Cryptanalysis of 2-Layer Nonlinear Piece in Hand Method

Xuyun Nie, Albrecht Petzoldt, Johannes Buchmann

Cryptanalysis of 2-layer Nonlinear Piece In Hand Method

Xuyun Nie[1,2,3,4], Albrecht Petzoldt[2], Johannes Buchmann[2]

[1] School of Computer Science and Engineering,
University of Electronic Science and Technology of China, Chengdu 611731, China
[2] Technische Universität Darmstadt, Department of Computer Science,
Hochschulstraße 10, 64289 Darmstadt, Germany
[3] State Key Laboratory of Information Security, Institute of Information Engineering,
Chinese Academy of Sciences, Beijing 100093, China
[4] Network and Data Security Key Laboratory of Sichuan Province
xynie@uestc.edu.cn, apetzoldt@cdc.informatik.tu-darmstadt.de,
buchmann@cdc.informatik.tu-darmstadt.de

Abstract. Piece in Hand method is a security enhancement method for Multivariate Public Key Cryptosystems (MPKCs). Since 2004, many types of this method have been proposed. In this paper, we consider the 2-layer nonlinear Piece in Hand method as proposed by Tsuji et al. in 2009. The key point of this method is to introduce an invertible quadratic polynomial map on the plaintext variables to construct perturbation of the original MPKC. Through our analysis, we find that the security of the enhanced scheme is mainly relying on the quadratic polynomials of this auxiliary map. The two examples proposed by Tsuji et al. for this map can not resist the Linearization Equation attack. Given a valid ciphertext, we can easily get a public key which is equivalent to the original MPKC. If there is an algorithm that can recover the plaintext corresponding to a valid ciphertext of the original MPKC, we can construct an algorithm that can recover the plaintext corresponding to a valid ciphertext of the enhanced MPKC.

Keywords: Multivariate Cryptography, Quadratic Polynomial, Algebraic Cryptanalysis, Linearization Equation, Piece in Hand

1 Introduction

Multivariate Public Key Cryptosystems (MPKCs) are promising candidates to resist the quantum computer attack [1]. The security of these schemes is based on the difficulty of solving systems of multivariate quadratic (MQ) equations over a finite field, which is an NP-hard problem in general.

Since 1988, many MPKCs have been proposed, such as MI [15], HFE [20], MFE [26], TTM [16], Rainbow [5], MQQ [13]etc. However, many of these schemes have shown to be insecure [19,11,6,17,2,14]. In order to enhance the security of MPKCs, many enhancement methods were proposed. There are plus/minus

[22,21], internal perturbation [3,4], Extended Multivariate public key Cryptosystems (EMC) [27] etc. All of these methods are subjected to different levels of attacks [12,7,9,8,18].

Piece in Hand (PH) method is another security enhancement method introduced and studied in a series of papers [23,24,10,25]. In [25], Tsuji et al. proposed the 2-layer nonlinear Piece in Hand method. For this, they introduced two vectors of polynomials: an auxiliary polynomial vector and a perturbation polynomial vector. The perturbation polynomial vector is used to add perturbation to the underlying MPKC, whereas the auxiliary polynomial vector is constructed to be efficiently invertible which will be used during the decryption process.
Since the information of the auxiliary polynomial vector is part of the public key, the security of the whole scheme relies on the structure of this vector. In their paper [25], the authors gave two examples for this vector, called $\boldsymbol{H}_1$ and $\boldsymbol{H}_2$.

In this paper we show that both $\boldsymbol{H}_1$ and $\boldsymbol{H}_2$ satisfy Linearization Equations (LEs) of the form

$$\sum a_{ij} \cdot x_i \cdot y_j + \sum b_i \cdot x_i + \sum c_j \cdot y_j + d = 0, \tag{1}$$

where x_i are the plaintext variables and y_j are the ciphertext variables.

After finding all the LEs and substituting a valid ciphertext into these equations, we can get a system of linear equations in the plaintext variables. By solving this system, we can represent some of the plaintext variables by linear combinations of the other plaintext variables. Hence, we can do elimination on the public key. And we can perform a similar analysis on the eliminated public key to check if there are Linearization Equations satisfied by the simplified public key.
In the case of $\boldsymbol{H}_1$, given a valid ciphertext, we can, after two eliminations on the public key, find a public key equivalent to that of the original MPKC. In the case of $\boldsymbol{H}_2$, given a valid ciphertext, we can achieve the same goal using three eliminations on the public key. This means that Piece in Hand method using these two auxiliary polynomial vectors can not enhance the security of the underlying MPKC. So, we must be very careful when designing the auxiliary polynomial vector of PH method.

The rest of this paper is organized as follows. In Section 2 we give a brief description of MPKCs and Linearization Equations. Section 3 introduces the 2-layer nonlinear Piece in Hand method. In Section 4, we present our cryptanalysis of the enhanced scheme and present the results of our computer experiments. Finally, in Section 5, we conclude the paper.

