Proposal for Piece In Hand Matrix Ver.2: General Concept 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
[‡] 21st Century Center OF Excellence Program, Chuo University
1–13–27 Kasuga, Bunkyo-ku, Tokyo, 112–8551 Japan
[§] Division of Management Science, Graduate School of Engineering
Tokyo University of Science, 1–3 Kagurazaka, Shinjuku-ku, Tokyo, 162–8601 Japan

Abstract. We proposed the concept, *piece in hand (soldiers in hand) matrix* and have developed the framework based on the concept so far. The piece in hand matrix is a general concept which can be applicable to any type of multivariate public key cryptosystems to enhance their security. In this paper, we make improvements in the PH matrix method as follows. (i) In the PH matrix method, an arbitrary number of additional variables can be introduced to the random polynomial term in the public key, which is eliminated by the multiplication of the PH matrix to the public key in the decryption. Thus these additional variables enables the public key to have more than one solution, and therefore increases the difficulty to solve the public key. We show, in an experimental manner, that the PH matrix method improved in this way is secure even against the Gröbner basis attack. (ii) In the nonlinear PH matrix method proposed previously, the degree of polynomials in the public key is more than two, and this may cause an undesirable increase in the length of the public key. In this paper, we propose a nonlinear PH matrix method, where the degree of the public key is kept the same as the degree of the public key of the original cryptosystem, which is normally two.

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

1 Introduction

The research of multivariate public key cryptosystems started with the works by Matsumoto et al. [8] in 1983 and Tsujii et al. [13] in 1986. Especially, the multivariate public key cryptosystem which was proposed by Matsumoto and Imai [9] in 1988 is known as *the Matsumoto-Imai cryptosystem* nowadays. In 1995 Patarin constructed an attack against the Matsumoto-Imai cryptosystem in a heuristic manner [11] and then proposed an improvement of the cryptosystem, called *HFE*, in 1996 [12]. Subsequently, Kipnis and Shamir introduced a general technique, called *relinearization*, to solve system of multivariate polynomial equations, and used it to attack HFE in 1999 [7]. Recently, Faugère and Joux showed in an experimental manner that computing a Gröbner basis of the public key is likely to be an efficient attack to HFE [3]. Because of the simplicity of this attack, it may be a threat to any type of proposed multivariate public key cryptosystem, and now seems to be thought of as a major attack against any such cryptosystem.

On the other hand, in the work [13] Tsujii et al. proposed a multivariate public key cryptosystem by introducing a trapdoor called *the sequential solution method*, and then the cryptosystem was broken by Hasegawa and Kaneko [4] for the special case where rational functions are used. Later on, in 1989, [14] proposed the revised version of [13], where birational transformation, named *core transformation*, was employed.[1] No attack to this revised version has been succeeded so far.

In 2000 Kasahara and Sakai proposed a multivariate public key cryptosystem with random variables [5] and have improved the cryptosystem in a series of works such as [6]. On the other hand, by introducing random terms to the Matsumoto-Imai cryptosystem, Ding proposed a multivariate public key cryptosystem called *the perturbed Matsumoto-Imai cryptosystem* [2].

In 2003 one of us [15] proposed the concept, *piece in hand matrix.* Thereafter we have developed the framework based on the concept in a series of works [16, 17, 18, 19] so far. The concept of the piece in hand (PH, for short) matrix has the following properties:[2] (i) The PH matrix is a general concept which can be applicable to any type of multivariate public key cryptosystems to enhance their security. (ii) In a framework of the PH matrix, the original public key, which is represented by a polynomial vector, is randomized by adding a random polynomial term and then published. In the decryption, the legitimate receiver can obtain the cipher text of the original cryptosystem by multiplying the PH matrix to eliminate the random term, and then recover the plain text according to the decryption of the original cryptosystem. (iii) There are two types of the PH matrices: a linear matrix whose elements are constants and a nonlinear matrix whose elements are functions of the plain text or random numbers.

