Security Enhancement of Various MPKCs by 2-layer Nonlinear Piece In Hand Method

Shigeo Tsujii[†] Kohtaro Tadaki[‡] Ryou Fujita[†]
Masahito Gotaishi[‡] Toshinobu Kaneko[§]

[†] 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
[§] Department of Electrical Engineering, Faculty of Science and Technology,
Tokyo University of Science
2641 Yamazaki, Noda-shi, Chiba, 278–8510 Japan

Abstract. Following the last proposal of the nonlinear Piece in Hand method, which has 3-layer structure, 2-layer nonlinear Piece in Hand method is proposed. Both of them aim at enhancing the security of existing and future multivariate public key cryptosystems. The new nonlinear Piece in Hand is compared with the 3-layer method and PMI+, which was proposed by Ding, et al.

Key words: public key cryptosystem, multivariate public key cryptosystem, Piece In Hand, multivariate polynomial

1 Introduction

The research into the Multivariate Public Key Cryptosystem (MPKC, for short) was launched in Japan during the 1980s [17, 21]. The first cryptosystem, which is globally known as *Matsumoto-Imai (MI, for short) cryptosystem* was launched around 1983 by Imai's research group [17] in Yokohama National University (at that time). This was followed by the *sequential solution method*, proposed by Tsujii, et al. [21], which was inspired by the sequential solution method used in the circuit theory.

MI cryptosystem, which became the origin of the practical MPKCs, has been presented in the EUROCRYPT 1988 [18]. Elements of extended field can be regarded both as vectors and as univariate polynomials. MI cryptosystem leverages this dual nature in a sophisticated way. In 1996 Patarin, who had successfully solved MI cryptosystem in 1995, invented Hidden Field Equation (HFE, for short) cryptosystem by extending the central map $\tilde{F}$ of MI cryptosystem [19].

On the other hand, the sequential solution method has been studied by Tsujii's group in the Tokyo Institute of Technology (at that time). One of their cryptosystems, which has been published in IEICE Transactions during 1986 [22], was solved by Kaneko, et al. in 1987 [11]. Afterwards Tsujii et al. proposed its improvement using a birational transformation called *core transformation* in order to prevent the (starting point of the) attack [23].

Since the papers of the study on the sequential solution method have been published exclusively in Japanese, it was hardly known outside Japan. Shamir has proposed the signature scheme based

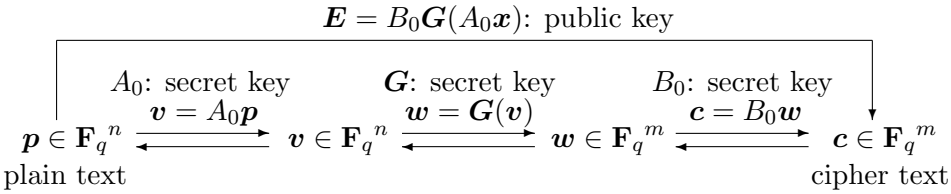

Figure 1: Scheme of Multivariate Public Key Cryptosystem

on the similar idea as the sequential solution method in 1993 [20]. Nevertheless it was attacked by Coppersmith, et al. [2].

The purpose of the research into MPKC during 1980s were as follows: (i) to explore the public key cryptosystem with an advantage over RSA such as computational efficiency, and (ii) to create alternative cryptosystems for the case RSA or ElGamal become vulnerable. Although, after it was discovered that prime factorization and discrete logarithm were solvable with quantum computers in 1994, extensive research has been conducted in this field such as invention of new MPKC or attacks by computing Gröbner bases, especially in Europe.

The security of MPKCs relies on the fact that solving a set of randomly chosen nonlinear polynomial equations over a finite field is NP-hard. However, it is very difficult to make the equations with trapdoors intractable.

In this paper, we propose a method to design the MPKC so that it is intractable even for quantum computers in post-quantum computer age. Therefore we assume that far stronger computational power than the practical world be available and consequently our discussion is free from the constraint of the current computer technology.

We have so far proposed a family of the methods called *Piece in Hand* (PH, for short), which reinforces the security of various MPKCs [24]. The first idea was the linear PH method, which was followed by the non-linear PH method. We have tested and discussed their security and various other properties [25, 26, 27, 28, 29, 30, 31].

In this paper we present the non-linear PH methods with two types of layer structure. Namely, the 3-layer and 2-layer nonlinear PH methods are described and their properties are discussed. In particular, the 2-layer nonlinear PH method has an advantage over other nonlinear PH methods proposed so far and even over PMI+, because it is applicable to the signature scheme. Finally, PH methods are compared with PMI+, another method of enhancing MI cryptosystem proposed by Ding, et al. [5].