2 Preliminaries

2.1 Multivariate Public Key Cryptography

To build a multivariate public key cryptosystem (MPKC), one starts with an easily invertible map $\mathcal{F} : \mathbb{F}^n \to \mathbb{F}^m$ (central map). To hide the structure of $\mathcal{F}$ in the public key, one combines it with two invertible affine maps $\mathcal{T} : \mathbb{F}^m \to \mathbb{F}^m$ and $\mathcal{U} : \mathbb{F}^n \to \mathbb{F}^n$. Therefore the public key has the form

$$\mathcal{E} : \mathbb{F}^n \to \mathbb{F}^m,\ \mathbf{y} = (y_1, \ldots, y_m) = \mathcal{E}(x_1, \ldots, x_n) = \mathcal{T} \circ \mathcal{F} \circ \mathcal{U}(x_1, \ldots, x_n). \quad (2)$$

The private key consists out of the three maps $\mathcal{T}, \mathcal{F}$ and $\mathcal{U}$ and therefore allows to invert the public key.

2.2 Linearization Equations

For MPKCs, a Linearization Equation (LE) is an equation in the $n + m$ plaintext/ciphertext variables $x_1, x_2, \ldots, x_n$, $y_1, y_2, \ldots, y_m$ of the form

$$\sum_{i=1}^{n}\sum_{j=1}^{t} a_{ij} \cdot x_i \cdot g_j(y_1, y_2, \ldots, y_m) + \sum_{j=1}^{l} c_j \cdot f_j(y_1, y_2, \ldots, y_m) + d = 0. \quad (3)$$

where f_j $(1 \leq j \leq l)$, g_j $(1 \leq j \leq l)$, are polynomial functions in the ciphertext variables. The highest degree of g_j, $1 \leq j \leq l$ is called the order of the LE.
For example, a First Order Linearization Equation (FOLE) looks like

$$\sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij} \cdot x_i \cdot y_j + \sum_{i=1}^{n} b_i \cdot x_i + \sum_{j=1}^{m} c_j \cdot y_j + d = 0. \quad (4)$$

Note that, given a valid ciphertext $\mathbf{y}' = (y'_1, y'_2, \ldots, y'_m)$, we can substitute it into equation (3) to get a linear equation in the plaintext variables. By finding all these equations we get a linear system which can be solved by Gaussian Elimination. After having found a solution, we can do elimination on the public key.

3 2-layer Piece In Hand Method

We use the same notation as in [25].
Let $\mathcal{E} : \mathbb{F}^n \to \mathbb{F}^m$ be the public map of a multivariate public key encryption scheme with $\{x_1, \ldots, x_n\}$ and $\{y_1, \ldots, y_m\}$ being the plaintext and ciphertext variables repectively and l be a positive integer.
To enhance the security of the MPKC, the inventors of the 2-layer nonlinear Piece in Hand method introduced an auxiliary polynomial vector $\boldsymbol{H}$ of l components and a perturbation polynomial vector $\boldsymbol{J}$. The elements of the auxiliary polynomial vector $\boldsymbol{H}$ are products of two random linear polynomials h_i and h_j, where the functions h_i are given by $h_i = \sum_{j=1}^{n} s_{ij} \cdot x_j$ $(i = 1, \ldots, l)$ with

$s_{ij} \in_R \mathbb{F}$. The perturbation polynomial vector $\boldsymbol{J}$ is a vector with $l(l-1)/2$ components constructed from the polynomials $h_i \cdot h_j$ $(1 \leq i < j \leq l)$. Note that the polynomial components of the vector $\boldsymbol{H}$ are designed to be easily invertible for decryption. Therefore, one can use the vector $\boldsymbol{H}$ to compute the values of h_i $(i = 1, \ldots, l)$ and sequentially calculate the value of the vector $\boldsymbol{J}$. By the above construction, one gets an enhanced public key $\tilde{\mathcal{E}} : \mathbb{F}^n \to \mathbb{F}^{m+l}$ of the form

$$\tilde{\mathcal{E}}(x_1, \ldots, x_n) = B \begin{pmatrix} \mathcal{E}(x_1, \ldots, x_n) + D\boldsymbol{J} \\ C\boldsymbol{H} \end{pmatrix} \tag{5}$$

where B is an $(m+l) \times (m+l)$ invertible matrix over $\mathbb{F}$, D is an $m \times \frac{l \cdot (l-1)}{2}$ matrix over $\mathbb{F}$, and C is an $l \times l$ invertible matrix over $\mathbb{F}$.

Secret key: The secret key includes

- the secret key of the underlying MPKC
- the matrices B, C and D
- the auxiliary polynomial vector $\boldsymbol{H}$ and
- the perturbation polynomial vector $\boldsymbol{J}$.

Public key: The $m + l$ components of the function $\tilde{\mathcal{E}}$.
Encryption: Given a plaintext $\boldsymbol{x'} = (x'_1, \ldots, x'_n)$, compute

$$\boldsymbol{y'} = (y'_1, \ldots, y'_{m+l}) = \tilde{\mathcal{E}}(x'_1, \ldots, x'_n).$$

Decryption: Given a valid ciphertext $\boldsymbol{y'} = (y'_1, \ldots, y'_{m+l})$, decryption includes the following steps:

1. Compute $\boldsymbol{v'} = (v'_1, \ldots, v'_{m+l}) = B^{-1}(y'_1, \ldots, y'_{m+l})^T$;
2. Compute $\boldsymbol{H} = C^{-1}(v'_{m+1}, \ldots, v'_{m+l})^T$ and get the values of h_i $(i = 1, \ldots, l)$;
3. Compute the value of $\boldsymbol{J}$ by substituting the values of h_i $(i = 1, \ldots, l)$ into its components;
4. Compute $\boldsymbol{x'} = (x'_1, \ldots, x'_n) = \mathcal{E}^{-1}(v'_1 - dj_1, \ldots, v'_m - dj_m)$, where $(dj_1, \ldots, dj_m)^T = D\boldsymbol{J}$.