In this paper, we make improvements in the PH matrix methods as follows: (i) In the PH matrix method, an arbitrary number of additional variables can be introduced to the random polynomial term in the public key, which is eliminated by the multiplication of the PH matrix to the public key in the decryption. Thus the number of variables can be increased more than the number of polynomials in the public key, where random numbers are substituted to the additional variables in the encryption, and also these additional variables in the public key can be made to have more than one solution. We show, in an experimental manner, that the PH matrix method improved in this way is secure even against the Gröbner basis attack. (ii) In the nonlinear PH matrix method proposed previously, the degree of polynomials in the public key is more than two, and this may cause an undesirable increase in the length of the public key. In this paper, we propose a nonlinear PH matrix method, where the degree of the public key is kept the same as the degree of the public key of the original cryptosystem, which is normally two.

1.1 Schemes of Multivariate Public Key Cryptosystems

We first review the schemes of multivariate public key cryptosystems. A multivariate public key cryptosystem such as in [8, 13, 9, 14, 12, 10, 5, 2, 6] can be considered to comply with the following scheme: Let $\mathbf{F}_q$ be a finite field which has q elements. A plain text is represented by a column vector $\boldsymbol{p} = (p_1, p_2, \dots, p_k)^T$, and a cipher text is represented by a column vector $\boldsymbol{c} = (c_1, c_2, \dots, c_n)^T$, where the components p_i and c_i are in $\mathbf{F}_q$, and T denotes the transpose of vector. Let $\mathbf{F}_q[\boldsymbol{x}]$ be the set

[1] The paper [14] was originally written in Japanese. An English translation of [14] is included in [17] as an appendix.

[2] It is possible to apply the concept to signature schemes. However, we only describe the application to encryption schemes in this paper.

of all polynomials in variables $x_1, x_2, \ldots, x_k$ with coefficients in $\mathbf{F}_q$. Then a polynomial vector $E(\boldsymbol{x}) \in \mathbf{F}_q[\boldsymbol{x}]^n$ and q form the public key in the cryptosystem. The encryption is given by the following transformation from $\boldsymbol{p}$ to $\boldsymbol{c}$:

$$\boldsymbol{c} = E(\boldsymbol{p}).$$

The secret key is an efficient method to solve the equation $E(\boldsymbol{x}) = \boldsymbol{c}$ on $\boldsymbol{x}$ for any given $\boldsymbol{c}$. Thus, $E(\boldsymbol{x})$ has to be constructed so that, without the knowledge about this method, it is difficult to find $\boldsymbol{p}$ for any $\boldsymbol{c}$ in polynomial-time.

Let us consider the situation that Bob has the secret key and Alice transmits her cipher text $\boldsymbol{c} \equiv E(\boldsymbol{p})$ to Bob. When Bob receives the cipher text, using the secret key he can efficiently decipher it to obtain the plain text $\boldsymbol{p}$. On the other hand, it is intractable for an eavesdropper, Catherine, to recover $\boldsymbol{p}$ from $\boldsymbol{c}$, since she has no knowledge about the secret key and she has to solve the equation $E(\boldsymbol{x}) = \boldsymbol{c}$ on $\boldsymbol{x}$ directly.

In most multivariate public key cryptosystems, the public key $E(\boldsymbol{x})$ has the following form:

$$E(\boldsymbol{x}) = (B \circ F_0 \circ A)(\boldsymbol{x}). \tag{1}$$

Here A and B are invertible linear transformations on ${\mathbf{F}_q}^k$ and ${\mathbf{F}_q}^n$, respectively. Thus we can assume that A is an invertible $k \times k$ matrix and B is an invertible $n \times n$ matrix, where the entries of both A and B are in $\mathbf{F}_q$. F_0 is a nonlinear function from ${\mathbf{F}_q}^k$ to ${\mathbf{F}_q}^n$ such that the components in $F_0(\boldsymbol{u})$ are polynomials in $\mathbf{F}_q[\boldsymbol{u}]$, where $\mathbf{F}_q[\boldsymbol{u}]$ is the set of all polynomials in variables $u_1, u_2, \ldots, u_k$ with coefficients in $\mathbf{F}_q$, and a vector $\boldsymbol{u} = (u_1, u_2, \ldots, u_k)^T$ is related to $\boldsymbol{x}$ by $\boldsymbol{u} = A\boldsymbol{x}$. In this type of cryptosystem, Bob keeps A and B secret (and so F_0 in some cryptosystems).

