Nonlinear Piece In Hand Matrix Method for Enhancing Security of Multivariate Public Key Cryptosystems

Shigeo Tsujii[†] Kohtaro Tadaki[‡] Ryou Fujita[†]

[†] Institute of Information Security
2–14–1 Tsuruya-cho, Kanagawa-ku, Yokohama-shi, 221–0835 Japan
[‡] Research and Development Initiative, Chuo University
1–13–27 Kasuga, Bunkyo-ku, Tokyo, 112–8551 Japan

Abstract. It is widely believed to take exponential time to find a solution of a system of random multivariate polynomials because of the NP-completeness of such a task. On the other hand, in most of multivariate public key cryptosystems proposed so far, the computational complexity of cryptanalysis is apt to be polynomial time due to the trapdoor structure. In this paper, we develop the concept, *piece in hand matrix* (PH matrix, for short), which aims to bring the computational complexity of cryptanalysis of multivariate public key cryptosystems close to exponential time by adding random polynomial terms to original cryptosystems. This is a general concept which can be applicable to any reasonable type of multivariate public key cryptosystems for the purpose of enhancing their security. There are two types of the PH matrices: a linear matrix whose elements are constants and a nonlinear matrix whose elements are polynomial functions of the plain text or random numbers. In the present paper, we focus our thought on the nonlinear PH matrix method and develop the framework of it. The nonlinear PH matrix method is obtained by generalizing the linear PH matrix method, and the nonlinearity may bring an additional randomization to the original linear PH matrix method. Thus, the nonlinear PH matrix method may enhance the security of the original multivariate public key cryptosystem more than the linear PH matrix method. We show, in an experimental manner, that this actually holds in the enhancement of the security of the Matsumoto-Imai cryptosystem and RSE(2)PKC against the Gröbner basis attack.

Key words: public key cryptosystem, multivariate polynomial, multivariate public key cryptosystem, piece in hand concept, nonlinear matrix

1 Introduction

In most of multivariate public key cryptosystems proposed so far, the computational complexity of cryptanalysis is apt to be polynomial time due to the trapdoor structure (see e.g. [11]). On the other hand, it is widely believed to take exponential time to find a solution of a system of random multivariate polynomials because of the NP-completeness of such a task [10]. The purpose of this paper is to develop the framework, called *piece in hand matrix method*, which aims to bring the computational complexity of cryptanalysis of multivariate public key cryptosystems close to exponential time by adding random polynomial terms to original cryptosystems. The piece in hand (PH, for short) matrix method is introduced and studied in a series of works [28, 29, 30, 31, 32, 33, 34]. In particular, the works [32, 33, 34] proposed the linear PH matrix method with random variables, which is the latest version of the linear PH matrix methods, and showed that this linear PH matrix method provides the substantial robustness against the Gröbner basis attack, based on computer experiments. In this paper, we develop the nonlinear PH matrix methods. Because of the nonlinearity of the PH matrix, the nonlinear PH matrix method may enhance the security of the original multivariate public key cryptosystem more than the linear PH matrix method in general. We then show, based on computer experiments, that this actually holds in the enhancement of the security of the Matsumoto-Imai cryptosystem [19] and RSE(2)PKC [15] against the Gröbner basis attack.

Recently, the research of multivariate public key cryptosystems have been made actively. One of the backgrounds of this trend seems to be formed by the sense of emergency against the possibility of advent of quantum computers in the future. Although public key cryptosystems based on the intractability of prime factorization or discrete logarithm problem are presently assumed to be secure, such security will not be guaranteed in the quantum computer age. On the other hand, multivariate public key cryptosystems are thought of as candidates of public key cryptosystem secure against quantum computers. Thus, it is important to develop multivariate public key cryptosystems and to study their security in the setting of the quantum computer age. From this point of view, we try to develop nonlinear PH matrix methods in this paper. By assuming the future when quantum computers appear, we place much more value on the enhance of security than the efficiency, such as the improvement of the information transmission rate (i.e., the size of cipher text divided by the size of plain text) or the reduction of key-length. Thus, while we try to improve the efficiency as much as possible in the nonlinear PH matrix method proposed in this paper, we do not stick to such an improvement at the price of compromising the security in the presence of quantum computer.

In the present paper, we focus our thought on the nonlinear PH matrix method and develop the framework of it. A nonlinear PH matrix method was already proposed by the works [30, 31]. In this nonlinear PH matrix method, however, the degree of polynomials in the public key is more than two, and this may cause an undesirable increase in the size of the public key. In the present paper, we propose a nonlinear PH matrix method, where the degree of polynomials in the public key is kept the same as the degree of polynomials in the public key of the original cryptosystem, which is normally two. We show, in an experimental manner, that the nonlinear PH matrix method improved in this way is secure even against the Gröbner basis attack.

This paper is organized as follows. We begin in Section 2 with some basic notation and a brief introduction of the schemes of multivariate public key cryptosystems in general. In Section 3, we briefly review the general prescription for enhancing the security of any reasonable multivariate public key cryptosystem by means of the primitive linear PH matrix method, introduced by [30, 31]. We then consider the enhancement of security by the PH matrix methods against the Gröbner basis attack from a general point of view. Based on the consideration, as a total countermeasure, we introduce the quadratic nonlinear PH matrix method in Section 4. We then show, based on computer experiments, that the quadratic nonlinear PH matrix method properly provides substantial robustness against the Gröbner basis attack in Section 5. We discuss about the immunity of the nonlinear PH matrix methods against known attacks in Section 6. We conclude this paper with the future direction of our work in Section 7.

2 Preliminaries

In this section we review the schemes of multivariate public key cryptosystems in general after introducing some notation about fields, polynomials, and matrices.

2.1 Notation

$\mathbf{F}_q$ is a finite field which has q elements with $q \geq 2$. $\mathbf{F}_q[x_1, \dots, x_k]$ is the set of all polynomials in variables $x_1, x_2, \dots, x_k$ with coefficients in $\mathbf{F}_q$. For every nonempty set S and every positive integers n and l, $S^{n \times l}$ denotes the set of all $n \times l$ matrices whose entries are in S, and S^n denotes the set of all column vectors consisting n components in S. Therefore $S^{n \times 1} = S^n$. We represent a column vector in general by bold face symbols such as $\boldsymbol{p}$, $\boldsymbol{E}$, and $\boldsymbol{X}$. For every matrix $A \in S^{n \times l}$, $A^T \in S^{l \times n}$ denotes the transpose of A. Let $\boldsymbol{f} = (f_1, \dots, f_n)^T$ and $\boldsymbol{g} = (g_1, \dots, g_k)^T$ be polynomial column vectors in $\mathbf{F}_q[x_1, \dots, x_k]^n$ and $\mathbf{F}_q[x_1, \dots, x_m]^k$, respectively, where $f_1, \dots, f_n \in \mathbf{F}_q[x_1, \dots, x_k]$ and $g_1, \dots, g_k \in \mathbf{F}_q[x_1, \dots, x_m]$. Then the *substitution* $\boldsymbol{f}(\boldsymbol{g}) \in \mathbf{F}_q[x_1, \dots, x_m]^n$ of $\boldsymbol{g}$ for the variables in $\boldsymbol{f}$ is defined by $\boldsymbol{f}(\boldsymbol{g}) \underset{\text{def}}{=} (h_1, \dots, h_n)^T$, where each h_i is the polynomial in $\mathbf{F}_q[x_1, \dots, x_m]$ obtained by substituting $g_1, \dots, g_k$ for the variables $x_1, \dots, x_k$ in f_i, respectively. Thus, for every $\boldsymbol{f} \in \mathbf{F}_q[x_1, \dots, x_k]^n$ and every $\boldsymbol{p} \in \mathbf{F}_q{}^k$, $\boldsymbol{f}(\boldsymbol{p})$ denotes simply the vector in $\mathbf{F}_q{}^n$ obtained by substituting $p_1, \dots, p_k$ for the variables $x_1, \dots, x_k$ in $\boldsymbol{f}$, respectively, where $\boldsymbol{p} = (p_1, \dots, p_k)^T$ with $p_1, \dots, p_k \in \mathbf{F}_q$. For every polynomial matrix $N \in \mathbf{F}_q[x_1, \dots, x_k]^{n \times l}$ and every polynomial column vector $\boldsymbol{g} \in \mathbf{F}_q[x_1, \dots, x_m]^k$, the *substitution* $N(\boldsymbol{g}) \in \mathbf{F}_q[x_1, \dots, x_m]^{n \times l}$ of $\boldsymbol{g}$ for the variables in N is defined in the same manner. Table 1 shows the summary of notation.