2 Basic schemes of MPKC and their security

Most MPKCs are constituted in the way shown in Figure 1. The meaning of Figure 1 is explained in what follows.

Key Generation: A plaintext variable vectors is expressed by n-dimensional vector $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)^T$ with $x_i \in \mathbf{F}_q$, $i = 1, 2, \ldots, n$.

(i) Transform $\boldsymbol{x}$ to an n-dimensional intermediate variable vector $\boldsymbol{v}$ by multiplying an $n \times n$ regular matrix A_0 from the left.

(ii) Generate a quadratic m-dimensional polynomial vector $\boldsymbol{G}$ in variable $\boldsymbol{v}$.[1] $\boldsymbol{G}$ is designed for the legitimate receiver or signer to efficiently compute the inverse function $\boldsymbol{G}^{-1}(\boldsymbol{w})$ of $\boldsymbol{w} = \boldsymbol{G}(\boldsymbol{v})$. It is quite common that m is equal to n, but here we do not exclude the overdefined system with $m \geq n$.

(iii) Generate a ciphertext variable vector

$$\boldsymbol{y} = B_0\boldsymbol{w} = B_0\boldsymbol{G}(\boldsymbol{v}) = B_0\boldsymbol{G}(A_0\boldsymbol{x}) = \boldsymbol{E}$$

by multiplying an $m \times m$ regular matrix B_0 to $\boldsymbol{w}$, i.e., $\boldsymbol{G}(\boldsymbol{v})$ from the left.

The public key polynomial vector $\boldsymbol{E}$ is an n-variable m-dimensional polynomial vector in variable $\boldsymbol{x}$. Thus, the the public key and the secret key are given as follows.

- Public Key: q, n, m, $\boldsymbol{E}$.
- Secret Key: A_0, B_0, $\boldsymbol{G}$.

Encryption: The ciphertext $\boldsymbol{c}$ is generated by assigning the plaintext vector $\boldsymbol{p}$ to $\boldsymbol{E}$ as $\boldsymbol{c} := \boldsymbol{E}(\boldsymbol{p})$.

Decryption:

(i) Calculate $B_0^{-1}\boldsymbol{c}$.

(ii) Calculate $\boldsymbol{G}^{-1}(B_0^{-1}\boldsymbol{c})$.

(iii) Calculate $\boldsymbol{p} = A_0^{-1}\boldsymbol{G}^{-1}(B_0^{-1}\boldsymbol{c})$.

Numerous varieties of MPKCs have been created by devising the structure of $\boldsymbol{G}$. Ding et al. [6] categorized them as shown in the Table 1. Besides the ones listed in the Table 1, there are some hybrid systems including the ℓ-Invertible Cycle (ℓ-IC) proposed by [6]. The known results on the attacks to MPKC are described as follows.

Attacks applicable to any MPKC: This type of attacks includes the computation of Gröbner bases and XL algorithm. The attacks by these algorithms do not attempt to find the secret key but invert the encryption procedure by directly solving the system of polynomial equations obtained from the public key and ciphertext. Therefore it is applicable to random polynomials as well as MPKCs. HFE is comparatively difficult to attack by Gröbner bases. But the HFE challenge with $n = 80$, posted by Courtois was successfully solved by Faugère et al. [8] in 2003 with their proprietary algorithm F5.

Attacks specific to an individual MPKC:

(a) Rank Attack

Rank attack was proposed by Wolf, et al. [2, 10, 32] to attack MPKCs of STS family. They noticed that polynomials in each step of the STS secret key have different rank of the quadratic form. Rank attack computes a matrix equivalent of B and deciphers with similar amount of computation

[1] Since a public key with high total degree increases the key size, we assume that the public key is quadratic. Note, however, that fundamentally polynomials are not limited to quadratic.

Table 1: Taxonomy of the MPKC [6]

System		Authors/Paper
Mixed-Field (or "Big Field")	MIA	MI Scheme A or C^* [18] Matsumoto and Imai
	HFE	Hidden Field Equation [19] Patarin Generalization of MIA
Single-Field (or "True")	UOV	Unbalanced Oil and Vinegar [16] Patarin et al.
	STS	Stepwise Triangular System [10, 32] Tsujii, et al. [22] Shamir [20] Kasahara and Sakai [14, 15]

as the legitimate receivers. Since the decryption time increases exponentially as the number of polynomials in each step r increases, r cannot be made so large.