1.2 General Prescription for Enhancement by the PH Matrix Method

In this subsection, we recall the general prescription for the enhancement of the security of any given multivariate public key cryptosystem by our PH matrix method, introduced by [16]. Let $\mathcal{K}$ be any multivariate public key cryptosystem whose public key is $E(\boldsymbol{x}) \in \mathbf{F}_q[x_1, \ldots, x_k]^n$, as described in the previous subsection. We construct new multivariate public key cryptosystem $\widetilde{\mathcal{K}}$ through an application of our PH method directly to the public key $E(\boldsymbol{x})$ of $\mathcal{K}$ in a sequential manner. A public key $\widetilde{E}(\boldsymbol{x})$ of $\widetilde{\mathcal{K}}$ is constructed from the original public key $E(\boldsymbol{x})$ of $\mathcal{K}$ by the transformation:

$$\widetilde{E}(x_1, \ldots, x_k) \equiv S \cdot E(x_1, \ldots, x_k) + R \cdot X[1, k]. \tag{2}$$

Here $X[1, k]$ denotes the column vector whose components are all monomials in $\mathbf{F}_q[x_1, \ldots, x_k]$ of total degree at most two, enumerated in any order. Thus, $X[1, k]$ can be chosen as

$$X[1, k] \equiv (x_1x_1, x_1x_2, \ldots, x_{k-1}x_k, x_kx_k, x_1, x_2, \ldots, x_k, 1)^T.$$

S is an $l \times n$ matrix whose entries are in $\mathbf{F}_q$, In order to make our PH method work properly, we assume that $l > n$. On the other hand, R is an $l \times t[1, k]$ matrix whose entries are in $\mathbf{F}_q$, where $t[1, k]$ is the number of components of $X[1, k]$. Note that $t[1, k] = \binom{k+2}{2} = (k^2 + 3k + 2)/2$. The term $R \cdot X[1, k]$ plays a role in randomizing $\widetilde{E}(\boldsymbol{x})$. Hence the R has to be chosen so that in $\widetilde{E}(\boldsymbol{x})$ each polynomial component in the vector $R \cdot X[1, k]$ cannot be indistinguishable from the polynomials which come from $E(\boldsymbol{x})$. 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 $\widetilde{\boldsymbol{c}} = \widetilde{E}(\boldsymbol{p})$.

We choose the R, PH matrix M, and S 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. *M is an $n \times l$ matrix such that $MR = 0$ and $\operatorname{rank} M = n$.* □

Condition 3. *$MS = I_n$, where I_n is the $n \times n$ identity matrix.* □

Then, q and $\widetilde{E}(\boldsymbol{x})$ form the public key of $\widetilde{\mathcal{K}}$. On the other hand, the PH matrix M together with the secret key of $\mathcal{K}$ for the public key q and $E(\boldsymbol{x})$ of $\mathcal{K}$ form the secret key of $\widetilde{\mathcal{K}}$. The decryption of $\widetilde{\mathcal{K}}$ proceeds as follows. Since $M\widetilde{E}(\boldsymbol{x}) = E(\boldsymbol{x})$ by the above conditions, on receiving the cipher text $\widetilde{\boldsymbol{c}} \equiv \widetilde{E}(\boldsymbol{p})$ for a plain text $\boldsymbol{p}$, Bob can efficiently calculate $\boldsymbol{c} \equiv E(\boldsymbol{p}) = M\widetilde{\boldsymbol{c}}$ 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 $\mathcal{K}$.

1.3 Countermeasures against the Gröbner Bases Attack

Recently, Faugère and Joux [3] showed in an experimental manner that computing a Gröbner basis of the public key is likely to be an efficient attack to HFE [12], which is one of the major variants of multivariate public key cryptosystem. The attack is simply to compute a Gröbner basis for the ideal generated by polynomial components in $E(\boldsymbol{x}) - \boldsymbol{c}$, where $\boldsymbol{c}$ is a cipher text vector. Thus, because of the simplicity of this attack, it may be a threat to any type of proposed multivariate public key cryptosystem.

