Computer Security Symposium 2017
23 - 25 October 2017

Tame Transformation Methodの安全性強化手法に対する安全性再考

伯田 恵輔[1,a)]

概要：Tame Transformation Method（TTM）は Moh によって提案された多変数多項式暗号である．Hrdina らは Frobenius 自己同型写像を用いた TTM の安全性強化手法を提案している．本稿では，Hrdina らによって提案された TTM の安全性強化手法に対する安全性を再考し，ある（妥当と考えられる）条件下において，上記手法の安全性が実際に強化されるための必要条件を導く．

キーワード：多変数多項式暗号，Tame Transformation Method，Frobenius 自己同型写像，多項式同型写像，アフィン代数幾何

Security reconsideration of a security-enhanced Tame Transformation Method

Keisuke Hakuta[1,a)]

Abstract: Tame Transformation Method (TTM for short) proposed by T.T. Moh (1999) is one of the multivariate polynomial cryptosystems. Hrdina, Kureš, and Vašík (2010) have proposed a security-enhanced version of TTM. In this paper we reconsider security of the security-enhanced version of TTM proposed by Hrdina *et al.* Under a reasonable assumption, we derive a necessary condition for the security-enhanced version of TTM to be cryptographically secure.

Keywords: Multivariate polynomial cryptography, Tame Transformation Method (TTM), Frobenius automorphism, polynomial automorphism, affine algebraic geometry

1. はじめに

2015 年 8 月に NSA（National Security Agency）から耐量子計算機暗号への移行計画が公表され，2016 年 2 月に NIST（National Institute of Standards and Technology）が耐量子計算機暗号の標準化計画を発表したことから，耐量子計算機暗号の研究はますます盛んになっている．耐量子計算機暗号の一つとして多変数多項式暗号が知られている（[4]）．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. [10], p. 251, [28], pp. 20–21)）．多変数多項式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くことにより，量子計算機による攻撃 [29] に耐性を持つことが期待される．しかしながら，多変数多項式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多項式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，いくつかの多変数多項式暗号方式についてはその脆弱性が指摘されている．そのため，安全性評価は重要な課題であり，多変数多項式暗号における中心的な研究テーマのひとつである．

多変数多項式暗号の一方式である Tame Transformation Method（TTM）（cf. [24], [25]）では，逆写像を効率的に

[1] 島根大学大学院総合理工学研究科
Interdisciplinary Graduate School of Science and Engineering, Shimane University
[a)] hakuta(at)cis.shimane-u.ac.jp

計算できる複数個の多項式写像（後述するアフィン自己同型写像，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 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**順自己同型写像分解問題（TDP: Tame automorphism Decomposition Problem）**という．Tame Transformation Method の安全性については，[2]，[5]，[6]，[11]，[26] などの結果が知られているが，これらは TTM のパラメータ選択の不備による攻撃手法であり，一般化された TTM（3.1 節）の暗号学的な安全性評価や一般の TDP が計算量的に困難であるかどうかは知られていない．

一方，Hrdina らは Frobenius 自己同型写像を用いた TTM の安全性強化手法を提案している [16]．上記の TTM の安全性強化手法は Patarin の攻撃（[27]）に対する対策として提案された．Hrdina らは TTM の安全性強化手法によって Patarin の攻撃を防ぐことができることについての理由を説明しているが，実際に安全性が強化されているかどうかについては評価していない．

本稿では，Hrdina らによって提案された TTM の安全性強化手法に対する安全性を再考し，ある（妥当と考えられる）条件下において，上記手法の安全性が実際に強化されるための必要条件を導く．

2. 記法・数学的準備

ここでは，本稿で使用する記法を纏める．多項式同型写像については，例えば [7] などを参照されたい．

$\mathbb{N} := \{1, 2, \ldots\}$ を自然数全体の集合，$\mathbb{N}_0 := \mathbb{N} \cup \{0\}$，$\mathbb{Z}$ を有理整数環とする．$\mathbb{K}$ を体，$\mathbb{K}^* := \mathbb{K} \setminus \{0\}$ を体 $\mathbb{K}$ の乗法群とする．$X_1, \ldots, X_n$ を不定元とし，$\mathbb{K}[X_1, \ldots, X_n]$ を体 $\mathbb{K}$ 上の n 変数多項式環とする．$n, \ell \in \mathbb{N}$，$f_i \in \mathbb{K}[X_1, \ldots, X_n]$ $(1 \leq i \leq \ell)$ とし，任意の $\mathbf{a} := (a_1, \ldots, a_n) \in \mathbb{K}^n$ に対し，

$$F(\mathbf{a}) := (f_1(\mathbf{a}), \ldots, f_\ell(\mathbf{a})) \tag{2.1}$$

と定義することによって，n 個の多項式の組 $F = (f_1, \ldots, f_\ell)$ を $\mathbb{K}^n$ から $\mathbb{K}^\ell$ への写像とみなすことができる．F は多項式写像と呼ばれる．$\mathrm{ME}_n(\mathbb{K})$ で $\mathbb{K}^n$ から $\mathbb{K}^n$ への多項式写像全体の集合を表し，$\mathrm{Maps}(\mathbb{K}^n, \mathbb{K}^n)$ で $\mathbb{K}^n$ から $\mathbb{K}^n$ への写像全体の集合を表す．また，$\mathrm{BME}_n(\mathbb{K})$ で $\mathbb{K}^n$ から $\mathbb{K}^n$ への全単射な多項式写像全体の集合を表す．式 (2.1) より，自然な写像

$$\pi : \quad \mathrm{ME}_n(\mathbb{K}) \quad \to \quad \mathrm{Maps}(\mathbb{K}^n, \mathbb{K}^n) \tag{2.2}$$

が存在する．$\mathrm{ME}_n(\mathbb{K})$，$\mathrm{BME}_n(\mathbb{K})$，$\mathrm{Maps}(\mathbb{K}^n, \mathbb{K}^n)$ は写像としての合成に関して半群をなす．これらの半群はそれぞれ恒等写像を単位元とする単位的半群であり，写像 π は単位的半群の間の準同型写像である．$\mathrm{ME}_n(\mathbb{K})$ の元であって，逆元を持つ元全体の集合を $\mathrm{GA}_n(\mathbb{K})$ と書く．$\mathrm{GA}_n(\mathbb{K})$ の元を多項式同型写像という．$\mathrm{GA}_n(\mathbb{K})$ は写像の合成に関して群をなす．$\mathrm{GA}_n(\mathbb{K}) \subset \mathrm{BME}_n(\mathbb{K})$ であることに注意しよう（後述する記号を用いると，$\mathbb{K} = \mathbb{F}_q$ ならば $\varphi_k^{(n)} \notin \mathrm{GA}_n(\mathbb{K})$ かつ $\varphi_k^{(n)} \in \mathrm{BME}_n(\mathbb{K})$ であるから $\mathrm{GA}_n(\mathbb{K}) \subsetneq \mathrm{BME}_n(\mathbb{K})$ が成立する）．各 $i = 1, \ldots, n$ に対して $\deg f_i = 1$ であるとき，多項式同型写像 $F = (f_1, \ldots, f_n)$ はアフィン自己同型写像と呼ばれる．以下の形の多項式写像

$$\begin{aligned} E_{a_i} = (X_1, \ldots, X_{i-1}, X_i + a_i, X_{i+1}, \ldots, X_n), \\ a_i \in \mathbb{K}[X_1, \ldots, \hat{X}_i, \ldots, X_n] \\ = \mathbb{K}[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n], \end{aligned} \tag{2.3}$$

