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

Ryou Fujita† Kohtaro Tadaki‡ Shigeo Tsujii†

† 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. The piece in hand (PH) is a general scheme which is applicable to any reasonable type of multivariate public key cryptosystems for the purpose of enhancing their security. In this paper, we propose a new class PH method called NLPHPV (NonLinear Piece in Hand Perturbation Vector) method. Although our NLPHPV uses similar perturbation vectors as is used for the previously known internal perturbation method, this new method can avoid redundant repetitions in decryption process. With properly chosen parameter sizes, NLPHPV achieves an observable gain in security from the original multivariate public key cryptosystem. We demonstrate these by both theoretical analyses and computer simulations against major known attacks and provides the concrete sizes of security parameters, with which we even expect the grater security against potential quantum attacks.

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

1 Introduction

Multivariate Public Key Cryptosystems (MPKCs, for short) originally proposed in 80's as possible alternatives to the traditional, widely-used public key cryptosystems, such as RSA and ElGamal cryptosystems. One of the motivations for researching MPKC is that the public key cryptosystems based on the intractability of prime factorization or discrete logarithm problem are presently assumed to be secure, but their security will not be guaranteed in the quantum computer age. On the other hand, no quantum algorithm is known so far to be able to solve efficiently the underlying problem of MPKCs, i.e., the problem of solving a set of multivariate quadratic or higher degree polynomial equations over a finite field.

Since the original research of MPKCs was started, many new schemes have been proposed so far. At the same time, many new methods to cryptanalyze MPKCs have also been discovered. Recently, for the purpose of resisting these attacks, the research on the method for enhancing security of MPKCs is becoming one of the main themes of this area. The piece in hand (PH, for short) matrix method aims to bring the computational complexity of cryptanalysis close to exponential time by adding random polynomial terms to original MPKC. The PH methods were introduced and studied in a series of papers [27, 28, 29, 30, 31, 32, 33, 34]. Among them, there are primary two types of the PH matrix methods; the linear PH matrix methods and the nonlinear PH matrix methods. In particular, the papers [31, 32, 33, 34] proposed the linear PH matrix method

with random variables and the nonlinear PH matrix method, and showed that these PH matrix methods lead to the substantial gain in security against the Gröbner basis attack under computer experiments.

Because of the nonlinearity of the PH matrix, the nonlinear PH matrix methods are expected to enhance the security of the original MPKC more than the linear PH matrix methods in general. Thus, in the present paper, we propose a new PH method, called NonLinear Piece in Hand Perturbation Vector (NLPHPV, for short) method, which can be applied to both encryption schemes and signature schemes in general.[1] The adopted application of perturbation vector is similar to the internal perturbation method [3] and the construction of R-SE(2)PKC [13], where random transformation is mixed with the "non-singular" transformation. In particular, on the internal perturbation method, computational complexity by the Gröbner basis attack is reported in [5], the paper showed that when r is not too small (i.e., $r \gtrsim 6$), the perturbed Matsumoto-Imai cryptosystem [3] is secure against the Gröbner basis attack, where r is the perturbation dimension. Note, however, that in exchange for enhancing the security, the decryption process of the internal perturbation method becomes q^r times slower than unperturbed one, where q is the number of field elements. This fact contrasts with our NLPHPV method in a sense that it does not require repeated processes of decryption process which grows exponentially, though the cipher text size becomes slightly large. From this point of views of efficiency, NLPHPV method can be a good alternative to the internal perturbation method. We also discuss on security benefit of the NLPHPV method against major known attacks, i.e., the Gröbner basis attack, the rank attack [37], and the differential attack [9]. Based on also our security considerations, we suggest concrete parameter sizes for the NLPHPV method.

This paper is organized as follows. We begin in Section 2 with some basic notation and a brief introduction of the schemes of MPKCs in general. We introduce the NLPHPV method in Section 3. We then show, based on computer experiments, that the NLPHPV method properly provides substantial security against the Gröbner basis attack in Section 4. We discuss the immunity of the NLPHPV method against known attacks in Section 5. Based on the discussion, we suggest parameters for the NLPHPV method 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 MPKCs in general after introducing some notations about fields, polynomials, and matrices.

2.1 Notations

We represent a column vector in general by bold face symbols such as $\boldsymbol{p}$, $\boldsymbol{E}$, and $\boldsymbol{X}$.

- $\mathbf{F}_q$: finite field which has q elements with $q \geq 2$.
- $\mathbf{F}_q[x_1, \ldots, x_k]$: set of all polynomials in variables $x_1, x_2, \ldots, x_k$ with coefficients in $\mathbf{F}_q$.
- $S^{n \times l}$: set of all $n \times l$ matrices whose entries are in a nonempty set S with positive integers n and l. Let $S^{n \times 1} = S^n$.

[1] In signature scheme, the parameters of the NLPHPV method are restricted to some region. We will deal with the issue in Section 3 and Subsection 5.2.

- S^n: set of all column vectors consisting n entries in S.
- $A^T \in S^{l\times n}$: transpose of A for matrix $A \in S^{n\times l}$.
- $\boldsymbol{f}(\boldsymbol{g}) = (h_1, \ldots, h_n)^T \in \mathbf{F}_q[x_1, \ldots, x_m]^n$: *substitution* of $\boldsymbol{g}$ for the variables in $\boldsymbol{f}$, where $\boldsymbol{f} = (f_1, \ldots, f_n)^T \in \mathbf{F}_q[x_1, \ldots, x_k]^n$, $\boldsymbol{g} = (g_1, \ldots, g_k)^T \in \mathbf{F}_q[x_1, \ldots, x_m]^k$ are polynomial column vectors. Each h_i is the polynomial in $\mathbf{F}_q[x_1, \ldots, x_m]$ obtained by substituting $g_1, \ldots, g_k$ for the variables $x_1, \ldots, x_k$ in f_i, respectively.
- $\boldsymbol{f}(\boldsymbol{p}) \in {\mathbf{F}_q}^n$: vector obtained by substituting $p_1, \ldots, p_k$ for the variables $x_1, \ldots, x_k$ in $\boldsymbol{f}$, respectively, for $\boldsymbol{f} \in \mathbf{F}_q[x_1, \ldots, x_k]^n$ and $\boldsymbol{p} \in {\mathbf{F}_q}^k$, where $\boldsymbol{p} = (p_1, \ldots, p_k)^T$ with $p_1, \ldots, p_k \in \mathbf{F}_q$.

