Solving the problem of Blockwise Isomorphism of Polynomials with Circulant matrices

Yasufumi Hashimoto [*]

Abstract

The problem of Isomorphism of Polynomials (IP problem) is known to be important to study the security of multivariate public key cryptosystems, one of major candidates of post-quantum cryptography, against key recovery attacks. In these years, several schemes based on the IP problem itself or its generalization have been proposed. At PQCrypto 2020, Santoso introduced a generalization of the problem of Isomorphism of Polynomials, called the problem of Blockwise Isomorphism of Polynomials (BIP problem), and proposed a new Diffie-Hellman type encryption scheme based on this problem with Circulant matrices (BIPC prolbem). Quite recently, Ikematsu et al. proposed an attack called the linear stack attack to recover an equivalent key of Santoso's encryption scheme. While this attack reduced the security of the scheme, it does not contribute to solve the BIPC problem itself. In the present paper, we describe how to solve the BIPC problem directly by simplifying the BIPC problem due to the conjugation property of circulant matrices. In fact, we experimentally solved the BIPC problem with the parameter, which has 256 bit security by Santoso's security analysis and has 72.7 bit security against the linear stack attack, by about 10 minutes.

Keywords. Isomorphism of Polynomials, Blockwise Isomorphism of Polynomials, circulant matrix

1 Introduction

The problem of Isomorphism of Polynomials (IP problem) is the problem to recover two affine maps S, T satisfying

$$\mathbf{g} = T \circ \mathbf{f} \circ S$$

for given polynomial maps $\mathbf{g}, \mathbf{f}$ over a finite field. This problem was introduced by Patarin [8] and has been discussed mainly in the context of the security analyses of multivariate public key cryptosystems, one of major candidates of post-quantum cryptography [7, 4, 2], since the public key $\mathbf{g}$ of most such cryptosystems are generated by $\mathbf{g} = T \circ \mathbf{f} \circ S$ with a (not necessarily public) quadratic map $\mathbf{f}$ inverted feasibly, and recovering S, T is enough to break the corresponding schemes (e.g. [1, 5]).

In these years, several schemes based on the IP problem or its generalization have been proposed. For example, Wang et al. [10] proposed a key exchange scheme and an encryption scheme based on the IP problem with S, T chosen in commutative rings of square matrices.

[*] Department of Mathematical Science, University of the Ryukyus, hashimoto@math.u-ryukyu.ac.jp

While the commutativity for S, T was required for convenience of these schemes, it yields a vulnerability; in fact, it was broken by Chen et al. [3] since the numbers of unknowns of the IP problem in Wang's schemes is too small. Later, at PQCrypto 2020, Santoso [9] introduced a generalization of the IP problem, called the problem of Blockwise Isomorphism of Polynomials (BIP problem), and proposed a new Diffie-Hellman type encryption scheme based on the BIP problem with Circulant matrices (BIPC problem). It had been considered that the BIP problem was more difficult against analogues of known attacks on the original IP problem (see, e.g. [1]) and then it had been expected that Santoso's scheme was secure enough under suitable parameter selections. However, Ikematsu et al. [6] discovered that this scheme is less secure than expected against the linear stack attack, which is an attack to recover an equivalent key by studying a special version of sufficiently larger size BIPC problem than the original BIPC problem. Remark that, while this attack works to reduce the security of Santoso's scheme, it does not contribute to solve the BIPC problem itself.

In the present paper, we describe how to solve the BIPC problem directly. Since any circulant matrices can be diagonalized or block-diagonalized simultaneously, the BIPC problem can be simplified drastically after (block-) diagonalization. Our approach is quite effective; in fact, the BIPC problem with the parameter, which has 256 bit security by Santoso's security analysis and has 72.7 bit security against the linear stack attack, was experimentally solved by about 10 minutes.

2 Isomorphism of Polynomials

In this section, we describe the Isomorphism of Polynomials, the Blockwise Isomorphism of Polynomials and the encryption scheme proposed by Santoso [9].

2.1 Isomorphism of Polynomials

Let q be a power of prime and $\mathbf{F}_q$ a finite field of order q. For integers $n, m \geq 1$, denote by $\mathrm{MQ}(n, m)$ the set of m-tuples of homogeneous quadratic polynomials ${}^t(f_1(\mathbf{x})), \dots, f_m(\mathbf{x}))$ of n variables $\mathbf{x} = {}^t(x_1, \dots, x_n)$ over $\mathbf{F}_q$. We call that $\mathbf{f}, \mathbf{g} \in \mathrm{MQ}(n, m)$ are *isomorphic* if there exist two invertible linear maps $S : \mathbf{F}_q^n \to \mathbf{F}_q^n$, $T : \mathbf{F}_q^m \to \mathbf{F}_q^m$ such that

$$\mathbf{g} = T \circ \mathbf{f} \circ S, \tag{1}$$

i.e.

$$\begin{pmatrix} g_1(\mathbf{x}) \\ \vdots \\ g_m(\mathbf{x}) \end{pmatrix} = T \begin{pmatrix} f_1(S(\mathbf{x})) \\ \vdots \\ f_m(S(\mathbf{x})) \end{pmatrix},$$

where $\mathbf{f} = {}^t(f_1(\mathbf{x}), \dots, f_m(\mathbf{x}))$ and $\mathbf{g} = {}^t(g_1(\mathbf{x}), \dots, g_m(\mathbf{x}))$. The *problem of Isomorphism of Polynomials (IP problem)* is the problem to recover invertible linear maps $S : \mathbf{F}_q^n \to \mathbf{F}_q^n$, $T : \mathbf{F}_q^m \to \mathbf{F}_q^m$ satisfying (1) for given $\mathbf{f}, \mathbf{g} \in \mathrm{MQ}(n, m)$.

2.2 Blockwise Isomorphism of Polynomials

For $n, m, k \geq 1$, let $\mathbf{f}, \mathbf{g} \in \mathrm{MQ}(n, mk)$ and divide $\mathbf{f}, \mathbf{g}$ by $\mathbf{f} = (\mathbf{f}_1, \ldots, \mathbf{f}_k)$, $\mathbf{g} = (\mathbf{g}_1, \ldots, \mathbf{g}_k)$ with $\mathbf{f}_1, \ldots, \mathbf{f}_k, \mathbf{g}_1, \ldots, \mathbf{g}_k \in \mathrm{MQ}(n, m)$. We call that $\mathbf{f}$ and $\mathbf{g}$ are *blockwise isomorphic* if there exist invertible or zero linear maps $S_1, \ldots, S_k : \mathbf{F}_q^n \to \mathbf{F}_q^n$, $T_1, \ldots, T_k : \mathbf{F}_q^m \to \mathbf{F}_q^m$ satisfying

$$\mathbf{g}_u = \sum_{1 \leq l \leq k} T_l \circ \mathbf{f}_{\overline{u+l-1}} \circ S_l \tag{2}$$

for $1 \leq u \leq k$, where $1 \leq \overline{a} \leq k$ is given by $\overline{a} \equiv a \bmod k$, i.e.