は多項式同型写像であり，その逆元 $E_{a_i}^{-1}$ は $E_{a_i}^{-1} = E_{-a_i}$ である．(2.3) の形の多項式同型写像 E_{a_i} は基本自己同型写像と呼ばれる．

アフィン自己同型写像全体の集合を $\mathrm{Aff}_n(\mathbb{K})$，基本自己同型写像全体の集合を $E_n(\mathbb{K})$ とおく．$\mathrm{Aff}_n(\mathbb{K})$ と $E_n(\mathbb{K})$ はそれぞれ $\mathrm{GA}_n(\mathbb{K})$ の部分群である．$\mathrm{Aff}_n(\mathbb{K}) \cong \mathbb{K}^n \rtimes GL_n(\mathbb{K})$ であることに注意しよう．$\mathrm{TA}_n(\mathbb{K}) := \langle \mathrm{Aff}_n(\mathbb{K}), E_n(\mathbb{K}) \rangle$ とおく．ここで，$\langle H_1, H_2 \rangle$ は部分群 $H_1, H_2 \subset G$ によって生成される G の部分群を表す．$\mathrm{TA}_n(\mathbb{K})$ も $\mathrm{GA}_n(\mathbb{K})$ の部分群であり，順部分群と呼ばれる．

多項式同型写像 $\phi \in \mathrm{GA}_n(\mathbb{K})$ は，$\phi \in \mathrm{TA}_n(\mathbb{K})$ のときに順自己同型写像（tame automorphism）であるといい，そうでないとき（$\phi \in \mathrm{GA}_n(\mathbb{K}) \setminus \mathrm{TA}_n(\mathbb{K})$ のとき）ϕ は野生自己同型写像（wild automorphism）であるという．

以下の形の多項式同型写像 $J_{a,f}$

$$\begin{aligned} J_{a,f} = (a_1 X_1 + f_1(X_2, \ldots, X_n), a_2 X_2 + f_2(X_3, \ldots, X_n), \\ \ldots, a_n X_n + f_n), a_i \in \mathbb{K} \ (i = 1, \ldots, n), \\ f_i \in \mathbb{K}[X_{i+1}, \ldots, X_n] \ (i = 1, \ldots, n-1), \ f_n \in \mathbb{K} \end{aligned}$$

は triangular 多項式同型写像（または de Jonquières 多項式同型写像）と呼ばれており，定義から明らかに多項式同型写像である．上記で定義した $J_{a,f}$ 全体の集合を $\mathrm{BA}_n(\mathbb{K})$ とかくことにする：

$$\begin{aligned} \mathrm{BA}_n(\mathbb{K}) := \{J_{a,f} \in \mathrm{GA}_n(\mathbb{K}) \mid a_i \in \mathbb{K} \ (i = 1, \ldots, n), \\ f_i \in \mathbb{K}[X_{i+1}, \ldots, X_n] \ (i = 1, \ldots, n-1), \ f_n \in \mathbb{K}\}. \end{aligned}$$

このとき，$\mathrm{TA}_n(\mathbb{K}) = \langle \mathrm{Aff}_n(\mathbb{K}), \mathrm{BA}_n(\mathbb{K}) \rangle$ であることが知られている．また，任意の体 $\mathbb{K}$ に対し，$\mathrm{GA}_2(\mathbb{K}) = \mathrm{TA}_2(\mathbb{K})$ であることが知られている（Jung-van der Kulk theorem [18]，[19]）．

任意の順自己同型写像 $\phi \in \mathrm{TA}_n(\mathbb{K})$ に対し，ある非負整数 $l \in \mathbb{N}_0$，$\epsilon, \epsilon' \in \{0, 1\} \subset \mathbb{Z}$，$\sigma_i \in \mathrm{Aff}_n(\mathbb{K})$ $(1 \leq i \leq l+1)$，$\sigma_i \notin \mathrm{BA}_n(\mathbb{K})$ $(1 \leq i \leq l+1)$，$\tau_i \in \mathrm{BA}_n(\mathbb{K})$ $(1 \leq i \leq l)$，$\tau_i \notin \mathrm{Aff}_n(\mathbb{K})$ $(1 \leq i \leq l)$ が存在し，

$$\phi = \sigma_1^\epsilon \circ \tau_1 \circ \sigma_2 \circ \cdots \circ \sigma_l \circ \tau_l \circ \sigma_{l+1}^{\epsilon'} \tag{2.4}$$

が成り立つ．式 (2.4) を $\phi \in \mathrm{TA}_n(\mathbb{K})$ の順自己同型写像分解（**TD: Tame automorphism Decomposition**）と呼ぶ．一般に，$\phi \in \mathrm{TA}_n(\mathbb{K})$ に対し，式 (2.4) の表現の仕方は一意的ではない．これは $\mathrm{TA}_n(\mathbb{K})$ が $\mathrm{Aff}_n(\mathbb{K})$ と $\mathrm{BA}_n(\mathbb{K})$ の融合積でないことに依る（[7], Example 5.2.2 参照）．

定義 1. **(*l*-triangular automorphism, [1], Definition 2.3)** $\phi \in \mathrm{TA}_n(\mathbb{K})$ は，$l+1$ 個以下のアフィン自己同型写像と l 個以下の *triangular* 多項式同型写像を用いて式 (2.4) の形で表現することができないとき，***l*-triangular automorphism*** という．

注意 1. 定義 1 より，任意の $\phi \in \mathrm{TA}_n(\mathbb{K})$ に対し，ある $l \in \mathbb{N}_0$ が存在し，ϕ は l-triangular automorphism である．

体 $\mathbb{K}$ に対し，$\mathbb{K}$ の標数を $p = \mathrm{char}(\mathbb{K})$ と書く．体 $\mathbb{K}$ が要素数 q の有限体 $\mathbb{F}_q$（$p = \mathrm{char}(\mathbb{F}_q)$, $q = p^m$, $m \geq 1$）のとき，(2.2) の写像 π を π_q と書くことにする：

$$\pi_q : \quad \mathrm{ME}_n(\mathbb{F}_q) \quad \to \quad \mathrm{Maps}(\mathbb{F}_q^n, \mathbb{F}_q^n).$$

写像 π_q は群の準同型写像

$$\pi_q : \quad \mathrm{GA}_n(\mathbb{F}_q) \quad \to \quad \mathrm{Sym}(\mathbb{F}_q^n)$$

を引き起こす [i]．ここで $\mathrm{Sym}(S)$ は有限集合 S 上の対称群を表す．ガロア拡大 $\mathbb{F}_q/\mathbb{F}_p$ に対し，$\mathbb{F}_q/\mathbb{F}_p$ のガロア群を $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ で表す．任意の $A \in \mathrm{Aff}_n(\mathbb{F}_q)$, $\xi \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ に対し，以下の形の多項式写像 $A \circ (X_1^\xi, \ldots, X_n^\xi)$ を**アフィン半線形変換**といい，アフィン半線形変換全体の集合を $\mathrm{A\Gamma L}_n(\mathbb{F}_q)$ で表す：

$$\mathrm{A\Gamma L}_n(\mathbb{F}_q) := \{A \circ (X_1^\xi, \ldots, X_n^\xi) \in \mathrm{BME}_n(\mathbb{F}_q) \mid A \in \mathrm{Aff}_n(\mathbb{F}_q),\ \xi \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)\}.$$

