Matsumoto-Imai 中間写像の tame 分解性について

矢城 信吾 †　　高木 剛 ‡

† 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
s-yashiro@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 多変数公開鍵暗号系は，多変数連立方程式の求解困難性を安全性の根拠として利用する方式である．その１つとして，Tame 多項式自己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）がある．TTM 方式の公開鍵が Tame 分解された場合，秘密鍵の Tame 多項式自己同型写像を求めることができ，TTM 方式は完全解読される．本稿では，多変数公開鍵暗号系の安全性評価の一歩として，TTM 方式以外の多変数公開鍵暗号系の１つである，Matsumoto-Imai 暗号系の Tame 分解問題性を検討し，線形写像によって変換された Matsumoto-Imai 中間写像が恒等的に 0 となる成分をもつとき，３種類の Tame 分解（アフィン多項式自己同型写像と trianglular 多項式自己同型写像の合成写像）にならないことを示す.

On Tameness of Matsumoto-Imai Central Maps

Shingo Yashiro†　　Tsuyoshi Takagi‡

†Graduate School of Mathematics, Kyushu University
744, Motooka, Nishi-ku, Fukuoka, 819-0395, JAPAN
s-yashiro@math.kyushu-u.ac.jp

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

Abstract Many Multivariate Public Key Cryptosystems (MPKC) are a public key cryptosystem whose security is based on the difficulty of solving a set of multivariate quadratic or higher degree polynomial equations over a finite field. For instance, Tame Transformation Method (TTM). The security of TTM is based on the intractability of Tame Decomposition Problem. In this paper, as a first step 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. Let us suppose that Matsumoto-Imai central maps satisfy the following conditions: Matsumoto-Imai central maps compose affine automotphisms and exists its components are zero. We show that Matsumoto-Imai central maps can not be decomposed 3 types of composite affine automorphisms and triangular automorphisms.

1　研究の背景

ランダムに選択された有限体上の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 ([5]). 多変数公開鍵暗号系の安全性は, この多変数連立方程式の求解困難性に基づいている. また, この暗号系に対し, 量子計算機による効率的な解読アルゴリズムが知られていないため, 耐量子計算機公開鍵暗号系として期待されている. しかし, 多変数連立方程式の求解困難性と多変数公開鍵暗号系で使われる多変数連立方程式系の求解問題は必ずしも一致しない. いくつかの多変数公開鍵暗号方式については脆弱性が報告されている ([1], [2], [7], [13], [14], [15]). このような背景より, 多変数公開鍵暗号系の安全性評価は重要な課題である.

多変数公開鍵暗号系の構成例の１つとして, Tame Transformation Method（TTM方式）([10], [11]) がある. この方式では, 特別な多項式自己同型写像 (後述するアフィン多項式自己同型写像と triangular 多項式自己同型写像) を複数個合成し, 合成した多項式自己同型写像を公開鍵として用いる. また, 秘密鍵を複数個の多項式自己同型写像とする. このアフィン多項式自己同型写像と triangular 多項式自己同型写像は逆写像を多項式時間で計算できる. したがって, TTM方式が安全であるための必要条件は, 合成された多項式自己同型写像から元の複数個の多項式自己同型写像に分解する問題の困難性にある. この問題を, Tame Decomposition Problem （Tame分解問題）という. ３変数以上の多項式環における分解方法は一般に知られておらず, Tame分解問題は困難であると考えられている ([11]).

一般の多変数公開鍵暗号系において, もし公開鍵からTame分解を効率よく計算できるアルゴリズムが存在すると, その多変数公開鍵暗号系で使われる秘密鍵を得ることできるようになり, 安全性を確保することはできないと考えられる. 以上より, 多変数公開鍵暗号系で利用される公開鍵に対するTame分解問題は多変数公開鍵暗号系の安全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系において, 公開鍵がTame分解可能か否かは知られていない. 一般に与えられた多項式自己同型写像がTame分解可能か否かを判定する問題はアフィン代数幾何学の研究テーマの１つであり, 未解決な問題または長年未解決であった問題が知られている ([12]).