$$\begin{aligned}
\mathbf{g}_1 =& T_1 \circ \mathbf{f}_1 \circ S_1 + T_2 \circ \mathbf{f}_2 \circ S_2 + \cdots + T_k \circ \mathbf{f}_k \circ S_k, \\
\mathbf{g}_2 =& T_1 \circ \mathbf{f}_2 \circ S_1 + T_2 \circ \mathbf{f}_3 \circ S_2 + \cdots + T_k \circ \mathbf{f}_1 \circ S_k, \\
\vdots& \\
\mathbf{g}_k =& T_1 \circ \mathbf{f}_k \circ S_1 + T_2 \circ \mathbf{f}_1 \circ S_2 + \cdots + T_k \circ \mathbf{f}_{k-1} \circ S_k.
\end{aligned}$$

The *problem of blockwise isomorphism of polynomials (BIP prolbem)* is the problem to recover invertible or zero linear maps $S_1, \ldots, S_k : \mathbf{F}_q^n \to \mathbf{F}_q^n$, $T_1, \ldots, T_k : \mathbf{F}_q^m \to \mathbf{F}_q^m$ satisfying (2) for given $\mathbf{f}, \mathbf{g} \in \mathrm{MQ}(n, mk)$.

2.3 Blockwise Isomorphism of Polynomials with Circulant matrices

Santoso's encryption scheme is based on BIP problem with circulant matrices.

Let I_n be the $n \times n$ identity matrix and $J_n := \begin{pmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ 1 & & & \end{pmatrix}$ the n-cyclic permutation matrix. A *circulant matrix* is a linear sum of $I_n, J_n, J_n^2, \ldots, J_n^{n-1}$, i.e. a circulant matrix is given by

$$a_0 I_n + a_1 J_n + a_2 J_n^2 + \cdots + a_{n-1} J_n^{n-1} = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-2} & a_{n-1} \\ a_{n-1} & a_0 & \ddots & a_{n-3} & a_{n-2} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ a_2 & a_3 & \ddots & a_0 & a_1 \\ a_1 & a_2 & \cdots & a_{n-1} & a_0 \end{pmatrix}$$

for some $a_0, \ldots, a_{n-1} \in \mathbf{F}_q$. Note that the multiplication between circulant matrices is commutative. Let $\mathrm{Circ}(n)$ be the set of $n \times n$ circulant matrices and

$$\Psi(n, m, k) := \left\{ (S_1, \ldots, S_k, T_1, \ldots, T_k) \;\middle|\; \begin{array}{l} S_1, \ldots, S_k \in \mathrm{Circ}(n), \\ T_1, \ldots, T_k \in \mathrm{Circ}(m), \end{array} \quad \text{invertible or } 0 \right\}.$$

For $\mathbf{f} \in \mathrm{MQ}(n, mk)$ and $\psi = (S_1, \ldots, S_k, T_1, \ldots, T_k) \in \Psi(n, m, k)$, define the operator $\boxast$ such that $\mathbf{g} = \psi \boxast \mathbf{f}$ is as given in (2). Note that $\psi, \varphi \in \Psi(n, m, k)$ is commutative for the operator $\boxast$, i.e. it holds

$$\varphi \boxast (\psi \boxast \mathbf{g}) = \psi \boxast (\varphi \boxast \mathbf{g})$$

for any $\mathbf{f} \in \mathrm{MQ}(n, mk)$ (see Lemma 1 in [9]).

2.4 Encryption scheme based on BIP with Circulant matrices

Santoso's El-Gammal-like encryption scheme is constructed as follows [9].

Parameters. $n, m, k \geq 1$: integers.

Secret key. $\Upsilon \in \Psi(n, m, k)$.

Public key. $\mathbf{f}, \mathbf{g} \in \mathrm{MQ}(n, mk)$ with $\mathbf{g} = \Upsilon \boxast \mathbf{f}$.

Encryption. For a plain-text $\nu \in \mathrm{MQ}(n, mk)$, choose $\psi \in \Psi(n, m, k)$ randomly and compute

$$\mathbf{c}_0 := \psi \boxast \mathbf{g}, \qquad \mathbf{c}_1 := \nu + \psi \boxast \mathbf{f}.$$

The cipher-text is $(\mathbf{c}_0, \mathbf{c}_1) \in \mathrm{MQ}(n, mk)^2$.

Decryption. The plain-text is recovered by

$$\nu = \mathbf{c}_1 - \Upsilon \boxast \mathbf{c}_0.$$

Since the operations by ψ and Υ are commutative, the cipher-text can be decrypted correctly.

2.5 Previous security analyses and parameter selections

We first note that this scheme was proven to be secure against one way under chosen plain-text attack (OW-CPA) under the assumption that the CDH-BIPC problem, an analogue of the Computational Diffie-Hellman problem for BIP with Circulant matrices, is hard [9]. Furthermore, it was pointed out that this scheme can be transformed into an IND-CCA secure encryption scheme by an approach of Fujisaki-Okamoto-like transformation. Until now, the following three attacks have been studied by by Santoso himself [9] and Ikematsu et al. [6].

(1) Attack by Bouillagust et al. Bouillagust et al. [1] proposed an attack to solve the IP problem to recover S, T with $\mathbf{g} = T \circ \mathbf{f} \circ S$. The basic approach is to find a pair of vectors $\mathbf{a}, \mathbf{b} \in \mathbf{F}_q^n$ such that $\bar{S}^{-1}\mathbf{a} = \mathbf{b}$, where $\bar{S}$ is an linear map with $\mathbf{g} = \bar{T} \circ \mathbf{f} \circ \bar{S}$. Santoso [9] generalized this attack on the BIP problem with circulant matrices and estimated the complexity by $O\left(k^2 n^5 2^{n\frac{k}{k+1}}\right)$.

(2) The Gröbner basis attack. The unknown parameters in $S_1, \ldots, S_k \in \mathrm{Circ}(n)$ and $T_1, \ldots, T_k \in \mathrm{Circ}(m)$ are $nk + mk$ in the total, and the coefficients of the quadratic polynomials in $\mathbf{g} = \Upsilon \boxast \mathbf{f}$ give a system of $\frac{1}{2}n(n+1)mk$ equations over $\mathbf{F}_q$, which are linear for the unknowns in T's, quadratic for the unknowns in S's and cubic in the total. The Gröbner basis attack is to solve such a system equations directly by the Gröbner basis algorithm. Santoso [9] estimated its complexity by $O\left(2^{k \log(nm)/4m}\right)$.