(b) Differential Attack

Differential attack [9, 7], which is designed for SFLASH and PMI, exploits the differential of the public key polynomials. Here the PMI, which was created by applying Internal Perturbation to MI, was proposed by Ding. We describe this more in detail in the later part of the paper where it is compared with the nonlinear PH method.

(c) Other Heuristic Attacks

There are some attacks including the combination of Gaussian elimination and the method comparing the coefficients, which was used by Kaneko et al. [12, 13] in order to attack both the plain sequential solution method and the one reinforced by PH method.

3 Direction of designing MPKC for the post-quantum computer age

As explained in the introduction, the purpose of the research into MPKC is categorized as follows:

(i) to explore the public key cryptosystem with an advantage over RSA such as speed and implementability.

(ii) to create alternative cryptosystems for the quantum computer age.

The signature scheme SFLASH, which had been selected by Nessie Consortium, was broken by Shamir et al. [7]. Although SFLASH, a use of MI cryptosystem as a signature scheme, was developed for the purpose of the efficiency rather than the security, the attack would have shown an uncertainty of evaluating MPKC. Shamir et al. emphasized in the concluding remark of [7] as follows:

Multivariate cryptographic schemes are very efficient but have a lot of exploitable mathematical structure. Their security is not fully understood, and new attacks against them are found on a regular basis. It would thus be prudent not to use them in any security-critical applications.

Besides, Ding et al. claimed that "We stress that it is still an original sin that no list of possible attacks can be exhaustive" in the paper where they proposed the ℓ-IC.

We share the idea with them and therefore we have been pursuing secure MPKCs since 2003.

It is currently impossible to list up all kinds of attacks to MPKC in advance. We are not sure whether it should be interpreted as, like Ding pointed out, "original sin of the mankind" or the "imperfection of the author of our being." Anyway we would have to make every effort of making the cryptosystem secure to the attacks yet to be found while exploring new attacks.

Based on the above concept, we have proposed concrete methods [24, 25, 26, 27, 28, 29, 30, 31], which we call *Piece in Hand* to improve the security, which are applicable to diverse MPKC although not applicable to every.

We have proposed linear and non-linear PH methods. Generally PH methods reinforce original cryptosystems by "perturbation," adding several random polynomials to public keys. The perturbation polynomials are removed using the secret key and the original ciphertexts, which can be easily decrypted, are revealed. In linear PH methods, perturbation polynomials are removed by applying linear transformation to the ciphertext [25, 26, 27, 28]. Sufficiently many random numbers are added to the random (perturbation) polynomials to make them resistant to the Gröbner bases attack. (Simultaneously random numbers are added to the original public keys in order to avoid being distinguished from the random polynomials).

Kaneko et al. [12] has shown that linear PH method is still vulnerable to the heuristic attack when the primitive sequential solution method [22] is used as the original system. They have concluded that linear PH method cannot improve all kinds of security of every MPKCs.

However, it should be noted that the PH method is an algorithm to improve the security of MPKC and not designed to be usable as an independent cryptosystem. Fundamentally it is impossible to make very weak cryptosystems such as simple permutation of plaintexts with it. Along this reasoning, it was noted in [28] that the PH method selects a reasonable public key cryptosystem as the original.

For example, when the original system is MI cryptosystem:

(i) it was qualitatively identified that the computation effort of Gröbner bases attack significantly increased, based on computer experiments [27, 28].

(ii) It is possible to cope with rank attack by carefully selecting the size of the field and the number of the perturbation polynomials.

(iii) PH method is protected from Differential Attacks in the same way as PMI is protected by the Plus-method [5].

Therefore it could be concluded that PH method effectively improves the security of many MPKCs excluding sequential solution method.

After proposing the linear PH methods, we have been examining nonlinear PH methods, which has wider area of application and more secure against various attacks including Gröbner bases.

Nonlinear PH method perturbs the public key of the original system with the perturbation polynomial (highly randomized polynomials). The perturbation polynomials are removed when it is decrypted in nonlinear PH methods [28, 29, 30, 31]. The information necessary in removing the perturbation polynomial is sent from the sender, because it is dependent on the plaintext. This information is called *auxiliary information*. The procedure of removing perturbation polynomials using the auxiliary information is not disclosed. The difference of the procedure is reflected on the layer structure of the PH methods such as 2- or 3-layer, as shown in the Figure 2 and 3, respectively. The auxiliary part is structured so that the size (the number of polynomials) is significantly smaller