上記の背景より, 本稿では, 先行研究 [6] に基づき, TTM方式以外の多変数公開鍵暗号系である Matsumoto-Imai 暗号系 ([8]) に焦点をあてる. Matsumoto-Imai 暗号系に使われる多項式写像の Tame 分解可能性を調べるために, ３つの Tame 分解（後述する $L_1 \circ J_1, L_2 \circ J_2, L_4 \circ J_4 \circ L_3 \circ J_3$ ($L_i : \mathbb{A}^n_{\mathbb{F}_q} \to \mathbb{A}^n_{\mathbb{F}_q}$ $(i = 1, 2, 3, 4)$ はアフィン多項式自己同型写像, $J_i : \mathbb{A}^n_{\mathbb{F}_q} \to \mathbb{A}^n_{\mathbb{F}_q}$ $(i = 1, 2)$ は triangular 多項式自己同型写像) にならないための条件を考える.

2　準備

2.1　記号の準備

k を体, $n \in \mathbb{N} := \{1, 2, \cdots\}$ を自然数, $x_1, \cdots, x_n$ を不定元とし, $R := k[x_1, \cdots, x_n]$ を n 変数多項式環とする. $\mathbb{A}^n_k$ を k 上の n 次元アフィン空間とし, $\mathbb{A}^n_k$ 上で定義された多項式自己同型写像全体の集合を $\mathrm{Aut}_k(R)$ とする.

$k := \mathbb{F}_q$ を標数 p で, 位数 $q = p^m$ の有限体とし, $\{v_1, \cdots, v_n\}$ を $\mathbb{F}_{q^n}$ の $\mathbb{F}_q$-線形空間としての基底とする. このとき, $\mathbb{A}^n_k$ から $\mathbb{F}_{q^n}$ への $\mathbb{F}_q$-線形写像を

$$\begin{array}{rccc} \phi : & \mathbb{A}^n_k & \longrightarrow & \mathbb{F}_{q^n} \\ & \cup\!\!| & & \cup\!\!| \\ & (x_1, \cdots, x_n) & \longmapsto & x_1 v_1 + \cdots + x_n v_n \end{array}$$

とかく. ϕ の逆写像 ϕ^{-1} は

$$\begin{array}{rccc} \phi^{-1} : & \mathbb{F}_{q^n} & \longrightarrow & \mathbb{A}^n_k \\ & \cup\!\!| & & \cup\!\!| \\ & x_1 v_1 + \cdots + x_n v_n & \longmapsto & (x_1, \cdots, x_n) \end{array}$$

とあらわせる. この同型写像 ϕ によって, 線形空間として, $\mathbb{A}^n_k$ と $\mathbb{F}_{q^n}$ を同一視する.

多項式自己同型写像の中には, 以下のような

自己同型写像がある ([3], [4]).

$$J = \begin{pmatrix} x_1 + g_1(x_2, \cdots, x_n) \\ x_2 + g_2(x_3, \cdots, x_n) \\ \vdots \\ x_{n-1} + g_{n-1}(x_n) \\ x_n \end{pmatrix}^T,$$

（ただし，$g_i \in k[x_{i+1}, \cdots, x_n]$ $(i = 1, \cdots, n-1)$ である.）このような形の自己同型写像を triangular 多項式自己同型写像（または，de Jonquières 多項式自己同型写像）という．定義から明らかなように，逆写像は

$$J^{-1} = \begin{pmatrix} x_1 - g_1(x_2, \cdots, x_n) \\ x_2 - g_2(x_3, \cdots, x_n) \\ \vdots \\ x_{n-1} - g_{n-1}(x_n) \\ x_n \end{pmatrix}^T$$

である．特に，標数 2 のとき，$J^{-1} = J$ となることに注意しておく．

$\mathbb{A}_k^n$ 上で定義された triangular 多項式自己同型写像全体を $\mathrm{J}(k, n)$ とかく．これは，$\mathrm{Aut}_k(R)$ の部分群となる．$\mathrm{J}(k, n)$ とアフィン多項式自己同型写像 $\mathrm{Aff}(k, n)$ によって生成される群を

$$\mathrm{T}(k, n) := \langle \mathrm{Aff}(k, n), J(k, n) \rangle$$

とおく．$\mathrm{T}(k, n)$ の元を，Tame 多項式自己同型写像という ([3], [4]).

有限体上の多項式環 $R = \mathbb{F}_q[x_1, \cdots, x_n]$ において，体の位数 q によって，$x_i^q \equiv x_i \pmod{I}$ $(i = 1, \cdots, n)$ の関係が成り立つ．このようなことから，$\mathrm{Aut}_k(R)$ の元を分類する上では，$I := (x_1^q - x_1, \cdots, x_n^q - x_n)$ による剰余環 $A := R/I$ を考えることにする．$\bar{x}_i \equiv x_i \pmod{I}$ $(i = 1, \cdots, n)$ とおくことで，

$$\mathbb{F}_q[x_1, \cdots, x_n]/I \cong \mathbb{F}_q[\bar{x}_1, \cdots, \bar{x}_n]$$

として考える．これより，$\bar{x}_i^q = \bar{x}_i$ と変数 n により，$J \in \mathrm{J}(k, n)$ の多項式 $g_1, \cdots, g_{n-1}$ には次数に関する条件が与えられる．例えば，$n = 3$ のとき，g_1 は 2 次式，g_2 は 1 次式となる ([6]).