ここで，各 i（$1 \leq i \leq n$）に対し，X_i^ξ は $\xi \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ の X_i への作用を表す．$\mathrm{A\Gamma L}_n(\mathbb{F}_q)$ は写像の合成に関して群をなし，**アフィン半線形群**という．明らかに，アフィン半線形群 $\mathrm{A\Gamma L}_n(\mathbb{F}_q)$ とアフィン自己同型群 $\mathrm{Aff}_n(\mathbb{F}_q)$ の間には

$$\mathrm{Aff}_n(\mathbb{F}_q) \subset \mathrm{A\Gamma L}_n(\mathbb{F}_q) \tag{2.5}$$

なる包含関係があり，$\mathrm{Aff}_n(\mathbb{F}_q) = \mathrm{A\Gamma L}_n(\mathbb{F}_q)$ が成立するのは $m = 1$ のとき，かつそのときに限る．

写像 sgn

$$\mathrm{sgn} : \mathrm{Sym}(S) \to \{\pm 1\}$$

を符号関数とする．符号関数 sgn は群準同型であり，$\mathrm{Ker}(\mathrm{sgn}) = \mathrm{Alt}(S)$ である，ここで，$\mathrm{Alt}(S)$ は S 上の交代群を表す．部分群 $G \subseteq \mathrm{GA}_n(\mathbb{F}_q)$ に対し，$\pi_q(G)$ は対称群 $\mathrm{Sym}(\mathbb{F}_q^n)$ の部分群である．

対称群 $\mathrm{Sym}(\mathbb{F}_q^n)$ の部分群 $\pi_q(\mathrm{TA}_n(\mathbb{F}_q))$ の代数的構造を調べることは数学的に自然であり，Maubach による以下の結果（[21], Theorem 2.3）が知られている：

定理 1. ([21], Theorem 2.3) $n \geq 2$ とする．q が奇数，または $q = 2$ ならば $\pi_q(\mathrm{TA}_n(\mathbb{F}_q)) = \mathrm{Sym}(\mathbb{F}_q^n)$ である．$q = 2^m$，$m \geq 2$ ならば $\pi_q(\mathrm{TA}_n(\mathbb{F}_q)) = \mathrm{Alt}(\mathbb{F}_q^n)$ である．

上記の結果（[21], Theorem 2.3）を受け，有限体上のアフィン自己同型写像，基本自己同型写像の置換としての符号も調べられており，Hakuta による以下の結果（[12], Corollary 1，及び [12], Corollary 2）が知られている：

系 1. ([12], Corollary 1) q が奇数，または $q = 2^m$，$m \geq 2$ ならば $\pi_q(\mathrm{EA}_n(\mathbb{F}_q)) \subset \mathrm{Alt}(\mathbb{F}_q^n)$ が成り立つ．

系 2. ([12], Corollary 2) $q = 2^m$, $m \geq 2$, または $q = 2$, $n \geq 3$ ならば $\pi_q(\mathrm{Aff}_n(\mathbb{F}_q)) \subset \mathrm{Alt}(\mathbb{F}_q^n)$ が成り立つ．

$\mathrm{GA}_n(\mathbb{F}_q)$，$\mathrm{TA}_n(\mathbb{F}_q)$，$\mathrm{ME}_n(\mathbb{F}_q)$，の代数的構造に関するその他の結果については，例えば [13]，[14]，[15]，[22]，[23] などを参照されたい．

3. TTM とその安全性強化手法

本節では Tame Transformation Method（TTM）とその安全性強化手法について概説する．

3.1 Tame Transformation Method（TTM）

TTM は Moh によって提案された多変数多項式暗号である（[24], [25]）．ここでは概要を述べることを目的としているため，より一般的な記述を採用している（[4], pp. 139–140）．

Algorithm 1 TTM の鍵ペア生成アルゴリズム

Input: 1^k
Output: (pk, sk)
1: $l+1$ 個の $\sigma_i \in \mathrm{Aff}_n(\mathbb{F}_q)$（$1 \leq i \leq l+1$）を選択
2: l 個の $\tau_j \in \mathrm{BA}_n(\mathbb{F}_q)$（$1 \leq j \leq l$）を選択
3: $\epsilon, \epsilon' \in \{0, 1\} \subset \mathbb{Z}$ を選択
4: $F \leftarrow \sigma_1^\epsilon \circ \tau_1 \circ \sigma_2 \circ \cdots \circ \sigma_l \circ \tau_l \circ \sigma_{l+1}^{\epsilon'} \in \mathrm{TA}_n(\mathbb{F}_q)$
5: $pk \leftarrow F$, $sk \leftarrow (\sigma_1, \ldots, \sigma_{l+1}, \tau_1, \ldots, \tau_l, \epsilon, \epsilon')$
6: **return** (pk, sk)

Algorithm 2 TTM の暗号化アルゴリズム

Input: 平文 $(x_1, \ldots, x_n)$，公開鍵 $pk = (f_1, \ldots, f_n) \in \mathrm{TA}_n(\mathbb{F}_q)$
Output: 暗号文 $(y_1, \ldots, y_n)$
1: $(y_1, \ldots, y_n) \leftarrow (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n))$
2: **return** $(y_1, \ldots, y_n)$

Algorithm 3 TTM の復号アルゴリズム

Input: 暗号文 $(y_1, \ldots, y_n)$,
秘密鍵 $sk = (\sigma_1, \ldots, \sigma_{l+1}, \tau_1, \ldots, \tau_l, \epsilon, \epsilon')$
Output: 平文 $(x_1, \ldots, x_n)$
1: $F^{-1} \leftarrow \sigma_{l+1}^{-\epsilon} \circ \tau_l^{-1} \circ \sigma_l^{-1} \circ \cdots \circ \sigma_2^{-1} \circ \tau_1^{-1} \circ \sigma_1^{-\epsilon'}$
2: $(x_1, \ldots, x_n) \leftarrow F^{-1}(y_1, \ldots, y_n)$
3: **return** $(x'_1, \ldots, x'_n)$

[i] これは，$\phi \in \mathrm{GA}_n(\mathbb{F}_q)$ を扱うのではなく，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 $\mathbb{F}_q[X_1, \ldots, X_n]/I$ における自己同型写像群 $\mathrm{Aut}_{\mathbb{F}_q} \mathbb{F}_q[X_1, \ldots, X_n]/I$ の元 $\phi \bmod I$ を考えていることに他ならない．

TTM は，合成写像 $F \in \mathrm{TA}_n(\mathbb{F}_q)$ 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 に対する順自己同型写像分解を計算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 $F \in \mathrm{TA}_n(\mathbb{F}_q)$ から順自己同型写像分解を計算する効率的なアルゴリズムが存在すると，TTM は効率的に解読することができる．

3.2 TTM の安全性強化手法

次に，Hrdina らによって提案された TTM の安全性強化手法（[16]）を説明する．ここでもより一般的な記述で TTM の安全性強化手法を説明する．実際の TTM の安全性強化手法（[16]）とは異なることに注意されたい．Hrdina らによる TTM の安全性強化手法（[16]）は Patarin の攻撃（[27]）に対する対策として提案された．$1 \leq k \leq m$ [ii] とし，$\varphi_k^{(n)} \in \mathrm{A\Gamma L}_n(\mathbb{F}_q)$ を

$$\varphi_k^{(n)}(X_1, \ldots, X_n) := (X_1^{p^k}, \ldots, X_n^{p^k}) \in \mathrm{A\Gamma L}_n(\mathbb{F}_q)$$