2.2 MPKCs in General

A MPKC as in [17, 25, 18, 26, 21, 19, 12, 13, 3, 14, 38, 36] are often made by the following building blocks:

Secret key: The secret key includes the following:

- the two invertible matrices $A_0 \in {\mathbf{F}_q}^{k\times k}$, $B_0 \in {\mathbf{F}_q}^{n\times n}$;
- the polynomial transformation $\boldsymbol{G} \in \mathbf{F}_q[x_1, \ldots, x_k]^n$ whose inverse is efficiently computable.

Public key: The public key includes the following:

- the finite field $\mathbf{F}_q$ including its additive and multiplicative structure;
- the polynomial vector $\boldsymbol{E} = B_0\,\boldsymbol{G}(A_0\boldsymbol{x}) \in \mathbf{F}_q[x_1, \ldots, x_k]^n$, where $\boldsymbol{x} = (x_1, \ldots, x_k)^T \in \mathbf{F}_q[x_1, \ldots, x_k]^k$.

Encryption: Given a plain text vector $\boldsymbol{p} = (p_1, \ldots, p_k)^T \in {\mathbf{F}_q}^k$, the corresponding cipher text is the vector $\boldsymbol{c} = \boldsymbol{E}(\boldsymbol{p})$.

Decryption: Given the cipher text vector $\boldsymbol{c} = (c_1, \ldots, c_n)^T \in {\mathbf{F}_q}^n$, decryption includes the following steps:

(i) Compute $\boldsymbol{w} = B_0^{-1}\boldsymbol{c} \in {\mathbf{F}_q}^n$,
(ii) Compute $\boldsymbol{v} \in {\mathbf{F}_q}^k$ from $\boldsymbol{w}$ by using the inverse transformation of $\boldsymbol{G}$,
(iii) Compute $\boldsymbol{p} = A_0^{-1}\boldsymbol{v} \in {\mathbf{F}_q}^k$.

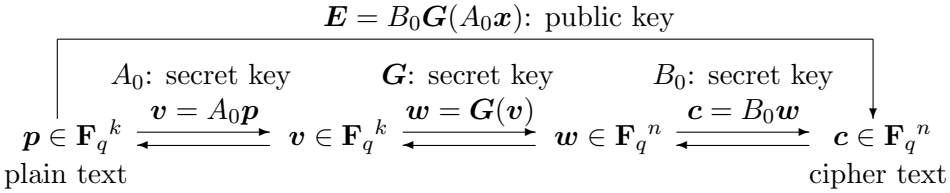

Figure 1: Scheme of Multivariate Public Key Cryptosystem

3 Nonlinear Piece In Hand Perturbation Vector (NLPHPV) Method

Let $\mathcal{K}$ be an arbitrary MPKC whose public key polynomial vector is given by $\boldsymbol{E} \in \mathbf{F}_q[x_1, \ldots, x_k]^n$, as described in Subsection 2.2. Let f, l and h be any positive integers. We set $g \underset{\text{def}}{=} n + l + h$. Let p and z be any positive integers with $p \leq k \leq z$, and let t be any nonnegative integer with $t \leq z - p$. The relation between these parameters and correspondence to plain text and random number is given in Figure 2.

Let $A \in {\mathbf{F}_q}^{(k-p)\times t}$ and $C \in {\mathbf{F}_q}^{f\times z}$ be randomly chosen matrices. Let $\boldsymbol{r} \in \mathbf{F}_q[x_1, \ldots, x_z]^h$ be a randomly chosen polynomial vector. In the NLPHPV method, a new MPKC $\widetilde{\mathcal{K}}$ is constructed from the given MPKC $\mathcal{K}$ for the purpose of enhancing the security. A public key $\widetilde{\boldsymbol{E}} \in \mathbf{F}_q[x_1, \ldots, x_z]^g$ of $\widetilde{\mathcal{K}}$ is constructed from the original public key $\boldsymbol{E}$ of $\mathcal{K}$.

Secret key: The secret key includes the following:

- secret key of $\mathcal{K}$;
- randomly chosen invertible matrix $B \in {\mathbf{F}_q}^{g\times g}$;
- polynomial transformation $\boldsymbol{H} \in \mathbf{F}_q[x_1, \ldots, x_f]^l$ whose inverse is efficiently computable;
- the *nonlinear piece in hand perturbation vector* $\boldsymbol{Q} \in \mathbf{F}_q[x_1, \ldots, x_f]^n$, which is randomly chosen.

Public key: The public key includes the following:

- the finite field $\mathbf{F}_q$ including its additive and multiplicative structure;
- the number of plain text variables in the NLPHPV method p;
- the polynomial vector $\widetilde{\boldsymbol{E}} \in \mathbf{F}_q[x_1, \ldots, x_z]^g$. $\widetilde{\boldsymbol{E}}$ is constructed as the following equation:

$$\widetilde{\boldsymbol{E}} \underset{\text{def}}{=} B \begin{pmatrix} \boldsymbol{E}\begin{pmatrix} \boldsymbol{x} \\ A\boldsymbol{\mu} \end{pmatrix} + \boldsymbol{Q}(\boldsymbol{f}) \\ \boldsymbol{H}(\boldsymbol{f}) \\ \boldsymbol{r} \end{pmatrix}. \tag{1}$$