Especially, from the point of view of Gröbner bases, the secret linear transformation B in a scheme whose public key has the form (1) may be useless. 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 concept might be also useless to the Gröbner attack in its primitive implementation presented in the previous sections. We first note that, by the definition of the PH matrix M, $M(\widetilde{E}(\boldsymbol{x}) - \widetilde{\boldsymbol{c}}) = E(\boldsymbol{x}) - \boldsymbol{c}$, where $\widetilde{\boldsymbol{c}} \equiv \widetilde{E}(\boldsymbol{p})$ is a cipher text vector of the enhanced cryptosystem $\widetilde{\mathcal{K}}$ and $\boldsymbol{c} \equiv E(\boldsymbol{p})$ is a 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 $(c_1, \dots, c_n)^T \equiv E(\boldsymbol{p})$ and $(\widetilde{c}_1, \dots, \widetilde{c}_l)^T \equiv \widetilde{E}(\boldsymbol{p})$ are cipher text vectors of $\mathcal{K}$ and $\widetilde{\mathcal{K}}$, respectively, and the polynomial vectors $(e_1, \dots, e_n)^T \equiv E(\boldsymbol{x})$ and $(\widetilde{e}_1, \dots, \widetilde{e}_l)^T \equiv \widetilde{E}(\boldsymbol{x})$ are the public keys of $\mathcal{K}$ and $\widetilde{\mathcal{K}}$, respectively. Thus, from the point of view of Gröbner bases the system $\widetilde{E}(\boldsymbol{x}) - \widetilde{\boldsymbol{c}} = \mathbf{0}$ of polynomial equations might not be necessarily more difficult to solve than the system $E(\boldsymbol{x}) - \boldsymbol{c} = \mathbf{0}$ due to the existence of the additional equations $g_1 = 0, \dots, g_{l-n} = 0$ for the former. In such a case, the PH method might be useless to the Gröbner attack. This paper proposes new PH matrix methods which overcome this weakness, through elaborations of the original PH matrix method, and is organized as follows.

In Section 2, we describe the linear PH method with random variables and consider its security. In the above consideration, the polynomials $e_1, \dots, e_n$ are assumed to be in $\mathbf{F}_q[x_1, \dots, x_k]$

implicitly, and therefore the weakness of the original PH method against the Gröbner attack is of concern. Thus, one of the countermeasures against the weakness is to introduce additional variables $x_{k+1}, \dots, x_m$ to the public key of $\widetilde{\mathcal{K}}$. Under this countermeasure, the g_i's in (3) are no longer polynomials in $\mathbf{F}_q[x_1, \dots, x_k]$, but in $\mathbf{F}_q[x_1, \dots, x_m]$, and therefore solving the system $\widetilde{E}(x_1, \dots, x_m) - \widetilde{\boldsymbol{c}} = \mathbf{0}$ of polynomial equations seems to be more difficult than solving the system $E(x_1, \dots, x_k) - \boldsymbol{c} = \mathbf{0}$. This is done by introducing to the term $R \cdot X[1, k]$ in (2) the additional variables $x_{k+1}, \dots, x_m$ which are set to random values by Alice on the encryption. We propose new PH matrix method based on this idea, and show that the new method properly works and provides substantial robustness against the Gröbner attack, based on computer experiments. We then present another countermeasure against the Gröbner basis attack through a nonlinearization of the to PH matrix in Section 3 In the previous work [17], we already proposed nonlinear PH matrix method. However, the order 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 length of the public key of the enhanced cryptosystem. In a new nonlinear PH matrix method proposed in this paper, the order of the public key of $\widetilde{\mathcal{K}}$ is always the same as the order of the public key of the original cryptosystem $\mathcal{K}$. Thus, the new nonlinear PH matrix method is more practical than the previous proposal. We conclude this paper with a discussion about the future direction of our work in Section 4.

2 Linear PH Matrix Method with Random Variables

In this section, as a countermeasure against the Gröbner attack, we introduce the linear PH matrix method with random variables, based on the general prescription for the enhancement of the security by the linear PH matrix method, described in Subsection 1.2. The point of the modification is to introduce to the public key of the enhanced cryptosystem additional variables. By this countermeasure, the computational complexity of the Gröbner attack is likely to increase exponentially in the number of the additional variables, as suggested by the experimental results below.