で定義する．Moh によって提案された TTM では，アフィン自己同型写像 $\sigma_i \in \mathrm{Aff}_n(\mathbb{F}_q)$ $(1 \leq i \leq l+1)$ と triangular 多項式同型写像 $\tau_j \in \mathrm{BA}_n(\mathbb{F}_q)$（$1 \leq j \leq l$）に対し，

$$F = \sigma_1^{\epsilon} \circ \tau_1 \circ \sigma_2 \circ \cdots \circ \sigma_l \circ \tau_l \circ \sigma_{l+1}^{\epsilon'} \in \mathrm{TA}_n(\mathbb{F}_q)$$

を公開鍵 pk としていた．Hrdina らによって提案された TTM の安全性強化手法では，公開鍵として $F \in \mathrm{TA}_n(\mathbb{F}_q)$ ではなく，代わりに $\widetilde{F}_{1,i}, \widetilde{F}_{2,j} \in \mathrm{BME}_n(\mathbb{F}_q)$（$1 \leq i, j \leq l$），

$$\begin{aligned} \widetilde{F}_{1,i} := {} & \sigma_1^{\epsilon} \circ (\tau_1 \circ \sigma_2) \circ \cdots \circ (\tau_{i-1} \circ \sigma_i) \\ & \circ (\tau_i \circ \varphi_k^{(n)} \circ \sigma_{i+1}) \\ & \circ (\tau_{i+1} \circ \sigma_{i+2}) \circ \cdots \circ (\tau_l \circ \sigma_{l+1}^{\epsilon'}), \end{aligned} \tag{3.1}$$

$$\begin{aligned} \widetilde{F}_{2,j} := {} & \sigma_1^{\epsilon} \circ (\tau_1 \circ \sigma_2) \circ \cdots \circ (\tau_{j-1} \circ \sigma_j) \circ \varphi_k^{(n)} \\ & \circ (\tau_j \circ \sigma_{j+1}) \circ \cdots \circ (\tau_l \circ \sigma_{l+1}^{\epsilon'}), \end{aligned} \tag{3.2}$$

を使うことが提案されている．なお，[16], p. 232 では，$l = 1$，$\epsilon = \epsilon' = 1$ かつ $\widetilde{F}_{2,1}$ の場合が提案されている．Hrdina らは，TTM の公開鍵として F ではなく $\widetilde{F}_{1,i}, \widetilde{F}_{2,j}$ を用いることにより Patarin の攻撃（[27]）を防ぐことができることについての理由を説明しているが，実際に安全性が強化されているかどうかについては評価していない．したがって，Hrdina らによって提案された TTM の安全性強化手法に対する安全性評価を行い，実際に安全性が強化されているか否か検討することが望ましい．

ところで，TTM の公開鍵 $F \in \mathrm{TA}_n(\mathbb{F}_q)$ は式 (2.4) を満たすため，その順自己同型写像分解が存在するが，式 (3.1) 及び式 (3.2) で定義された $\widetilde{F}_{1,i}, \widetilde{F}_{2,j}$ は

$$\widetilde{F}_{1,i}, \widetilde{F}_{2,j} \in \mathrm{BME}_n(\mathbb{F}_q) \setminus \mathrm{TA}_n(\mathbb{F}_q)$$

であり，これらの順自己同型写像分解は存在しない．したがって，順自己同型写像分解問題の観点から上記の安全性強化手法に対する安全性評価を行うことはできない．

そこで次節では，この問題を回避することを目的として，$\widetilde{F}_{1,i}, \widetilde{F}_{2,j}$ を擬似的に順自己同型写像として扱うための手法（模倣的順自己同型写像）を検討し，そのフレームワークのもとで $\varphi_k^{(n)}$ の性質を明らかにする．

4. アフィン半線形変換の置換としての符号

上記の問題点を回避するため，本節では全単射な多項式写像 $\varphi_k^{(n)} = (X_1^{p^k}, \ldots, X_n^{p^k}) \in \mathrm{A\Gamma L}_n(\mathbb{F}_q)$ の性質を調べる．

定義 2. (模倣的順自己同型写像 (Mimicked tame automorphism) [23]) 全単射な多項式写像 $F \in \mathrm{BME}_n(\mathbb{F}_q)$ に対し，ある順自己同型写像 $G \in \mathrm{TA}_n(\mathbb{F}_q)$ が存在して

$$\pi_q(F) = \pi_q(G)$$

を満たすとき，F を模倣的順自己同型写像 [iii] という．

本節の主結果は以下のとおりである：

主定理 1. ($\varphi_k^{(n)}$ は模倣的順自己同型写像) $n \geq 2$ とする．任意の $1 \leq k \leq m$ に対し，全単射な多項式写像 $\varphi_k^{(n)} \in \mathrm{A\Gamma L}_n(\mathbb{F}_q)$ は模倣的順自己同型写像である．

主定理 1 を示すため，4.1 節では Frobenius 写像の置換としての符号を調べ，4.2 節では $\varphi_k^{(n)}$ の置換としての符号を調べる．また，$\varphi_k^{(n)}$ の置換としての符号に関する結果の帰結として，主定理 1 が成り立つことを示す．

4.1 Frobenius 写像の置換としての符号

本節では Frobenius 写像の置換としての符号を決定する．任意の素数 p と正整数 $m \geq 1$ に対し，$\mathbb{F}_q = \mathbb{F}_{p^m}$ と $\mathbb{F}_p^m$ は $\mathbb{F}_p$-線形同型である．$\{\beta_1, \ldots, \beta_m\}$ を $\mathbb{F}_q$ の m 次元 $\mathbb{F}_p$-線形空間としての基底とする．このとき，正規基底が常に存在する（cf. [20]）．$\{\beta_1, \ldots, \beta_m\}$ が正規基底であるとき，ある $\alpha \in \mathbb{F}_q$ が存在し，全ての i（$1 \leq i \leq m$）に対して $\beta_i = \alpha^{p^{i-1}}$ が成り立つ．$\mathbb{F}_q$ の m 次元 $\mathbb{F}_p$-線形空間としての正規基底を $\{\alpha, \alpha^{p^1}, \ldots, \alpha^{p^{m-1}}\}$ とし，$\mathbb{F}_p^m$ から $\mathbb{F}_{p^m}$ への $\mathbb{F}_p$-線形空間としての同型写像 ψ を

$$\begin{array}{rccc} \psi: & \mathbb{F}_p^m & \to & \mathbb{F}_{p^m} \\ & (a_1, \ldots, a_m) & \mapsto & a_1\alpha^{p^0} + \cdots + a_m\alpha^{p^{m-1}} \end{array}$$

とかく．ここで，各 i（$1 \leq i \leq m$）に対し，$a_i \in \mathbb{F}_p$ である．ψ の逆写像は

[ii] [16] では $1 \leq k \leq m-1$ としているが，4 節の結果を述べる際に必要となるため，$1 \leq k \leq m$ としている．当然ながら $k = m$ の場合，$\pi_q(\varphi_m^{(n)})$ は恒等置換である．