(3) Linear stack attack. The linear stack attack [6] is an attack to recover $\Upsilon_1, \ldots, \Upsilon_N \in \Psi(n, m, k)$ such that $\mathbf{g} = \sum_{1 \leq i \leq N} \Upsilon_i \boxast \mathbf{f}$ for sufficiently large N (usually $\sim \frac{1}{2}n^2 m$). It is easy to check that, if such $\Upsilon_1, \ldots, \Upsilon_N$ are recovered, the cipher-text $(\mathbf{c}_0, \mathbf{c}_1)$ is decrypted by $\nu = \mathbf{c}_1 - \sum_{1 \leq i \leq N} \Upsilon_i \boxast \mathbf{c}_0$. Its complexity is (heuristically) estimated by $O\left(n^6 m^3 k^3\right)$.

Table 1 shows the the parameter selections by Santoso [9] based on the security analyses (i), (ii) above, and their security against the attack (iii).

Table 1: Parameter selections of Santoso's encryption scheme and previous security analyses

(n, m, k)	(1), (2) [9]	(3) [6]
(84,2,140)	128 bit	62.7 bit
(206,2,236)	256 bit	72.7 bit
(16,2,205)	128 bit	50.0 bit
(16,2,410)	256 bit	53.0 bit

3 Solving the BIP problem with Circulant matrices

In this section, we describe how to solve the BIP problem with circulant matrices. Before it, we study the conjugations of circulant matrices to simplify the problem.

3.1 Conjugations of circulant matrices

Let $n \geq 1$ be an integer and p the characteristic of $\mathbf{F}_q$. When $p \nmid n$, denote by θ_n an n-th root of 1, i.e. θ_n is an element of $\mathbf{F}_q$ or its extension field satisfying $\theta_n^n = 1$ and $\theta_n^l \neq 1$ for $1 \leq l \leq n-1$. Define the $n \times n$ matrix Θ_n by

$$\Theta_n := \left(\theta_n^{(i-1)(j-1)}\right)_{1 \leq i,j \leq n} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \theta_n & \cdots & \theta_n^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \theta_n^{n-1} & \cdots & \theta_n^{(n-1)^2} \end{pmatrix}.$$

We also define the $n \times n$ matrices B_n by the lower triangular matrix whose (i,j)-entries $(i \geq j)$ is $\binom{i-1}{j-1}$, and L_n by the upper triangular matrix whose $(i, i+1)$-entries are 1 $(1 \leq i \leq n)$ and other entries are 0, i.e.

$$B_n := \begin{pmatrix} 1 & & & & \\ 1 & 1 & & & \\ 1 & 2 & 1 & & \\ \vdots & \vdots & \vdots & \ddots & \\ 1 & n-1 & \binom{n-1}{2} & \cdots & 1 \end{pmatrix}, \qquad L_n := \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & 0 & 1 \\ & & & & 0 \end{pmatrix}.$$

Note that

$$L_n^2 := \begin{pmatrix} 0 & 0 & 1 & & \\ & \ddots & \ddots & \ddots & \\ & & 0 & 0 & 1 \\ & & & 0 & 0 \\ & & & & 0 \end{pmatrix}, \quad \ldots, \quad L_n^{n-1} := \begin{pmatrix} & & & & 1 \\ & & & & \\ & & & & \\ & & & & \\ & & & & \end{pmatrix}$$

and $L_n^n = 0_n$. We also denote by

$$\mathrm{diag}(a_1, \ldots, a_n) := \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix}, \qquad A \otimes B := \begin{pmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{n1}B & \cdots & a_{nn}B \end{pmatrix}$$

for scalars or matrices $a_1, \ldots, a_n$ and matrices $A = (a_{ij})_{i,j}$, B. Then the following lemmas hold.

Lemma 3.1. *Let n be an integer factored by $n = n_1 p^r$ with $p \nmid n_1$, $r \geq 0$. Then there exists an $n \times n$ permutation matrix K_n such that*

$$Q_n^{-1} J_n Q_n = \mathrm{diag}\left(1, \theta_{n_1}, \ldots, \theta_{n_1}^{n_1-1}\right) \otimes \left(I_{p^r} + L_{p^r}\right),$$

where $Q_n := K_n \cdot (\Theta_{n_1} \otimes B_{p^r})$.

Proof. (i) When $p \nmid n$ ($r = 0$), the (i,j)-entries of $J_n \Theta_n$ and $\Theta_n \mathrm{diag}\left(1, \theta_n, \ldots, \theta_n^{n-1}\right)$ are $\theta_n^{i(j-1)}$ for $1 \leq i \leq n-1$ and 1 for $i = n$ since $\theta_n^n = 1$. Then it holds

$$J_n \Theta_n = \Theta_n \mathrm{diag}\left(1, \theta_n, \ldots, \theta_n^{n-1}\right).$$

(ii) When $n = p^r$ ($n_1 = 1$), the (i,j)-entries of $J_n B_n$ are $\binom{i}{j-1}$ for $j-1 \leq i \leq n-1$, 1 for $(i,j) = (n,1)$ and 0 otherwise. On the other hand, the (i,j)-entries of $B_n\left(I_n + L_n\right)$ is 1 for $j = 1$, $\binom{i-1}{j-2} + \binom{i-1}{j-1} = \binom{i}{j-1}$ for $2 \leq j \leq i+1$ and 0 otherwise. Since $\binom{p^r}{j-1} = 0$ in $\mathbf{F}_q$ for $2 \leq j \leq p^r$, we have

$$J_{p^r} B_{p^r} = B_{p^r}\left(I_{p^r} + L_{p^r}\right).$$

(iii) Since both J_n and $J_{n_1} \otimes J_{p^r}$ are of n-cyclic, these are conjugate to each other in the symmetric group $\mathfrak{S}_n$, i.e. there exists an $n \times n$ permutation matrix K_n such that

$$K_n^{-1} J_n K_n = J_{n_1} \otimes J_{p^r}.$$

We thus obtain

$$\begin{aligned} Q_n^{-1} J_n Q_n =& \left(\Theta_{n_1} \otimes B_{p^r}\right)^{-1} \left(J_{n_1} \otimes J_{p^r}\right) \left(\Theta_{n_1} \otimes B_{p^r}\right) \\ =& \left(\Theta_{n_1}^{-1} J_{n_1} \Theta_{n_1}\right) \otimes \left(B_{p^r}^{-1} J_{p^r} B_{p^r}\right) \\ =& \mathrm{diag}\left(1, \theta_{n_1}, \ldots, \theta_{n_1}^{n_1-1}\right) \otimes \left(I_{p^r} + L_{p^r}\right). \end{aligned}$$