Examples for the auxiliary vector $\boldsymbol{H}$ and the perturbation vector $\boldsymbol{J}$

In [25], the authors gave two examples for the choice of the auxiliary vector $\boldsymbol{H}$, denoted by $\boldsymbol{H}_1$ and $\boldsymbol{H}_2$, respectively.
For arbitrary l, the vector $\boldsymbol{H}_1$ is given by

$$\boldsymbol{H}_1 = (u_1, \ldots, u_l)^T = \begin{pmatrix} h_1h_2 + \alpha_1 \\ h_2h_3 + \alpha_2 \\ h_3h_1 + \alpha_3 \\ h_1h_4 + \alpha_4 \\ h_1h_5 + \alpha_5 \\ \vdots \\ h_1h_{l-1} + \alpha_{l-1} \\ h_1h_l + \alpha_l \end{pmatrix}. \tag{6}$$

with $\alpha_1, \ldots, \alpha_l \in_R \mathbb{F}$. For our experiments (see Subsection 4.3) we use the value $l = 8$.
Apparently, given the value of the vector $(u_1, \ldots, u_l)$, we can get from the first three equations of (6)

$$h_1 = \left(\frac{(u_1 - \alpha_1)(u_3 - \alpha_3)}{(u_2 - \alpha_2)} \right)^{\frac{1}{2}} \tag{7}$$

and then get the values of $h_2, h_3, \ldots, h_l$ in turn.
For the auxiliary map $\boldsymbol{H}_2$, the value l is fixed to 15. We have

$$\boldsymbol{H}_2 = (u_1, \ldots, u_{15})^T = \begin{pmatrix} h_1 h_2 + \alpha_1 \\ h_2 h_3 + \alpha_2 \\ h_3 h_4 + \alpha_3 \\ h_4 h_5 + \alpha_4 \\ h_5 h_1 + \alpha_5 \\ h_6^2 + h_1 h_3 + \alpha_6 \\ h_7^2 + h_3 h_5 + \alpha_7 \\ h_8^2 + h_5 h_2 + \alpha_8 \\ h_9^2 + h_2 h_4 + \alpha_9 \\ h_{10}^2 + h_4 h_1 + \alpha_{10} \\ h_1 h_{10} + h_6 h_{11} + \alpha_{11} \\ h_2 h_9 + h_7 h_{12} + \alpha_{12} \\ h_3 h_8 + h_8 h_{13} + \alpha_{13} \\ h_4 h_7 + h_9 h_{14} + \alpha_{14} \\ h_5 h_6 + h_{10} h_{15} + \alpha_{15} \end{pmatrix} \tag{8}$$

where $\alpha_i \in_R \mathbb{F}$ $(i = 1, \ldots, l)$. Similarly to $\boldsymbol{H}_1$, $\boldsymbol{H}_2$ can be easily inverted.
The perturbation vector $\boldsymbol{J}$ used in [25] is given as follows:

$$\boldsymbol{J} = (j_1, j_2, \ldots, j_{l(l-1)/2}) = \begin{pmatrix} h_1 h_2 + \beta_1 \\ h_1 h_3 + \beta_2 \\ \vdots \\ h_1 h_l + \beta_{l-1} \\ h_2 h_3 + \beta_l \\ \vdots \\ h_2 h_l + \beta_{2l-3} \\ h_3 h_4 + \beta_{2l-2} \\ \vdots \\ h_{l-1} h_l + \beta_{l(l-1)/2} \end{pmatrix} \tag{9}$$

where $\beta_i \in_R \mathbb{F}$ $(i = 1, \ldots, l(l-1)/2)$.

4 Cryptanalysis of the 2-layer PH Method

Although the perturbation map $\boldsymbol{J}$ can hide the weak point of the underlying MPKC scheme, the security of the enhanced scheme depends mainly on the design of the auxiliary map $\boldsymbol{H}$. Bad design of the vector $\boldsymbol{H}$ will bring some new security problems to the scheme. Both vectors $\boldsymbol{H}_1$ and $\boldsymbol{H}_2$ of [25] are not properly chosen to enhance the security of the underlying scheme, since they satisfy Linearization Equations.

In this section, we present our cryptanalysis of the 2-layer PH method with auxiliary polynomial vector $\boldsymbol{H}_1$ and $\boldsymbol{H}_2$, respectively. Given a valid ciphertext $\boldsymbol{y}' = (y'_1, \ldots, y'_{m+l})^T$, our goal is to find the corresponding plaintext. Namely, we have to solve the system

$$\begin{cases} y'_1 = \tilde{\mathcal{E}}_1(x_1, \ldots, x_n) \\ \qquad \vdots \\ y'_{m+l} = \tilde{\mathcal{E}}_{m+l}(x_1, \ldots, x_n) \end{cases}. \tag{10}$$

4.1 Case of $\boldsymbol{H}_1$

Through theoretical analysis, we find that the system $\tilde{\mathcal{E}}$ satisfies Linearization Equations, which are brought in by the vector $\boldsymbol{H}_1$. Given a valid ciphertext we can, after finding all FOLEs, recover the corresponding plaintext easily.