3 TTM・Matsumoto-Imai 暗号方式について

この節では，本稿で使われる暗号方式である，TTM 方式と Matsumoto-Imai 暗号方式について述べる．

3.1 Tame Transformation Method

TTM 方式は T.T.Moh によって提案された多変数公開鍵暗号系である ([10], [11]). 本来，T.T.Moh によって考案されたのは [10], [11] の形であるが，概要を述べることを目的とするため [3] に沿って概説する．TTM 方式では，Alice は l 個の Tame 多項式自己同型写像 $G_1, \cdots, G_l$ $(G_i : \mathbb{A}_{\mathbb{F}_q}^n \to \mathbb{A}_{\mathbb{F}_q}^n \ (i = 1, \cdots, l))$ を選び，それらの合成写像 $G_1 \circ \cdots \circ G_l$ を F とする．この $F = (f_1, \cdots, f_n)$ を公開鍵 pk とする．また，$\{G_1, \cdots, G_l\}$ は秘密鍵 sk として Alice が保管しておく．この各 G_i は，G_i^{-1} を多項式時間で計算することができる．次に，Bob が平文 $(x_1, \cdots, x_n) \in \mathbb{A}_{\mathbb{F}_q}^n$ を Alice の公開鍵 pk を使って暗号化する．

$$\begin{aligned} & (y_1, \cdots, y_n) \\ = \ & (f_1(x_1, \cdots, x_n), \cdots, f_n(x_1, \cdots, x_n)) \end{aligned}$$

によって，暗号文 $(y_1, \cdots, y_n)$ を得る．この暗号文を Alice に送り，Alice がこの内容を

$$(x_1, \cdots, x_n) = (G_l^{-1} \circ \cdots \circ G_1^{-1})(y_1, \cdots, y_n)$$

によって復号する．これをアルゴリズムとしてまとめると，つぎのようになる．

Algorithm 1 Key Generation (TTM)

Input: $l \in \mathbb{N}$.

Output: (pk, sk).

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

Algorithm 2 Encryption (TTM)

Input: Plain text $(x_1, \cdots, x_n) \in \mathbb{A}^n_{\mathbb{F}_q}$,
Public key $pk = F = (f_1, \cdots, f_n)$,
$(F : \mathbb{A}^n_{\mathbb{F}_q} \to \mathbb{A}^n_{\mathbb{F}_q})$.
Output: Cipher text $(y_1, \cdots, y_n) \in \mathbb{A}^n_{\mathbb{F}_q}$.

1. Compute $(y_1, \cdots, y_n)$
$= (f_1(x_1, \cdots, x_n), \cdots, f_n(x_1, \cdots, x_n))$.
2. **Return:** $(y_1, \cdots, y_n)$.

Algorithm 3 Decryption (TTM)

Input: Cipher text $(y_1, \cdots, y_n) \in \mathbb{A}^n_{\mathbb{F}_q}$,
Private key $sk = \{G_1, \cdots, G_l\}$,
$(G_i : \mathbb{A}^n_{\mathbb{F}_q} \to \mathbb{A}^n_{\mathbb{F}_q})$,
$(i = 1, \cdots, l)$.
Output: Plain text $(x_1, \cdots, x_n) \in \mathbb{A}^n_{\mathbb{F}_q}$.

1. Compute $(x_1, \cdots, x_n)$
$= (G_l^{-1} \circ \cdots \circ G_1^{-1})(y_1, \cdots, y_n)$.
2. **Return:** $(x_1, \cdots, x_n)$.

3.2 Matsumoto-Imai 暗号方式

Matsumoto-Imai 暗号方式について述べる ([3], [13], [14]). ここでは，概要を述べることを目的としているため，single-branch Matsumoto-Imai 方式について概説する ([3]).