□

Lemma 3.2. *Let n be an integer factored by $n = n_1 p^r$ with $p \nmid n_1$, $r \geq 0$ and $Q_n := K_n(\Theta_{n_1} \otimes B_{p^r})$. Then, for $S \in \mathrm{Circ}(n)$, there exist $s_{11}, \ldots, s_{1p^r} \in \mathbf{F}_q$ and $s_{21}, \ldots, s_{2p^r}, s_{31}, \ldots, \ldots, \ldots, s_{n_1 p^r} \in \mathbf{F}_q(\theta_{n_1})$ such that*

$$\begin{aligned} Q_n^{-1} S Q_n =& \mathrm{diag}\Big(s_{11} I_{p^r} + s_{12} L_{p^r} + \cdots + s_{1p^r} L_{p^r}^{p^r-1}, \\ & s_{21} I_{p^r} + s_{22} L_{p^r} + \cdots + s_{2p^r} L_{p^r}^{p^r-1}, \\ & \cdots, s_{n_1 1} I_{p^r} + s_{n_1 2} L_{p^r} + \cdots + s_{n_1 p^r} L_{p^r}^{p^r-1}\Big) \\ =& \mathrm{diag}\left(\begin{pmatrix} s_{11} & s_{12} & \cdots & s_{1p^r} \\ & \ddots & \ddots & \vdots \\ & & s_{11} & s_{12} \\ & & & s_{11} \end{pmatrix}, \ldots, \begin{pmatrix} s_{n_1 1} & s_{n_1 2} & \cdots & s_{n_1 p^r} \\ & \ddots & \ddots & \vdots \\ & & s_{n_1 1} & s_{n_1 2} \\ & & & s_{n_1 1} \end{pmatrix}\right). \end{aligned}$$

Proof. A circulant matrix S is written by

$$S = a_1 I_n + a_2 J_n + \cdots + a_n J_n^{n-1}$$

for some $a_1, \ldots, a_n \in \mathbf{F}_q$. Then, according to Lemma 3.1, we have

$$\begin{aligned} Q_n^{-1} S Q_n =& a_1 I_n + a_2 \cdot \operatorname{diag}\left(1, \theta_{n_1}, \ldots, \theta_{n_1}^{n_1-1}\right) \otimes \left(I_{p^r} + L_{p^r}\right) \\ &+ a_3 \cdot \operatorname{diag}\left(1, \theta_{n_1}^2, \ldots, \theta_{n_1}^{2(n_1-1)}\right) \otimes \left(I_{p^r} + L_{p^r}\right)^2 \\ &+ \cdots + a_n \cdot \operatorname{diag}\left(1, \theta_{n_1}^{n-1}, \ldots, \theta_{n_1}^{(n_1-1)(n-1)}\right) \otimes \left(I_{p^r} + L_{p^r}\right)^{n-1}. \end{aligned}$$

Since $L_{p^r}^{p^r} = 0$, the matrices $I_{p^r}, I_{p^r} + L_{p^r}, (I_{p^r} + L_{p^r})^2, \ldots, (I_{p^r} + L_{p^r})^{n-1}$ are linear sums of $I_{p^r}, L_{p^r}, L_{p^r}^2, \ldots, L_{p^r}^{p^r-1}$. Thus we can easily check that Lemma 3.2 holds. □

3.2 Equivalent keys

Let $n, m \geq 1$ be integers factored by $n = n_1 p^a$, $m = m_1 p^b$ with $a, b \geq 0$, $p \nmid n_1, m_1$. For $1 \leq l \leq k$, define

$$\begin{aligned} \bar{\mathbf{f}}_l &:= Q_m^{-1} \circ \mathbf{f}_l \circ Q_n, & \bar{\mathbf{g}}_l &:= Q_m^{-1} \circ \mathbf{g}_l \circ Q_n, \\ \bar{S}_l &:= Q_n^{-1} \circ S_l \circ Q_n, & \bar{T}_l &:= Q_m^{-1} \circ T_l \circ Q_m. \end{aligned}$$

Note that, due to Lemma 3.2, we see that $\bar{S}_l, \bar{T}_l$ are written by

$$\begin{aligned} \bar{S}_l =& \operatorname{diag}\left(\begin{pmatrix} s_{11}^{(l)} & s_{12}^{(l)} & \cdots & s_{1p^a}^{(l)} \\ & \ddots & \ddots & \vdots \\ & & s_{11}^{(l)} & s_{12}^{(l)} \\ & & & s_{11}^{(l)} \end{pmatrix}, \ldots, \begin{pmatrix} s_{n_1 1}^{(l)} & s_{n_1 2}^{(l)} & \cdots & s_{n_1 p^a}^{(l)} \\ & \ddots & \ddots & \vdots \\ & & s_{n_1 1}^{(l)} & s_{n_1 2}^{(l)} \\ & & & s_{n_1 1}^{(l)} \end{pmatrix}\right), \\ \bar{T}_l =& \operatorname{diag}\left(\begin{pmatrix} t_{11}^{(l)} & t_{12}^{(l)} & \cdots & t_{1p^b}^{(l)} \\ & \ddots & \ddots & \vdots \\ & & t_{11}^{(l)} & t_{12}^{(l)} \\ & & & t_{11}^{(l)} \end{pmatrix}, \ldots, \begin{pmatrix} t_{m_1 1}^{(l)} & t_{m_1 2}^{(l)} & \cdots & t_{m_1 p^b}^{(l)} \\ & \ddots & \ddots & \vdots \\ & & t_{m_1 1}^{(l)} & t_{m_1 2}^{(l)} \\ & & & t_{m_1 1}^{(l)} \end{pmatrix}\right). \end{aligned} \tag{3}$$

Since

$$\begin{aligned} Q_m^{-1} \circ (T_l \circ \mathbf{f}_u \circ S_l) \circ Q_n =& (Q_m^{-1} \circ T_l \circ Q_m) \circ (Q_m^{-1} \circ \mathbf{f}_u \circ Q_n) \circ (Q_n^{-1} \circ S_l \circ Q_n) \\ =& \bar{T}_l \circ \bar{\mathbf{f}}_u \circ \bar{S}_l, \end{aligned}$$

we have

$$\bar{\mathbf{g}}_u = \sum_{1 \leq l \leq k} \bar{T}_l \circ \bar{\mathbf{f}}_{\overline{u+l-1}} \circ \bar{S}_l. \tag{4}$$

This means that the BIP problem with Circulant matrices is reduced to the problem recovering $\bar{S}_1,\dots,\bar{S}_k,\bar{T}_1,\dots,\bar{T}_k$ in the forms (3) for given $\bar{\mathbf{f}}$ and $\bar{\mathbf{g}}$. Furthermore, since

$$(\alpha^2\bar{T}_l)\circ\bar{\mathbf{f}}_u\circ(\alpha^{-1}\bar{S}_l)=\bar{T}_l\circ\bar{\mathbf{f}}_u\circ\bar{S}_l$$

for any $\alpha\in\mathbf{F}_q\backslash\{0\}$ and

$$0\circ\bar{\mathbf{f}}_u\circ\bar{S}_l=\bar{T}_l\circ\bar{\mathbf{f}}_u\circ 0=0,$$

we can take $s_{11}^{(l)}=1$ for $1\le l\le k$ without loss generality. In the next subsection, we describe how to recover other parameters in $\bar{S}_l$ and $\bar{T}_l$.