Linearization Equations

In the expression of the polynomial vector $\boldsymbol{H}_1$ (see (6)), we have

$$u_1 = h_1 h_2 + \alpha_1 \text{ and } u_2 = h_2 h_3 + \alpha_2.$$

Hence we get

$$h_3(u_1 - \alpha_1) = h_1(u_2 - \alpha_2). \tag{11}$$

Since the matrices B and C are invertible, the elements u_i $(i = 1, \ldots, l)$ can be expressed by linear equations in the ciphertext variables, namely $u_i = \sum_{j=1}^{m+l} t_{ij} \cdot y_j$ $(i = 1, \ldots, l)$. Analogously we get $h_i = \sum_{j=1}^{n} s_{ij} \cdot x_j$ $(i = 1, \ldots, l)$. Hence equation (11) implies that the plaintext variables $\{x_1, \ldots, x_n\}$ and ciphertext variables $\{y_1, \ldots, y_{m+l}\}$ satisfy an equation of the form:

$$\sum_{i=1}^{n} \sum_{j=1}^{m+l} a_{ij} \cdot x_i \cdot y_j + \sum_{i=1}^{n} b_i \cdot x_i + \sum_{j=1}^{m+l} c_j \cdot y_j + d = 0. \tag{12}$$

This equation is exactly a FOLE. Similarly, from each of the pairs $h_j(u_i - \alpha_i) = h_i(u_j - \alpha_j)$ $(1 \le i < j \le l, i \ne 2)$ and the pair $h_1(u_2 - \alpha_2) = h_2(u_3 - \alpha_3)$, we can get an additional FOLE. Hence there exist at least $(l-2)(l-1)/2 + 1$ linear independent Linearization Equations of type (12).

To find these FOLEs, we randomly generate $D_1 \geq n(m+l)+n+m+l+1$ plaintext/ciphertext pairs and substitute them into equation (12). By doing so, we get a system of D_1 linear equations in the $n(m+l)+n+m+l+1$ unknowns $a_{ij},\ b_i,\ c_j$ and d which can be solved by Gaussian Elimination. We denote the solution space by V and its dimension by D. Hence, we derive D linearly independent equations of type (12) in the plaintext and ciphertext variables.

The work above depends only on the public key and can be done once for a given public key.

By substituting the given ciphertext $\mathbf{y}' = (y'_1, \ldots, y'_{m+l})$ into the Linearization Equations found above we get D linear equations in the plaintext variables. Let's assume that t_1 of these equations are linearly independent.

First Elimination

By substituting the t_1 equations found above into the public key $\tilde{\mathcal{E}}$ of the 2-layer nonlinear PH scheme, we can eliminate t_1 equations from $\tilde{\mathcal{E}}$. By doing so, we get a simplified public key $\tilde{\mathcal{E}}'$ of the form

$$\begin{cases} y'_j = \tilde{\mathcal{E}}'_j(w_1, \ldots, w_{n-t_1}) \\ 1 \leq j \leq m+l \end{cases} . \tag{13}$$

Second Elimination

In the practical setting of [25], the characteristic of the underlying field $\mathbb{F}$ was chosen to be 2. Using this property, we can find another type of Linearization Equations satisfied by the simplified public key $\tilde{\mathcal{E}}'$.

We denote by u'_i $(i = 1, \ldots, l)$ the value of u_i corresponding to the given ciphertext $\mathbf{y}' = (y'_1, \ldots, y'_{m+l})$. Such we get

$$\begin{cases} u'_1 = h_1 h_2 + \alpha_1 \\ u'_2 = h_2 h_3 + \alpha_2 \\ u'_3 = h_3 h_1 + \alpha_3 \\ u'_4 = h_1 h_4 + \alpha_4 \\ u'_5 = h_1 h_5 + \alpha_5 \\ \vdots \\ u'_{l-1} = h_1 h_{l-1} + \alpha_{l-1} \\ u'_l = h_1 h_l + \alpha_l \end{cases} . \tag{14}$$

According to FOLEs similar to equation (11), we find

$$\begin{cases} h_2 = \frac{u_2'-\alpha_2}{u_3'-\alpha_3} h_1 \\ h_3 = \frac{u_2'-\alpha_2}{u_1'-\alpha_1} h_1 \\ h_4 = \frac{u_4'-\alpha_4}{u_1'-\alpha_1} \cdot \frac{u_2'-\alpha_2}{u_3'-\alpha_3} h_1 \\ h_5 = \frac{u_5'-\alpha_5}{u_1'-\alpha_1} \cdot \frac{u_2'-\alpha_2}{u_3'-\alpha_3} h_1 \\ \vdots \\ h_l = \frac{u_l'-\alpha_l}{u_1'-\alpha_1} \cdot \frac{u_2'-\alpha_2}{u_3'-\alpha_3} h_1 \end{cases} . \tag{15}$$