Table 1: Summary of notation

the set in which each element is included	column vector		
	$n \times 1$		$k \times 1$
$\mathbf{F}_q$	$\boldsymbol{f}(\boldsymbol{p}) \in \mathbf{F}_q^n$ $\uparrow$	$\leftarrow$	$\boldsymbol{p} \in \mathbf{F}_q^k$
$\mathbf{F}_q[x_1, \dots, x_k]$	$\boldsymbol{f} \in \mathbf{F}_q[x_1, \dots, x_k]^n$		
$\mathbf{F}_q[x_1, \dots, x_m]$	$\downarrow$ $\boldsymbol{f}(\boldsymbol{g}) \in \mathbf{F}_q[x_1, \dots, x_m]^n$	$\leftarrow$	$\boldsymbol{g} \in \mathbf{F}_q[x_1, \dots, x_m]^k$

the set in which each element is included	column vector		matrix
	$k \times 1$		$n \times l$
$\mathbf{F}_q$	$\boldsymbol{p} \in \mathbf{F}_q^k$	$\rightarrow$	$N(\boldsymbol{p}) \in \mathbf{F}_q^{n \times l}$ $\uparrow$
$\mathbf{F}_q[x_1, \dots, x_k]$			$N \in \mathbf{F}_q[x_1, \dots, x_k]^{n \times l}$
$\mathbf{F}_q[x_1, \dots, x_m]$	$\boldsymbol{g} \in \mathbf{F}_q[x_1, \dots, x_m]^k$	$\rightarrow$	$\downarrow$ $N(\boldsymbol{g}) \in \mathbf{F}_q[x_1, \dots, x_m]^{n \times l}$

2.2 Schemes of Multivariate Public Key Cryptosystems

A multivariate public key cryptosystem (MPKC, for short) such as in [18, 26, 19, 27, 22, 20, 14, 15, 5, 36] can be considered to comply with the following scheme: A plain text is represented by a column vector $\boldsymbol{p} = (p_1, \dots, p_k)^T \in \mathbf{F}_q{}^k$, and a cipher text is represented by a column vector $\boldsymbol{c} = (c_1, \dots, c_n)^T \in \mathbf{F}_q{}^n$. Then, q, k, and a polynomial column vector $\boldsymbol{E} \in \mathbf{F}_q[x_1, \dots, x_k]^n$ form the public key of the cryptosystem. The encryption is given by the transformation $\boldsymbol{c} = \boldsymbol{E}(\boldsymbol{p})$ from $\boldsymbol{p}$ to $\boldsymbol{c}$. The secret key of the cryptosystem gives an efficient method to solve the system $\boldsymbol{E} = \boldsymbol{c}$ of polynomial equations on $(x_1, \dots, x_k)$ for any given $\boldsymbol{c} \in \mathbf{F}_q{}^n$. Thus, $\boldsymbol{E}$ has to be constructed so that, without the knowledge about this method, it is difficult to find $\boldsymbol{p}$ for any given $\boldsymbol{c}$ in polynomial-time.

Let us consider the situation that the legitimate receiver, Bob, has the secret key and the sender, Alice, wants to transmit her cipher text $\boldsymbol{c} \underset{\text{def}}{=} \boldsymbol{E}(\boldsymbol{p})$ to Bob. When Bob receives the cipher text $\boldsymbol{c}$ sent from Alice, using the secret key he can efficiently decipher it to obtain the plain text $\boldsymbol{p}$. On the other hand, it has to be intractable for the eavesdropper, Catherine, to recover $\boldsymbol{p}$ from $\boldsymbol{c}$, based on the fact that she has no knowledge about the secret key.

In most MPKCs, the public key $\boldsymbol{E} \in \mathbf{F}_q[x_1, \dots, x_k]^n$ has the following form:

$$\boldsymbol{E} = B_0\, \boldsymbol{G}(A_0 \boldsymbol{x}). \tag{1}$$

Here $\boldsymbol{x}$ denotes $(x_1, \dots, x_k)^T \in \mathbf{F}_q[x_1, \dots, x_k]^k$. A_0 and B_0 are invertible matrices in $\mathbf{F}_q{}^{k \times k}$ and $\mathbf{F}_q{}^{n \times n}$, respectively. $\boldsymbol{G}$ is a polynomial column vector in $\mathbf{F}_q[x_1, \dots, x_k]^n$, where the polynomial vector $A_0 \boldsymbol{x} \in \mathbf{F}_q[x_1, \dots, x_k]^k$ is substituted for the variables $x_1, \dots, x_k$ in $\boldsymbol{G}$ according to our convention above. In this type of cryptosystem, while keeping A_0, B_0, and $\boldsymbol{G}$ secret from anyone else, Bob publishes the public key $\boldsymbol{E}$ in the form of a system of trimmed multivariate polynomials obtained by simplifying the right-hand side of (1). Normally, $\boldsymbol{G}$ consists only of polynomials in $\mathbf{F}_q[x_1, \dots, x_k]$ of total degree at most two in order to avoid the blowup of the size of the public key $\boldsymbol{E}$. In such a case, the multivariate public key cryptosystem is called a *quadratic multivariate public key cryptosystem* (QMPKC, for short).

3 Primitive Linear PH Matrix Method

In this section, we review a primitive form of a general prescription for enhancing the security of any reasonable MPKC based on the PH concept, called the *primitive linear PH matrix method*, introduced by [30, 31]. This version of a PH matrix method is an illustrative implementation of the PH concept, and serves as the starting point of all advanced PH matrix methods. Based on this primitive linear PH matrix method, we develop nonlinear PH matrix method in subsequent sections. We briefly describe the primitive linear PH matrix method in what follows. See Appendix A for a complete description of the primitive linear PH matrix method. We then consider the enhancement of security by the primitive linear PH matrix method against the Gröbner basis attack and explore possible improvements in the method. As a result, we find that the nonlinearization of the PH matrix may provide the substantial robustness against the Gröbner basis attack.

Let $\mathcal{K}$ be an arbitrary QMPKC whose public key is given by $\boldsymbol{E} \in \mathbf{F}_q[x_1, \dots, x_k]^n$, as described in Subsection 2.2. In the PH matrix method, a new QMPKC $\widetilde{\mathcal{K}}$ is constructed from the given QMPKC $\mathcal{K}$ for the purpose of enhancing the security. A public key $\widetilde{\boldsymbol{E}} \in \mathbf{F}_q[x_1, \dots, x_k]^l$ of $\widetilde{\mathcal{K}}$ is constructed from the original public key $\boldsymbol{E}$ of $\mathcal{K}$ by multiplying a certain matrix and adding a certain polynomial vector which plays a role in randomizing $\widetilde{\boldsymbol{E}}$. In order to make the PH matrix method work properly, we assume that $l > n$.

A plain text of $\widetilde{\mathcal{K}}$ is represented by a vector in ${\mathbf{F}_q}^k$ in the same way as in $\mathcal{K}$. For any plain text vector $\boldsymbol{p} \in {\mathbf{F}_q}^k$ of $\widetilde{\mathcal{K}}$, the corresponding cipher text of $\widetilde{\mathcal{K}}$ is represented by a vector $\widetilde{\boldsymbol{c}} \in {\mathbf{F}_q}^l$ and is calculated by $\widetilde{\boldsymbol{c}} = \widetilde{\boldsymbol{E}}(\boldsymbol{p})$.

As a part of the secret key of $\widetilde{\mathcal{K}}$, the *PH matrix* $M \in {\mathbf{F}_q}^{n\times l}$ is introduced so that the multiplication of $\widetilde{\boldsymbol{E}}$ by the PH matrix M from the left simplifies $\widetilde{\boldsymbol{E}}$ and results in the original public key $\boldsymbol{E}$ as follows:

$$M\widetilde{\boldsymbol{E}} = \boldsymbol{E}. \tag{2}$$

This is a crucial property of the PH matrix in our PH matrix methods in general.

Then, the triple $(q, k, \widetilde{\boldsymbol{E}})$ forms the public key of $\widetilde{\mathcal{K}}$. On the other hand, the PH matrix M, together with the secret key of $\mathcal{K}$ corresponding to the public key $(q, k, \boldsymbol{E})$ of $\mathcal{K}$, forms the secret key of $\widetilde{\mathcal{K}}$. The decryption of $\widetilde{\mathcal{K}}$ proceeds as follows. Based on the relation (2), on receiving the cipher text $\widetilde{\boldsymbol{c}} = \widetilde{\boldsymbol{E}}(\boldsymbol{p})$ for a plain text $\boldsymbol{p}$, Bob can efficiently calculate $\boldsymbol{c} \underset{\text{def}}{=} \boldsymbol{E}(\boldsymbol{p}) = M\widetilde{\boldsymbol{c}}$ by the multiplication of $\widetilde{\boldsymbol{c}}$ by M from the left. Then, according to the decryption procedure of $\mathcal{K}$, Bob can recover the plain text $\boldsymbol{p}$ using the secret key of $\mathcal{K}$.