Matsumoto-Imai 方式では，Alice は 2 つのアフィン多項式自己同型写像 $L_1, L_2 \in \mathrm{Aff}(k, n)$ を選び，拡大体 $\mathbb{F}_{q^n}$ の $\mathbb{F}_q$-線形空間としての基底を $\{v_1, \cdots, v_n\}$ と 1 つ固定しておく．次に，$\gcd(q^n - 1, q^\theta + 1) = 1$ $(0 < \theta < n)$ を満たす θ を 1 つ選び

$$\begin{array}{rccc} \bar{F}^{(\theta)} : & \mathbb{F}_{q^n} & \longrightarrow & \mathbb{F}_{q^n} \\ & \cup & & \cup \\ & m & \longmapsto & m^{q^\theta+1} \end{array}$$

と写像を定義する．この θ によって定義される写像は全単射である．それは，$t(q^\theta + 1) \equiv 1 \pmod{q^n - 1}$ となる t によって，

$$\bar{F}^{(\theta)-1}(m) = m^t$$

とできるからである．

Alice は合成写像として，

$$F^{(\theta)} := L_1 \circ \phi^{-1} \circ \bar{F}^{(\theta)} \circ \phi \circ L_2$$

とおく．この $F^{(\theta)}$ を公開鍵 pk としておき，2 つのアフィン多項式自己同型写像 $\{L_1, L_2\}$ を秘密鍵 sk とする．ここで，$F^{(\theta)} := (f_1, \cdots, f_n)$ とおく．Bob が平文 $(x_1, \cdots, x_n) \in \mathbb{A}^n_{\mathbb{F}_q}$ を公開鍵 pk を使って，暗号文 $(y_1, \cdots, y_n)$ をつくる．この $(y_1, \cdots, y_n)$ を Alice に送信し，Alice は秘密鍵 sk を用いて，

$$(x_1, \cdots, x_n) = (L_2^{-1} \circ \bar{F}^{(\theta)-1} \circ L_1^{-1})(y_1, \cdots, y_n)$$

を計算し，復号する．

本稿では [3] に従い，写像 $\bar{F}^{(\theta)}$ を Matsumoto-Imai 中間写像，写像 $F^{(\theta)}$ を Matsumoto-Imai 公開鍵写像とよぶ．

また，$\bar{F}^{(\theta)}$ は拡大体 $\mathbb{F}_{q^n}$ における写像であるが，同型写像 $\phi : \mathbb{A}^n_{\mathbb{F}_q} \to \mathbb{F}_{q^n}$ により同一視し，$\phi^{-1} \circ \bar{F}^{(\theta)} \circ \phi$ も同様に，Matsumo-Imai 中間写像と呼ぶことにする．

Algorithm 4 Key Generation (MI)

Input: (n, θ).
Output: (pk, sk).

1. Select affine automorphisms L_1, L_2 and $\mathbb{F}_q$-linear map ϕ.
2. Compute $F^{(\theta)} \leftarrow L_1 \circ \phi \circ \bar{F}^{(\theta)} \circ \phi^{-1} \circ L_2$.
3. $pk \leftarrow F^{(\theta)}, sk \leftarrow \{L_1, L_2\}$.
4. **Return:** (pk, sk).

Algorithm 5 Encryption (MI)

Input: Plain text $(x_1, \cdots, x_n) \in \mathbb{A}^n_{\mathbb{F}_q}$,
Public key $pk = F^{(\theta)} = (f_1, \cdots, f_n)$,
$(F^{(\theta)} : \mathbb{A}^n_{\mathbb{F}_q} \to \mathbb{A}^n_{\mathbb{F}_q})$.
Output: Cipher text $(y_1, \cdots, y_n) \in \mathbb{A}^n_{\mathbb{F}_q}$.

1. Compute $(y_1, \cdots, y_n)$
$= (f_1(x_1, \cdots, x_n), \cdots, f_n(x_1, \cdots, x_n))$.
2. **Return:** $(y_1, \cdots, y_n)$.

Algorithm 6 Decryption (MI)

Input: Cipher text $(y_1, \cdots, y_n) \in \mathbb{A}^n_{\mathbb{F}_q}$,
Private key $sk = \{L_1, L_2\}$,
$(L_i : \mathbb{A}^n_{\mathbb{F}_q} \to \mathbb{A}^n_{\mathbb{F}_q})$,
$(i = 1, 2)$.

Output: Plain text $(x_1, \cdots, x_n) \in \mathbb{A}^n_{\mathbb{F}_q}$.

1. Compute $(x_1, \cdots, x_n)$
$= L_2^{-1} \circ \phi \circ \bar{F}^{(\theta)} \circ \phi^{-1} \circ L_1^{-1}(y_1, \cdots, y_n)$.
2. **Return:** $(x_1, \cdots, x_n)$.