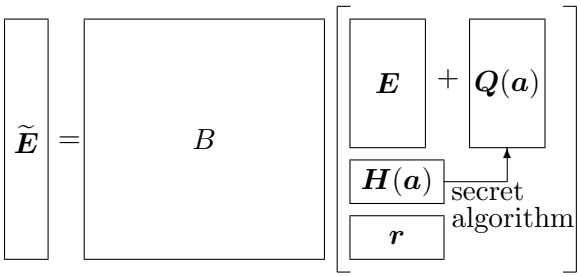

Figure 2: Concept of 3-layer nonlinear PH method

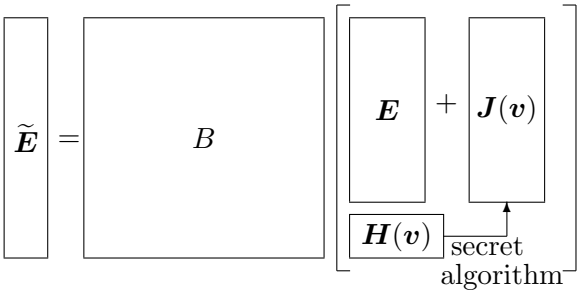

Figure 3: Concept of 2-layer nonlinear PH method

than the perturbed part (original + perturbation), such as $10 \sim 15\%$ of the original. In this paper, we propose a new nonlinear PH method with the 2 layer structure, which is the improved version of the one presented in [30].

4 Description of 3-layer PH method [31]

The structure of the public key of the 3-layer PH method is shown in the Figure 4. In the auxiliary

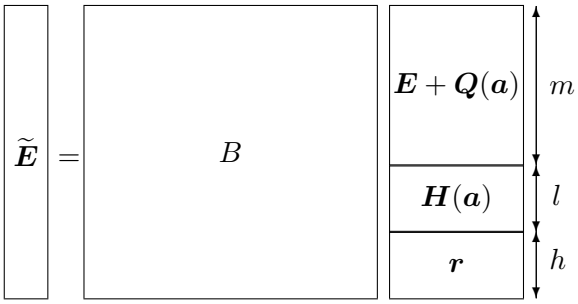

Figure 4: Structure of 3-layer nonlinear PH method

part $\boldsymbol{H}(\boldsymbol{a})$, $\boldsymbol{a}$ is an l-dimensional vector which is acquired by converting the n-dimensional plaintext vector by a linear transformation. The linear transformation is expressed by an $l \times n$ matrix with $l < n$. As explained above, l is chosen as $10 \sim 15\%$ of n. The function $\boldsymbol{H}$ is a reversible polynomial maps with small size l, such as the public key of HFE.

The decryption process is given as follows:

(i) The ciphertext vector B^{-1} is multiplied from the left to $\widetilde{\boldsymbol{c}} = \widetilde{\boldsymbol{E}}(\boldsymbol{p})$, and consequently $\boldsymbol{w} = B^{-1}\widetilde{\boldsymbol{E}}(\boldsymbol{p})$ is determined. Here, $\boldsymbol{p}$ is the plaintext vector.

(ii) $\boldsymbol{a}(\boldsymbol{p})$ is calculated by inverting the transformation $\boldsymbol{H}(\boldsymbol{a}(\boldsymbol{p})) = \boldsymbol{w}_H$, where $\boldsymbol{w}_H$ is the part of $\boldsymbol{w}$ corresponding to $\boldsymbol{H}(\boldsymbol{a})$.

(iii) $\boldsymbol{Q}(\boldsymbol{a})$ is calculated by substituting $\boldsymbol{a}(\boldsymbol{p})$ to the variables of $\boldsymbol{Q}$, and consequently the ciphertext of the original cryptosystem is revealed.

(iv) The plaintext $\boldsymbol{p}$ is obtained by decrypting the original cryptosystem.

The security of 3-layer PH method is discussed in the later section together with the comparison with 2 layer method and PMI+. The improvement of the security against Gröbner bases attack for the plaintext vector with $n = 28 \sim 30$ was observed in the experiment. The result is shown in the Tables 2 and 3.

Table 2: Computational times of the GB attack for PMI+

Parameters			Computational time
n	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

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

Table 3: Computational time of the GB attack for the enhanced MI cryptosystem by the 3-layer nonlinear PH method

Parameters			Computational times
n	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

Computation of Gröbner bases for the plain MI cryptosystem with $n = 30$ takes approximately 0.07 seconds. Thus it would be found that the calculation amount grows to 10^4 times as large as for the MI with the same plaintext size in both PMI+ and 3-layer PH method. When the security of the MPKC is evaluated by computer experiments, we face a serious dilemma. The insecurity could be identified by the successful computation. But "successful" improvement could be identified only by the failure of the calculation as an attack. Therefore it is necessary to develop a methodology of evaluating the computational amount. This theoretical estimation is another important but difficult problem, which is left to the future study. The 3-layer nonlinear PH method was presented in PQCrypto 2008. See [31] for the detail of the method.