[iii] [23] では，$F \in \mathrm{GA}_n(\mathbb{F}_q)$ に対して模倣的順自己同型写像が定義されているが，本稿では $\mathrm{BME}_n(\mathbb{F}_q)$ まで拡張した場合の定義に変更していることに注意されたい．

$$\begin{array}{rccc}\psi^{-1}: & \mathbb{F}_{p^m} & \to & \mathbb{F}_p^m \\ & a_1\alpha^{p^0}+\cdots+a_m\alpha^{p^{m-1}} & \mapsto & (a_1,\ldots,a_m)\end{array}$$

である．不定元 X_i と X_j を入れ替えるアフィン自己同型写像 $T_{i,j}^{(m)} \in \mathrm{Aff}_m(\mathbb{F}_p)$ を

$$T_{i,j}^{(m)} := (X_1,\ldots,X_{i-1},X_j,X_{i+1},\ldots, X_{j-1},X_i,X_{j+1},\ldots,X_n) \in \mathrm{Aff}_m(\mathbb{F}_p)$$

で定義する．$\mathbb{F}_{p^m}$ 上の p 乗 Frobenius 写像を ξ とする：$\xi:\mathbb{F}_q\to\mathbb{F}_q,\ x\mapsto x^p$．このとき，次が成り立つ：

命題 1. (Frobenius 写像 ξ^k の置換としての符号) $1\le k\le m$ とする．このとき，p^k 乗 *Frobenius* 写像 ξ^k の置換としての符号に関して以下の等式が成立する：

$$\mathrm{sgn}\left(\pi_q\left(\xi^k\right)\right) = \begin{cases}-1 & (p=2,\ m=2,\ k=1,\ \text{または}\\ & \quad p\equiv 3 \bmod 4,\ m:\text{偶数},\ k:\text{奇数}),\\ 1 & (\text{その他のとき}).\end{cases} \tag{4.1}$$

Proof. $\{\alpha,\alpha^{p^1},\ldots,\alpha^{p^{m-1}}\}$ が正規基底であることから

$$(\psi^{-1}\circ\xi\circ\psi)(a_1,\ldots,a_m)=(a_m,a_1,\ldots,a_{m-1})$$

である．したがって，

$$\pi_q\left(\psi^{-1}\circ\xi\circ\psi\right) = \pi_q\left(T_{1,m}^{(m)}\circ T_{1,m-1}^{(m)}\circ\cdots\circ T_{1,3}^{(m)}\circ T_{1,2}^{(m)}\right) \tag{4.2}$$

が成り立つ．式 (4.2) の両辺の sgn をとることにより，

$$\mathrm{sgn}\left(\pi_q(\xi)\right)=\prod_{i=2}^{m}\mathrm{sgn}\left(\pi_q\left(T_{1,i}^{(m)}\right)\right) \tag{4.3}$$

を得る．[12], Lemma 1 を用いることにより，式 (4.3) は

$$\mathrm{sgn}\left(\pi_q(\xi)\right)=\begin{cases}1 & (p=2,\ m\ge 3),\\ (-1)^{m-1} & (p=2,\ m=2),\\ (-1)^{\frac{p-1}{2}(m-1)} & (p:\text{奇数}),\end{cases}$$

$$=\begin{cases}-1 & (p=2,\ m=2,\ \text{または}\\ & \quad p\equiv 3 \bmod 4,\ m:\text{偶数}),\\ 1 & (\text{その他のとき}),\end{cases}$$

と変形することができる．写像 sgn, π_q がそれぞれ群準同型写像であることから $\mathrm{sgn}\left(\pi_q\left(\xi^k\right)\right)=\mathrm{sgn}\left(\pi_q(\xi)\right)^k$ が成り立ち，式 (4.1) を得る． □

4.2 $\varphi_k^{(n)}$ の置換としての符号

本節では全単射な多項式写像 $\varphi_k^{(n)}\in \mathrm{A\Gamma L}_n(\mathbb{F}_q)$ の置換としての符号を決定し，その帰結として，主定理 1 が成り立つことを示す．

命題 2. ($n\ge 2$ の場合における $\varphi_k^{(n)}$ の置換としての符号) $n\ge 2$ とし，$1\le k\le m$ とする．このとき，全単射な多項式写像 $\varphi_k^{(n)}\in \mathrm{A\Gamma L}_n(\mathbb{F}_q)$ の置換としての符号に関して以下の等式が成立する：

$$\mathrm{sgn}\left(\pi_q\left(\varphi_k^{(n)}\right)\right) = \begin{cases}-1 & (p\equiv 3 \bmod 4,\ m:\text{偶数},\ n,k:\text{奇数}),\\ 1 & (\text{その他のとき}).\end{cases} \tag{4.4}$$

Proof. $\varphi_{1,k}^{(n)}\in \mathrm{BME}_n(\mathbb{F}_q)$ を

$$\varphi_{1,k}^{(n)}(X_1,\ldots,X_n):=(X_1^{p^k},X_2,\ldots,X_n)$$

で定義する．このとき，

$$\varphi_k^{(n)}=\left(T_{1,n}^{(n)}\circ\varphi_{1,k}^{(n)}\circ T_{1,n}^{(n)}\right)\circ\cdots\circ\left(T_{1,2}^{(n)}\circ\varphi_{1,k}^{(n)}\circ T_{1,2}^{(n)}\right)\circ\varphi_{1,k}^{(n)}$$

が成り立ち，写像 sgn, π_q がそれぞれ群準同型写像であることから

$$\mathrm{sgn}\left(\pi_q\left(\varphi_k^{(n)}\right)\right)=\mathrm{sgn}\left(\pi_q\left(\varphi_{1,k}^{(n)}\right)\right)^n$$

を得る．さらに，$\varphi_{1,k}^{(n)}=\underbrace{\varphi_{1,1}^{(n)}\circ\cdots\circ\varphi_{1,1}^{(n)}}_{k\text{ 個}}$ であることから

$$\mathrm{sgn}\left(\pi_q\left(\varphi_k^{(n)}\right)\right)=\left(\mathrm{sgn}\left(\pi_q\left(\varphi_{1,1}^{(n)}\right)\right)\right)^{kn}$$

である．任意の $\mathbf{x^{(0)}}:=(x_2^{(0)},\ldots,x_n^{(0)})\in\mathbb{F}_q^{n-1}$ をひとつ取って固定し，写像 $\varphi_{1,1,\mathbf{x^{(0)}}}^{(n)}$ を以下で定義する：

$$\begin{array}{rccl}\varphi_{1,1,\mathbf{x^{(0)}}}^{(n)}: & \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ & (x_1,\ldots,x_n) & \longmapsto & (x_1^p,x_2,\ldots,x_n) \\ & & & \quad (x_2,\ldots,x_n)=\mathbf{x^{(0)}}\text{のとき},\\ & (x_1,\ldots,x_n) & \longmapsto & (x_1,\ldots,x_n) \\ & & & \quad \text{その他のとき}.\end{array}$$

写像 $\varphi_{1,1,\mathbf{x^{(0)}}}^{(n)}$ は明らかに全単射（すなわち置換）であり，

$$\pi_q\left(\varphi_{1,1}^{(n)}\right)=\pi_q\left(\prod_{\mathbf{x^{(0)}}\in\mathbb{F}_q^{n-1}}\varphi_{1,1,\mathbf{x^{(0)}}}^{(n)}\right) \tag{4.5}$$