Here $\boldsymbol{x} = (x_1, \ldots, x_p)^T \in \mathbf{F}_q[x_1, \ldots, x_p]^p$, $\boldsymbol{\mu} = (x_{p+1}, \ldots, x_{p+t})^T \in \mathbf{F}_q[x_{p+1}, \ldots, x_{p+t}]^t$, $\boldsymbol{\lambda} = (x_{p+1}, \ldots, x_z)^T \in \mathbf{F}_q[x_{p+1}, \ldots, x_z]^{z-p}$, $\boldsymbol{f} = (f_1, \ldots, f_f)^T = C\begin{pmatrix} \boldsymbol{x} \\ \boldsymbol{\lambda} \end{pmatrix} \in \mathbf{F}_q[x_1, \ldots, x_z]^f$. Note that, in the right-hand side of (1), the vector $A\boldsymbol{\mu} \in \mathbf{F}_q[x_{p+1}, \ldots, x_{p+t}]^{k-p}$ is substituted for the variables $x_{p+1}, \ldots, x_k$ in the original public key $\boldsymbol{E}$ while keeping the variables $x_1, \ldots, x_p$ in $\boldsymbol{E}$ unchanged. $\boldsymbol{Q}(\boldsymbol{f})$ plays a role in masking the original public key $\boldsymbol{E}$ and randomizing it. $\boldsymbol{r}$ is appended to the polynomial sets in order to cope with the differential attack [9, 6].

Note that t random variables $x_{p+1}, \ldots, x_{p+t}$ in $\boldsymbol{\mu}$ are included in $\boldsymbol{E}$ from $z - p$ random variables $x_{p+1}, \ldots, x_z$ in $\boldsymbol{\lambda}$. Then, increasing the value $\binom{z-p}{t}$ makes these random variables indistinguishable.

Remark 3.1. We may replace $\boldsymbol{E}\begin{pmatrix} \boldsymbol{x} \\ A\boldsymbol{\mu} \end{pmatrix}$ in (1) with $\boldsymbol{E}\left(D\begin{pmatrix} \boldsymbol{x} \\ \boldsymbol{\mu} \end{pmatrix}\right)$ in a more general form. Here $D \in {\mathbf{F}_q}^{k\times(p+t)}$ is a randomly chosen matrix such that, for any $\boldsymbol{p}, \boldsymbol{p}' \in {\mathbf{F}_q}^p$ and any

$\boldsymbol{u}_1, \boldsymbol{u}_1' \in {\mathbf{F}_q}^t$, if $D\begin{pmatrix} \boldsymbol{p} \\ \boldsymbol{u}_1 \end{pmatrix} = D\begin{pmatrix} \boldsymbol{p}' \\ \boldsymbol{u}_1' \end{pmatrix}$, then $\boldsymbol{p} = \boldsymbol{p}'$. This condition on D is needed to recover the plain text uniquely. However, D can be rewritten as $D = U\begin{pmatrix} I_p & 0 \\ 0 & A \end{pmatrix}$ for some invertible matrix $U \in {\mathbf{F}_q}^{k\times k}$. Thus, the transformation $\boldsymbol{E}\begin{pmatrix} \boldsymbol{x} \\ A\boldsymbol{\mu} \end{pmatrix}$ is equivalent to $\boldsymbol{E}\left(D\begin{pmatrix} \boldsymbol{x} \\ \boldsymbol{\mu} \end{pmatrix}\right)$ since A_0 is randomly chosen in original MPKC $\mathcal{K}$.

In signature scheme, the requirement of the uniqueness in decryption is removed. Thus, the matrix D can be randomly chosen and the distinction between plain text and random variables is also removed.

Encryption: Given a plain text vector $\boldsymbol{p} = (p_1, \ldots, p_p)^T \in {\mathbf{F}_q}^p$ and a random number $\boldsymbol{u} = (u_1, \ldots, u_{z-p})^T \in {\mathbf{F}_q}^{z-p}$, the corresponding cipher text is the vector $\widetilde{\boldsymbol{c}} = \widetilde{\boldsymbol{E}}\begin{pmatrix} \boldsymbol{p} \\ \boldsymbol{u} \end{pmatrix}$.

Decryption: Given the cipher text vector $\widetilde{\boldsymbol{c}} = (\widetilde{c}_1, \ldots, \widetilde{c}_g)^T \in {\mathbf{F}_q}^g$, decryption includes the following steps:

(i) Compute $B^{-1}\widetilde{\boldsymbol{c}}$. By (1), we see that

$$B^{-1}\widetilde{\boldsymbol{c}} = \begin{pmatrix} \boldsymbol{E}\begin{pmatrix} \boldsymbol{p} \\ \boldsymbol{y} \end{pmatrix} + \boldsymbol{Q}(\boldsymbol{f}(\boldsymbol{z})) \\ \boldsymbol{H}(\boldsymbol{f}(\boldsymbol{z})) \\ \boldsymbol{r}(\boldsymbol{z}) \end{pmatrix},$$

where $\boldsymbol{z} \underset{\text{def}}{=} \begin{pmatrix} \boldsymbol{p} \\ \boldsymbol{u} \end{pmatrix} \in {\mathbf{F}_q}^z$, $\boldsymbol{u} = \begin{pmatrix} \boldsymbol{u}_1 \\ \boldsymbol{u}_2 \end{pmatrix} \in {\mathbf{F}_q}^{z-p}$, $\boldsymbol{u}_1 \in {\mathbf{F}_q}^t$, $\boldsymbol{u}_2 \in {\mathbf{F}_q}^{z-p-t}$, $\boldsymbol{y} \underset{\text{def}}{=} A\boldsymbol{u}_1 \in {\mathbf{F}_q}^{k-p}$.

(ii) Compute $\boldsymbol{f}(\boldsymbol{z})$ from the value $\boldsymbol{H}(\boldsymbol{f}(\boldsymbol{z}))$ by using the inverse transformation of $\boldsymbol{H}$.

(iii) Compute $\boldsymbol{Q}(\boldsymbol{f}(\boldsymbol{z}))$ by substitution of $\boldsymbol{f}(\boldsymbol{z})$ for $\boldsymbol{Q}$.