By substituting (15) into (6), we get

$$\begin{cases} u_1 = \frac{u_2'-\alpha_2}{u_3'-\alpha_3} h_1^2 + \alpha_1 \\ u_2 = \frac{u_2'-\alpha_2}{u_1'-\alpha_1} \cdot \frac{u_2'-\alpha_2}{u_3'-\alpha_3} h_1^2 + \alpha_2 \\ u_3 = \frac{u_2'-\alpha_2}{u_1'-\alpha_1} h_1^2 + \alpha_3 \\ u_4 = \frac{u_4'-\alpha_4}{u_1'-\alpha_1} \cdot \frac{u_2'-\alpha_2}{u_3'-\alpha_3} h_1^2 + \alpha_4 \\ u_5 = \frac{u_5'-\alpha_5}{u_1'-\alpha_1} \cdot \frac{u_2'-\alpha_2}{u_3'-\alpha_3} h_1^2 + \alpha_5 \\ \vdots \\ u_l = \frac{u_l'-\alpha_l}{u_1'-\alpha_1} \cdot \frac{u_2'-\alpha_2}{u_3'-\alpha_3} h_1^2 + \alpha_l \end{cases} . \tag{16}$$

Due to $u_i = \sum_{j=1}^{m+l} t_{ij} \cdot y_j$ $(i = 1, \ldots, l)$ and $h_i = \sum_{j=1}^{n} s_{ij} \cdot x_j$ $(i = 1, \ldots, l)$ and using the fact that squaring is a linear operation on a field of characteristic 2, we have at least one equation satisfied by ciphertext variables and the remaining plaintext variables of the form

$$\begin{cases} \sum_{j=1}^{m+l} \tilde{a}_j \cdot y_j' + \sum_{i=1}^{n-t_1} \tilde{b}_i \cdot w_i^2 + \tilde{c} = 0 \\ \forall w_1, \ldots, w_{n-t_1} \in \mathbb{F} \end{cases} . \tag{17}$$

It is easy to solve the above linear system for the $\tilde{a}_i$, $\tilde{b}_j$ and $\tilde{c}$. Let $\{\tilde{a}_1^{(\rho)}, \cdots, \tilde{a}_{m+l}^{(\rho)}, \tilde{b}_1^{(\rho)}, \cdots, \tilde{b}_{n-t_1}^{(\rho)}, \tilde{c}^{(\rho)},\ 1 \le \rho \le r\}$ be a basis of the solution space of the system (17). Set

$$\begin{cases} \sum_{j=1}^{n-t_1} (\tilde{b}_j^{(\rho)})^{1/2} \cdot w_j + (\sum_{i=1}^{m+l} \tilde{a_i}^{(\rho)} \cdot y_i' + \tilde{c}^{(\rho)})^{1/2} = 0 \\ 1 \le \rho \le r \end{cases} . \tag{18}$$

For any vector $\mathbf{w} = (w_1, \ldots w_{n-t_1})$, $\mathbf{w}$ and the corresponding ciphertext $(y_1, \ldots, y_{m+l}) = \tilde{\mathcal{E}}'(\mathbf{w})$ satisfy equation (18). Therefore we can represent at least one variable of the set $\{w_1, \ldots, w_{n-t_1}\}$ as a linear equation in the remaining variables. Denote the remaining variables by $v_1, \ldots, v_{n-t_1-1}$.
Substituting this linear expression into the system (13), we can get a new public key with $(n - t_1 - 1)$ unknowns, denoted as

$$\begin{cases} y_j' = \tilde{\mathcal{E}}_j''(v_1, \ldots, v_{n-t_1-1}) \\ 1 \le j \le m + l \end{cases} . \tag{19}$$

Eliminating Perturbation

Furthermore, after two eliminations, the vector $\boldsymbol{J}$ becomes a constant vector, namely, the perturbation of Piece in Hand method is eliminated. The reason for this is shown as follows. From (16), we get

$$h_1 = \left(\frac{(u'_1 - \alpha_1)(u'_3 - \alpha_3)}{u'_2 - \alpha_2} \right)^{1/2}. \tag{20}$$

Substituting (20) and (15) into (9), the vector $\boldsymbol{J}$ becomes a constant vector on $\mathbb{F}$. For example,

$$j_1 = h_1 h_2 + \beta_1 = u'_1 - \alpha_1 + \beta_1,$$
$$j_{l+1} = h_2 h_4 + \beta_{l+1} = \left(\frac{(u'_2 - \alpha_2)(u'_4 - \alpha_4)}{u'_3 - \alpha_3} \right) + \beta_{l+1}.$$

Hence, the public key $\tilde{\mathcal{E}}''$ of equation (19) is equivalent to the public key of the underlying MPKC scheme.

If there exists an algorithm which recovers the plaintext corresponding to a valid ciphertext for the underlying MPKC scheme, we can therefore find the values of the variables $v_1, \ldots, v_{n-t_1-1}$ corresponding to the valid ciphertext $\mathbf{y}'$. Using the linear equations found during the two eliminations above, we can recover the values of the remaining plaintexts variables.

4.2 Case of $\boldsymbol{H_2}$

Let $y' = (y'_1, \ldots, y'_{m+15})$ be a valid ciphertext of the Piece in Hand MPKC with auxiliary map $\boldsymbol{H}_2$. Again we want to find the corresponding plaintext $x' = (x'_1, \ldots, x'_n)$ by solving the system (10).