を満たす．式 (4.5) は共通部分のない $\mathbb{F}_q^n$ 上の置換の積である．また，固定された $\mathbf{x^{(0)}}=(x_2^{(0)},\ldots,x_n^{(0)})\in\mathbb{F}_q^{n-1}$ に対し，明らかに

$$\mathrm{sgn}\left(\pi_q\left(\varphi_{1,1,\mathbf{x^{(0)}}}^{(n)}\right)\right)=\mathrm{sgn}\left(\pi_q(\xi)\right)$$

が成立する．よって，

$$\begin{aligned}\mathrm{sgn}\left(\pi_q\left(\varphi_k^{(n)}\right)\right)&=\left(\mathrm{sgn}\left(\pi_q\left(\varphi_{1,1}^{(n)}\right)\right)\right)^{kn}\\ &=\left(\prod_{\mathbf{x^{(0)}}\in\mathbb{F}_q^{n-1}}\mathrm{sgn}\left(\pi_q\left(\varphi_{1,1,\mathbf{x^{(0)}}}^{(n)}\right)\right)\right)^{kn}\\ &=\left(\mathrm{sgn}\left(\pi_q(\xi)\right)\right)^{nkq^{n-1}}\end{aligned}$$

となり，上式と命題 1 より式 (4.4) を得る． □

命題 1，及び命題 2 をまとめることにより系 3 を得る．

系 3. **($\varphi_k^{(n)}$ の置換としての符号)** $n \geq 1$，$1 \leq k \leq m$ とする．このとき，全単射な多項式写像 $\varphi_k^{(n)} \in \mathrm{A\Gamma L}_n(\mathbb{F}_q)$ の置換としての符号に関して以下の等式が成立する：

$$\mathrm{sgn}\left(\pi_q\left(\varphi_k^{(n)}\right)\right) = \begin{cases} -1 & (p=2,\ m=2, n=1,\ k=1,\ \text{または} \\ & \quad p \equiv 3 \bmod 4,\ m:\text{偶数},\ n,k:\text{奇数}), \\ 1 & (\text{その他のとき}). \end{cases}$$

特に，$p=2$ かつ $n \geq 2$ ならば $\pi_q(\varphi_k^{(n)})$ は偶置換である．

系 3 を用いて主定理 1 を示す．

主定理 1 の証明

[21], Theorem 2.3 より，p が奇素数または $(p,m)=(2,1)$ のとき $\pi_q(\mathrm{TA}_n(\mathbb{F}_q)) = \mathrm{Sym}(\mathbb{F}_q^n)$ が成り立つ．したがって，$\pi_q(\varphi_k^{(n)}) \in \mathrm{Sym}(\mathbb{F}_q^n) = \pi_q(\mathrm{TA}_n(\mathbb{F}_q))$ となり，ある順自己同型写像 $\phi \in \mathrm{TA}_n(\mathbb{F}_q)$ が存在して $\pi_q(\varphi_k^{(n)}) = \pi_q(\phi)$ を満たすから $\varphi_k^{(n)}$ は模倣的順自己同型写像である．

一方，$p=2$，$m \geq 2$ のとき $\pi_q(\mathrm{TA}_n(\mathbb{F}_q)) = \mathrm{Alt}(\mathbb{F}_q^n)$ が成り立つ．また，系 3 より $\pi_q(\varphi_k^{(n)}) \in \mathrm{Alt}(\mathbb{F}_q^n)$ が成り立つ．よって，$\pi_q(\varphi_k^{(n)}) \in \mathrm{Alt}(\mathbb{F}_q^n) = \pi_q(\mathrm{TA}_n(\mathbb{F}_q))$ となり，ある順自己同型写像 $\phi \in \mathrm{TA}_n(\mathbb{F}_q)$ が存在して $\pi_q(\varphi_k^{(n)}) = \pi_q(\phi)$ を満たすから $\varphi_k^{(n)}$ は模倣的順自己同型写像である． □

[16] で提案された式 (3.1) 及び式 (3.2) の $\widetilde{F}_{1,i}, \widetilde{F}_{2,j} \in \mathrm{BME}_n(\mathbb{F}_q)$ は模倣的順自己同型写像であることが主定理 1 からただちに従う（系 4）．

系 4. **($\widetilde{F}_{1,i}, \widetilde{F}_{2,j} \in \mathrm{BME}_n(\mathbb{F}_q)$ は模倣的順自己同型写像)** $n \geq 2$ とする．このとき，式 (3.1) 及び式 (3.2) によって定義された $\widetilde{F}_{1,i}, \widetilde{F}_{2,j} \in \mathrm{BME}_n(\mathbb{F}_q)$ は模倣的順自己同型写像である．

次節では，主定理 1 と系 4 を使用する．一方，系 3 と [12], Corollary 2 より系 5 もただちに従う．系 5 は次節以降の結果と直接の関係はないが，本研究の副産物として得られた結果であり，ここで述べておく．特に，系 5 (2) は [12], Corollary 2 に対する一つの拡張となっている．

系 5. 上記の記号のもとで，以下が成立する:
(1) $m \geq 2$ かつ $n \geq 1$ ならば

$$\pi_q(\mathrm{Aff}_n(\mathbb{F}_q)) \subsetneq \pi_q(\mathrm{A\Gamma L}_n(\mathbb{F}_q)) \tag{4.6}$$

が成り立つ．
(2) $p=2$ かつ $n \geq 3$ ならば任意の $m \geq 1$ に対し，

$$\pi_q(\mathrm{A\Gamma L}_n(\mathbb{F}_q)) \subset \mathrm{Alt}(\mathbb{F}_q^n) \tag{4.7}$$

が成り立つ．言い換えると，$p=2$ かつ $n \geq 3$ ならば任意のアフィン半線形変換は偶置換である．

Proof. 包含関係 (2.5) が成立するから $\pi_q(\mathrm{Aff}_n(\mathbb{F}_q)) \neq \pi_q(\mathrm{A\Gamma L}_n(\mathbb{F}_q))$ を示せば十分である．もし，$\varphi_{1,1}^{(n)}$ が模倣的アフィン自己同型写像（ある $A \in \mathrm{Aff}_n(\mathbb{F}_q)$ が存在して $\pi_q(\varphi_{1,1}^{(n)}) = \pi_q(A)$ が成立）であれば $\varphi_1^{(n)}$ も模倣的アフィン自己同型写像となり，したがって $\varphi_k^{(n)}$ も模倣的アフィン自己同型写像となる．このとき，$\pi_q(\mathrm{Aff}_n(\mathbb{F}_q)) = \pi_q(\mathrm{A\Gamma L}_n(\mathbb{F}_q))$ を満たす．これより，$\varphi_{1,1}^{(n)} = (X_1^p, X_2, \ldots, X_n)$ が模倣的アフィン自己同型写像でないことを示せばよいが，これは Frobenius 写像の性質から明らかである．よって，包含関係 (4.6) が成立する．包含関係 (4.7) は系 3 と [12], Corollary 2 から明らかである． □

5. TTM の安全性強化手法の安全性再考

本節では上述した TTM の安全性強化手法に対して安全性を再考する．5.1 節では，TDP に関連する数学計算問題を整理する．5.2 節では，Hrdina らによって提案された TTM の安全性強化手法に対する安全性を再考し，ある（妥当と考えられる）条件下において，上記手法の安全性が実際に強化されるための必要条件を導く．