(iv) Compute $\boldsymbol{E}\begin{pmatrix} \boldsymbol{p} \\ \boldsymbol{y} \end{pmatrix}$ from the value $\boldsymbol{E}\begin{pmatrix} \boldsymbol{p} \\ \boldsymbol{y} \end{pmatrix} + \boldsymbol{Q}(\boldsymbol{f}(\boldsymbol{z}))$.

(v) Compute $\begin{pmatrix} \boldsymbol{p} \\ \boldsymbol{y} \end{pmatrix}$ by using the secret key of $\mathcal{K}$. Note that $\boldsymbol{y}$ is discarded after the decryption.

In signature scheme, it is needed to compute $\boldsymbol{u}$ by solving linear equation $\begin{pmatrix} 0 & A & 0 \\ & C & \end{pmatrix}\begin{pmatrix} \boldsymbol{p} \\ \boldsymbol{\lambda} \end{pmatrix} = \begin{pmatrix} \boldsymbol{y} \\ \boldsymbol{f}(\boldsymbol{z}) \end{pmatrix}$ for unknown $\boldsymbol{\lambda}$, and to check if $\boldsymbol{r}\begin{pmatrix} \boldsymbol{p} \\ \boldsymbol{u} \end{pmatrix} = \boldsymbol{r}(\boldsymbol{z})$ for the solution $\boldsymbol{u}$, where $\boldsymbol{r}(\boldsymbol{z})$ is the value given above.[2] Since the probability that $\begin{pmatrix} \boldsymbol{p} \\ \boldsymbol{u} \end{pmatrix}$ satisfies this criteria is $1/q^h$ on average, h must be small as possible in signature scheme.

[2]The equation is replaced with $\begin{pmatrix} D & 0 \\ C & \end{pmatrix}\begin{pmatrix} \boldsymbol{x} \\ \boldsymbol{\lambda} \end{pmatrix} = \begin{pmatrix} D\begin{pmatrix} \boldsymbol{p} \\ \boldsymbol{u}_1 \end{pmatrix} \\ \boldsymbol{f}(\boldsymbol{z}) \end{pmatrix}$ for unknown $\boldsymbol{x}$ and $\boldsymbol{\lambda}$ when the matrix D above is randomly chosen.

The encryption and decryption processes in the NLPHPV method are schematically represented in Figure 3.

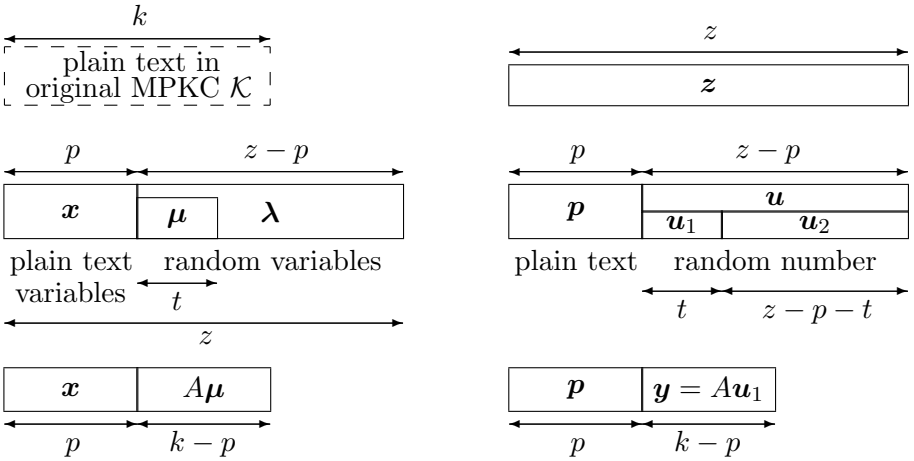

Figure 2: Plain text and random number

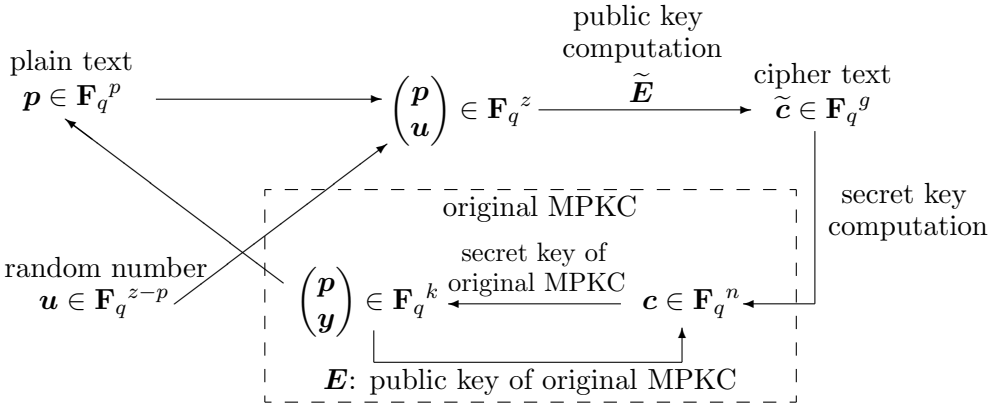

Figure 3: NonLinear Piece in Hand Perturbation Vector method

4 Experimental Results

In this section, based on computer experiments, we clarify the enhancement of the security by the NLPHPV method proposed in the previous section.

Recently, Faugère and Joux [8] showed in an experimental manner that computing a Gröbner basis (GB, for short) of the public key is likely to be an efficient attack to HFE [21], which is one of major MPKCs. In fact, they broke the first HFE challenge (80bits) proposed by Patarin. The attack used by them is 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.