5 Proposal of 2-layer nonlinear PH method

Consider the 3-layer nonlinear PH method [31] where an existing public key of MPKC (e.g. HFE) is used as the auxiliary part $\boldsymbol{H}$, as an example. The security of this system is analyzed as follows:

It is quite unlikely that the regular matrix B be disclosed to the attacker. In addition, even if the B^{-1} is found and $\boldsymbol{a}$ is worked out by the attacker, its holistic security is not reduced because the attacker still cannot know the function $\boldsymbol{Q}(\boldsymbol{a})$. However, it would be necessary to develop a nonlinear PH method which does not depend on any MPKC for structuring $\boldsymbol{H}$.

The layer of random polynomials $\mathbf{r}$ was assumed necessary for the countermeasure against the differential attack. But if the layer of auxiliary part is not structured from MPKC, it might be possible to make it carry the auxiliary information while simultaneously work as the countermeasure against differential attack. For that purpose, we propose the auxiliary part with the following structure.

Auxiliary polynomial vector $\boldsymbol{H}$ is constructed with the products of two random linear polynomials h_i and h_j with respect to the variable $\boldsymbol{v}$. Here the variable vector $\boldsymbol{v}$ is an intermediate variable vector with n components. But since the vector $\boldsymbol{v}$ is acquired by applying a linear transformation to the plaintext variable vector $\boldsymbol{x}$ with n components, h_i's are expressed as $h_i = \sum_{j=1}^{n} a_{i,j}x_j$ $(i = 1, \ldots, l)$ with $a_{i,j} \in_R \mathbf{F}_q$. Here the "plaintext variable" is defined as the combination of the true plaintext variables and the variables to which random numbers are substituted on the encryption.

There would be various ways to structure $\boldsymbol{H}$ using h_i's. A simple case is given as follows:

$$\boldsymbol{H} = \begin{pmatrix} h_1h_2 + \alpha_1 \\ h_2h_3 + \alpha_2 \\ h_3h_1 + \alpha_3 \\ h_1h_4 + \alpha_4 \\ h_1h_5 + \alpha_5 \\ \vdots \\ h_1h_{l-1} + \alpha_{l-1} \\ h_1h_l + \alpha_l \end{pmatrix} \tag{1}$$

with $\alpha_i \in_R \mathbf{F}_q$ $(i = 1, 2, \ldots, l)$. The perturbation polynomial vectors $\boldsymbol{J}$ are vector with $l(l-1)/2$ components constructed from the polynomials h_ih_j $(i < j;\ i, j = 1, 2, \ldots, l)$, and given as follows:

$$\boldsymbol{J} = \begin{pmatrix} h_1h_2 + \beta_1 \\ h_1h_3 + \beta_2 \\ \vdots \\ h_1h_l + \beta_{l-1} \\ h_2h_3 + \beta_l \\ \vdots \\ h_2h_l + \beta_{2l-3} \\ h_3h_4 + \beta_{2l-2} \\ \vdots \\ h_{l-1}h_l + \beta_{l(l-1)/2} \end{pmatrix} \tag{2}$$

with $\beta_i \in_R \mathbf{F}_q$ $(i = 1, 2, \ldots, l(l-1)/2)$. The value of perturbation polynomial vectors are acquired as follows.

In the first, second and third components of the vector (1), α_1, α_2 and α_3 are eliminated first. Afterwards the product $h_1^2h_2h_3$ is formed, and the value of h_1^2 is computed by dividing the

product by the second component of the vector (1). Secondly, the product $h_1^2 h_4 h_5$ is computed after eliminating α_4 and α_5 from the corresponding components of the vector (1). Then the value of $h_4 h_5$ is computed by dividing $h_1^2 h_4 h_5$ with h_1^2. In this way, all values $h_i h_j$ $(i < j;\ i, j = 1, 2, \ldots, l)$ are calculated.

Since this process includes division by polynomials, the size q of the finite field $\mathbf{F}_q$ must be sufficiently large. If the probability of h_1 becoming 0 should be negligible, the field should be defined so that $q \gtrsim 2^{80}$. If the sender is able to regenerate and resend the ciphertext in case where the legitimate receiver faces with division by 0, the field should be defined so that $q \gtrsim 2^{10}$.