5.1 TDP に関連する数学計算問題

前述したように，TTM は順自己同型写像分解問題の計算困難性に基づく多変数多項式暗号である．

定義 3. **(順自己同型写像分解問題 (TDP: Tame automorphism Decomposition Problem))** 順自己同型写像 $F \in \mathrm{TA}_n(\mathbb{F}_q)$ が与えられたとき，その順自己同型写像分解である式 (2.4) の $\sigma_i \in \mathrm{Aff}_n(\mathbb{F}_q)$ $(1 \leq i \leq l+1)$，$\tau_i \in \mathrm{BA}_n(\mathbb{F}_q)$ $(1 \leq i \leq l)$ を計算する問題を順自己同型写像分解問題（**TDP: Tame automorphism Decomposition Problem**）という．TDP を解くことが計算量的に困難であるという仮定を順自己同型写像分解仮定（**TDA: Tame automorphism Decomposition Assumption**）という．

ところが，TTM は順自己同型写像自体を分解する TDP が計算量的に困難であったとしても，以下に示す MTDP を解くことが出来れば安全性を確保することはできない．

定義 4. **(模倣的順自己同型写像分解問題 (MTDP: Mimicked Tame automorphism Decomposition Problem))** 全単射多項式写像 $F \in \mathrm{BME}_n(\mathbb{F}_q)$ が与えられたとき，その模倣的順自己同型写像に対応する（つまり，$\pi_q(F) = \pi_q(G)$ を満たす）$G \in \mathrm{TA}_n(\mathbb{F}_q)$ に対し，G の TDP を計算する問題を模倣的順自己同型写像分解問題（**MTDP: Mimicked Tame automorphism Decomposition Problem**）という．MTDP を解くこと

が計算量的に困難であるという仮定を模倣的順自己同型写像分解仮定（**MTDA: Mimicked Tame automorphism Decomposition Assumption**）という．

TDP を解くアルゴリズムが存在すれば MTDP を解くアルゴリズムも存在する．すなわち，MTDP を解くことは TDP を解くことよりも容易ということである．言い換えると，MTDA が成り立つならば TDA も成り立つ．そのため，TTM の安全性の根拠となる数学計算問題として，TDP ではなく MTDP の計算困難性を評価する必要がある．前節の系 4 により，式 (3.1) 及び式 (3.2) の $\widetilde{F}_{1,i}, \widetilde{F}_{2,j} \in \mathrm{BME}_n(\mathbb{F}_q)$ は模倣的順自己同型写像であるから，$\widetilde{F}_{1,i}, \widetilde{F}_{2,j}$ に対する MTDP を考えることができる．

5.2 TTM の安全性強化のための必要条件

本節では，Hrdina らによって提案された TTM の安全性強化手法に対する安全性を再考し，妥当と考えられる条件下において，上記手法の安全性の強化が可能となるための必要条件を導く．まず，以下の用語を定義する．

定義 5. **(l-模倣的順自己同型写像 (l-Mimicked Tame Automorphism))** $F \in \mathrm{BME}_n(\mathbb{F}_q)$ を全単射多項式写像とする．F が模倣的順自己同型写像であり，F に対応する（つまり，$\pi_q(F) = \pi_q(G)$ を満たす）t-triangular automorphism $G \in \mathrm{TA}_n(\mathbb{F}_q)$ のうち，t の最小値が l であるとき，F は **l-模倣的順自己同型写像**（l-mimicked tame automorphism）であるという．

定義 6. **(長さ関数 (length function))**
写像 $\ell : \mathrm{BME}_n(\mathbb{F}_q) \to \mathbb{N}_0 \cup \{\infty\}$ を以下で定義する:

$$\ell(F) := \begin{cases} \epsilon & F \text{ が } l\text{-模倣的かつ } l = 0, \\ (2l-1) + (\epsilon + \epsilon') & F \text{ が } l\text{-模倣的かつ } l \geq 1, \\ \infty & \textit{otherwise.} \end{cases}$$

ただし，F が l-模倣的であるとき，$\ell(F)$ は右辺の最小値によって定義する．ℓ を長さ関数（*length function*）という．

注意 2. 定義 1，注意 1，定義 5 より，定義 6 の長さ関数 ℓ は，全単射な多項式写像 $F \in \mathrm{BME}_n(\mathbb{F}_q)$ に対し，最小の t に対する t-triangular automorphism で模倣した際の式 (2.4) に現れるアフィン自己同型写像，及び triangular 多項式同型写像の個数の総和の最小値を意味する．

長さ関数 ℓ に対し，以下の補題は基本的である．紙数の都合により証明は割愛するが，[17], Section 1.6 と同様の方針によって示すことができる．

補題 1. **(長さ関数 ℓ の性質)**
(1) 任意の $F \in \mathrm{GA}_n(\mathbb{F}_q)$ に対し，$\ell(F) = \ell(F^{-1})$.
(2) 任意の $F_1, F_2 \in \mathrm{BME}_n(\mathbb{F}_q)$ に対し，

$$|\ell(F_1) - \ell(F_2)| \leq \ell(F_1 \circ F_2) \leq \ell(F_1) + \ell(F_2).$$

ここで，$|\cdot|$ は通常の意味での絶対値である．

補題 1 より，模倣的順自己同型写像 $\widetilde{F}_{1,i}, \widetilde{F}_{2,j}$ の長さに関する以下の系（系 6）が成立する．

系 6. **($\widetilde{F}_{1,i}, \widetilde{F}_{2,j}$ の長さの上限と下限)** $F \in \mathrm{TA}_n(\mathbb{F}_q)$ とする．このとき，式 (3.1) 及び式 (3.2) で定義された模倣的順自己同型写像 $\widetilde{F}_{1,i}, \widetilde{F}_{2,j}$ の長さに関して以下が成立する:

$$|\ell(F) - \ell(\varphi_k^{(n)})| \leq \ell(\widetilde{F}_{1,i}), \ell(\widetilde{F}_{2,j}) \leq \ell(F) + \ell(\varphi_k^{(n)}).$$

一般の模倣的順自己同型写像に対する MTDP の計算量は正確に見積もられていない．しかしながら，部分的な結果として [8]，[9]，[30] などが知られており，また，[3], Section 2.4 の結果を MTDP に対して単純に適用することにより，次の Assumption 1 が得られると考えられる．

Assumption 1. **(l-模倣的順自己同型写像に対する MTDP の計算量に関する仮定)** l-模倣的順自己同型写像に対する MTDP の計算量は q, n, l に依存する．さらに，固定した q, n に対し，l-模倣的順自己同型写像に対する MTDP の計算量は l に関して単調増加である．

系 6 より，Hrdina らによって提案された TTM の安全性強化手法 [16] が Assumption 1 のもとで，実際に強化されるための必要条件は以下のとおりである．

主定理 2. **(TTM 安全性強化手法 [16] の安全性が強化されるための必要条件)** Assumption 1 のもとで，$\widetilde{F}_{1,i}, \widetilde{F}_{2,j} \in \mathrm{BME}_n(\mathbb{F}_q)$ に対する MTDP が，もとの $F \in \mathrm{TA}_n(\mathbb{F}_q)$ に対する MTDP より困難となるための必要条件は

$$\ell(F) < \ell(\widetilde{F}_{1,i}), \ell(\widetilde{F}_{2,j}) \leq \ell(F) + \ell(\varphi_k^{(n)})$$