3.1 Countermeasure against Gröbner Basis Attack

Recently, Faugère and Joux [8] showed in an experimental manner that computing a Gröbner basis of the public key is likely to be an efficient attack to HFE [22], which is one of major QMPKCs. In fact, they broke the first HFE challenge (80bits) proposed by Patarin. The attack used by them is simply to compute a Gröbner basis for the ideal generated by polynomial components in $\boldsymbol{E} - \boldsymbol{c}$, where $\boldsymbol{E}$ is a public key and $\boldsymbol{c}$ is a cipher text vector. Thus, because of the simplicity of this attack, it may be a threat to many types of proposed multivariate public key encryption schemes.

Especially, from the point of view of Gröbner bases, the secret invertible matrix B_0 may be useless in an MPKC whose public key has the form (1). This is because any ideal I generated by polynomials remains unchanged under the transformation of the generators of I by an invertible matrix. Thus, by the following reason, the PH matrix concept might be also useless to the Gröbner basis attack in its primitive linear implementation. We first note, by the relation (2), that $M(\widetilde{\boldsymbol{E}} - \widetilde{\boldsymbol{c}}) = \boldsymbol{E} - \boldsymbol{c}$, where $\widetilde{\boldsymbol{c}} \underset{\text{def}}{=} \widetilde{\boldsymbol{E}}(\boldsymbol{p}) \in {\mathbf{F}_q}^l$ is a cipher text vector of the enhanced cryptosystem $\widetilde{\mathcal{K}}$ and $\boldsymbol{c} \underset{\text{def}}{=} \boldsymbol{E}(\boldsymbol{p}) \in {\mathbf{F}_q}^n$ is the corresponding cipher text vector of the original cryptosystem $\mathcal{K}$. We can then show that there exist linear combinations $g_1, \dots, g_{l-n}$, with coefficients in $\mathbf{F}_q$, of $\widetilde{e}_1 - \widetilde{c}_1, \dots, \widetilde{e}_l - \widetilde{c}_l$ such that

$$\langle \widetilde{e}_1 - \widetilde{c}_1, \dots, \widetilde{e}_l - \widetilde{c}_l \rangle = \langle e_1 - c_1, \dots, e_n - c_n, g_1, \dots, g_{l-n} \rangle, \tag{3}$$

where

$$(c_1, \dots, c_n)^T \underset{\text{def}}{=} \boldsymbol{c} \quad \text{and} \quad (\widetilde{c}_1, \dots, \widetilde{c}_l)^T \underset{\text{def}}{=} \widetilde{\boldsymbol{c}},$$

and

$$(e_1, \dots, e_n)^T \underset{\text{def}}{=} \boldsymbol{E} \in \mathbf{F}_q[x_1, \dots, x_k]^n \quad \text{and} \quad (\widetilde{e}_1, \dots, \widetilde{e}_l)^T \underset{\text{def}}{=} \widetilde{\boldsymbol{E}} \in \mathbf{F}_q[x_1, \dots, x_k]^l$$

are the public keys of $\mathcal{K}$ and $\widetilde{\mathcal{K}}$, respectively [1]. Thus, from the point of view of Gröbner bases, the system $\widetilde{\boldsymbol{E}} - \widetilde{\boldsymbol{c}} = \boldsymbol{0}$ of polynomial equations on $(x_1, \dots, x_k)$ might not be necessarily more difficult to solve than the system $\boldsymbol{E} - \boldsymbol{c} = \boldsymbol{0}$ of polynomial equations on $(x_1, \dots, x_k)$ due to the existence of the additional polynomial equations $g_1 = 0, \ldots, g_{l-n} = 0$ for the former. In such a case, the primitive linear PH matrix method might be useless to the Gröbner basis attack. However, there are two types of countermeasures on this point.

Countermeasure I. One of the countermeasures against the Gröbner basis attack is just to nonlinearize the PH matrix, i.e., to employ a matrix function N of a plain text as a PH matrix. Since an ideal I generated by polynomials may change under the replacement of the generators of I by the product of N and them, the nonlinear PH matrix N may provide the substantial robustness against the Gröbner basis attack, unlike in the case of the primitive implementation of a linear PH matrix method.

Countermeasure II. The works [32, 33, 34] introduced a version of a linear PH matrix method, called the *linear PH matrix method with random variables*, which may overcome the weakness above, through elaborations of the primitive linear PH matrix method. In the above consideration, the polynomials $e_1, \ldots, e_n$ are assumed to be in $\mathbf{F}_q[x_1, \ldots, x_k]$ implicitly, and therefore the weakness of the primitive linear PH matrix method against the Gröbner basis attack is of concern. Hence, the other countermeasure against the weakness is to introduce additional variables $x_{k+1}, \ldots, x_m$ to the public key $\widetilde{\boldsymbol{E}}$ of $\widetilde{\mathcal{K}}$. Under this countermeasure, the g_i's in (3) are no longer polynomials in $\mathbf{F}_q[x_1, \ldots, x_k]$, but in $\mathbf{F}_q[x_1, \ldots, x_m]$, and therefore solving the system $\widetilde{\boldsymbol{E}} - \widetilde{\boldsymbol{c}} = \mathbf{0}$ of polynomial equations on $(x_1, \ldots, x_m)$ seems to be more difficult than solving the system $\boldsymbol{E} - \boldsymbol{c} = \mathbf{0}$ of polynomial equations on $(x_1, \ldots, x_k)$. This is done by introducing the additional variables $x_{k+1}, \ldots, x_m$ which are set to random values by Alice on the encryption. The works [32, 33, 34] proposed the linear PH matrix method with random variables as an implementation of this idea, and showed that this method properly works and provides the substantial robustness against the Gröbner basis attack, based on computer experiments.

In the next section, we propose the quadratic nonlinear PH matrix method, where additional variables are introduced in the same manner as we made changes and improvements in the primitive linear PH matrix method to obtain the linear PH matrix method with random variables in the works [32, 33, 34]. Thus, Countermeasures I and II are both taken in the quadratic nonlinear PH matrix method. Therefore, the quadratic nonlinear PH matrix method may have more security against the Gröbner basis attack than the primitive linear PH matrix method. Furthermore, in the quadratic nonlinear PH matrix method, the degree of polynomials in the public key remains two, just like in the original QMPKC. Thus, the quadratic nonlinear PH matrix method might be secure and practical, compared to the nonlinear PH matrix methods proposed so far.

4 Nonlinearization of the PH Matrix Method

In this section, we introduce nonlinear PH matrix methods as a generalization of the primitive linear PH matrix method described in the previous section. In the primitive linear PH matrix method, the PH matrix is a constant matrix. On the other hand, in the nonlinear PH matrix methods, the PH matrix is generalized over a polynomial matrix. This generalization may enable the PH matrix method to acquire immunity against any specialized attack to the linear PH matrix methods. This is because the nonlinearity may bring an additional randomization to the original linear PH matrix method. Thus, the nonlinear PH matrix methods may enhance the security of the original MPKC $\mathcal{K}$ more than the linear PH matrix methods.

In Subsection 4.1 below, we introduce a practical nonlinear PH matrix method, called the *quadratic nonlinear PH matrix method.* A nonlinear PH matrix method was already proposed by the previous works [30, 31]. In the previous method, however, the degree of the randomization of the public key of the enhanced cryptosystem $\widetilde{\mathcal{K}}$ seems insufficient because of the use of Fermat's little theorem. In the quadratic nonlinear PH matrix method, the degree of the randomization of the public key of $\widetilde{\mathcal{K}}$ seems to be made greater than the previous method. Thus, the quadratic nonlinear PH matrix method might be more practical than the previous proposals, from the point of view of the security.

The degree of polynomials in the public key of the enhanced cryptosystem $\widetilde{\mathcal{K}}$ is more than two in the previous method, and this may cause an undesirable increase in the size of the public key of the enhanced cryptosystem. In the quadratic nonlinear PH matrix method, the degree of polynomials in the public key is kept the same as the degree of polynomials in the public key of the original cryptosystem. Furthermore, the quadratic nonlinear PH matrix method is designed so as to be immune against the Gröbner basis attack. Thus, the quadratic nonlinear PH matrix method might be secure and practical, compared to the nonlinear PH matrix methods proposed so far.

4.1 Quadratic Nonlinear PH Matrix Method

The quadratic nonlinear PH matrix method is described as follows.

Let $\mathcal{K}$ be an arbitrary QMPKC whose public key is given by $\boldsymbol{E} \in \mathbf{F}_q[x_1, \dots, x_k]^n$, as described in Subsection 2.2. We construct a new QMPKC $\widetilde{\mathcal{K}}$ based on $\mathcal{K}$ as follows. Let l, f, m, and h be any positive integers with $l \geq f$. We set $g \underset{\text{def}}{=} l + n + m + h$. Let p and z be any positive integers with $p < k < z$, and let t be any positive integer with $t < z - p$.