Now it is possible for the legitimate receiver to calculate $\boldsymbol{J}$ using the values of the quadratic polynomials $h_i h_j$ $(i < j;\ i, j = 1, 2, \ldots, l)$ computed in the above way, as shown in (2).

The rank of the quadratic form of $h_i h_j$ is 1. The rank of the perturbation polynomials $\boldsymbol{J}$ are effectively increased and thereby the randomness of the perturbation polynomials are increased by multiplying a matrix D with each element in $\mathbf{F}_q$ from the left. However, if $l(l-1)/2 \leq m$, it is

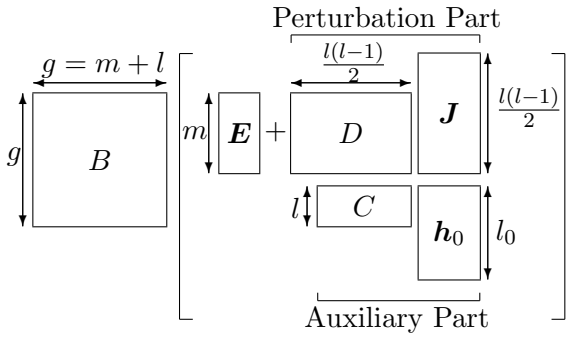

Figure 5: Constitution of 2-layer nonlinear PH method

possible to make the matrix D regular and it is possible for the attackers to attack against $B' = BD$ instead of B, cancelling the effect of D. So the number of rows and columns are chosen so that $l(l-1)/2 \approx 2m$, and therefore the matrix D has a wide shape with n rows and $l(l-1)/2$ columns. Consequently the rank of each quadratic perturbation polynomial is set around m.

In concrete, n is chosen to be larger than commonly defined in most papers ($n = 100 \sim 200$) by assuming the post-quantum computer age. For example, $l = 36$ and $n = 333$.

Now, it is desirable to raise the rank of quadratic perturbation polynomials. For that purpose,

a matrix $\mathbf{H}$ can be constructed in the following way:

$$\boldsymbol{H} = \begin{pmatrix} h_1h_2 + \alpha_1 \\ h_2h_3 + \alpha_2 \\ h_3h_4 + \alpha_3 \\ h_4h_5 + \alpha_4 \\ h_5h_1 + \alpha_5 \\ h_6^2 + h_1h_3 + \alpha_6 \\ h_7^2 + h_3h_5 + \alpha_7 \\ h_8^2 + h_5h_2 + \alpha_8 \\ h_9^2 + h_2h_4 + \alpha_9 \\ h_{10}^2 + h_4h_1 + \alpha_{10} \\ h_1h_{10} + h_6h_{11} + \alpha_{11} \\ h_2h_9 + h_7h_{12} + \alpha_{12} \\ h_3h_8 + h_8h_{13} + \alpha_{13} \\ h_4h_7 + h_9h_{14} + \alpha_{14} \\ h_5h_6 + h_{10}h_{15} + \alpha_{15} \end{pmatrix}.$$

Here each component of $\boldsymbol{H}$ and $\boldsymbol{J}$ is chosen from an extension field of $\mathbf{F}_2$. On decryption, each of $h_1, \ldots, h_5$ is first calculated by solving the first five equations in $\boldsymbol{H}$. This is possible because each element of the extended field of $\mathbf{F}_2$ has a unique square root. Hence the five products h_1h_3, h_3h_5, h_5h_2, h_2h_4, h_4h_1 of these polynomials and the constants $\alpha_6, \ldots, \alpha_{10}$ are subtracted from the 6th to the 10th equations in $\boldsymbol{H}$ to calculate $h_6^2, \ldots, h_{10}^2$. Again, each of $h_6, \ldots, h_{10}$ is uniquely calculated due to the uniqueness of square root. Finally, the values of $h_{11}, \ldots, h_{15}$ are obtained using the 11th to the 15th equations in $\boldsymbol{H}$. Now it is possible to remove the perturbation polynomials using all these values of h_i's.

The effect of the PH method to MI cryptosystem on the computational complexity of Gröbner bases attack is shown in the Table 4. The experimental result for $n = 25, 31$ in Table 4 shows that the computational complexity of computing Gröbner bases of MI cryptosystem enhanced by the PH method was increased by approximately $10^3 \sim 10^4$ times. Here all computer experiments measuring the time of computing Gröbner bases were performed with the following environment: (i) Computer: PROSIDE edAEW416R2 workstation. (ii) CPU: 2.80GHz AMD Opteron Model 854 processors. (iii) Memory: 64GB RAM. (iv) Formula Manipulation System: Magma V2.12-21. (v) Gröbner bases Algorithm: F_4, by executing the internal function of Magma GroebnerBasis(), which was executed with default setting. (vi) Term order: Degree Reverse Lexicographic (DRL or grevlex, for short).