We report in Table 1 and Table 2 the time required for the GB attack against the perturbed Matsumoto-Imai-Plus cryptosystem (PMI+, for short) [6] and the Matsumoto-Imai cryptosystem (MI, for short) [18] enhanced by the NLPHPV method. Note that $n = k$ and $q = 2$ for the public keys $\boldsymbol{E} \in \mathbf{F}_q[x_1, \ldots, x_k]^n$ of MI by its specification. We deal with the case of $p = z = k$, $f = l$

Table 1: Computational times of the GB attack for PMI+

Parameters			Computational times
k	r	a	in second
28	6	0	845
28	6	5	733
28	6	10	563
28	6	15	436
29	6	15	747
30	6	15	1305

k: number of plain text variables
r: perturbation dimension
a: number of Plus polynomials

Table 2: Computational times of the GB attack for the enhanced MI by the NLPHPV method

Parameters			Computational times
k	l	h	in second
28	17	3	290
28	17	4	289
28	17	5	263
29	17	3	537
29	17	8	402
29	17	10	349
30	17	3	936
30	17	8	701
30	17	13	513

in the NLPHPV method. As an practical example of the polynomial transformation $\boldsymbol{H}$ in the NLPHPV method, we use the public key polynomials of the HFE,[3] though we can choose any $\boldsymbol{H}$. The computation times are evaluated on 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 1 and Table 2, due to the constraint of computing ability, only the cases of $k = 28, 29, 30$ are computed. Since MI may have polynomial time complexity about $O(k^7)$ of cryptanalysis, as shown in [5] and our preliminary experimental results, it is quite difficult at present to compare MI with the enhanced MI in a practical length of a plain text such as 200bits. If we can experimentally cryptanalyze the MI enhanced by the NLPHPV method in the practical length of a plain text in order to compare it with the original MI, then this implies that the cryptosystem enhanced by NLPHPV method is useless in itself. This is a limitation and dilemma of the security evaluation by computer experiments. On the other hand, our another computer experiments with the same facilities show that it takes about 0.07 seconds to cryptanalyze the plain MI with $k = 30$ by the GB attack. Since plain MI with $k = 30$ was cryptanalyzed within about 0.07 seconds under our environment, it would be estimated that the perturbation by internal or NLPHPV enhances the F_4 time complexity by about 10^4 times. This fact shows that the internal perturbation method and the NLPHPV method enhance the security of MI against the GB attack.

We now consider the applicability of the internal perturbation method and the NLPHPV method. The internal perturbation method requires q^r times decryption complexity of the original MPKC. On the other hand, the NLPHPV method requires at most a few times decryption complexity of the original MPKC regardless of the value of q. Though the application of the NLPHPV method requires the increase of cipher text size, in terms of the decryption time, the NLPHPV method seems to be a possible alternative to the internal perturbation method in the enhancement of the security against the GB attack.

Remark 4.1. In the above, we only dealt with the case that no random variable was introduced. For the purpose of enhancing the security further, it is possible to introduce random variables.

[3]The optimal choice of $\boldsymbol{H}$ is still open. We will clarify this point in the future work.

Table 3: Comparison between computational times of the GB attack for MI and the enhanced MI by the NLPHPV method

Cryptosystems	Parameters								Computational times in second
	p	k	z	g	f	l	h	t	
MI		15							$< 10^{-2}$
		20							0.01
		25							0.03
		30							0.07
		35							0.2
		40							0.4
		45							0.7
		50							1
		55							2
		60							4
The enhanced MI by the NLPHPV method	15	20	40	35	10	10	5	10	75
	15	20	43	35	10	10	5	10	129
	15	20	45	35	10	10	5	10	260
	15	20	46	35	10	10	5	10	320
	15	20	47	35	10	10	5	10	1029
	15	20	40	40	10	10	10	10	97
	15	20	43	40	10	10	10	10	161
	15	20	47	40	10	10	10	10	284
	15	20	48	40	10	10	10	10	495
	15	20	49	40	10	10	10	10	1077

We report in Table 3 and Table 4 the time required for the GB attack against MPKC (MI or R-SE(2)PKC (RSE, for short)) and the MPKC enhanced by the NLPHPV method. Note that $n = k$ and $q = 2$ for the public keys $\boldsymbol{E} \in \mathbf{F}_q[x_1, \ldots, x_k]^n$ of MI and RSE by their specifications. Table 3 and Table 4 give the comparison of the particular case with a plain text of 15 bits (MI with $k = 15$ and the enhanced MI with $z = 47$, $g = 35$, or RSE with $k = 15$ and the enhanced RSE with $z = 44$, $g = 35$). This shows that the time required for cryptanalysis is increased by more than 10^5 times by the application of the NLPHPV method. This fact shows that the NLPHPV method enhances the security of MI and RSE against the GB attack. Table 3 and Table 4 show that the increase of the number $z - p$ of random variables $x_{p+1}, \ldots, x_z$ increases the time required for the GB attack against the enhanced cryptosystem $\widetilde{\mathcal{K}}$ and provides substantial security against the GB attack.

5 Discussion on Security

In this section, we discuss the security of the NLPHPV method against major known attacks. The main purpose of this section is to enclose the secure parameter region of the NLPHPV method by both theoretical and experimental observations.

Table 4: Comparison between computational times of the GB attack for RSE and the enhanced RSE by the NLPHPV method

Cryptosystems	Parameters								Computational times in second
	p	k	z	g	f	l	h	t	
RSE		15							0.01
		20							0.03
		25							0.1
		30							0.2
		35							0.5
		40							1
		45							2
		50							5
		55							9
		60							16
The enhanced RSE by the NLPHPV method	15	20	40	35	10	10	5	10	40
	15	20	41	35	10	10	5	10	71
	15	20	42	35	10	10	5	10	179
	15	20	43	35	10	10	5	10	713
	15	20	44	35	10	10	5	10	2791
	15	20	40	40	10	10	10	10	51
	15	20	42	40	10	10	10	10	82
	15	20	44	40	10	10	10	10	231
	15	20	45	40	10	10	10	10	877
	15	20	46	40	10	10	10	10	2327

5.1 GB Attack

As stated in the previous section, based on computer experiments, the NLPHPV method properly provides substantial security, and enhances the security of the Matsumoto-Imai cryptosystem against the GB attack. In the case where the original MPKC is other than Matsumoto-Imai cryptosystem, or in the case where signature scheme is considered, we will clarify their security against the GB attack in the full version of this paper. A purely theoretical treatment of their security is also an issue in the future.