Key-Generation. In the key-generation stage, the public key and secret key of $\mathcal{K}$ are chosen first. Then, a public key $\widetilde{\boldsymbol{E}} \in \mathbf{F}_q[x_1, \dots, x_z]^g$ of $\widetilde{\mathcal{K}}$ is constructed from the original public key $\boldsymbol{E}$ of $\mathcal{K}$ as follows. In the construction, an invertible matrix $B \in {\mathbf{F}_q}^{g \times g}$, a polynomial matrix $S \in \mathbf{F}_q[x_1, \dots, x_m]^{l \times f}$ of total degree 1, a polynomial vector $\boldsymbol{d} \in \mathbf{F}_q[x_1, \dots, x_m]^l$ of total degree 2, a polynomial vector $\boldsymbol{a} \in \mathbf{F}_q[x_1, \dots, x_z]^m$ of total degree 1, a polynomial vector $\boldsymbol{L} \in \mathbf{F}_q[x_1, \dots, x_z]^f$ of total degree 1, a polynomial vector $\boldsymbol{Q} \in \mathbf{F}_q[x_1, \dots, x_f]^n$ of total degree 2, and a polynomial vector $\boldsymbol{r} \in \mathbf{F}_q[x_1, \dots, x_z]^h$ of total degree 2 are randomly chosen. The public key $\widetilde{\boldsymbol{E}} \in \mathbf{F}_q[x_1, \dots, x_z]^g$ of $\widetilde{\mathcal{K}}$ is then calculated by the following equation:

$$\widetilde{\boldsymbol{E}} \underset{\text{def}}{=} B \begin{pmatrix} S(\boldsymbol{a})\boldsymbol{L} + \boldsymbol{d}(\boldsymbol{a}) \\ \boldsymbol{E}\begin{pmatrix} \boldsymbol{x} \\ A\boldsymbol{\lambda} \end{pmatrix} + \boldsymbol{Q}(\boldsymbol{L}) \\ \boldsymbol{H}(\boldsymbol{a}) \\ \boldsymbol{r} \end{pmatrix}, \tag{4}$$

where $\boldsymbol{x} = (x_1, \dots, x_p)^T \in \mathbf{F}_q[x_1, \dots, x_p]^p$ and $\boldsymbol{\lambda} = (x_{p+1}, \dots, x_{p+t})^T \in \mathbf{F}_q[x_{p+1}, \dots, x_{p+t}]^t$. A is a randomly chosen matrix in ${\mathbf{F}_q}^{(k-p) \times t}$. Note that, in the right-hand side of (4), the vector $A\boldsymbol{\lambda} \in \mathbf{F}_q[x_{p+1}, \dots, x_{p+t}]^{k-p}$ is substituted for the variables $x_{p+1}, \dots, x_k$ in the original public key $\boldsymbol{E}$ while keeping the variables $x_1, \dots, x_p$ in $\boldsymbol{E}$ unchanged. Here, $\boldsymbol{H} \in \mathbf{F}_q[x_1, \dots, x_m]^m$ is a bijective quadratic polynomial transformation whose inverse is efficiently computable. An example of $\boldsymbol{H}$ is given below. The quadratic polynomial vector $\boldsymbol{Q}(\boldsymbol{L})$ plays a role in masking the original public key $\boldsymbol{E}$ and randomizing it. $\boldsymbol{L}$ is multiplied by $S(\boldsymbol{a})$ from the left to ensure the nonlinearity. In order to make this nonlinear PH matrix method work properly, we choose q or $l - f$ to be large enough compared with f. Note that the polynomial matrix $S(\boldsymbol{a})$ is a nonlinearization of the constant matrix S in the primitive linear PH matrix method [30, 31] (see Appendix A). The nonlinearity of $S(\boldsymbol{a})$ gives the nonlinear PH matrix methods an advantage in the security over the linear PH matrix methods, and therefore is the heart of the nonlinear PH matrix methods in general. Since $S(\boldsymbol{a})\boldsymbol{L}$ is of total degree 2, we can check that the public key $\widetilde{\boldsymbol{E}}$ is a quadratic polynomial vector. Thus, the total degree of the public key of the enhanced cryptosystem $\widetilde{\mathcal{K}}$ is kept the same as the total degree of the public key of the original cryptosystem $\mathcal{K}$, as desired. The polynomial vectors $\boldsymbol{r}$ and $\boldsymbol{d}(\boldsymbol{a})$ play a role in randomizing $\widetilde{\boldsymbol{E}}$ also, and correspond to the term $R\boldsymbol{X}$ in the primitive linear PH matrix method [30, 31] (see Appendix A). In addition to randomizing $\widetilde{\boldsymbol{E}}$, introducing $\boldsymbol{r}$ is a countermeasure against the differential attack [9, 7]. The role of the polynomial vector $\boldsymbol{a}$ is explained below.

Then, the quadruple $(q, z, \widetilde{\boldsymbol{E}}, p)$ forms the public key of $\widetilde{\mathcal{K}}$. Bob publishes it after the key-generation. On the other hand, B^{-1}, S, $\boldsymbol{d}$, $\boldsymbol{Q}$, and $\boldsymbol{H}$, together with the secret key of $\mathcal{K}$ corresponding to the public key $(q, k, \boldsymbol{E})$ of $\mathcal{K}$, form the secret key of $\widetilde{\mathcal{K}}$. Table 2 shows the summary of parameters and key.

Encryption. A plain text of $\widetilde{\mathcal{K}}$ is represented by a vector in ${\mathbf{F}_q}^p$. Now, assume that Alice wants to send Bob a plain text vector $\boldsymbol{p} \in {\mathbf{F}_q}^p$. The corresponding cipher text of $\widetilde{\mathcal{K}}$ is represented by a vector $\widetilde{\boldsymbol{c}} \in {\mathbf{F}_q}^g$, and is calculated by Alice through $\widetilde{\boldsymbol{c}} \underset{\text{def}}{=} \widetilde{\boldsymbol{E}} \begin{pmatrix} \boldsymbol{p} \\ \boldsymbol{u} \end{pmatrix}$, where $\boldsymbol{u} \underset{\text{def}}{=} \begin{pmatrix} \boldsymbol{w} \\ \boldsymbol{v} \end{pmatrix} \in {\mathbf{F}_q}^{z-p}$ is chosen randomly by Alice on the encryption of $\boldsymbol{p}$. $\boldsymbol{w}$ and $\boldsymbol{v}$ are column vectors in ${\mathbf{F}_q}^t$, ${\mathbf{F}_q}^{z-p-t}$, respectively. Table 3 shows the summary of encryption.

Decryption. The decryption of $\widetilde{\mathcal{K}}$ proceeds as follows. First, by (4), we see that

$$\begin{pmatrix} S(\boldsymbol{a}(\boldsymbol{z}))\boldsymbol{L}(\boldsymbol{z}) + \boldsymbol{d}(\boldsymbol{a}(\boldsymbol{z})) \\ \boldsymbol{E}\begin{pmatrix} \boldsymbol{p} \\ \boldsymbol{y} \end{pmatrix} + \boldsymbol{Q}(\boldsymbol{L}(\boldsymbol{z})) \\ \boldsymbol{H}(\boldsymbol{a}(\boldsymbol{z})) \\ \boldsymbol{r}(\boldsymbol{z}) \end{pmatrix} = B^{-1}\widetilde{\boldsymbol{c}}, \tag{5}$$

where $\boldsymbol{z} \underset{\text{def}}{=} \begin{pmatrix} \boldsymbol{p} \\ \boldsymbol{u} \end{pmatrix} \in {\mathbf{F}_q}^z$, $\boldsymbol{y}$ is a column vector in ${\mathbf{F}_q}^{k-p}$ given by $\boldsymbol{y} \underset{\text{def}}{=} A\boldsymbol{w}$. Therefore, on receiving the cipher text $\widetilde{\boldsymbol{c}}$, Bob can efficiently obtain the values $S(\boldsymbol{a}(\boldsymbol{z}))\boldsymbol{L}(\boldsymbol{z})+\boldsymbol{d}(\boldsymbol{a}(\boldsymbol{z}))$, $\boldsymbol{E}\begin{pmatrix} \boldsymbol{p} \\ \boldsymbol{y} \end{pmatrix}+\boldsymbol{Q}(\boldsymbol{L}(\boldsymbol{z}))$, and $\boldsymbol{H}(\boldsymbol{a}(\boldsymbol{z}))$ from the multiplication of $\widetilde{\boldsymbol{c}}$ by B^{-1} from the left. Then, using the inverse transformation of $\boldsymbol{H}$, the value $\boldsymbol{a}(\boldsymbol{z})$ is efficiently obtained. Thus, Bob can efficiently calculate $S(\boldsymbol{a}(\boldsymbol{z}))$ and $\boldsymbol{d}(\boldsymbol{a}(\boldsymbol{z}))$ and therefore he can efficiently calculate the value $S(\boldsymbol{a}(\boldsymbol{z}))\boldsymbol{L}(\boldsymbol{z})$.