Similarly to the case of $\boldsymbol{H}_1$, from the first five equations in (8), we can get five FOLEs between u_i and h_i $(1 \le i \le 5)$ by

$$\begin{cases} h_3(u_1 - \alpha_1) = h_1(u_2 - \alpha_2) \\ h_4(u_2 - \alpha_2) = h_2(u_3 - \alpha_3) \\ h_5(u_3 - \alpha_3) = h_3(u_4 - \alpha_4) \\ h_1(u_4 - \alpha_4) = h_4(u_5 - \alpha_5) \\ h_2(u_5 - \alpha_5) = h_5(u_1 - \alpha_1) \end{cases}.$$

Apparently, these five equations are linearly independent. Hence, we can get at least five Linearization Equations satisfied by plain- and ciphertext variables of the form (12).
Using the same method as in Subsection 4.1, we do the first elimination on the system (10). Suppose we eliminated $t_1 \ge 4$ variables in the system. Denote the remaining plaintext variables by $w_1, \ldots, w_{n-t_1}$ and let

$$\begin{cases} y'_j = \tilde{\mathcal{E}}'_j(w_1, \ldots, w_{n-t_1}) \\ 1 \le j \le m + 15 \end{cases} \tag{21}$$

be the simplified public key.
Using a similar method as in Subsection 4.1, we can perform two additional eliminations on the system (21). Due to the limitation of paper size, we omit the details of this part here. We will present them in the full version of this paper. But we should point out the following facts.
For the public key $\tilde{\mathcal{E}}'_j(w_1, \ldots, w_{n-t_1})$, plain- and ciphertext variables satisfy equations of the form

$$\sum_{j=1}^{m+l} \tilde{a}_j \cdot y_j + \sum_{i=1}^{n-t_1} \tilde{b}_i \cdot w_i^2 + \tilde{c} = 0. \tag{22}$$

By substituting the ciphertext $\mathbf{y}'$ into these equations and using the fact that squaring is a linear function over fields of characteristic 2, we can find $t_2 \geq 6$ linear equations in the plaintext variables. We can therefore eliminate t_2 variables from the public key. After this elimination, the simplified public key has the form

$$\begin{cases} y'_j = \tilde{\mathcal{E}}''_j(v_1, \ldots, v_{n-t_1-t_2}) \\ 1 \leq j \leq m+15 \end{cases}. \tag{23}$$

The public key $\tilde{\mathcal{E}}''$ satisfies equations of the form

$$\sum_{j=1}^{m+15} \tilde{\tilde{a}}_j \cdot y_j + \sum_{i=1}^{n-t_1-t_2} \tilde{\tilde{b}}_i \cdot v_i + \tilde{\tilde{c}} = 0. \tag{24}$$

By substituting the ciphertext $\mathbf{y}'$ into these equations, we can find $t_3 \geq 5$ linear equations in the variables $v_1, \ldots, v_{n-t_1-t_2}$. Therefore, we can eliminate t_3 variables from the system (23) and get a new public key $\tilde{\mathcal{E}}'''$ of the form

$$\begin{cases} y'_j = \tilde{\mathcal{E}}'''_j(u_1, \ldots, u_{n-t_1-t_2-t_3}) \\ 1 \leq j \leq m+15 \end{cases}. \tag{25}$$

For the public key $\tilde{\mathcal{E}}'''$, the perturbation vector $\boldsymbol{J}$ becomes a constant vector. Hence, $\tilde{\mathcal{E}}'''$ is equivalent to the public key of the underlying MPKC.
Analogously to Subsection 4.1 we can therefore, under the assumption that there exists an algorithm which, for the underlying MPKC, finds for a given ciphertext the corresponding plaintext, construct an algorithm which, for any given ciphertext $\mathbf{y}' = (y'_1, \ldots, y'_{m+15})$, recovers the corresponding plaintext $\mathbf{x}' = (x'_1, \ldots, x'_n)$.

4.3 Complexity and Experimental Verification

In our concrete attack scenario we set $\mathbb{F} = GF(256)$ and $m = n = 25$. As the underlying MPKC we used the $C^\star$ scheme of Matsumoto and Imai. We implemented the Piece in Hand cryptosystem in two different ways using $\boldsymbol{H}_1$ (with $l = 8$) and $\boldsymbol{H}_2$ as auxiliary matrix respectively. For our attack we chose randomly a valid ciphertext $\mathbf{y}' = (y'_1, \ldots, y'_{m+l}) \in \mathbb{F}^{m+l}$. Our goal was to find the corresponding plaintext $\mathbf{x}' = (x'_1, \ldots, x'_n) \in \mathbb{F}^n$.

Case of H_1 In the first step we computed 900 ($> n(m+l)+n+m+l+1 = 884$) plaintext/ciphertext pairs and substituted them into the Linearization Equation of type (12). We did Gaussian Elimination on this linear system and found a basis of all FOLEs. The complexity of the Gaussian Elimination is equal to $(n(m+l)+n+m+l+1)^3$ operations on the finite field $\mathbb{F}$. In our experiments,

$$(n(m+l)+n+m+l+1)^3 = 884^3 \leq 2^{30}.$$

We found that the dimension of the space spanned by all FOLEs is $D = (l-2)(l-1)/2 = 22$.
Computing the plaintext/ciphertext pairs and solving this large linear system proved to be the most time-consuming step of our attack. In our experiments, it took about 70 seconds, where it took about 68 seconds on generating the plaintext/ciphertext pairs and about 2 seconds on the Gaussian Elimination. This step is independent of the given ciphertext $\mathbf{y}'$ and has to be done for a given public key only once.
After substituting the ciphertext $\mathbf{y}'$ into these equations we obtained 7 linear equations in the plaintext variables.

