己同型写像である.

5 まとめ

本稿では, 標数 2 の素体上定義された 3 変数 Matsumoto-Imai 中間写像が tame 多項式自己同型写像であることを証明した. また, 上述の Matsumoto-Imai 中間写像に対し, 基本多項式自己同型写像とアフィン多項式自己同型写像の合成の形を具体的に示した.

一般に多変数公開鍵暗号方式は, 変数の個数は任意の値が取れるように構成されており, 有限体についても, より広範に使えるように構成されているため, 本稿の結果が多変数公開鍵暗号の安全性評価に直接結び付くわけではない. しかしながら, 本稿で示した結果を一般化していくことは, 多変数公開鍵暗号の安全性評価に向けた重要な課題であると考えられる.

参考文献

[1] V. Dubois, P.-A. Fouque, A. Shamir and J. Stern, Practical Cryptanalysis of SFLASH, *Proceedings of Advances in Cryptology – CRYPTO 2007*, Vol.4622 of Lecture Notes in Computer Science (2007), Springer-Verlag, 1–12.

[2] V. Dubois, P.-A. Fouque and J. Stern, Cryptanalysis of SFLASH with Slightly Modified Parameters, *Proceedings of Advances in Cryptology – EUROCRYPT 2007*, Vol.4515 of Lecture Notes in Computer Science (2007), Springer-Verlag, 264–275.

[3] J. Ding, J. E. Gower and D. S. Schmidt, *Multivariate Public Key Cryptosystems*, Advances in Information Security, Vol.25, Springer, 2006.

[4] Arno van den Essen, *Polynomial Automorphisms and the Jacobian Conjecture*, Progress in Mathematics, Vol.190, Birkhäuser Verlag, Basel-Boston-Berlin, 2000.

[5] A. Kipnis and A. Shamir, Cryptanalysis of the HFE Public Key Cryptosystem, *Proceedings of Advances in Cryptology – CRYPTO '99*, Vol.1666 of Lecture Notes in Computer Science (1999), Springer-Verlag, 19–30.

[6] M. R. Garey and D. S. Johnson, *Computer and Intractability: A guide to the theory of NP-completeness*, Freeman, New-York, 1979.

[7] S. Maubach, Polynomial automorphisms over finite fields, *Serdica Math. J.* **27** (2001), No.4, 343–350.

[8] T. Matsumoto and H. Imai, Public Quadratic Polynominal-Tuples for Efficient Signature-Verification and Message-Encryption, *Proceedings of Advances in Cryptology – EUROCRYPT '88*, Vol.330 of Lecture Notes in Computer Science (1988), Springer-Verlag, 419–453.

[9] T. T. Moh, A Fast Public Key System with Signature and Master Key Functions, *Comm. Algebra* **27** (1999), No.5, 2207–2222.

[10] T. T. Moh, An Application of Algebraic Geometry to Encryption: Tame Transformation Method, *Rev. Mat. Iberoamericana* **19** (2003), No.2, 667–685.

[11] M. Nagata, *On automorphism group of $k[x, y]$*, Department of Mathematics, Kyoto University, Lectures in Mathematics, No.5, Kinokuniya Book Store Co. Ltd., Tokyo, 1972.

[12] J. Patarin, Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt '88, *Proceedings of Advances in Cryptology – CRYPTO '95*, Vol.963 of Lecture Notes in Computer Science (1995), Springer-Verlag, 248–261.

[13] J. Patarin, Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt '88, *Des. Codes Cryptogr.* **20** (2000), No.2, 175–209.

[14] J. Patarin and L. Goubin, Trapdoor One-Way Permutations and Multivariate Polynomials, *Proceedings of the First International Conference on Information Security and Cryptology 1997 – ICISC '97*, Vol.1334 of Lecture Notes in Computer Science (1997), Springer-Verlag, 356–368. Extended version is avairable at `http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.41.9400`

[15] K. Rusek, Polynomial Automorphisms, Preprint 456, Inst. of Math. Polish Acad. of Sciences, IMPAN, Warsaw, 1989.