2.1 The New Method

Let $\mathcal{K}$ be any quadratic multivariate public key cryptosystem whose public key is given as $E(x_1, \dots, x_k) \in \mathbf{F}_q[x_1, \dots, x_k]^n$. We construct a new quadratic multivariate public key cryptosystem $\widetilde{\mathcal{K}}$ based on $\mathcal{K}$ as follows. Let p and m be any positive integers with $p < k < m$.

Key-Generation. In the key-generation stage, the public key and secret key of $\mathcal{K}$ are chosen first. Then, a public key $\widetilde{E}(x_1, \dots, x_m) \in \mathbf{F}_q[x_1, \dots, x_m]^l$ of $\widetilde{\mathcal{K}}$ is constructed from the original public key $E(x_1, \dots, x_k)$ of $\mathcal{K}$ by the following transformation:

$$\widetilde{E}(x_1, \dots, x_m) \equiv S \cdot E(x_1, \dots, x_p, y_1, \dots, y_{k-p}) + R \cdot X[1, m], \tag{4}$$

where $(y_1, \dots, y_{k-p}) = (x_1, \dots, x_m)A$ and A is a $m \times (k-p)$ matrix with elements in $\mathbf{F}_q$ randomly chosen. $X[1, m]$ denotes the column vector whose components are all monomials in $\mathbf{F}_q[x_1, \dots, x_m]$ of total degree at most two, enumerated in any order. Thus, $X[1, m]$ can be chosen as

$$X[1, m] \equiv (x_1x_1, x_1x_2, \dots, x_{m-1}x_m, x_mx_m, x_1, x_2, \dots, x_m, 1)^T.$$

S is an $l \times n$ matrix whose entries are in $\mathbf{F}_q$, In order to make our PH method work properly, we assume that $l > n$. On the other hand, R is an $l \times t[1, m]$ matrix whose entries are in $\mathbf{F}_q$, where $t[1, m]$ is the number of components of $X[1, m]$. Note that $t[1, m] = (m^2 + 3m + 2)/2$. The S, R, and PH matrix M are randomly chosen so as to satisfy Conditions 1, 2, and 3 in Subsection 1.2. Note that, as in the case of the original method, this choice can be efficiently possible. Bob publishes p, m, q, and $\widetilde{E}(x_1, \ldots, x_m)$ after the key-generation.

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 is represented by a vector $\widetilde{\boldsymbol{c}} \in {\mathbf{F}_q}^l$ in $\widetilde{\mathcal{K}}$, and is calculated through $\widetilde{\boldsymbol{c}} \equiv \widetilde{E}(\boldsymbol{p}^T, \boldsymbol{r}^T)$ by Alice, where $\boldsymbol{r} \in {\mathbf{F}_q}^{m-p}$ is chosen randomly by Alice before the encryption of $\boldsymbol{p}$.

Decryption. The decryption of $\widetilde{\mathcal{K}}$ proceeds as follows. We first note that, by Conditions 2 and 3,

$$M\widetilde{E}(x_1, \ldots, x_m) = E(x_1, \ldots, x_p, (x_1, \ldots, x_m)A). \tag{5}$$

Thus, on receiving the cipher text

$$\widetilde{\boldsymbol{c}} \equiv \widetilde{E}(\boldsymbol{p}^T, \boldsymbol{r}^T) \tag{6}$$

for the plain text $\boldsymbol{p}$, Bob can efficiently obtain the value $E(\boldsymbol{p}^T, \boldsymbol{s}^T)$ from the multiplication of $\widetilde{\boldsymbol{c}}$ by M, where $\boldsymbol{s}$ is a column vector in ${\mathbf{F}_q}^{k-p}$ such that $\boldsymbol{s}^T = (\boldsymbol{p}^T, \boldsymbol{r}^T)A$. Then, according to the decryption procedure of $\mathcal{K}$, Bob can efficiently recover the plain text $\boldsymbol{p}$ using the secret key of $\mathcal{K}$. Note that $\boldsymbol{s}$ is discarded after the decryption.

2.2 Consideration on the Security

2.2.1 Strength against the Gröbner Bases Attack

For any cipher text vector $\widetilde{\boldsymbol{c}}$, the corresponding plain text vector $\boldsymbol{p}$ is unique in (6). On the other hand, $\boldsymbol{r}$ is not necessarily unique, since A is not invertible and R is chosen randomly. The nonuniqueness of $\boldsymbol{r}$ may provides substantial robustness against the Gröbner attack, as suggested by the experimental results shown below.