3.3 Solving the BIP problem with Circulant matrices

For $1\le u\le k$ and $1\le v\le m$, denote by

$$\bar{\mathbf{f}}_u(\mathbf{x})={}^t(\bar{f}_{u1}(\mathbf{x}),\dots,\bar{f}_{um}(\mathbf{x})),\qquad \bar{f}_{uv}(\mathbf{x})=\sum_{1\le i\le j\le n}\alpha_{ij}^{(uv)}x_ix_j,$$
$$\bar{\mathbf{g}}_u(\mathbf{x})={}^t(\bar{g}_{u1}(\mathbf{x}),\dots,\bar{g}_{um}(\mathbf{x})),\qquad \bar{g}_{uv}(\mathbf{x})=\sum_{1\le i\le j\le n}\beta_{ij}^{(uv)}x_ix_j.$$

We can recover $\bar{S}_l$ and $\bar{T}_l$ as follows.

3.3.1 Recovering $\bar{T}_l$.

We first study the polynomial $\bar{g}_{um}(\mathbf{x})$ for $1\le u\le k$. Since $\bar{S}_l,\bar{T}_l$ are as in (3) and $s_{11}^{(l)}=1$, we see that the coefficient of x_1^2 of $\bar{g}_{um}(\mathbf{x})$ in (4) gives the equation

$$\beta_{11}^{(um)}=\sum_{1\le l\le k}\alpha_{11}^{(\overline{u+l-1},m)}t_{m_11}^{(l)}. \tag{5}$$

Since the set of the equations (5) for $1\le u\le k$ is a system of k linear equations of k variables $t_{m_11}^{(1)},\dots,t_{m_11}^{(k)}$, one can recover $t_{m_11}^{(1)},\dots,t_{m_11}^{(k)}$ by solving this system.

Next, the coefficient of x_1^2 of $\bar{g}_{u,m-1}(\mathbf{x})$ in (4) gives

$$\beta_{11}^{(u,m-1)}=\sum_{1\le l\le k}\left(\alpha_{11}^{(\overline{u+l-1},m-1)}t_{m_11}^{(l)}+\alpha_{11}^{(\overline{u+l-1},m)}t_{m_12}^{(l)}\right).$$

Since $t_{m_11}^{(1)},\dots,t_{m_11}^{(k)}$ are already given, one can recover $t_{m_12}^{(1)},\dots,t_{m_12}^{(k)}$ by solving the equations above for $1\le u\le k$. Other parameters in $\bar{T}$ can be recovered by the equations derived from the coefficients of x_1^2 in $\bar{g}_{u,m-2}(\mathbf{x}),\dots,\bar{g}_{u,1}(\mathbf{x})$ recursively.

3.3.2 Recovering $\bar{S}_l$.

Study $\bar{g}_{um}(\mathbf{x})$ again. Since $s_{11}^{(l)}=1$, the coefficient of x_1x_2 of $\bar{g}_{um}(\mathbf{x})$ gives the equation

$$\beta_{12}^{(um)}=\sum_{1\le l\le k}\left(2\alpha_{11}^{(\overline{u+l-1},m)}s_{12}^{(l)}+\alpha_{12}^{(\overline{u+l-1},m)}\right)t_{m_11}^{(l)}. \tag{6}$$

Since $t_{m_1 1}^{(l)}$ is already given, one can recover $s_{12}^{(l)}$ by solving the system of k linear equations of k variables $s_{12}^{(1)}, \ldots, s_{12}^{(k)}$ derived from the equation (6) for $1 \leq u \leq k$.

Next, the coefficient of $x_1 x_3$ in $\bar{g}_{um}(\mathbf{x})$ is

$$\beta_{13}^{(um)} = \sum_{1 \leq l \leq k} \left(2\alpha_{11}^{(\overline{u+l-1},m)} s_{13}^{(l)} + \alpha_{12}^{(\overline{u+l-1},m)} s_{12}^{(l)} + \alpha_{13}^{(\overline{u+l-1},m)} \right) t_{m_1 1}^{(l)}. \tag{7}$$

Since $t_{m_1 1}^{(l)}, s_{12}^{(l)}$ are already given, $s_{13}^{(l)}$ can be recovered from the equation above for $1 \leq l \leq k$. It is easy to see that one can recover other parameters $s_{14}^{(l)}, \ldots, s_{n_1 p^a}^{(l)}$ by the systems of linear equations derived from the coefficients of $x_1 x_4, \ldots, x_1 x_n$ in $\bar{g}_{um}(\mathbf{x})$ recursively.

Remark 3.3. *If q is even, $s_{12}^{(l)}$ does not appear in the equation* (6) *and then $s_{12}^{(l)}$ cannot be recovered from the coefficient of $x_1 x_2$. On the other hand, the equation* (7) *derived from the coefficient of $x_1 x_3$ includes $s_{12}^{(l)}$ but not $s_{13}^{(l)}$. This means that $s_{12}^{(l)}$ is recovered from the coefficient of $x_1 x_3$ instead of $x_1 x_2$. Similarly, we can easily check that $s_{13}^{(l)}, \ldots, s_{1p^a}^{(l)}$ are recovered from the coefficients of $x_1 x_4, \ldots, x_1 x_{p^a}, x_2 x_{p^a}$ respectively instead of $x_1 x_3, \ldots, x_1 x_{p^a}$.*

Remark 3.4. *There is a possibility that the parameters in $(\bar{S}_1, \ldots, \bar{S}_k, \bar{T}_1, \ldots, \bar{T}_k)$ are not fixed uniquely from the linear equations derived from the coefficients of x_1^2 in $\bar{g}_{u1}(\mathbf{x}), \ldots, \bar{g}_{um}(\mathbf{x})$ and of $x_1 x_2, \ldots, x_1 x_n$ in $\bar{g}_{um}(\mathbf{x})$. If such a case occurs, recover the parameters in $(\bar{S}_1, \ldots, \bar{S}_k, \bar{T}_1, \ldots, \bar{T}_k)$ as possible, study the coefficients not used to recover such parameters and state the equations for the parameters not fixed uniquely yet. Then one can expect to fix them uniquely. For example, the coefficients of x_2^2 includes $s_{12}^{(l)}$ quadratically and then it helps to fix $s_{12}^{(l)}$.*

3.3.3 Complexity.

It is easy to see that, to compute $\bar{\mathbf{f}}, \bar{\mathbf{g}}$ totally, we need (at most) $O(n^3 mk)$ arithmetics on $\mathbf{F}_q(\theta_{n_1}, \theta_{m_1})$. However, we use only the coefficients of $x_1^2, x_1 x_2, \ldots, x_1 x_n$ and then the number of required arithmetics in this process is $O(n^2 mk)$. Furthermore, since the attacker solves the systems of k linear equations of k variables in m times for recovering $\bar{T}_l$ and in n times for recovering $\bar{S}_l$, the number of required arithmetics for recovering them is (at most) $O(k^3(n+m))$ over $\mathbf{F}_q(\theta_{n_1}, \theta_{m_1})$. We thus conclude that the total number of arithmetics on $\mathbf{F}_q(\theta_{n_1}, \theta_{m_1})$ of our approach is estimated by $O(kn^2 m + k^3 n + k^3 m)$.