We choose q or $l - f$ to be large enough compared with f so that fq^{-l+f-1} is sufficiently small compared with 1. For simplicity, we here assume that the plain text vector $\boldsymbol{p}$ distributes uniformly over ${\mathbf{F}_q}^p$. Then it follows from Theorem 4.1 that $S(\boldsymbol{a}(\boldsymbol{z}))$ has full column rank in all likelihood. For the sake of completeness, we include the proof of the theorem in Appendix B.

Theorem 4.1. *Let l and n be positive integers with $l \geq n$. Assume that an $l \times n$ matrix A is randomly chosen from ${\mathbf{F}_q}^{l\times n}$. Then the probability that the matrix A has full column rank is at least $1 - nq^{-l+n-1}$.* □

Table 2: Summary of parameters and key of quadratic nonlinear PH matrix method

public parameters		q	number of elements of finite field $\mathbf{F}_q$	
		p	quadratic nonlinear PH matrix method	number of plain text variables
		z		number of all variables (plain text and random numbers)
		g		number of cipher text variables
public key	polynomial vector	$\widetilde{\boldsymbol{E}} \in \mathbf{F}_q[x_1, \ldots, x_z]^g$		

secret parameters		k	original MPKC $\mathcal{K}$	number of plain text variables
		n		number of cipher text variables
		f	quadratic nonlinear PH matrix method	number of rows of $\boldsymbol{L}$
		l		number of rows of $\boldsymbol{d}$
		m		number of rows of $\boldsymbol{H}$
		h		number of rows of $\boldsymbol{r}$
		t		number of rows of $\boldsymbol{\lambda}$
conditions of parameters		$p < k < z$, $f \leq l$, $g = l + n + m + h$, $t < z - p$		
secret key	matrix	$B^{-1} \in \mathbf{F}_q^{g \times g}$	invertible	randomly chosen
	polynomial vector	$\boldsymbol{d} \in \mathbf{F}_q[x_1, \ldots, x_m]^l$	total degree 2	randomly chosen
		$\boldsymbol{Q} \in \mathbf{F}_q[x_1, \ldots, x_f]^n$		
		$\boldsymbol{H} \in \mathbf{F}_q[x_1, \ldots, x_m]^m$	bijective quadratic polynomial transformation	
	polynomial matrix	$S \in \mathbf{F}_q[x_1, \ldots, x_m]^{l \times f}$	total degree 1	randomly chosen
		secret key of original MPKC $\mathcal{K}$		
components of public key (secret, not used in decryption)	matrix	$A \in \mathbf{F}_q^{(k-p) \times t}$	randomly chosen	
	polynomial vector	$\boldsymbol{E} \in \mathbf{F}_q[x_1, \ldots, x_k]^n$	public key of $\mathcal{K}$	
		$\boldsymbol{a} \in \mathbf{F}_q[x_1, \ldots, x_z]^m$	total degree 1	randomly chosen
		$\boldsymbol{L} \in \mathbf{F}_q[x_1, \ldots, x_z]^f$		
		$\boldsymbol{r} \in \mathbf{F}_q[x_1, \ldots, x_z]^h$	total degree 2	

Thus, by performing Gaussian elimination for $S(\boldsymbol{a}(\boldsymbol{z}))$, Bob can efficiently calculate an invertible matrix $N(\boldsymbol{z}) \in {\mathbf{F}_q}^{l \times l}$ such that $N(\boldsymbol{z})S(\boldsymbol{a}(\boldsymbol{z})) = \begin{pmatrix} I_f \\ 0 \end{pmatrix}$ in all likelihood, where the right-hand side

Table 3: Summary of encryption

the set in which each element is included	column vector		
	number of columns		
	p	t	$z-p-t$
$\mathbf{F}_q[x_1,\ldots,x_p]$	$\boldsymbol{x} \in \mathbf{F}_q[x_1,\ldots,x_p]^p$		
$\mathbf{F}_q$	$\downarrow$ $\boldsymbol{p} \in \mathbf{F}_q^p$ plain text	random numbers $\boldsymbol{w} \in \mathbf{F}_q^t$ $\uparrow$	$\boldsymbol{v} \in \mathbf{F}_q^{z-p-t}$
$\mathbf{F}_q[x_{p+1},\ldots,x_{p+t}]$		$\boldsymbol{\lambda} \in \mathbf{F}_q[x_{p+1},\ldots,x_{p+t}]^t$	

the set in which each element is included	column vector				
	number of columns				
	g		z	p	$z-p$
$\mathbf{F}_q$	cipher text $\widetilde{\boldsymbol{c}} = \widetilde{\boldsymbol{E}}\begin{pmatrix}\boldsymbol{p}\\\boldsymbol{u}\end{pmatrix} \in \mathbf{F}_q^g$ $\uparrow$	$\leftarrow$	$\boldsymbol{z} \in \mathbf{F}_q^z$ $\boldsymbol{z} = \begin{pmatrix}\boldsymbol{p}\\\boldsymbol{u}\end{pmatrix}$	plain text $\boldsymbol{p} \in \mathbf{F}_q^p$	random numbers $\boldsymbol{u} \in \mathbf{F}_q^{z-p}$ $\boldsymbol{u} = \begin{pmatrix}\boldsymbol{w}\\\boldsymbol{v}\end{pmatrix}$
$\mathbf{F}_q[x_1,\ldots,x_z]$	$\widetilde{\boldsymbol{E}} \in \mathbf{F}_q[x_1,\ldots,x_z]^g$ public key polynomial vector				

is the reduced row echelon form of $S(\boldsymbol{a}(\boldsymbol{z}))$.[1] It follows that

$$N(\boldsymbol{z})S(\boldsymbol{a}(\boldsymbol{z}))\boldsymbol{L}(\boldsymbol{z}) = \begin{pmatrix} I_f \\ 0 \end{pmatrix} \boldsymbol{L}(\boldsymbol{z}) = \begin{pmatrix} \boldsymbol{L}(\boldsymbol{z}) \\ 0 \end{pmatrix}. \tag{6}$$

Thus, using the matrix $N(\boldsymbol{z})$ and the column vector $S(\boldsymbol{a}(\boldsymbol{z}))\boldsymbol{L}(\boldsymbol{z})$, Bob can efficiently calculate the value $\boldsymbol{L}(\boldsymbol{z})$ and therefore the value $\boldsymbol{Q}(\boldsymbol{L}(\boldsymbol{z}))$. Then Bob can efficiently calculate the value $\boldsymbol{E}\begin{pmatrix}\boldsymbol{p}\\\boldsymbol{y}\end{pmatrix}$ from the value $\boldsymbol{E}\begin{pmatrix}\boldsymbol{p}\\\boldsymbol{y}\end{pmatrix} + \boldsymbol{Q}(\boldsymbol{L}(\boldsymbol{z}))$. Note here that $S(\boldsymbol{a}(\boldsymbol{z}))$ is a function of the plain text $\boldsymbol{p}$ and this dependency on $\boldsymbol{p}$ is an essential part of the nonlinear PH matrix methods in general. If Bob knows the plain text $\boldsymbol{p}$, then he can compute the value $S(\boldsymbol{a}(\boldsymbol{z}))$ immediately. However, Bob has to compute $S(\boldsymbol{a}(\boldsymbol{z}))$ before recovering the plain text $\boldsymbol{p}$ in the decryption, as we see above. For the purpose of resolving this dilemma, the additional polynomial vector $\boldsymbol{a}$ is introduced into the scheme. By using the value $\boldsymbol{a}(\boldsymbol{z})$ as an additional information, Bob can calculate the value $S(\boldsymbol{a}(\boldsymbol{z}))$ before recovering the plain text $\boldsymbol{p}$, and the decryption proceeds without any trouble. Finally, according to the decryption procedure of $\mathcal{K}$, Bob can efficiently recover the plain text $\boldsymbol{p}$ using the secret key of $\mathcal{K}$. Note that $\boldsymbol{y}$ is discarded after the decryption. In this scheme we see, from (6), that the matrix

[1] If the reduced row echelon form of $S(\boldsymbol{a}(\boldsymbol{z}))$ does not have this form, then the decryption is failed.