We report in Table 1 the time required to compute a reduced Gröbner base of the public key both of HFE and of the HFE enhanced by the linear PH method with random variables. The running-times are given for hp AlphaServer ES45 workstation with Alpha 21264 (EV68) processor at 1250 MHz and 32GB of RAM. We use the algorithm F_4 implemented on the computational algebra system Magma V2.12-14. Note that $n = k$ and $q = 2$ for the public keys $E(x_1, \ldots, x_k) \in \mathbf{F}_q[x_1, \ldots, x_k]^n$ of HFE by its specifications. In the table, d denotes the degree of the univariate polynomial in the encryption of the HFE scheme. In the lower half of the table, the linear PH matrix method with random variables is applied to the public keys of HFE with $q = 2$, $n = k = 20$, and $\operatorname{rank} R = l - n$. The table shows that the increase of the number $m - k$ of random variables $x_{k+1}, \ldots, x_m$ increases the running-time required to compute a reduced Gröbner base of the public key $\widetilde{E}(x_1, \ldots, x_m) \in \boldsymbol{F}_2[x_1, \ldots, x_m]^l$ of the enhanced cryptosystem $\widetilde{\mathcal{K}}$. Thus, it would seem that the linear PH matrix method with random variables provides substantial robustness against the Gröbner attack.

cryptosystems	p	k	m	l	running-times in second
HFE $(128 < d < 513)$		10			< 1
		25			686
		28			1404
the enhanced HFE by the PH method $(d < 513)$	10	20	30	25	1364
	10	20	35	25	5301
	10	20	37	25	8788
	10	20	32	28	3437
	10	20	36	28	9903
	10	20	38	28	15091

Table 1: Comparison between running-times for HFE and the enhanced HFE by the PH method.

In the above examples on the enhanced HFE by the PH method, due to the constraint of computing ability, only the cases of $p = 10$ and $l = 25, 28$ are computed where the ratios p/l of plain text to cipher text are $10/25 = 40\%$ and $10/28 \approx 36\%$, which seem to be inefficient. In realistic situations, however, p will usually be selected to be more than 100 and $l - p$ be $10 \sim 20$. Thus the ratio is not so inefficient in practice. We will continue to make examples for more large parameters.

2.2.2 Strength against Other Possible Attacks

It is not desirable that an eavesdropper, Catherine, can find the PH matrix M from a cipher text $\widetilde{\boldsymbol{c}}$ and the public key $\widetilde{E}(x_1, \ldots, x_m)$. This is because, if so, then she can easily obtain the value $E(\boldsymbol{p}^T, \boldsymbol{s}^T)$ due to the equation (5). However, in this PH matrix method, it would seem difficult to do so because of the existence of the y_i's in (4).

Assume, contrarily to the fact, that $p = k$ and therefore

$$\widetilde{E}(x_1, \ldots, x_m) \equiv S \cdot E(x_1, \ldots, x_k) + R \cdot X[1, m] \tag{7}$$

holds. Then, by trying to eliminate the variables $x_{k+1}, \ldots, x_m$ in $M'\widetilde{E}(x_1, \ldots, x_m)$, Catherine may construct a matrix M' such that $M'\widetilde{E}(x_1, \ldots, x_m) = E(x_1, \ldots, x_k)$. This M' works in the same manner as the original PH matrix M, and therefore she may be able to calculate the value $E(\boldsymbol{p})$. This possibility seems to be excluded by introducing the y_i's in (4), since they are the linear combinations of all variables $x_1, \ldots, x_m$. Thus the attack by constructing a matrix M' which behaves just like as the original PH matrix M may not be successful in this PH matrix method with random variables.