5.2 Rank Attack

In 2004 Wolf, Braeken, and Preneel [37] introduced an attack against a class of MPKCs, called *step-wise triangular schemes* (STS, for short), based on the rank calculation of the public key (see also [23, 1, 10]). On the other hand, recently, Ito, Fukushima, and Kaneko [11] proposed an attack against the MPKC which is obtained by applying the linear PH matrix method to the sequential solution method as an original MPKC. Their attack makes use of an STS-like structure of the MPKC.

In fact, the structure of the public key of the NLPHPV method can be seen as a gSTS (general step-wise triangular structure) [37]. The detailed description is given below. Let $A' =$

$\begin{pmatrix} & C & \\ I_p & & 0 \\ 0 & A & 0 \\ & R & \end{pmatrix} \in {\mathbf{F}_q}^{z\times z}$ be an invertible matrix, where A, C are as in Section 3, I_p is the identity matrix in ${\mathbf{F}_q}^{p\times p}$, and R is a specific matrix in ${\mathbf{F}_q}^{(z-k-f)\times z}$. For A', we define $\boldsymbol{x}' = (x'_1, \ldots, x'_f, \ldots, x'_{f+k}, \ldots, x'_z)^T \underset{\text{def}}{=} A' \begin{pmatrix} \boldsymbol{x} \\ \boldsymbol{\lambda} \end{pmatrix}$, where $\boldsymbol{x}$, $\boldsymbol{\lambda}$ are as in Section 3. Let $\boldsymbol{x}'_1 = (x'_1, \ldots, x'_f)^T$, $\boldsymbol{x}'_2 = (x'_{f+1}, \ldots, x'_{f+k})^T$, and $\boldsymbol{x}'_3 = (x'_{f+k+1}, \ldots, x'_z)^T$ be parts of $\boldsymbol{x}'$. Then, $\boldsymbol{x}'_1 = C \begin{pmatrix} \boldsymbol{x} \\ \boldsymbol{\lambda} \end{pmatrix}$, $\boldsymbol{x}'_2 = \begin{pmatrix} \boldsymbol{x} \\ A\boldsymbol{\mu} \end{pmatrix}$, where $\boldsymbol{\mu}$ is as in Section 3. We denote $\boldsymbol{H} = (h_1, \ldots, h_l)^T \in \mathbf{F}_q[x_1, \ldots, x_f]^l$, $\boldsymbol{Q} = (q_1, \ldots, q_n)^T \in \mathbf{F}_q[x_1, \ldots, x_f]^n$, $\boldsymbol{E} = (e_1, \ldots, e_n)^T \in \mathbf{F}_q[x_1, \ldots, x_k]^n$, where $\boldsymbol{H}$, $\boldsymbol{Q}$, and $\boldsymbol{E}$ are as in Section 3. By substitution of $\boldsymbol{x}'_1$ for the variables in $\boldsymbol{H}$, we obtain $\boldsymbol{H}(\boldsymbol{x}'_1)$, which is equal to $\boldsymbol{H}(\boldsymbol{f})$ in (1). Similarly, $\boldsymbol{Q}(\boldsymbol{x}'_1)$ and $\boldsymbol{E}(\boldsymbol{x}'_2)$ are equal to $\boldsymbol{Q}(\boldsymbol{f})$ and $\boldsymbol{E}\begin{pmatrix} \boldsymbol{x} \\ A\boldsymbol{\mu} \end{pmatrix}$ in (1), respectively. We define $\boldsymbol{r}' = (r'_1, \ldots, r'_h)^T \underset{\text{def}}{=} \boldsymbol{r}\left((A')^{-1}\boldsymbol{X}\right) \in \mathbf{F}_q[x_1, \ldots, x_z]^h$, where $\boldsymbol{X} = (x_1, \ldots, x_z)^T \in \mathbf{F}_q[x_1, \ldots, x_z]^z$ and $\boldsymbol{r}$ is as in Section 3. Then, $\boldsymbol{r}'(\boldsymbol{x}') = \boldsymbol{r}\left((A')^{-1}A'\begin{pmatrix} \boldsymbol{x} \\ \boldsymbol{\lambda} \end{pmatrix}\right) = \boldsymbol{r}\begin{pmatrix} \boldsymbol{x} \\ \boldsymbol{\lambda} \end{pmatrix} = \boldsymbol{r}$.

Using $\boldsymbol{H}(\boldsymbol{x}'_1)$, $\boldsymbol{Q}(\boldsymbol{x}'_1)$, $\boldsymbol{E}(\boldsymbol{x}'_2)$, and $\boldsymbol{r}'(\boldsymbol{x}')$ above, we construct the gSTS corresponding to (1) as follows:

$$\begin{array}{ll} \text{Step 1} & \left\{ \begin{array}{rcl} y'_1 & = & h_1(x'_1, \ldots, x'_f), \\ & \vdots & \\ y'_l & = & h_l(x'_1, \ldots, x'_f), \end{array} \right. \\ \text{Step 2} & \left\{ \begin{array}{rcl} y'_{l+1} & = & q_1(x'_1, \ldots, x'_f) + e_1(x'_{f+1}, \ldots, x'_{f+k}), \\ & \vdots & \\ y'_{l+n} & = & q_n(x'_1, \ldots, x'_f) + e_n(x'_{f+1}, \ldots, x'_{f+k}), \end{array} \right. \\ \text{Step 3} & \left\{ \begin{array}{rcl} y'_{l+n+1} & = & r'_1(x'_1, \ldots, x'_f, \ldots, x'_{f+k}, \ldots, x'_z), \\ & \vdots & \\ y'_g & = & r'_h(x'_1, \ldots, x'_f, \ldots, x'_{f+k}, \ldots, x'_z). \end{array} \right. \end{array} \tag{2}$$

We denote $\boldsymbol{y}' = (y'_1, \ldots, y'_g)^T$. Then, $\widetilde{\boldsymbol{E}} = B\boldsymbol{y}'$, where $\widetilde{\boldsymbol{E}}$, B are as in Section 3.