4 主結果

4.1 主定理

今回得られた結果について述べる．以下，体 k の標数は 2 とし，$q = 2$ とする．Matsumoto-Imai 暗号系は標数 2 のときに限り，θ を取ることができる．また **Theorem.4.1** においては，$q = 2^m, k = \mathbb{F}_q$ でも議論が成立する．

ここで，$\mathbb{F}_{q^n}$ を構成するための基底 $\{v_1, \cdots, v_n\}$ を，1 つ固定しておき，同型写像 $\phi : \mathbb{A}^n_{\mathbb{F}_q} \to \mathbb{F}_{q^n}$ により，$\bar{F}^{(\theta)}$ を $\bar{F}^{(\theta)} : \mathbb{A}^n_{\mathbb{F}_q} \to \mathbb{A}^n_{\mathbb{F}_q}$ とする．$\bar{F}^{(\theta)}$ は構成上 $\mathbb{F}_{q^n}$ の $\mathbb{F}_q$ 基底に依存するが，基底を取り換えた場合は $\mathbb{F}_q$-線形変換を施すことによって同一視されることから，1 つを固定しておく．

Theorem 4.1. $\bar{F}^{(\theta)} : \mathbb{A}^n_{\mathbb{F}_q} \to \mathbb{A}^n_{\mathbb{F}_q}$ を *Matsumoto-Imai* 中間写像，$L \in \mathrm{Aff}(k, n)$ をアフィン多項式自己同型写像とし

$$(L \circ \bar{F}^{(\theta)})(\bar{x}_1, \cdots, \bar{x}_n) = (\bar{y}_1^{(\theta)}, \cdots, \bar{y}_{n-1}^{(\theta)}, \bar{y}_n^{(\theta)})$$

において，恒等的に $\bar{y}_i^{(\theta)} \equiv 0$ となる i が存在すると仮定する．このとき，$L \circ \bar{F}^{(\theta)}$ は次のような分解をもたない．：

$$L \circ \bar{F}^{(\theta)} = \begin{cases} J_1 \circ L_1, \\ L_1 \circ J_1, \\ J_2 \circ L_1 \circ J_1. \end{cases}$$

ここで，$L_1 \in \mathrm{Aff}(k, n), J_1, J_2 \in \mathrm{J}(k, n)$.

Proof. 証明の方針として，$L \circ \bar{F}^{(\theta)}$ が分解可能だと仮定して，矛盾を示す．必要ならば，$\bar{y}_n^{(\theta)} \equiv 0$ と仮定しても一般性を失わない．

(1) $L \circ \bar{F}^{(\theta)} = J_1 \circ L_1$ と仮定する．各写像をそれぞれ

$$J_1(\bar{x}_1, \cdots, \bar{x}_n) = \begin{pmatrix} \bar{x}_1 + g_1(\bar{x}_2, \cdots, \bar{x}_n) \\ \bar{x}_2 + g_2(\bar{x}_3, \cdots, \bar{x}_n) \\ \vdots \\ \bar{x}_{n-1} + g_{n-1}(\bar{x}_n) \\ \bar{x}_n \end{pmatrix}^T,$$

$$L_1(\bar{x}_1, \cdots, \bar{x}_n) = (\sum_{j=1}^n a_{1j}\bar{x}_j, \cdots, \sum_{j=1}^n a_{nj}\bar{x}_j)$$

とする．これより

$$(J_1 \circ L_1)(\bar{x}_1, \cdots, \bar{x}_n) = \begin{pmatrix} \sum_{j=1}^n a_{1j}\bar{x}_j + g_1(\sum_{j=1}^n a_{2j}\bar{x}_j, \cdots, \sum_{j=1}^n a_{nj}\bar{x}_j) \\ \vdots \\ \sum_{j=1}^n a_{nj}\bar{x}_j \end{pmatrix}^T.$$

仮定より，第 n 成分は

$$\sum_{j=1}^n a_{nj}\bar{x}_j = 0$$

である．各 $\bar{x}_j$ は k 上 1 次独立より，$a_{nj} = 0$ $(j = 1, \cdots, n)$ であるが，これは L_1 の自己同型性に反する．