3 Nonlinearization of the PH Matrix

Another countermeasure against the Gröbner attack is to nonlinearize the PH matrix, i.e., to employ, as a PH matrix, a polynomial matrix $M(x_1, \ldots, x_k)$ whose entries are in $\mathbf{F}_q[x_1, \ldots, x_k]$. Since an ideal I generated by polynomials may change under the replacement of the generators of I by the product of $M(x_1, \ldots, x_k)$ and them, unlike in the case of linear M, the nonlinear PH matrix may provide substantial robustness against the Gröbner attack. In the previous work [17], we already proposed nonlinear PH matrix method. However, the order of polynomials in the public key of the enhanced cryptosystem $\widetilde{\mathcal{K}}$ is more than two in the previous method due to the use of Fermat's little theorem. This may cause an undesirable increase in the length of the public key of the enhanced cryptosystem. In this section, we propose a new nonlinear PH matrix method without using Fermat's little theorem, where the order of the public key of $\widetilde{\mathcal{K}}$ is always the same as the order of the public key of the original cryptosystem $\mathcal{K}$. Thus, the new nonlinear PH matrix method is more practical than the previous proposal, from the point of view of the length of public key.

Let $\mathcal{K}$ be any quadratic multivariate public key cryptosystem whose public key is given as $E(x_1,\dots,x_k) \in \mathbf{F}_q[x_1,\dots,x_k]^n$. We construct a new quadratic multivariate public key cryptosystem $\widetilde{\mathcal{K}}$ based on $\mathcal{K}$ as follows, through the modification of the linear PH matrix methods presented in the previous sections. Let l and h be any positive integers with $l \geq h$.

Key-Generation. In the key-generation stage, the public key and secret key of $\mathcal{K}$ are chosen first. Then, a public key $\widetilde{E}(x_1,\dots,x_k) \in \mathbf{F}_q[x_1,\dots,x_k]^l$ of $\widetilde{\mathcal{K}}$ is constructed from the original public key $E(x_1,\dots,x_k)$ of $\mathcal{K}$ as follows. In the construction, a quadratic polynomial vector $C(x_1,\dots.x_k) \in \mathbf{F}_q[x_1,\dots,x_k]^h$, an $n \times h$ matrix T, and a column vector $\boldsymbol{u} \in {\mathbf{F}_q}^n$ are randomly chosen first. Then polynomial vectors $F(x_1,\dots,x_k) \in \mathbf{F}_q[x_1,\dots,x_k]^n$ and $\overline{E}(x_1,\dots,x_k) \in \mathbf{F}_q[x_1,\dots,x_k]^l$ are calculated in sequence by the following equations:

$$
\begin{aligned}
F(x_1,\dots,x_k) &\equiv E(x_1,\dots,x_k) - TC(x_1,\dots,x_k) - \boldsymbol{u},\\
\overline{E}(x_1,\dots,x_k) &\equiv S\begin{pmatrix} 1 \\ F(x_1,\dots,x_k) \end{pmatrix} + RX[1,k].
\end{aligned}
$$

Here $X[1,k]$ is defined in the same manner as in Subsection 1.2. S is an $l \times (n+1)$ matrix whose entries are in $\mathbf{F}_q$, In order to make this PH method work properly, we assume that $l > n+1$. On the other hand, R is an $l \times t[1,k]$ matrix whose entries are in $\mathbf{F}_q$. In this notation, the $(n+1) \times l$ nonlinear PH matrix $M(x_1,\dots,x_k)$ is defined as follows:

$$
M(x_1,\dots,x_k) \equiv (TC(x_1,\dots,x_k) + \boldsymbol{u} \quad I_n)M.
$$

The S, R, and M are randomly chosen so as to satisfy the following three conditions. This choice is efficiently possible, as in the case of the linear PH matrix methods.

Condition 4. $l \geq (n+1) + \operatorname{rank} R$. □

Condition 5. *M is an $(n+1) \times l$ matrix such that $MR = 0$ and $\operatorname{rank} M = n+1$.* □

Condition 6. *$MS = I_n$, where I_{n+1} is the $(n+1) \times (n+1)$ identity matrix.* □