In the second step we computed 100 plaintext/ciphertext pairs and substituted them into the Linearization Equation of type (17). By doing so, we got 15 linearly independent equations of the form (17). By evaluating equation (18), we got 1 linear equation in the plaintext variables.

We substituted the 8 linear equations found in the previous steps into the public key and obtained a new public key $\tilde{\mathcal{E}}''$ of 33 equations in 17 variables, which proved to be of the form of a $C^\star$ public key (i.e. the perturbation was eliminated).

In the last step of the attack, we attacked the new public key $\tilde{\mathcal{E}}''$ with the Linearization Equation attack of Patarin [19]. We computed 500 plaintext/ciphertext pairs and substituted them into the Linearization Equation of type (12). By doing so, we got 25 linear independent equations of type (12). After substituting the ciphertext y' we obtained 17 linear equations in the plaintext variables which enabled us to reconstruct the plaintext $\mathbf{x}'$.
The running time of the whole attack was about 90 seconds.

Case of H_2 In the first step we computed 1100 ($> (n(m+15)+n+m+15+1) = 1066$) plaintext/ciphertext pairs and substituted them into the Linearization Equation of type (12). We solved the resulting linear system for the variables a_{ij}, b_i, c_j and d to find a basis of all FOLEs. By doing so, we found 5 linear independent Linearization Equations. After substituting the ciphertext $\mathbf{y}'$ into these equations we obtained 4 linear equations in the plaintext variables. The complexity of this step is equal to $1066^3 \leq 2^{31}$. It took about 104 seconds in our experiments, where it took about 102 seconds on generating the plaintext/ciphertext pairs and about 2 second on the Gaussian Elimination. This step has to be performed for each public key only once.

In the second step we computed 100 plaintext/ciphertext pairs and substituted them into the Linearization Equation of type (22). By doing so, we got 14 linear independent equations of form (22). After substituting the ciphertext $\mathbf{y}'$, we got 6 linear equations in the plaintext variables.
In the third step we computed again 100 plaintext/ciphertext pairs and substituted them into the Linearization Equation of type (24). We obtained 25 linear independent equations. By substituting the ciphertext $\mathbf{y}'$ into these equations, we got 5 linear equations in the plaintext variables.
We substituted the 15 linear equations found in the previous steps into the public key and obtained a new public key $\tilde{\mathcal{E}}'''$ of 40 equations in 10 variables, which proved to be of the form of a $C^\star$ public key (i.e. the perturbation was eliminated).
In the last step of the attack, we attacked the new key $\tilde{\mathcal{E}}'''$ with the Linearization Equation attack of Patarin [19]. We computed 500 plaintext/ciphertext pairs and substituted them into the Linearization Equation of type (12). By doing so, we obtained 25 linear independent equations. After substituting the ciphertext $\mathbf{y}'$ we got 10 linear equations in the plaintext variables which enabled us to reconstruct the plaintext $\mathbf{x}'$.
The running time of the whole attack was about 127 seconds.

All experiments were performed on a server with 24 AMD Opteron processors and 128 GB RAM. However, for our experiments we used only a single core. The attack was programmed in Magma code and required about 120 MB of memory.

5 Conclusion

In this paper, we presented the cryptanalysis of two examples of the 2-layer nonlinear Piece in Hand method. As we showed, both examples do not enhance the security of the underlying MPKC because they can not resist Linearization Equation attacks. From this paper, we find that the security of the 2-layer nonlinear Piece in Hand method depends mainly on the construction of the auxiliary polynomial vector $\boldsymbol{H}$. We should therefore design the auxiliary polynomial vector $\boldsymbol{H}$ in such a way that it resists existing attacks.

Acknowledgements

We want to thank the anonymous reviewers for their comments which helped to improve the paper. The first author is supported by the National Key Basic Research Program of China (2013CB834203), the National Natural Science Foundation of China (No. 61103205), the Fundamental Research Funds for the Central Universities under Grant ZYGX2010J069. The second author thanks the Horst Görtz Foundation for financial support.

References

[1] D. Bernstein, J. Buchmann and E. Dahmen (Eds.). *Post-Quantum Cryptography*. Springer, 2009.

[2] O. Billet and H. Gilbert. Cryptanalysis of Rainbow. *Security and Cryptography for Networks - SCN 2006*, LNCS, volume 4116, pages 336-347. Springer, 2006.

[3] J. Ding. A new variant of the Matsumoto-Imai cryptosystem through perturbation. *Public key Cryptography - PKC'04*, LNCS, volume 2947, pages 305-318. Springer, 2004.

[4] J. Ding and D. Schmidt. Cryptanalysis of HFEV and the internal perturbation of HFE. *Public key Cryptography - PKC'05*, LNCS, volume 3386, pages 288-301. Springer, 2005.

[5] J. Ding and D. Schmidt. Rainbow, a new multivariate public key signature scheme. *The Third International Conference of Applied Cryptography and Network Security - ACNS 2005*, LNCS volume 3531, pages 164-175. Springer, 2005.