6 Comparison among 2- and 3-layer nonlinear PH Methods, and PMI+

Nonlinear PH methods are aimed at improving the security of MPKCs. It was intended to be applicable to as many MPKCs as possible, although it might be impossible to apply to every MPKC. On the other hand, PMI+ was proposed as a system to increase the randomness of MI cryptosystem by adding perturbation polynomials. But the methodology of *Internal Perturbation* used in PMI+ should be applicable to other MPKCs.

Table 4: Comparison between running-times for MI and the enhanced MI by the 2-layer nonlinear PH method.

Cryptosystems	n	l	Running-times in second
MI ($q = 256$)	25		0.26
	31		0.82
	35		1.7
	41		4.4
	51		16
	71		127
	101		1074
	111		1857
The enhanced MI by the PH method ($q = 256$)	25	15	384
	27	15	2002
	29	15	7074
	31	15	19640

In nonlinear PH methods, the perturbation polynomial vector $\boldsymbol{J}$ are eliminated by calculating the value of each polynomial h_i in $\boldsymbol{H}$ based on a secret algorithm using the auxiliary information. On the other hand, in PMI/PMI+, the vector space to which the plaintext belongs is projected to a vector space with low dimension, and then the image of the projection for the plaintext is retrieved by exhaustive search. Thus these two perturbation methods are different in this respect. Comparison of the features of these two methods, such as efficiency and applicable attacks, is described in the Table 5.

Although the 2-layer nonlinear PH method was proposed in order to enhance the security against Gröbner bases attack, the discussion of the security against other attacks are as follows.

6.1 Rank Attacks

The rank attack itself was already explained in the case of STS in the previous section. Since the main part (i.e. the original public key $\boldsymbol{E}$ plus the perturbation) of the 2 layer PH method has sufficiently large rank (close to n) and sufficiently large number n of polynomials, the vulnerability to the rank attack would depend on the auxiliary part. Since the decryption process includes division by polynomials, the size of the finite field must be of considerable large (e.g. $q \gtrsim 2^5$), and practically the number l of the polynomials is greater or equal to 20. Consequently $q^r \gtrsim 2^{100}$ and therefore rank attacks are rarely possible.

6.2 Differential Attack

As described above, the differential attack is aimed at PMI cryptosystem. In the PMI decryption process, the set to which the plaintext belongs is a linear space and is sorted out into q^r subsets. The perturbation polynomials are then eliminated by exhaustive search. The plaintext vector is transformed into an r-dimensional vector with a linear transformation. Afterwards the r-dimensional vector is assigned to n quadratic polynomials in r variables. Here the polynomials are added to the

Table 5: Comparison between the nonlinear PH methods and PMI+

Feature		Method		
		Nonlinear Piece in Hand method		PMI+
		3-layer method	2-layer method	
Method of eliminating perturbation polynomials		Auxiliary system is used. Invertible nonlinear transformation (such as HFE) is used as the auxiliary system.	Auxiliary system is used. Products of two random linear polynomials are used as the auxiliary system.	The linear space which plaintexts belong to is divided into several subsets. It is found which subset a plaintext belongs to by exhaustive search.
Time to recover the original cryptosystem		Short	Short (The process includes division. Acceptable probability of the denominator becoming 0 be required in the specification)	Long (increases as the security against Gröbner bases attacks improves)
Efficiency of transmission $\left(\frac{\text{Plaintext length}}{\text{Ciphertext length}}\right)$		$0.8 \sim 0.9$	$0.8 \sim 0.9$	approximately 0.9
Security	Gröbner bases attack	Comparatively low, since the number of independent perturbation polynomials depends on the size of the auxiliary part.	Higher than 3-layer PH method or PMI+, since the number of independent perturbation polynomials can equal to the size n of the original public key.	Comparatively low, since the number of the subsets of plaintexts cannot be so large for keeping the decryption efficient.
	Rank attack	It is possible to avoid by appropriately choosing the size of the finite field and the size of the auxiliary part.	As described in the 3-layer method	Presumed to be strong
	Differential attack	Differential attack was invented to attack MPKCs which use MI as the original cryptosystem. In the nonlinear PH methods, however, it is possible to avoid differential attack by appropriately defining the number of auxiliary polynomials.		Differential attack was avoided by applying Plus method.
Way of enhancing the security	Introduction of additional variables with random numbers	It is possible to introduce additional variables to the variables in the perturbation and auxiliary polynomials for improving the security against the Gröbner bases attack etc. (The additional variables are also introduced to a part of the variables of plaintext to prevent the original public key distinguishable.)		The original paper of PMI+ did not use any additional variables, but it is possible to add them by applying the idea of this paper.