Finally, a public key $\widetilde{E}(x_1,\dots,x_k)$ of $\widetilde{\mathcal{K}}$ is calculated by the following equation:

$$
\widetilde{E}(x_1,\dots,x_k) \equiv B\begin{pmatrix} \overline{E}(x_1,\dots,x_k) \\ C(x_1,\dots,x_k) \end{pmatrix}, \tag{8}
$$

where B is a randomly chosen $(l+h) \times (l+h)$ invertible matrix. Thus, the order of the public key of $\widetilde{\mathcal{K}}$ is the same as the order of the public key of the original cryptosystem $\mathcal{K}$. Bob then publishes k, q, and $\widetilde{E}(x_1, \ldots, x_k)$. We here check that, by Conditions 5 and 6,

$$\begin{aligned} M(x_1, \ldots, x_k)\overline{E}(x_1, \ldots, x_k) =& (TC(x_1, \ldots, x_k) + \boldsymbol{u} \quad I_n)MS \begin{pmatrix} 1 \\ F(x_1, \ldots, x_k) \end{pmatrix} \\ &+ (TC(x_1, \ldots, x_k) + \boldsymbol{u} \quad I_n)MRX[1, k] \\ =& (TC(x_1, \ldots, x_k) + \boldsymbol{u} \quad I_n) \begin{pmatrix} 1 \\ F(x_1, \ldots, x_k) \end{pmatrix} \\ =& TC(x_1, \ldots, x_k) + \boldsymbol{u} + F(x_1, \ldots, x_k) \\ =& E(x_1, \ldots, x_k). \end{aligned}$$

Thus, $M(x_1, \ldots, x_k)$ properly works as a PH matrix although it is a polynomial matrix. Note also that the public key $\overline{E}(x_1, \ldots, x_k)$ is certainly a quadratic polynomial vector.

Encryption. A plain text of $\widetilde{\mathcal{K}}$ is represented by a vector in ${\mathbf{F}_q}^k$ in the same way as in $\mathcal{K}$. Now, assume that Alice wants to send Bob a plain text vector $\boldsymbol{p}$. The corresponding cipher text is represented by a vector $\widetilde{\boldsymbol{c}} \in {\mathbf{F}_q}^{l+h}$ in $\widetilde{\mathcal{K}}$, and is calculated through $\widetilde{\boldsymbol{c}} \equiv \widetilde{E}(\boldsymbol{p})$ by Alice.

Decryption. The decryption of $\widetilde{\mathcal{K}}$ proceeds as follows. On receiving the cipher text $\widetilde{\boldsymbol{c}}$ for the plain text $\boldsymbol{p}$, Bob can efficiently obtain the values $\overline{E}(\boldsymbol{p})$ and $C(\boldsymbol{p})$ from the multiplication of $\widetilde{\boldsymbol{c}}$ by B^{-1} using the equation (8). By $M(x_1, \ldots, x_k)\overline{E}(x_1, \ldots, x_k) = E(x_1, \ldots, x_k)$, we here see that $(TC(\boldsymbol{p}) + \boldsymbol{u} \quad I_n)M\overline{E}(\boldsymbol{p}) = E(\boldsymbol{p})$. Thus, using the values $\overline{E}(\boldsymbol{p})$ and $C(\boldsymbol{p})$, Bob can then efficiently calculate the value $E(\boldsymbol{p})$. Then, according to the decryption procedure of $\mathcal{K}$, Bob can recover the plain text $\boldsymbol{p}$ using the secret key of $\mathcal{K}$.

4 Concluding Remarks

In this paper, we have elaborated the piece in hand (PH) matrix methods in order that the security of a wide class of multivariate public key cryptosystems is likely to be enhanced by them even against the Gröbner bases attack. In the future work, we will demonstrate the enhancement of security both by the linear PH matrix method with random variables (Section 2) and by the nonlinear PH matrix method (Section 3) for all proposed multivariate public key cryptosystems in an experimental manner 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 improve the framework of the PH concept, this issue 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 $\widetilde{E}$ for a multivariate public key cryptosystem whose security is enhanced by the PH concept. We leave the consideration of the stronger security to a future study.

Acknowledgments

The authors are grateful to Mr. Gwénolé Ars for discussions and helpful comments. Especially, he pointed out that the relation (3) holds for the original linear PH matrix method proposed previously.

References

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] M. Kasahara and R. Sakai. A construction of public-key cryptosystem based on singular simultaneous equations and its variants. Technical Report of IEICE, ISEC2005-7 (2005-05), May 2005.

[7] 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.

[8] 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.

[9] 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.

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

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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/`.

[18] 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.

[19] 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.