In this gSTS, the number of layers is 3, the numbers of new variables (step-width) are f, k, $z-k-f$, and the numbers of equations (step-height) are l, n, h, respectively. This structure may bring down undesirable vulnerability against the rank attack. In the following, we discuss the security of the NLPHPV method against two rank attacks; high rank attack and low rank attack.

5.2.1 High Rank Attack

In the high rank attack against the gSTS, to separate the part of Step 3 in (2) from the public key, the attacker searches vectors $\boldsymbol{v} = (v_1, \ldots, v_g)^T \in {\mathbf{F}_q}^g$. The vectors form together an invertible matrix whose row is a row of the secret key B^{-1} or its linear equivalent copy, since multiplying B^{-1} to the public key $\widetilde{\boldsymbol{E}}$ separates their layers. The attacker can find each of the vectors $\boldsymbol{v}$ with a

probability $1/q^h$ by checking whether

$$\text{rank}\left(\sum_{i=1}^{g} v_i P_i\right) \leq f + k,$$

for randomly chosen $v_1, \ldots v_g \in \mathbf{F}_q$, where P_i are matrices, in a quadratic form, of the public key polynomial vector $\widetilde{\boldsymbol{E}} = (\widetilde{e}_1, \ldots, \widetilde{e}_g)^T = (\boldsymbol{X}^T P_1 \boldsymbol{X}, \ldots, \boldsymbol{X}^T P_g \boldsymbol{X})^T$, with $\boldsymbol{X} = (x_1, \ldots, x_z)^T \in \mathbf{F}_q[x_1, \ldots, x_z]^z$.

One of the simple countermeasures is to make the step-height of Step 3 thick, i.e., to make the number h of polynomials in the randomly chosen polynomial vector $\boldsymbol{r}$ in the NLPHPV method large. If q^h is large enough, the probability $1/q^h$ becomes negligible. However, larger h loses efficiency of cryptosystem in signature scheme as mentioned in Section 3.

In the case that h is not too large, one of the countermeasures against the weakness is to combine Step 2 with Step 3, i.e., to set $f + k = z$. Then, both on Step 2 and on Step 3 in (2), the rank is $z = f + k$, and the difference of the rank between these steps disappears. Also, the combination of Step 2 and Step 3 replaces the probability $1/q^h$ by $1/q^{n+h}$. In the case where n is large enough, this probability becomes negligible, and therefore the high rank attack could be intractable.

5.2.2 Low Rank Attack

In the low rank attack against the gSTS, the attacker can find $\boldsymbol{w} = (w_1, \ldots, w_g)^T \in {\mathbf{F}_q}^z$ with a probability $1/q^f$ by checking whether the unknown $\boldsymbol{v} = (v_1, \ldots, v_g)$ has f solutions in equation

$$\left(\sum_{i=1}^{g} v_i P_i\right) \boldsymbol{w} = \boldsymbol{0},$$

for randomly chosen $w_1, \ldots w_g \in \mathbf{F}_q$.

One of the countermeasures against the weakness is to widen the step-width of Step 1, i.e., to choose f to be large enough. Then, the probability $1/q^f$ becomes small, and therefore the low rank attack could be intractable.

5.3 Differential Attack

In 2005 Fouque, Granboulan, and Stern [9] adapted the differential cryptanalysis to MPKCs in order to break MI and its variant, called PMI [3]. In the differential attack, the attacker tries to find $\boldsymbol{v} = (v_1, \ldots, v_z)^T \in {\mathbf{F}_q}^z$ such that dim $(\ker\ (L_{\boldsymbol{v}})) = \delta$, where $L_{\boldsymbol{v}} \in {\mathbf{F}_q}^{z \times z}$, $L_{\boldsymbol{v}}\boldsymbol{X} = \widetilde{\boldsymbol{E}}(\boldsymbol{X} + \boldsymbol{v}) - \widetilde{\boldsymbol{E}}(\boldsymbol{X}) - \widetilde{\boldsymbol{E}}(\boldsymbol{v}) + \widetilde{\boldsymbol{E}}(\boldsymbol{0})$, $\boldsymbol{X} = (x_1, \ldots, x_z)^T \in \mathbf{F}_q[x_1, \ldots, x_z]^z$, and δ is a specific value.

We confirmed, by computer experiments, that the dimensions of the kernel in the NLPHPV method are the same in almost all cases. Moreover, note that the differential cryptanalysis might be applied only to Matsumoto-Imai type cryptosystems and the application of Plus method might recover their security against the cryptanalysis [6]. In the NLPHPV method 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 NLPHPV method has a structure like Plus method. Thus, the NLPHPV method might be immune against the differential cryptanalysis. We will clarify this point in the future work.

6 Consideration on Secure Parameter Setting

Based on the discussion on the security in the previous section, we suggest a secure parameter setting of the NLPHPV method in Table 5.

In recently proposed major MPKCs, public key sizes for encryption schemes are 175 KB in PMI+ [6] and 160.2 KB in ℓIC i+ [7], and for signature schemes 15 KB in Rainbow [4] and 9.92 KB in ℓIC- [7]. The main purpose of these schemes is to implement them on small devices with limited computing resources. On the other hand, we assume the situation in the future when quantum computers appear, and place much more value on the security than the efficiency, such as the reduction of key size. Let us consider the security level of the quantum computer age where quantum computers are available. Then, the simple application of the Grover's algorithm to exhaustive search of 2^N candidates reduces the time complexity $O(2^N)$ to $O(\sqrt{2^N})$. On the other hand, nowadays, the exhaustive search of 2^{80} candidates is thought to be impossible and the complexity 2^{80} is selected as the standard security level in present cryptographic community. Therefore, we assume that the security level of the quantum computer age is greater than the complexity 2^{160}. Note that we omit the evaluation of the size of secret key below. This is because the size of secret key of a MPKC is much smaller than that of public key and different in various MPKCs.