(2) $L \circ \bar{F}^{(\theta)} = L_1 \circ J_1$ と仮定する．このとき，$(L_1 \circ J_1)(\bar{x}_1, \cdots, \bar{x}_n)$ の第 n 成分は次のようにかける．

$$\begin{gathered} a_{n1}(\bar{x}_1 + g_1(\bar{x}_2, \cdots, \bar{x}_n)) \\ + a_{n2}(\bar{x}_2 + g_2(\bar{x}_3, \cdots, \bar{x}_n)) \\ + \cdots \\ + a_{nn-1}(\bar{x}_{n-1} + g_{n-1}(\bar{x}_n)) \\ + a_{nn}\bar{x}_n = 0. \end{gathered}$$

これは

$$a_{n1}\bar{x}_1 + h(\bar{x}_2, \cdots, \bar{x}_n) = 0$$

$(h \in k[\bar{x}_2, \cdots, \bar{x}_n])$ と書け，各単項式は k 上 1 次独立より，$a_{n1} = 0$ となる．以下，同じ操作を繰り返すことにより

$$a_{n1} = a_{n2} = \cdots = a_{nn} = 0$$

となるが，L_1 の自己同型性に反する．

(3) $L \circ \bar{F}^{(\theta)} = J_2 \circ L_1 \circ J_1$ と仮定して，同様な方法で矛盾を示す．$J_2 \in \mathrm{J}(k,n)$ を取ると，$(J_2 \circ L_1 \circ J_1)(\bar{x}_1, \cdots, \bar{x}_n)$ の第 n 成分と，定理の仮定より

$$0 = \sum_{j=1}^{n} a_{nj}\bar{x}_j$$

であるから，矛盾がいえる．

Q.E.D

triangle 多項式自己同型写像 $J_1, J_2 \in \mathrm{J}(k,n)$ に対して，その合成 $J_2 \circ J_1$ もまた，triangle 多項式自己同型写像である． これらのことから，次の系を得る．

Corollary 4.2. *Matsumoto-Imai* 中間写像とアフィン自己同型写像の合成において，恒等的に 0 の成分があるならば，それは

$$\bar{F}^{(\theta)} = L_2 \circ J_2 \circ L_1 \circ J_1 \qquad (1)$$

となるような *Tame* 分解をもたない．

4.2 例

Theorem.4.1 の仮定を満たすような，例を挙げる．Matsumoto-Imai 公開鍵写像 $F^{(\theta)}$ を構成したとき，$q = 2, n = 3$ の場合は，先行研究として [6] がある．これにより，$\theta = 1, 2$ の場合，$F^{(\theta)}$ は Tame 多項式自己同型写像である．この場合は，**Theorem.4.1** の仮定を満たさないが，$q = 2, n = 5$ の場合に，仮定を満たすものが存在する．$\theta = 1, 3$ のおける，$\bar{F}^{(\theta)}$ を構成する．なお，$\mathbb{F}_{2^5}$ を既約多項式 $t^5 + t + 1$ を使って表現している．$\bar{F}^{(\theta)}$ は構成上 $\mathbb{F}_{q^n}$ の $\mathbb{F}_q$ 基底に依存するが，基底を取り換えた場合は $\mathbb{F}_q$-線形変換を施すことによって同一視されることに注意しておく．このとき

$$\bar{F}^{(1)}(\bar{x}_1, \cdots, \bar{x}_n) = (\bar{f}_1^{(1)}, \bar{f}_2^{(1)}, \bar{f}_3^{(1)}, \bar{f}_4^{(1)}, \bar{f}_5^{(1)}),$$

$$\begin{aligned}
\bar{f}_1^{(1)} &= \bar{x}_1 \\
&\quad + \bar{x}_2\bar{x}_3 + \bar{x}_2\bar{x}_4 + \bar{x}_2\bar{x}_5 + \bar{x}_3\bar{x}_5 + \bar{x}_4\bar{x}_5, \\
\bar{f}_2^{(1)} &= \bar{x}_3 + \bar{x}_4 \\
&\quad + \bar{x}_1\bar{x}_2 + \bar{x}_1\bar{x}_4 + \bar{x}_2\bar{x}_3 + \bar{x}_2\bar{x}_4 + \bar{x}_4\bar{x}_5, \\
\bar{f}_3^{(1)} &= \bar{x}_3 + \bar{x}_5 \\
&\quad + \bar{x}_1\bar{x}_2 + \bar{x}_1\bar{x}_3 + \bar{x}_1\bar{x}_4 + \bar{x}_2\bar{x}_4 + \bar{x}_2\bar{x}_5 \\
&\quad + \bar{x}_3\bar{x}_4 + \bar{x}_3\bar{x}_5 + \bar{x}_4\bar{x}_5, \\
\bar{f}_4^{(1)} &= \bar{x}_2 \\
&\quad + \bar{x}_1\bar{x}_4 + \bar{x}_1\bar{x}_5 + \bar{x}_2\bar{x}_4 + \bar{x}_3\bar{x}_5 + \bar{x}_4\bar{x}_5, \\
\bar{f}_5^{(1)} &= \bar{x}_4 + \bar{x}_5 \\
&\quad + \bar{x}_1\bar{x}_3 + \bar{x}_2\bar{x}_3 + \bar{x}_2\bar{x}_5 + \bar{x}_3\bar{x}_4 + \bar{x}_3\bar{x}_5.
\end{aligned}$$