$N(\boldsymbol{z})$ works as a PH matrix. In particular, since $N(\boldsymbol{z})$ depends on the plain text $\boldsymbol{p}$, $N(\boldsymbol{z})$ serves as a nonlinear PH matrix, as desired.

Note that the positive integer m has to be chosen to be sufficiently small compared with k. Otherwise, this nonlinear PH matrix method reduces to the primitive linear PH matrix method with random variables applied to the original public key $\boldsymbol{E} = \boldsymbol{H}(\boldsymbol{a})$. Also, if m is too much large compared with p, cipher text length g for p is large accordingly, so it causes problems in key length and the information transmission rate.

The public key (4) might look like the form of the so-called "Plus method" [22, 23] with respect to the multiplication by the matrix B from the left. Note, however, that this is not simply the form of Plus method due to the existence of the matrix $S(\boldsymbol{a})$ which is multiplied to the polynomial vector $\boldsymbol{L}$ from the left. A certain combination of B and $S(\boldsymbol{a})$ is multiplied to the polynomial vector $\boldsymbol{L}$ from the left as a net matrix, and forms a part of the public key $\widetilde{\boldsymbol{E}}$ of $\widetilde{\mathcal{K}}$. This net matrix is no longer constant and the multiplication of such a matrix is different from Plus method. This is a crucial point of the nonlinear PH matrix methods in general.

Example of $\boldsymbol{H}$. In the case where $q = 2^j$ with a positive integer j, we can choose as $\boldsymbol{H}$ the bijective quadratic polynomial transformation $\boldsymbol{H}_{\mathrm{MI}} \in \mathbf{F}_q[x_1, \dots, x_m]^m$ which was introduced by [19] to construct the Matsumoto-Imai cryptosystem. $\boldsymbol{H}_{\mathrm{MI}} = (h_1, \dots, h_m)^T$ is defined as follows. Let $\mathbf{K}$ be an extension of degree m of $\mathbf{F}_q$, and let $\beta_1, \dots, \beta_m \in \mathbf{K}$ be a basis of $\mathbf{K}$ as an $\mathbf{F}_q$-vector space. Then, the homogeneous quadratic polynomials $h_1, \dots, h_m \in \mathbf{F}_q[x_1, \dots, x_m]$ can be defined by the condition that $h_1(\boldsymbol{a})\beta_1 + \cdots + h_m(\boldsymbol{a})\beta_m = (a_1\beta_1 + \cdots + a_m\beta_m)^{q^\theta+1}$ for all $\boldsymbol{a} = (a_1, \dots, a_m)^T \in {\mathbf{F}_q}^m$. Here θ is a positive integer chosen so as to satisfy $\gcd(q^\theta + 1, q^m - 1) = 1$. It is then shown that the mapping ${\mathbf{F}_q}^m \ni \boldsymbol{a} \mapsto \boldsymbol{H}_{\mathrm{MI}}(\boldsymbol{a})$ is bijective and its inverse is efficiently computable.

5 Experimental Results

It is important to give a formal proof of the enhancement of the security by the quadratic nonlinear PH matrix method proposed in the previous section against all possible attacks. At present, however, it would seem difficult to give such a proof. Thus, based on computer experiments, we try to clarify the enhancement in this section. Our experimental results below suggest that the quadratic nonlinear PH matrix method is more secure against the Gröbner basis attack than the linear PH matrix method with random variables [32, 33, 34] when the Matsumoto-Imai cryptosystem (MI, for short) or RSE(2)PKC (RSE, for short) is chosen as the original QMPKC $\mathcal{K}$.

We report in Table 4 and Table 5 the time required to compute reduced Gröbner bases of the public keys both of QMPKC (MI or RSE) and of the QMPKC enhanced by the PH matrix method. Note that $n = k$ and $q = 2$ for the public keys $\boldsymbol{E} \in \mathbf{F}_q[x_1, \dots, x_k]^n$ of MI and RSE by their specifications. For the detail of the linear PH matrix method with random variables, see [34]. The running-times are given for PROSIDE edAEW416R2 workstation with AMD Opteron Model 854 processors at 2.80GHz and 64GB of RAM. We use the algorithm F_4 implemented on the computational algebra system Magma V2.12-21. In Table 4 and Table 5, due to the constraint of computing ability, only the cases of $p = 25$, $g = 47$ and $p = 30$, $g = 50$ are computed, where the information transmission rate (i.e., the ratio of the size of plain text to the size of cipher text) are $25/47 \approx 53\%$ and $30/50 = 60\%$. These seem to be inefficient. In realistic situations, however, p will usually be selected to be more than 200 and $g - p$ be $20 \sim 30$. Thus the ratio is not so inefficient

Table 4: Comparison between running-times for MI and the enhanced MI by the PH matrix method

Cryptosystems	p	k	z	g	f	l	m	h	t	Running-times in second	
MI		25								0.03	
		30								0.07	
		35								0.2	
		40								0.4	
		45								0.7	
		50								1	
		55								2	
		60								4	
										linear	quadratic nonlinear
The enhanced MI by the PH method	25	35	50	47	3	5	3	4	3	3	52
	25	35	51	47	3	5	3	4	3	6	260
	25	35	52	47	3	5	3	4	3	22	1307
	25	35	54	47	3	5	3	4	3	58	not available
	25	35	56	47	3	5	3	4	3	829	not available
	30	40	54	50	2	3	3	4	3	3	59
	30	40	55	50	2	3	3	4	3	5	263
	30	40	56	50	2	3	3	4	3	7	1281
	30	40	58	50	2	3	3	4	3	47	not available
	30	40	60	50	2	3	3	4	3	1016	not available

in practice. As stated in the introduction, the aim of the PH matrix method is to realize the exponential time complexity of cryptanalysis. However, since MI and RSE may have polynomial time complexity about $O(k^7)$ of cryptanalysis from [6] and our preliminary experimental results, it is quite difficult at present to compare MI or RSE with the enhanced these QMPKCs in a practical length of a plain text such as 200bits. If we can experimentally cryptanalyze the MI or RSE enhanced by the PH matrix method in the practical length of a plain text in order to compare it with the original MI or RSE, then this implies that the cryptosystem enhanced by PH matrix method is useless in itself. This is limitation and dilemma of the security evaluation by computer experiments. Table 4 and Table 5 give the comparison of the particular case with a plain text of 25 bits (MI or RSE with $k = 25$ and the enhanced these QMPKCs with $z = 52$). This shows that the time required for cryptanalysis is increased by more than 10^4 times by the application of the quadratic nonlinear PH matrix method. This fact shows that the quadratic nonlinear PH matrix method enhances the security of MI and RSE against the Gröbner basis attack.

Table 4 and Table 5 show that the increase of the number $z - p$ of additional variables $x_{p+1}, \ldots, x_z$ increases the running-time required to compute a reduced Gröbner basis of the public key $\widetilde{\boldsymbol{E}} \in \boldsymbol{F}_2[x_1, \ldots, x_z]^g$ of the enhanced cryptosystem $\widetilde{\mathcal{K}}$, as desired. The quadratic nonlinear PH matrix method provides substantial robustness against the Gröbner basis attack about $10 \sim 10^2$ times more than the linear PH matrix method with random variables. We will continue to make

Table 5: Comparison between running-times for RSE and the enhanced RSE by the PH matrix method

Cryptosystems	p	k	z	g	f	l	m	h	t	Running-times in second	
RSE		25								0.08	
		30								0.2	
		35								0.5	
		40								1	
		45								2	
		50								5	
		55								9	
		60								16	
										linear	quadratic nonlinear
The enhanced RSE by the PH method	25	35	50	47	3	5	3	4	3	6	50
	25	35	51	47	3	5	3	4	3	13	250
	25	35	52	47	3	5	3	4	3	19	1309
	25	35	54	47	3	5	3	4	3	131	not available
	25	35	56	47	3	5	3	4	3	1622	not available
	30	40	54	50	2	3	3	4	3	8	58
	30	40	55	50	2	3	3	4	3	11	264
	30	40	56	50	2	3	3	4	3	28	1285
	30	40	58	50	2	3	3	4	3	158	not available
	30	40	60	50	2	3	3	4	3	1770	not available

more examples of the running-times for more large parameters, where we might expect a further advantage of the quadratic nonlinear PH matrix method.

6 Discussion on Security

In this section, we discuss the immunity of the nonlinear PH matrix methods against known attacks.

6.1 Gröbner Basis Attack

As stated in the previous section, based on computer experiments, the quadratic nonlinear PH matrix method properly provides substantial robustness, and enhances the security of the Matsumoto-Imai cryptosystem and RSE(2)PKC against the Gröbner basis attack.