3.3.4 Experiments.

We implemented our attack on Magma ver.2.24-5 under macOS Mojave ver.10.14.16, Intel Core i5, 3 GHz. In Table 2, we describe the experimental results of our attack for the parameters selected in [9] and studied in [6]. This shows that our approach is quite effective to solve the BIP problem with Circulant matrices.

4 Conclusion

The present paper shows that solving the BIP problem with Circulant matrices directly is not difficult since the secret maps $S_1, \ldots, S_k, T_1, \ldots, T_k$ are known to be circulant. We consider that,

Table 2: Parameter selections of the proposed encryption scheme

(n,m,k)	(1), (2) [9]	(3)	[6]	Our Attack
(42,2,102)	—	—	4.8 days	9.9 sec.
(84,2,140)	128 bit	62.7 bit	—	34.5 sec.
(206,2,236)	256 bit	72.7 bit	—	619 sec.
(16,2,205)	128 bit	50.0 bit	10 hr.	15.5 sec.
(16,2,410)	256 bit	53.0 bit	—	150 sec.

while the original BIP problem is difficult enough at the present time, it will be solved similarly if the secret maps to be recovered have some kind of “special” structures. Then, to build a secure scheme based on the BIP problem, one should choose the secret maps as randomly as possible.

Acknowledgments. The author was supported by JST CREST no. JPMJCR14D6 and JSPS Grant-in-Aid for Scientific Research (C) no. 17K05181.

References

[1] C. Bouillaguet, J.-C. Faugére, P.-A. Fouque, L. Perret, Isomorphism of Polynomials: New Results, `http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=20524EF65899B40DEE494630B0574F53?doi=10.1.1.156.9570&rep=rep1&type=pdf`, 2009.

[2] A. Casanova, J.C. Faugère, G. Macario-Rat, J. Patarin, L. Perret, J. Ryckeghem, GeMSS: A Great Multivariate Short Signature, `https://www-polsys.lip6.fr/Links/NIST/GeMSS.html`

[3] J. Chen, C.H. Tan, X. Li, Practical Cryptanalysis of a Public Key Cryptosystem Based on the Morphism of Polynomials Problem, Tsinghua Science and Technology **23** (2018), pp. 671–679.

[4] M.-S.Chen, J. Ding, M. Kannwischer, J. Patarin, A. Petzoldt, D. Schmidt, B.-Y. Yang, Rainbow Signature, `https://www.pqcrainbow.org/`.

[5] J.-C. Faugére, L. Perret, Polynomial Equivalence Problems: Algorithmic and Theoretical Aspects, Eurocrypt 2006, LNCS **4004** (2006), pp. 30–47.

[6] Y. Ikematsu, and S. Nakamura, B. Santoso, T. Yasuda, Security Analysis on an El-Gamal-like Multivariate Encryption Scheme Based on Isomorphism of Polynomials, `https://eprint.iacr.org/2021/169`, 2021.

[7] NIST, Post-Quantum Cryptography, Round 3 submissions, `https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions`.

[8] , J. Patarin, Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms, Eurocrypto 1996, LNCS **1070** (1997), pp. 33-48.

[9] B. Santoso Generalization of Isomorphism of Polynomials with Two Secrets and Its Application to Public Key Encryption, PQCrypto 2020, LNCS **12100** (2020), pp.340–359.

[10] H. Wang, H. Zhang, S. Mao, W. Wu, L. Zhang, New Public-Key Cryptosystem Based on the Morphism of Polynomials Problem, Tsinghua Science and Technology **21** (2016), pp. 302-311.

A Toy example

We now demonstrate how to solve the BIPC problem for $(q, n, m, k) = (2, 6, 2, 2)$ as a toy example. The public keys $\mathbf{f} = (\mathbf{f}_1, \mathbf{f}_2) = (f_{11}, f_{12}, f_{21}, f_{22})$ and $\mathbf{g} = (\mathbf{g}_1, \mathbf{g}_2) = (g_{11}, g_{12}, g_{21}, g_{22})$ are as follows.

$$f_{11}(\mathbf{x}) = {}^t\mathbf{x}\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ & 1 & 0 & 0 & 0 & 1 \\ & & 0 & 0 & 0 & 0 \\ & & & 0 & 0 & 0 \\ & & & & 1 & 1 \\ & & & & & 0 \end{pmatrix}\mathbf{x}, \qquad f_{12}(\mathbf{x}) = {}^t\mathbf{x}\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ & 1 & 1 & 0 & 0 & 1 \\ & & 1 & 0 & 1 & 1 \\ & & & 0 & 0 & 0 \\ & & & & 1 & 1 \\ & & & & & 1 \end{pmatrix}\mathbf{x},$$

$$f_{21}(\mathbf{x}) = {}^t\mathbf{x}\begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 0 \\ & 1 & 1 & 1 & 1 & 1 \\ & & 0 & 1 & 0 & 0 \\ & & & 0 & 1 & 1 \\ & & & & 0 & 0 \\ & & & & & 1 \end{pmatrix}\mathbf{x}, \qquad f_{22}(\mathbf{x}) = {}^t\mathbf{x}\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 \\ & 0 & 0 & 1 & 1 & 1 \\ & & 0 & 1 & 0 & 0 \\ & & & 0 & 0 & 1 \\ & & & & 1 & 1 \\ & & & & & 1 \end{pmatrix}\mathbf{x},$$

$$g_{11}(\mathbf{x}) = {}^t\mathbf{x}\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 1 \\ & 0 & 1 & 0 & 0 & 0 \\ & & 1 & 0 & 0 & 1 \\ & & & 0 & 1 & 1 \\ & & & & 1 & 0 \\ & & & & & 1 \end{pmatrix}\mathbf{x}, \qquad g_{12}(\mathbf{x}) = {}^t\mathbf{x}\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ & 1 & 0 & 0 & 0 & 0 \\ & & 0 & 1 & 1 & 1 \\ & & & 1 & 1 & 1 \\ & & & & 0 & 0 \\ & & & & & 1 \end{pmatrix}\mathbf{x},$$

$$g_{21}(\mathbf{x}) = {}^t\mathbf{x}\begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ & 0 & 1 & 1 & 0 & 1 \\ & & 1 & 1 & 0 & 1 \\ & & & 0 & 0 & 1 \\ & & & & 1 & 0 \\ & & & & & 1 \end{pmatrix}\mathbf{x}, \qquad g_{22}(\mathbf{x}) = {}^t\mathbf{x}\begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ & 1 & 1 & 1 & 1 & 0 \\ & & 0 & 0 & 0 & 1 \\ & & & 0 & 0 & 0 \\ & & & & 1 & 0 \\ & & & & & 0 \end{pmatrix}\mathbf{x},$$