$$\bar{F}^{(3)}(\bar{x}_1, \cdots, \bar{x}_n) = (\bar{f}_1^{(3)}, \bar{f}_2^{(3)}, \bar{f}_3^{(3)}, \bar{f}_4^{(3)}, \bar{f}_5^{(3)}),$$

$$\begin{aligned}
\bar{f}_1^{(3)} &= \bar{x}_1 + \bar{x}_2 + \bar{x}_3 + \bar{x}_5, \\
\bar{f}_2^{(3)} &= \bar{x}_2 + \bar{x}_4 + \bar{x}_5 \\
&\quad + \bar{x}_1\bar{x}_2 + \bar{x}_1\bar{x}_3 + \bar{x}_1\bar{x}_5 + \bar{x}_2\bar{x}_3 + \bar{x}_2\bar{x}_4 \\
&\quad + \bar{x}_3\bar{x}_4 + \bar{x}_3\bar{x}_5 + \bar{x}_4\bar{x}_5, \\
\bar{f}_3^{(3)} &= \bar{x}_3 + \bar{x}_4 + \bar{x}_5, \\
\bar{f}_4^{(3)} &= \bar{x}_3 + \bar{x}_5 \\
&\quad + \bar{x}_1\bar{x}_2 + \bar{x}_1\bar{x}_3 + \bar{x}_1\bar{x}_5 + \bar{x}_2\bar{x}_3 + \bar{x}_2\bar{x}_4 \\
&\quad + \bar{x}_3\bar{x}_4 + \bar{x}_3\bar{x}_5 + \bar{x}_4\bar{x}_5, \\
\bar{f}_5^{(3)} &= \bar{x}_2 + \bar{x}_3 \\
&\quad + \bar{x}_1\bar{x}_2 + \bar{x}_1\bar{x}_3 + \bar{x}_1\bar{x}_5 + \bar{x}_2\bar{x}_3 + \bar{x}_2\bar{x}_4 \\
&\quad + \bar{x}_3\bar{x}_4 + \bar{x}_3\bar{x}_5 + \bar{x}_4\bar{x}_5.
\end{aligned}$$

と書ける．これらをアフィン自己同型写像

$$\begin{aligned}
L^{(1)} &= (\bar{x}_1, \bar{x}_4, \bar{x}_2, \bar{x}_2 + \bar{x}_3, \bar{x}_2 + \bar{x}_3 + \bar{x}_5), \\
L^{(3)} &= \begin{pmatrix} \bar{x}_1 + \bar{x}_2 + \bar{x}_3 \\ \bar{x}_2 + \bar{x}_3 + \bar{x}_4 \\ \bar{x}_4 \\ \bar{x}_3 + \bar{x}_4 \\ \bar{x}_2 + \bar{x}_3 + \bar{x}_5 \end{pmatrix}^T
\end{aligned}$$

によって

$$\begin{aligned}
&(L^{(1)} \circ \bar{F}^{(1)})(\bar{x}_1, \cdots, \bar{x}_n) \\
= \ &(\bar{y}_1^{(1)}, \bar{y}_2^{(1)}, \bar{y}_3^{(1)}, \bar{y}_4^{(1)}, \bar{y}_5^{(1)}),
\end{aligned}$$