6.2 STS Attack

In 2004 Wolf, Braeken, and Preneel [35] introduced an attacks against a class of QMPKCs, called *step-wise triangular schemes* (STS, for short), based on the rank calculation of the public key (see also [24, 2]). On the other hand, Ito, Fukushima, and Kanako proposed an attack utilizing the particular structure in STS on a QMPKC based on the sequential solution method to which the linear PH matrix method is applied [13]. In the nonlinear PH matrix methods proposed in this paper, even if a QMPKC of STS type is chosen as a original MPKC $\mathcal{K}$, the structure can be hidden by adding the random polynomial vector $\boldsymbol{Q}$, which is not eliminated by matrix multiplication, to the original public key polynomial vector $\boldsymbol{E}$ directly when a public key $\widetilde{\boldsymbol{E}}$ of the enhanced cryptosystem $\widetilde{\mathcal{K}}$ is constructed. Thus, the nonlinear PH matrix methods might be immune against this type of attacks.

6.3 Differential Attack

In 2005 Fouque, Granboulan, and Stern [9] adapted differential cryptanalysis to MPKCs. They applied the differential cryptanalysis to break the Matsumoto-Imai cryptosystem and its variant, the perturbed Matsumoto-Imai cryptosystem (PMI, for short) [5]. Then, in 2006, Ding and Gower [7] proposed a revised version of PMI, called *PMI+*, which is obtained by the application of Plus method to PMI, and showed its immunity against the the differential cryptanalysis. The differential cryptanalysis might be applied only to Matsumoto-Imai type cryptosystems and the application of Plus method might recover their security against the differential cryptanalysis. In the nonlinear PH matrix methods proposed in this paper, the original MPKC $\mathcal{K}$ can be chosen to be any MPKC, not limited to Matsumoto-Imai type cryptosystems, and the nonlinear PH matrix methods has a structure like Plus method. Thus, the nonlinear PH matrix methods might be immune against the differential cryptanalysis. We will clarify this point in the future work.

7 Concluding Remarks

In this paper, we have developed the notion of piece in hand (PH) concept, which can be applicable to any reasonable type of MPKCs for the purpose of enhancing their security. We have presented the quadratic nonlinear PH matrix method based on the concept. In the future work, we will demonstrate the enhancement of security by the methods against the Gröbner basis attack, the STS attack, and the differential attack in an experimental manner for all proposed MPKCs extensively.

From the practical point of view, it is also important to evaluate the key length and the efficiency of encryption and decryption in the enhanced cryptosystem. However, since the aim of the present paper is mainly to develop the framework of nonlinear PH matrix methods as a countermeasure against the advent of quantum computers in the future, this practical issue of current interest is discussed in another paper. Because of the same reason, we have not considered the stronger security such as IND-CCA type security but considered just the encryption primitive $\widetilde{\boldsymbol{E}}$ for an MPKC which is obtained by applying the nonlinear PH matrix method. We leave the consideration of the stronger security to a future study.

References

[1] G. Ars. Private communication, December 2004.

[2] D. Coppersmith, J. Stern, and S. Vaudenay. Attacks on the birational permutation signature schemes. *Proc. CRYPTO '93*, Lecture Notes in Computer Science, Vol.773, pp.435–443, Springer, 1994.

[3] N. Courtois, M. Daum, and P. Felke. On the security of HFE, HFEv- and Quartz. *Proc. PKC 2003*, Lecture Notes in Computer Science, Vol.2567, pp.337–350, Springer, 2003.

[4] N. Courtois, A. Klimov, J. Patarin, and A. Shamir. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. *Proc. EUROCRYPT 2000*, Lecture Notes in Computer Science, Vol.1807, pp.392–407, Springer, 2000.

[5] J. Ding. A new variant of the Matsumoto-Imai cryptosystem through perturbation. *Proc. PKC 2004*, Lecture Notes in Computer Science, Vol.2947, pp.305–318, Springer, 2004.

[6] J. Ding, J. E. Gower, D. Schmidt, C. Wolf, and Z. Yin. Complexity estimates for the F4 attack on the perturbed Matsumoto-Imai cryptosystem. *Proc. IMA Int. Conf. 2005*, Lecture Notes in Computer Science, Vol.3796, pp.262–277, Springer, 2005.

[7] J. Ding and J. E. Gower. Inoculating multivariate schemes against differential attacks. *Proc. PKC 2006*, Lecture Notes in Computer Science, Vol.3958, pp.290–301, Springer, 2006.

[8] J. C. Faugère and A. Joux. Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases. *Proc. CRYPTO 2003*, Lecture Notes in Computer Science, Vol.2729, pp.44–60, Springer, 2003.

[9] P. A. Fouque, L. Granboulan, and J. Stern. Differential cryptanalysis for multivariate schemes. *Proc. EUROCRYPT 2005*, Lecture Notes in Computer Science, Vol.3494, pp.341–353, Springer, 2005.

[10] M. Garey and D. Johnson, Computers and Intractability, A Guide to the Theory of NP-Completeness, Freeman, 1979.

[11] L. Granboulan, A. Joux, and J. Stern. Inverting HFE is quasipolynomial. *Proc. CRYPTO 2006*, Lecture Notes in Computer Science, Vol.4117, pp.345–356, Springer, 2006.

[12] S. Hasegawa and T. Kaneko. An attacking method for a public-key cryptosystem based on the difficulty of solving a system of non-linear equations. *Proc. 10th SITA*, JA5-3, November 1987. In Japanese.

[13] D. Ito, Y. Fukushima, and T. Kaneko. On the security of piece in hand concept based on sequential solution method. Technical Report of IEICE, ISEC2006-30, SITE2006-27 (2006-7), July 2006. In Japanese.

[14] M. Kasahara and R. Sakai. A new principle of public key cryptosystem and its realization. Technical Report of IEICE, ISEC2000-92 (2000-11), November 2000. In Japanese.

[15] M. Kasahara and R. Sakai. A construction of public key cryptosystem for realizing ciphertext of size 100 bit and digital signature scheme. *IEICE Transactions on Fundamentals*, E87-A, No.1 (2004), 102–109.

[16] A. Kipnis, J. Patarin, and L. Goubin. Unbalanced Oil and Vinegar signature schemes. *Proc. EUROCRYPT '99*, Lecture Notes in Computer Science, Vol.1592, pp.206–222, Springer, 1999.

[17] A. Kipnis and A. Shamir. Cryptanalysis of the HFE public key cryptosystem by relinearization. *Proc. CRYPTO '99*, Lecture Notes in Computer Science, Vol.1666, pp.19–30, Springer, 1999.

[18] T. Matsumoto, H. Imai, H. Harashima, and H. Miyakawa. A class of asymmetric cryptosystems using obscure representations of enciphering functions. *1983 National Convention Record on Information Systems, IECE Japan*, S8-5, 1983. In Japanese.

[19] T. Matsumoto and H. Imai. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. *Proc. EUROCRYPT '88*, Lecture Notes in Computer Science, Vol.330, pp.419–453, Springer, 1988.

[20] T. T. Moh. A public key system with signature and master key functions. *Communications in Algebra*, 27, 2207–2222, 1999.

[21] J. Patarin. Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt '88. *Proc. CRYPTO '95*, Lecture Notes in Computer Science, Vol.963, pp.248-261, Springer, 1995.

[22] J. Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms. *Proc. EUROCRYPT '96*, Lecture Notes in Computer Science, Vol.1070, pp.33–48, Springer, 1996.

[23] J. Patarin, L. Goubin, and N. Courtois. C^*_{-+} and HM: Variations around two schemes of T. Matsumoto and H. Imai. *Proc. ASIACRYPT '98*, Lecture Notes in Computer Science, Vol.1514, pp.35–49, Springer, 1998.

[24] A. Shamir. Efficient signature schemes based on birational permutations. *Proc. CRYPTO '93*, Lecture Notes in Computer Science, Vol.773, pp.1–12, Springer, 1994.

[25] K. Tadaki and S. Tsujii. On the enhancement of security by piece in hand matrix method for multivariate public key cryptosystems. *Proc. SCIS2007*, 2C1-3, 2007.

[26] S. Tsujii, K. Kurosawa, T. Itoh, A. Fujioka, and T. Matsumoto. A public-key cryptosystem based on the difficulty of solving a system of non-linear equations. *IEICE Transactions* (D), J69-D, No.12 (1986), 1963–1970. In Japanese.

[27] S. Tsujii, A. Fujioka, and Y. Hirayama. Generalization of the public-key cryptosystem based on the difficulty of solving a system of non-linear equations. *IEICE Transactions* (A), J72-A, No.2 (1989), 390–397. In Japanese. An English translation of [27] is included in [30] as an appendix.

[28] S. Tsujii. A new structure of primitive public key cryptosystem based on soldiers in hand matrix. Technical Report TRISE 02-03, Chuo University, July 2003.