である．

$\widetilde{F}_{1,i}, \widetilde{F}_{2,j}$ を決定する際に，アフィン自己同型写像，及び triangular 多項式同型写像をうまく選ぶことによって，次の Assumption 2 が成り立つと考えられる．

Assumption 2. **($\widetilde{F}_{1,i}, \widetilde{F}_{2,j}$ の長さの下限に関する仮定)** $\widetilde{F}_{1,i}, \widetilde{F}_{2,j} \in \mathrm{BME}_n(\mathbb{F}_q)$ が $|\ell(F) - \ell(\varphi_k^{(n)})| \leq \ell(\widetilde{F}_{1,i}), \ell(\widetilde{F}_{2,j}) \leq \ell(F)$ を満たす確率は無視できる程小さい．言い換えると，無視できる確率を除いて

$$\ell(F) < \ell(\widetilde{F}_{1,i}), \ell(\widetilde{F}_{2,j}) \leq \ell(F) + \ell(\varphi_k^{(n)})$$

が成り立つ．

Assumption 1, 2 のもとで，TTM の安全性強化手法 [16] の安全性について以下が成り立つ：

主定理 3. **(TTM の安全性強化手法の安全性)** Assumption 1, 2 のもとで，$\widetilde{F}_{1,i}, \widetilde{F}_{2,j} \in \mathrm{BME}_n(\mathbb{F}_q)$ に対する MTDP の計算量は，もとの $F \in \mathrm{TA}_n(\mathbb{F}_q)$ に対する MTDP の計算量より大きい．言い換えると，Assumption 1, 2 のもとで，TTM 安全性強化手法は実際に安全性が強化されている．

6. まとめ

本稿では，Hrdina らによって提案された TTM 安全性強化手法に対する安全性を再考し，Assumption 1 のもとで TTM 安全性強化手法の安全性が実際に強化されるための必要条件を導いた（主定理 2）．また，Assumption 1, 2 のもとで TTM 安全性強化手法の安全性が強化されていることを示した（主定理 3）．

本稿の結果は TTM 安全性強化手法が Gröbner 基底など他の代数攻撃に対して安全であることを主張するものではない．今後の課題として，Assumption 1, 2 に関する計算機実験や数学的な証明，TTM 安全性強化手法の各種代数攻撃への耐性評価などが挙げられる．

謝辞　本研究は JSPS 科研費 若手研究 (B) 16K16066 の助成を受けたものです．

参考文献

[1] Y. Bodnarchuk, On generators of the tame invertible polynomial maps group, Internat. J. Algebra Comput., **15** (2005), no. 5-6, 851–867.

[2] J.-M. Chen and T.T. Moh, On the Goubin-Courtois attack on TTM, Cryptology ePrint Archive, Report 2001/072, 2001.

[3] M. Dickerson, The inverse of an automorphism in polynomial time, J. Symbolic Computation, **13** (1992), no. 2, 209–220.

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

[5] J. Ding and T. Hodges, Cryptanalysis of an implementation scheme of TTM, J. Algebra Appl., **3** (2004), no. 3, 273–282.

[6] J. Ding, and D. Schmidt, The new TTM implementation schemes of the TTM cryptosystem are not secure, In: K. Feng, H. Niederreiter, C. Xing (eds.) Coding, Cryptography and Combinatorics, Progress in Computer Science and Applied Logic, vol. 23, pp. 113–127, Birkhäuser, Basel (2004).

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

[8] J.-C. Faugére and L. Perret, An efficient algorithm for decomposing multivariate polynomials and its applications to cryptography, J. Symbolic Computat., **44** (2009), no. 12, 1676–1689.

[9] J.-C. Faugére and L. Perret, High order derivatives and decomposition of multivariate polynomials, In: J.P. May (ed.) Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation–ISSAC 2009, pp. 207-214, ACM, New York (2009).

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

[11] L. Goubin, N. Courtois, Cryptanalysis of the TTM cryptosystem, In: T. Okamoto (ed.) Advances in Cryptology–ASIACRYPT 2000, Lecture Notes in Computer Science, vol. 1976, pp. 44–57, Springer, Berlin, Heidelberg (2000).

[12] K. Hakuta, On permutations induced by tame automorphisms over finite fields, Acta Math. Vietnam., 2017, in press.
https://doi.org/10.1007/s40306-017-0217-0

[13] K. Hakuta, Sign of permutations induced by Anick and Nagata-Anick automorphisms over finite fields, J. Math. Res., **9** (2017), no. 4, 23–29.

[14] K. Hakuta, H. Sato, and T. Takagi, On tameness of Matsumoto-Imai central maps in three variables over the finite field $\mathbb{F}_2$, Adv. Math. Commun., **10** (2016), no. 2, 221–228.

[15] K. Hakuta and T. Takagi, Sign of permutation induced by Nagata automorphism over finite fields, J. Math. Res., **9** (2017), no. 5, in press.

[16] J. Hrdina, M. Kureš, and P. Vašík, A note on tame polynomial automorphisms and the security of TTM cryptosystem, Appl. Comput. Math., **9** (2010), no. 2, 226–233.

[17] J.E. Humphreys, Reflection groups and Coxeter groups, Cambridge studies in advanced mathematics 29, Cambridge University Press, Cambridge, 1990.

[18] H.W.E. Jung, Über ganze birationale Transformationen der Ebene, J. Reine Angew. Math., **184** (1942), 161–174.

[19] W. van der Kulk, On polynomial rings in two variables, Nieuw Arch. Wisk., **3** (1953), no. 1, 33–41.

[20] H.W. Lenstra, Jr. and R.J. Schoof, Primitive normal bases for finite fields, Math. Comp. **48** (1987), no. 177, 217–231.

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

[22] S. Maubach and A. Rauf, The profinite polynomial automorphism group, J. Pure Appl. Algebra, **219** (2015), no. 10, 4708–4727.

[23] S. Maubach and R. Willems, Polynomial automorphisms over finite fields: Mimicking tame maps by the Derksen group, Serdica Math. J., **37** (2011), no. 4, 305–322.

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

[25] T.T. Moh, An application of algebraic geometry to encryption: tame transformation method, Rev. Mat. Iberoamericana, **19** (2003), no. 2, 667–685.

[26] T.T. Moh, J.-M. Chen and B.-Y. Yang, Building instances of TTM immune to the Goubin-Courtois attack and the Ding-Schmidt attack, Cryptology ePrint Archive, Report 2004/168, 2004.

[27] J. Patarin, Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt '88, Des. Codes Cryptogr., **20** (2000), no. 2, 175–209.

[28] J. Patarin and L. Goubin, Trapdoor One-Way Permutations and Multivariate Polynomials, In: Y. Han, T. Okamoto, S. Qing (eds.) Information and Communications Security–ICICS 1997, Lecture Notes in Computer Science, vol. 1334, pp. 356–368, Springer, Berlin, Heidelberg (1997).

[29] P.W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, In: S. Goldwasser (ed.) Proceedings of the 35th Annual Symposium on Foundations of Computer Science, pp. 124–134, IEEE Computer Society Press (1994).

[30] D. Ye, Z. Dai, and K. Lam, Decomposing attacks on asymmetric cryptography based on mapping compositions, J. Cryptology, **14** (2001), no. 2, 137–150.