$$
\begin{aligned}
\bar{y}_1^{(1)} &= \bar{x}_1 \\
&\quad +\bar{x}_2\bar{x}_3+\bar{x}_2\bar{x}_4+\bar{x}_2\bar{x}_5+\bar{x}_3\bar{x}_5+\bar{x}_4\bar{x}_5, \\
\bar{y}_2^{(1)} &= \bar{x}_2 \\
&\quad +\bar{x}_1\bar{x}_4+\bar{x}_1\bar{x}_5+\bar{x}_2\bar{x}_4+\bar{x}_3\bar{x}_5+\bar{x}_4\bar{x}_5, \\
\bar{y}_3^{(1)} &= \bar{x}_3+\bar{x}_4 \\
&\quad +\bar{x}_1\bar{x}_2+\bar{x}_1\bar{x}_4+\bar{x}_2\bar{x}_3+\bar{x}_2\bar{x}_4+\bar{x}_4\bar{x}_5, \\
\bar{y}_4^{(1)} &= \bar{x}_4+\bar{x}_5 \\
&\quad +\bar{x}_1\bar{x}_3+\bar{x}_2\bar{x}_3+\bar{x}_2\bar{x}_5+\bar{x}_3\bar{x}_4+\bar{x}_3\bar{x}_5, \\
\bar{y}_5^{(1)} &= 0,
\end{aligned}
$$

$$
\begin{aligned}
&(L^{(3)}\circ\bar{F}^{(3)})(\bar{x}_1,\cdots,\bar{x}_n) \\
=\ &(\bar{y}_1^{(3)},\bar{y}_2^{(3)},\bar{y}_3^{(3)},\bar{y}_4^{(3)},\bar{y}_5^{(3)}),
\end{aligned}
$$

$$
\begin{aligned}
\bar{y}_1^{(3)} &= \bar{x}_1 \\
&\quad +\bar{x}_1\bar{x}_2+\bar{x}_1\bar{x}_3+\bar{x}_1\bar{x}_5+\bar{x}_2\bar{x}_3+\bar{x}_2\bar{x}_4 \\
&\quad +\bar{x}_3\bar{x}_4+\bar{x}_3\bar{x}_5+\bar{x}_4\bar{x}_5, \\
\bar{y}_2^{(3)} &= \bar{x}_2+\bar{x}_5, \\
\bar{y}_3^{(3)} &= \bar{x}_3+\bar{x}_5 \\
&\quad +\bar{x}_1\bar{x}_2+\bar{x}_1\bar{x}_3+\bar{x}_1\bar{x}_5+\bar{x}_2\bar{x}_3+\bar{x}_2\bar{x}_4 \\
&\quad +\bar{x}_3\bar{x}_4+\bar{x}_3\bar{x}_5+\bar{x}_4\bar{x}_5, \\
\bar{y}_4^{(3)} &= \bar{x}_4 \\
&\quad +\bar{x}_1\bar{x}_2+\bar{x}_1\bar{x}_3+\bar{x}_1\bar{x}_5+\bar{x}_2\bar{x}_3+\bar{x}_2\bar{x}_4 \\
&\quad +\bar{x}_3\bar{x}_4+\bar{x}_3\bar{x}_5+\bar{x}_4\bar{x}_5, \\
\bar{y}_5^{(3)} &= 0.
\end{aligned}
$$

Corollary.4.2 より

$$\bar{F}^{(\theta)} = L_2\circ J_2\circ L_1\circ J_1$$

となるような分解をもたない.

5 結び

本稿では，Matsumoto-Imai 中間写像がアフィン多項式自己同型写像により恒等的に 0 となるような成分をもつとき，3 つの Tane 分解できないことを示した．しかし，一般に Matsumoto-Imai 中間写像が，Tame 分解可能か否かは未解決問題である．本稿で得られた結果を拡張し，多変数公開鍵暗号の安全性評価に向けて，整理していくことが重要な課題であると考えている．

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 Automorphism and the Jacobian Conjecture*, Progress in Mathematics, Vol.190, Birkhäuser Verlag, Basel-Boston-Berlin, (2000).

[5] M. R. GAREY and D. S. JOHNSON, *Computer and Intractability : A guide to the theory of NP-completeness*, Freeman, NewYork,1979.

[6] K. HAKUTA, H. SATO and T. TAKAGI, *On Tameness of Matsumoto-Imai Central Maps with Three Variables (in Japanese)*, Computer Security Symposium 2011,19-21,(2011).

[7] 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.

[8] T. MATSUMOTO and H. IMAI, *Public Quadratic Polynomial-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] S. MAUBACH, *Polynomial automorphism over finite fields*, Serdica Math. J.**27** (2001), No.4, 343-350.

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

[11] T. T. MOH, *An Application of Algebraic Geometry to Encryption: Tame Transformation Method*, Rev. Mat. Iberoamerica **19** (2003), No.2, 667-685.

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

[13] 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.

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

[15] 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. Extend version is avairable at http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.41.9400.

[16] K. RUSEK, *Polynomial Automorphisms*, Preprint 456, Inst. of Math. Polish Acad. of Sciences, IMPAN, Warsaw, 1989.