[29] S. Tsujii, R. Fujita, and K. Tadaki. Proposal of MOCHIGOMA (piece in hand) concept for multivariate type public key cryptosystem. Technical Report of IEICE, ISEC2004-74 (2004-09), September 2004. Available at URL: `http://lab.iisec.ac.jp/~tsujii/ISEC2004-74.pdf` .

[30] S. Tsujii, K. Tadaki, and R. Fujita. Piece in hand concept for enhancing the security of multivariate type public key cryptosystems: public key without containing all the information of secret key. Cryptology ePrint Archive, Report 2004/366, December 2004. Available at URL: `http://eprint.iacr.org/2004/366` .

[31] S. Tsujii, K. Tadaki, and R. Fujita. Piece in hand concept for enhancing the security of multivariate type public key cryptosystems: public key without containing all the information of secret key. *Proc. SCIS2005*, 2E1-3, pp.487–492, 2005. Available at URL: `http://lab.iisec.ac.jp/~tsujii/SCIS2005-2E1-3.pdf` .

[32] S. Tsujii, K. Tadaki, and R. Fujita. Proposal for piece in hand (soldiers in hand) matrix — general concept for enhancing security of multivariate public key cryptosystems — Ver.2. *Proc. SCIS2006*, 2A4-1, 2006. In Japanese. Available at URL: `http://lab.iisec.ac.jp/~tsujii/SCIS2006-2A4-1.pdf` .

[33] S. Tsujii, K. Tadaki, and R. Fujita. Proposal for piece in hand matrix ver.2: general concept for enhancing security of multivariate public key cryptosystems. Workshop Record of the International Workshop on Post-Quantum Cryptography (PQCrypto 2006), pp.103–117, 2006. Available at URL: `http://postquantum.cr.yp.to/pqcrypto2006record.pdf` .

[34] S. Tsujii, K. Tadaki, and R. Fujita. Proposal for piece in hand matrix: general concept for enhancing security of multivariate public key cryptosystems. *IEICE Transactions on Fundamentals*, E90-A, No.5 (2007), 992–999. Available at URL: `http://lab.iisec.ac.jp/~tsujii/TTF07.pdf` .

[35] C. Wolf, A. Braeken, and B. Preneel. Efficient cryptanalysis of RSE(2)PKC and RSSE(2)PKC. *Proc. SCN 2004*, Lecture Notes in Computer Science, Vol.3352, pp.294–309, Springer, 2004.

[36] C. Wolf and B. Preneel. Taxonomy of Public Key Schemes based on the problem of Multivariate Quadratic equations. Cryptology ePrint Archive, Report 2005/077, December 2005. Available at URL: `http://eprint.iacr.org/2005/077` .

A Primitive Linear PH Matrix Method

In what follows, we give a complete description of the primitive linear PH matrix method, introduced by [30, 31]. This version of a PH matrix method is an illustrative implementation of the PH concept, and serves as the starting point of all advanced PH matrix methods. The primitive linear PH matrix method [30, 31] is described as follows.

Let $\mathcal{K}$ be an arbitrary QMPKC whose public key is given by $\boldsymbol{E} \in \mathbf{F}_q[x_1, \dots, x_k]^n$, as described in Subsection 2.2. In the primitive linear PH matrix method, a new QMPKC $\widetilde{\mathcal{K}}$ is constructed from the given QMPKC $\mathcal{K}$ for the purpose of enhancing the security. A public key $\widetilde{\boldsymbol{E}} \in \mathbf{F}_q[x_1, \dots, x_k]^l$ of $\widetilde{\mathcal{K}}$ is constructed from the original public key $\boldsymbol{E}$ of $\mathcal{K}$ by the transformation:

$$\widetilde{\boldsymbol{E}} \underset{\text{def}}{=} S\boldsymbol{E} + R\boldsymbol{X}.$$

Here $\boldsymbol{X}$ denotes the column vector whose components are all monomials in $\mathbf{F}_q[x_1,\dots,x_k]$ of total degree at most two, enumerated in any order. Thus, $\boldsymbol{X}$ can be chosen as

$$\boldsymbol{X} \underset{\text{def}}{=} (x_1x_1, x_1x_2, \dots, x_{k-1}x_k, x_kx_k, x_1, x_2, \dots, x_k, 1)^T.$$

S is a matrix in ${\mathbf{F}_q}^{l\times n}$. In order to make the PH matrix method work properly, we assume that $l > n$. On the other hand, R is a matrix in ${\mathbf{F}_q}^{l\times t}$, where t is the number of components in $\boldsymbol{X}$. Note that $t = \binom{k+2}{2} = (k^2+3k+2)/2$ for $q \geq 3$.[2] The term $R\boldsymbol{X}$ plays a role in randomizing $\widetilde{\boldsymbol{E}}$. Hence R has to be chosen so that neither the hidden original public key $\boldsymbol{E}$ nor any equivalent polynomial vector which enables an eavesdropper to obtain Alice's plain text can be identified in the actual public key $\widetilde{\boldsymbol{E}}$. A plain text of $\widetilde{\mathcal{K}}$ is represented by a vector in ${\mathbf{F}_q}^k$ in the same way as in $\mathcal{K}$. For any plain text vector $\boldsymbol{p} \in {\mathbf{F}_q}^k$ of $\widetilde{\mathcal{K}}$, the corresponding cipher text of $\widetilde{\mathcal{K}}$ is represented by a vector $\widetilde{\boldsymbol{c}} \in {\mathbf{F}_q}^l$ and is calculated by $\widetilde{\boldsymbol{c}} = \widetilde{\boldsymbol{E}}(\boldsymbol{p})$.

In addition to the matrices S and R, we introduce the *PH matrix* $M \in {\mathbf{F}_q}^{n\times l}$ as a part of secret key of $\widetilde{\mathcal{K}}$. In the key-generation stage, the matrices R, M, and S are chosen in sequence so as to satisfy the following three conditions. We can show that this choice is efficiently possible.

Condition 1. *$l \geq n + \operatorname{rank} R$.* □

Condition 2. *$MR = 0$ and $\operatorname{rank} M = n$.* □

Condition 3. *$MS = I_n$, where I_n is the identity matrix in ${\mathbf{F}_q}^{n\times n}$.* □

By the above conditions we see that the multiplication of $\widetilde{\boldsymbol{E}}$ by the PH matrix M from the left simplifies $\widetilde{\boldsymbol{E}}$ and results in the original public key $\boldsymbol{E}$ as follows:

$$M\widetilde{\boldsymbol{E}} = \boldsymbol{E}. \tag{7}$$

This is a crucial property of the PH matrix in our PH matrix methods in general.

Then, the triple $(q, k, \widetilde{\boldsymbol{E}})$ forms the public key of $\widetilde{\mathcal{K}}$. On the other hand, the PH matrix M, together with the secret key of $\mathcal{K}$ corresponding to the public key $(q, k, \boldsymbol{E})$ of $\mathcal{K}$, forms the secret key of $\widetilde{\mathcal{K}}$. The decryption of $\widetilde{\mathcal{K}}$ proceeds as follows. Based on the relation (7), on receiving the cipher text $\widetilde{\boldsymbol{c}} \underset{\text{def}}{=} \widetilde{\boldsymbol{E}}(\boldsymbol{p})$ for a plain text $\boldsymbol{p}$, Bob can efficiently calculate $\boldsymbol{c} \underset{\text{def}}{=} \boldsymbol{E}(\boldsymbol{p}) = M\widetilde{\boldsymbol{c}}$ by the multiplication of $\widetilde{\boldsymbol{c}}$ by M from the left. Then, according to the decryption procedure of $\mathcal{K}$, Bob can efficiently recover the plain text $\boldsymbol{p}$ using the secret key of $\mathcal{K}$.

B The proof of Theorem 4.1

In order to prove Theorem 4.1, we need the following well-known theorem.

Theorem B.1. *Let l and n be positive integers with $l \geq n$. Assume that an $l \times n$ matrix A is randomly chosen from ${\mathbf{F}_q}^{l\times n}$. Then the probability $P(l,n)$ that the matrix A has full column rank is given by*

$$P(l,n) = \left(1 - \frac{1}{q^l}\right)\left(1 - \frac{1}{q^{l-1}}\right)\left(1 - \frac{1}{q^{l-2}}\right)\cdots\left(1 - \frac{1}{q^{l-n+1}}\right).$$

PROOF of Theorem 4.1. We note the inequality $(1+x)^n \geq 1 + nx$ for every positive integer n and every real number $x \geq -1$. The result follows from Theorem B.1. □

[2] In the case of $q = 2$, we can eliminate the monomials $x_1^2, \dots, x_k^2$ from $\boldsymbol{X}$ using the so-called *field equations* $x_i^2 = x_i$ $(i = 1, \dots, k)$. Thus t is calculated to be $(k^2+k+2)/2$ in such a case.