Table 5: Parameter Setting

	Parameters										Public Key Size
	q	p	k	n	z	g	f	l	h	t	
Encryption scheme	256		260	260							8.89 MB
The enhanced encryption scheme by the NLPHPV method	256	256	260	260	420	300	20	20	20	82	26.65 MB
Signature scheme	256		30	20							9.92 KB
The enhanced signature scheme by the NLPHPV method	256		30	20	50	30	20				39.78 KB

6.1 Encryption Scheme

The plain text size is 2048 bits. Information transmission rate (i.e., the size of plain text divided by the size of cipher text) is $256/300 \approx 0.853$. The public key size increases about 3 times from the original encryption scheme. In the original encryption scheme, the numbers of plain text and cipher text variables are 260.

In the high rank attack against this scheme, the probability with which the attacker find each of the vectors $\boldsymbol{v}$ is $1/q^h$. Therefore, the attack complexity of the high attack is $q^h = 2^{160}$ on average. On the other hand, in the low rank attack, the probability with which the attacker find $\boldsymbol{w}$ is $1/q^f$. Therefore, the attack complexity of the low rank attack is $q^f = 2^{160}$ on average. For these reasons, these rank attacks are intractable. Also, since $\binom{z-p}{t} = \binom{164}{82} \approx 2^{160}$, it is also intractable to distinguish random variables.

6.2 Signature Scheme

The signature size is 400 bits. In the original signature scheme, the number of input variables is 20, and 30 output variables. The public key size increases about 4 times from the original signature scheme.

In the high rank attack against this scheme, the probability with which the attacker find each of the vectors $\boldsymbol{v}$ is $1/q^{n+h}$ not $1/q^h$, since $z = f + k$ as noted in Subsection 5.2. Therefore, the attack complexity of the high rank attack is $q^{n+h} > q^n = 2^{720}$. On the other hand, in the low rank attack, the probability with which the attacker find $\boldsymbol{w}$ is $1/q^f$. Therefore, the attack complexity of the low rank attack is $q^f = 2^{160}$ on average. For these reasons, these rank attacks are intractable.

7 Concluding Remarks

In this paper, we proposed a new class of PH methods called NonLinear Piece in Hand Perturbation Vector (NLPHPV) method. NLPHPV is more efficient than previously known internal perturbation methods in terms of the decryption process avoiding redundant repetitive steps. Based on computer experiments, we have shown the enhancement of the security of the Matsumoto-Imai cryptosystem by the method against the Gröbner basis attack. Then, by considering the security against known other attacks, we have suggested a secure parameter setting of the NLPHPV method for the quantum computer age. From the practical view point of current interest, it is also important to evaluate the efficiency of both encryption and decryption in the cryptosystem enhanced by the method. However, since the aim of the present paper is mainly to develop the framework of nonlinear PH matrix methods as a potential countermeasure against the advent of quantum computers in the future, this practical issue is not considered in this paper but discussed in another paper. Because of the same reason, we have not considered some provable security, for example IND-CCA of the class of PH methods for encryption but considered just the encryption primitive $\widetilde{\boldsymbol{E}}$ for an MPKC which is obtained by applying the NLPHPV method. We leave the consideration of the stronger security to a future study.

Acknowledgments

The authors are grateful to Dr. Tomohiro Harayama and Mr. Masahito Gotaishi for helpful discussions and comments.

This work is supported by the "Strategic information and COmmunications R&D Promotion programmE" (SCOPE) from the Ministry of Internal Affairs and Communications of Japan.

References

[1] 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.

[2] 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.

[3] 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.

[4] J. Ding and D. Schmidt. Rainbow, a new multivariable polynomial signature scheme. *Proc. ACNS 2005*, Lecture Notes in Computer Science, Vol.3531, pp.164–175, Springer, 2005.

[5] 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.

[6] 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.

[7] J. Ding, C. Wolf, and B. Y. Yang. ℓ-Invertible Cycles for $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic ($\mathcal{MQ}$) public key cryptography. *Proc. PKC 2007*, Lecture Notes in Computer Science, Vol.4450, pp.266–281, Springer, 2007.

[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] L. Goubin and N. Courtois. Cryptanalysis of the TTM cryptosystem. *Proc. ASIACRYPT 2000*, Lecture Notes in Computer Science, Vol.1976, pp.44–57, Springer, 2000.

[11] 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.

[12] 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.

[13] 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.

[14] M. Kasahara and R. Sakai. A construction of public-key cryptosystem based on singular simultaneous equations. *IEICE Transactions on Fundamentals*, E88-A, No.1 (2005), 74–80.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

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

[20] 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.

[21] 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.

[22] 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.

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

[24] 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.

[25] 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.

[26] 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 [26] is included in [29] as an appendix.

[27] 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.

[28] 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 .

[29] 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 .

[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. *Proc. SCIS2005*, 2E1-3, pp.487–492, 2005. Available at URL: http://lab.iisec.ac.jp/~tsujii/SCIS2005-2E1-3.pdf .

[31] 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 .

[32] 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 .

[33] 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 .

[34] S. Tsujii, K. Tadaki, and R. Fujita. Nonlinear piece in hand matrix method for enhancing security of multivariate public key cryptosystems. *Proc. SCC 2008*, pp.124–144, 2008.

[35] L. C. Wang, Y. H. Hu, F. Lai, C. Y. Chou, and B. Y. Yang. Tractable rational map signature. *Proc. PKC 2005*, Lecture Notes in Computer Science, Vol.3386, pp.244–257, Springer, 2005.

[36] L. C. Wang, B. Y. Yang, Y. H. Hu, and F. Lai. A "medium-field" multivariate public-key encryption scheme. *Proc. CT-RSA 2006*, Lecture Notes in Computer Science, Vol.3860, pp.132–149, Springer, 2006.

[37] 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.

[38] 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 .