where the coefficient matrices are expressed by triangular matrices. Our aim is to recover recover $S_1, S_2 \in \mathrm{Circ}(6)$, $T_1, T_2 \in \mathrm{Circ}(2)$ satisfying

$$\begin{aligned} \begin{pmatrix} g_{11}(\mathbf{x}) \\ g_{12}(\mathbf{x}) \end{pmatrix} &= T_1 \begin{pmatrix} f_{11}(S_1(\mathbf{x})) \\ f_{12}(S_1(\mathbf{x})) \end{pmatrix} + T_2 \begin{pmatrix} f_{21}(S_2(\mathbf{x})) \\ f_{22}(S_2(\mathbf{x})) \end{pmatrix}, \\ \begin{pmatrix} g_{21}(\mathbf{x}) \\ g_{22}(\mathbf{x}) \end{pmatrix} &= T_1 \begin{pmatrix} f_{21}(S_1(\mathbf{x})) \\ f_{22}(S_1(\mathbf{x})) \end{pmatrix} + T_2 \begin{pmatrix} f_{11}(S_2(\mathbf{x})) \\ f_{12}(S_2(\mathbf{x})) \end{pmatrix}. \end{aligned} \tag{8}$$

Let θ be a cubic root of 1 (i.e. $\theta^2 + \theta + 1 = 0$),

$$K_6 := \begin{pmatrix} 1 & & & & & \\ & & & 1 & & \\ & & & & 1 & \\ & 1 & & & & \\ & & 1 & & & \\ & & & & & 1 \end{pmatrix}, \quad \Theta_3 := \begin{pmatrix} 1 & 1 & 1 \\ 1 & \theta & \theta^2 \\ 1 & \theta^2 & \theta \end{pmatrix}, \quad Q_2 = B_2 := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

and $Q_6 := K_6\,(\Theta_3 \otimes B_2)$. Then $\bar{\mathbf{f}}_1 = Q_2^{-1} \circ \mathbf{f}_1 \circ Q_6 = (\bar{f}_{11}, \bar{f}_{12})$, $\bar{\mathbf{f}}_2 = Q_2^{-1} \circ \mathbf{f}_2 \circ Q_6 = (\bar{f}_{21}, \bar{f}_{22})$, $\bar{\mathbf{g}}_1 = Q_2^{-1} \circ \mathbf{g}_1 \circ Q_6 = (\bar{g}_{11}, \bar{g}_{12})$, $\bar{\mathbf{g}}_2 = Q_2^{-1} \circ \mathbf{g}_2 \circ Q_6 = (\bar{g}_{21}, \bar{g}_{22})$ are as follows.

$$\bar{f}_{11}(\mathbf{x}) = {}^t\mathbf{x} \begin{pmatrix} 1 & 1 & 0 & \theta & 0 & \theta^2 \\ & 0 & \theta^2 & 1 & \theta & 1 \\ & & 1 & 1 & 0 & \theta \\ & & & \theta & \theta^2 & 1 \\ & & & & 1 & 1 \\ & & & & & \theta^2 \end{pmatrix} \mathbf{x}, \qquad \bar{f}_{12}(\mathbf{x}) = {}^t\mathbf{x} \begin{pmatrix} 1 & 0 & 1 & \theta^2 & 1 & \theta \\ & 1 & 0 & 0 & 0 & 0 \\ & & \theta^2 & 1 & 0 & 0 \\ & & & \theta & 0 & 0 \\ & & & & \theta & 1 \\ & & & & & \theta^2 \end{pmatrix} \mathbf{x},$$

$$\bar{f}_{21}(\mathbf{x}) = {}^t\mathbf{x} \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ & 1 & 1 & 0 & 1 & 0 \\ & & \theta & \theta & 0 & \theta \\ & & & 1 & \theta^2 & 1 \\ & & & & \theta^2 & \theta^2 \\ & & & & & 1 \end{pmatrix} \mathbf{x}, \qquad \bar{f}_{22}(\mathbf{x}) = {}^t\mathbf{x} \begin{pmatrix} 0 & 1 & 0 & \theta^2 & 0 & \theta \\ & 1 & \theta^2 & 0 & \theta & 0 \\ & & 0 & 1 & 0 & 1 \\ & & & \theta^2 & 1 & 0 \\ & & & & 0 & 1 \\ & & & & & \theta 1 \end{pmatrix} \mathbf{x},$$

$$\bar{g}_{11}(\mathbf{x}) = {}^t\mathbf{x} \begin{pmatrix} 0 & 0 & \theta^2 & \theta & \theta & \theta^2 \\ & 0 & 1 & \theta & 1 & \theta^2 \\ & & \theta^2 & 1 & 0 & 0 \\ & & & 1 & 0 & 1 \\ & & & & \theta & 1 \\ & & & & & 1 \end{pmatrix} \mathbf{x}, \qquad \bar{g}_{12}(\mathbf{x}) = {}^t\mathbf{x} \begin{pmatrix} 1 & 1 & 1 & \theta^2 & 1 & \theta \\ & 0 & 1 & 0 & 1 & 0 \\ & & \theta^2 & \theta & 0 & 1 \\ & & & \theta & 1 & 0 \\ & & & & \theta & \theta^2 \\ & & & & & \theta^2 \end{pmatrix} \mathbf{x},$$

$$\bar{g}_{21}(\mathbf{x}) = {}^t\mathbf{x} \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 1 \\ & 0 & \theta^2 & 0 & \theta & 0 \\ & & 1 & 0 & 0 & 1 \\ & & & \theta & 1 & 1 \\ & & & & 1 & 0 \\ & & & & & \theta^2 \end{pmatrix} \mathbf{x}, \qquad \bar{g}_{22}(\mathbf{x}) = {}^t\mathbf{x} \begin{pmatrix} 1 & 1 & \theta & \theta & \theta^2 & \theta^2 \\ & 0 & \theta^2 & \theta^2 & \theta & \theta \\ & & \theta & \theta & 0 & 1 \\ & & & \theta^2 & 1 & 0 \\ & & & & \theta^2 & \theta^2 \\ & & & & & \theta \end{pmatrix} \mathbf{x}.$$