MI public key, working as the perturbation polynomials. Since the legitimate receiver knows the hidden structure, the receiver can find the value of the perturbation polynomials in the maximum q^r attempts (64 attempts in the case of $q = 2, r = 6$) and then eliminate them to reveal the original MPKC (i.e. MI cryptosystem).

On the other hand, attackers do not know the linear transformation from the n-dimensional to r-dimensional vectors. However, they know that the dimension of the kernel is $n - r$. Thus, based on this information, they can break the cryptosystem with the computational complexity not significantly exceeding the one for decription [9]. Ding and Gower [5] coped with the differential attack by appending several random polynomials to the public key. The resulting cryptosystem is called the *PMI+*. They recommended to append 10 random polynomials where $n = 136, r = 6$.

The 2-layer PH method does not include the map from the high dimensional vector space to the low dimensional. Thus the attack based on the kernel of the linear transformation is not possible. PMI could be identified as a variation of nonlinear PH method where the auxiliary part is not

disclosed. Because of this structure, however, the decryption process involves exhaustive search. The exhaustive search requires q^r attempts at most. Therefore the decryption time increases exponentially with r. So r must be far smaller than n ($n = 136$, $r = 6$ in the recommendation of [4]). Therefore there are r independent variables in the perturbation polynomials. The number of linearly independent polynomials is $r(r + 1)/2$, which is 21 in the above recommendation of [4]. Thus, the effect of the perturbation is quite limited in PMI and PMI+.

7 Conclusion

In this paper we have proposed the 2-layer nonlinear PH method in order to improve the security of various reasonable MPKCs. We compared their features of 2- and 3-layer nonlinear PH Methods, and PMI+, and discussed the advantage and disadvantage of each method. We have to research into the theoretical structure of MPKCs while keeping various kinds of attacks in mind. We wish this paper would serve readers by giving as one step of the study. Namely, in this paper we have evaluated the enhancement of security by the nonlinear PH methods, mainly on MI cryptosystem. However, we believe that they are applicable to various appropriate MPKCs.

Another important issue is the application to the signature. We believe that they are applicable to the signature scheme and are studying into this matter. The concrete algorithm would be published in the near future.

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] B. Buchberger. Ein Algorithmus zum auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. PhD thesis, Innsbruck, 1965.

[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, 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.

[4] 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.

[5] 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.

[6] 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.

[7] V. Dubois, P. A. Fouque, A. Shamir, and J. Stern. Practical cryptanalysis of SFLASH. *Proc. CRYPTO 2007*, Lecture Notes in Computer Science, Vol.4622, pp.1–12, 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] 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.

[12] 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.

[13] T. Kaneko, Y. Igarashi, D. Ito, and K. Hayakawa. On the security of Piece In Hand Matrix Multivariate Public Key Cryptosystems — MPKC systems proposed in SCIS'07 —. Technical Report of IEICE, ISEC2008-17, SITE2008-11 (2008-07), July 2008. In Japanese.

[14] 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.

[15] 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.

[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] 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] 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.

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

[21] S. Tsujii. Public key cryptosystem using nonlinear equations. *Proc. 8th SITA*, pp.156–157, December 1985. In Japanese.

[22] 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.

[23] 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 [23] is included in [26] as an appendix.

[24] 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.

[25] 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.

[26] 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` .

[27] 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` .

[28] 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` .

[29] S. Tsujii, K. Tadaki, and R. Fujita. Nonlinear piece in hand matrix method for enhancing security of multivariate public key cryptosystems. Proceedings of the First International Conference on Symbolic Computation and Cryptography (SCC 2008), pp.124–144, 2008.

[30] S. Tsujii, T. Kaneko, K. Tadaki, and M. Gotaishi. Design Policy of MPKC based on Piece in Hand Concept. Technical Report of IEICE, ISEC2008-18, SITE2008-12 (2008-07), July 2008. In Japanese.

[31] R. Fujita, K. Tadaki, and S. Tsujii. Nonlinear piece in hand perturbation vector method for enhancing security of multivariate public key cryptosystems. *Proc. PQCrypto 2008*, Lecture Notes in Computer Science, Vol.5299, pp.148–164, Springer, 2008.

[32] 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.