Then the problem of recovering S_1, S_2, T_1, T_2 with (8) is reduced to the problem of recovering $\bar{S}_1 = Q_6^{-1} \circ S_1 \circ Q_6$, $\bar{S}_2 = Q_6^{-1} \circ S_2 \circ Q_6$, $\bar{T}_1 = Q_2^{-1} \circ T_1 \circ Q_2$, $\bar{T}_2 = Q_2^{-1} \circ T_2 \circ Q_2$ satisfying

$$\begin{aligned} \begin{pmatrix} \bar{g}_{11}(\mathbf{x}) \\ \bar{g}_{12}(\mathbf{x}) \end{pmatrix} &= \bar{T}_1 \begin{pmatrix} \bar{f}_{11}(\bar{S}_1(\mathbf{x})) \\ \bar{f}_{12}(\bar{S}_1(\mathbf{x})) \end{pmatrix} + \bar{T}_2 \begin{pmatrix} \bar{f}_{21}(\bar{S}_2(\mathbf{x})) \\ \bar{f}_{22}(\bar{S}_2(\mathbf{x})) \end{pmatrix}, \\ \begin{pmatrix} \bar{g}_{21}(\mathbf{x}) \\ \bar{g}_{22}(\mathbf{x}) \end{pmatrix} &= \bar{T}_1 \begin{pmatrix} \bar{f}_{21}(\bar{S}_1(\mathbf{x})) \\ \bar{f}_{22}(\bar{S}_1(\mathbf{x})) \end{pmatrix} + \bar{T}_2 \begin{pmatrix} \bar{f}_{11}(\bar{S}_2(\mathbf{x})) \\ \bar{f}_{12}(\bar{S}_2(\mathbf{x})) \end{pmatrix}. \end{aligned} \tag{9}$$

Due to Lemma 3.2, we see that $\bar{S}_1, \bar{S}_2, \bar{T}_1, \bar{T}_2$ are written by

$$\begin{aligned} \bar{S}_1 &= \mathrm{diag}\left(\begin{pmatrix} 1 & s_{12}^{(1)} \\ & 1 \end{pmatrix}, \begin{pmatrix} s_{21}^{(1)} & s_{22}^{(1)} \\ & s_{21}^{(1)} \end{pmatrix}, \begin{pmatrix} s_{31}^{(1)} & s_{32}^{(1)} \\ & s_{31}^{(1)} \end{pmatrix} \right), \\ \bar{S}_2 &= \mathrm{diag}\left(\begin{pmatrix} 1 & s_{12}^{(2)} \\ & 1 \end{pmatrix}, \begin{pmatrix} s_{21}^{(2)} & s_{22}^{(2)} \\ & s_{21}^{(2)} \end{pmatrix}, \begin{pmatrix} s_{31}^{(2)} & s_{32}^{(2)} \\ & s_{31}^{(2)} \end{pmatrix} \right), \\ \bar{T}_1 &= \begin{pmatrix} t_1^{(1)} & t_2^{(1)} \\ & t_1^{(1)} \end{pmatrix}, \qquad \bar{T}_2 = \begin{pmatrix} t_1^{(2)} & t_2^{(2)} \\ & t_1^{(2)} \end{pmatrix}. \end{aligned}$$

We first study the coefficients of x_1^2 in $\bar{g}_{12}, \bar{g}_{22}$. The relation (9) gives the following equations.

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} t_1^{(1)} \\ t_1^{(2)} \end{pmatrix}.$$

We then get $t_1^{(1)} = 1$ and $t_1^{(2)} = 1$. Similarly, from the coefficients of x_1^2 in $\bar{g}_{11}, \bar{g}_{21}$, we have

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} t_2^{(1)} \\ t_2^{(2)} \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} t_1^{(1)} \\ t_1^{(2)} \end{pmatrix}.$$

From the equations above, we obtain $t_2^{(1)} = 1$ and $t_2^{(2)} = 0$. We thus have T_1, T_2 as

$$T_1 = Q_2 \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} Q_2^{-1} = J_2, \qquad T_2 = Q_2 \begin{pmatrix} 1 & \\ & 1 \end{pmatrix} Q_2^{-1} = I_2. \tag{10}$$

Next, we study the coefficient of x_1x_3 in $\bar{g}_{12}, \bar{g}_{22}$. From (9) and (10), we have

$$\begin{pmatrix} 1 \\ \theta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} s_{21}^{(1)} \\ s_{21}^{(2)} \end{pmatrix}.$$

We then get $s_{21}^{(1)} = 1$, $s_{21}^{(2)} = \theta$. Similarly, the following equations are derived from the coefficients of x_1x_4, x_1x_5 and x_1x_6 in $\bar{g}_{12}, \bar{g}_{22}$.

$$\begin{aligned} \begin{pmatrix} \theta^2 \\ \theta \end{pmatrix} &= \begin{pmatrix} \theta^2 & \theta^2 \\ \theta^2 & \theta^2 \end{pmatrix} \begin{pmatrix} s_{21}^{(1)} \\ s_{21}^{(2)} \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} s_{22}^{(1)} \\ s_{22}^{(2)} \end{pmatrix}, \\ \begin{pmatrix} 1 \\ \theta^2 \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} s_{31}^{(1)} \\ s_{31}^{(2)} \end{pmatrix}, \\ \begin{pmatrix} \theta \\ \theta^2 \end{pmatrix} &= \begin{pmatrix} \theta & \theta \\ \theta & \theta \end{pmatrix} \begin{pmatrix} s_{31}^{(1)} \\ s_{31}^{(2)} \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} s_{32}^{(1)} \\ s_{32}^{(2)} \end{pmatrix}. \end{aligned}$$

Then we get $s_{22}^{(1)} = 1$, $s_{22}^{(2)} = 0$, $s_{31}^{(1)} = 1$, $s_{31}^{(2)} = \theta^2$, $s_{32}^{(1)} = 1$ and $s_{32}^{(2)} = 0$. To recover the remaining parameters $s_{12}^{(1)}, s_{12}^{(2)}$, we study the coefficients of x_2^2 in $\bar{g}_{12}, \bar{g}_{22}$ and have

$$0 = s_{12}^{(1)2} + s_{12}^{(2)}, \qquad 0 = s_{12}^{(1)} + s_{12}^{(2)2}.$$

Since $s_{12}^{(1)}, s_{12}^{(2)} \in \mathbf{F}_2$, the solution of the equations above is $s_{12}^{(1)} = s_{12}^{(2)}$. Since the unique solution is not give yet, we further study the coefficients x_2x_3 in $\bar{g}_{12}, \bar{g}_{22}$ and have the equations

$$1 = s_{12}^{(1)} s_{21}^{(1)} + \theta^2 s_{21}^{(2)}, \qquad \theta^2 = \theta^2 s_{21}^{(1)} + s_{12}^{(2)} s_{21}^{(2)}.$$

Since $s_{21}^{(1)} = 1$, $s_{21}^{(2)} = \theta$, we obtain $s_{12}^{(1)} = s_{12}^{(2)} = 0$. We thus conclude that

$$\begin{aligned} S_1 =& Q_6 \cdot \operatorname{diag}\left(\begin{pmatrix} 1 & 0 \\ & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} \right) Q_6^{-1} = I_6 + J_6 + J_6^2 + J_6^4 + J_6^5, \\ S_2 =& Q_6 \cdot \operatorname{diag}\left(\begin{pmatrix} 1 & 0 \\ & 1 \end{pmatrix}, \begin{pmatrix} \theta & 0 \\ & \theta \end{pmatrix}, \begin{pmatrix} \theta^2 & 0 \\ & \theta^2 \end{pmatrix} \right) Q_6^{-1} = J_6^4. \end{aligned} \tag{11}$$

The solution of this BIPC problem is given by (10) and (11). □