[6] J. Ding, L. Hu, X. Nie, J. Li and J. Wagner. High Order Linearization Equation (HOLE) Attack on Multivariate Public Key Cryptosystems. *Public Key Cryptography - PKC 2007*, LNCS volume 4450, pages 233-248. Springer, 2007.

[7] V. Dubois, P. Fouque, A. Shamir and J. Stern. Practical Cryptanalysis of SFLASH. *Advance in Cryptology - CRYPTO 2007*, LNCS volume 4622, pages 1-12. Springer, 2007.

[8] V. Dubois, L. Granboulan and J. Stern. Cryptanalysis of HFE with Internal Perturbation. *Public Key Cryptography - PKC 2007*, LNCS volume 4450, pages 249-265. Springer, 2007.

[9] P.-A. Fouque, L. Granboulan and J. Stern. Differential Cryptanalysis for Multivariate Schemes *Advances in Cryptology - EUROCRYPT 2005*, LNCS volume 3494, pages 341-353, Springer 2005, .

[10] 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*, LNCS volume 5299, pages 148-164. Springer, 2008.

[11] J. Faugère and A. Joux. Algebraic Cryptanalysis of Hidden Field Equation (HFE) cryptosystems using Gröbner bases. it Advances in Cryptology - CRYPTO 2003, LNCS volume 2729, pages 44 - 60. Springer, 2003.

[12] J. Faugère, A. Joux, L. Perret and J. Treger. Cryptanalysis of the Hidden Matrix Cryptosystem. *Progress in Cryptology - LATINCRYPT 2010*, LNCS volume 6212, pages 241-254. Springer, 2010.

[13] D. Gligoroski,S. Markovski, S. Knapskog. Multivariate Quadratic Trapdoor Functions Based on Multivariate Quadratic Quasigroups. *In: Proceedings of The American Conference on Applied Mathematics (MATH 2008)*, Cambridge, Massachusetts, USA (March 2008).

[14] M. Mohamed, J. Ding, J. Buchmann et al. Algebraic Attack on the MQQ Public Key Cryptosystem. *In Proceedings of the 8th International Conference on Cryptology And Network Security, (CANS09)*, LNCS volume 5888, pages 392¨C401, Springer 2009.

[15] T. Matsumoto and H. Imai. Public quadratic polynomial-tuples for efficient signature verification and message encryption. In C. G. Guenther, editor, *Advances in cryptology –EUROCRYPT'88*, LNCS volume 330, pages 419-453. Springer, 1988.

[16] T. Moh. A fast public key system with signature and master key functions. Lecture Notes at EE department of Stanford University, May 1999. http://www.usdsi.com/ttm.html.

[17] X. Nie, L. Hu, J. Li, C. Updegrove and J. Ding. Breaking A New Instance of TTM Cryptosystem. *Advances in ACNS2006*, LNCS volume 3989, pages 210-225. Springer, 2006.

[18] X. Nie, Z. Xu and J. Buchmann. Cryptanalysis of Hash-based Tamed Transformation and Minus Signature Scheme. *Post-Quantum Cryptography - PQCrypto 2013*, LNCS volume 7932, pages 155-164. Springer, 2013.

[19] J. Patarin. Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88. In D.Coppersmith, editor, *Advances in Cryptology – Crypto'95* LNCS volume 963, pages 248-261. Springer, 1995.

[20] J. Patarin. Hidden field equations (HFE) and isomorphism of polynomials (IP): Two new families of asymmetric algorithms. In U. Maurer, editor, *Eurocrypt'96* LNCS volume 1070, pages 33-48. Springer, 1996.

[21] J. Patarin, N. Courtois and L. Goubin. Flash, a fast multivariate signature algorithm. *Progress in Cryptology, CT-RSA 2001*, LNCS volume 2020, pages 298-307. Springer, 2001.

[22] J. Patarin, L. Goubin and N. Courtois. C^*_{-+} and HM: variations around two schemes of T. Matsumoto and H.Imai. *Advances in Cryptology - ASIACRYPT'98*, LNCS volume 1514, pages 35-50. Springer, 1998.

[23] S. Tsujii, K. Tadaki and R. Fujioka. Piece in Hand concept for enhanceing the security of multivariate type public key cryptosystem: public key without containing all the information of secret key. IACR eprint 2004/366, http://eprint.iacr.org.

[24] S. Tsujii, K. Tadaki and R. Fujioka. Proposal for piece in hand matrix ver.2: General concept for enhancing security of multivariate pulic key cryptosystem. IACR eprint 2006/051, http://eprint.iacr.org.

[25] S. Tsujii, K. Tadaki, R. Fujita M. Gotaishi and T. Kaneko. Security Enhancement of Various MPKCs by 2-layer Nonlinear Piece in Hand Method. *IEICE TRANS. Fundamentals*, Vol. E92-A, NO. 10, pages 2438-2447, 2009.

[26] L. Wang, B. Yang, Y. Hu and F. Lai. A Medium-Field Multivariate Public key Encryption Scheme. *CT-RSA 2006: The Cryptographers' Track at the RSA Conference 2006*, LNCS volume 3860, pages 132-149. Springer, 2006.

[27] H. Wang, H. Zhang, Z. Wang and M. Tang. Extended multivariate public key cryptosystems with secure encryption function. *SCIENCE CHINA Information Sciences*, June 2011 Vol. 54 No. 6: 1161-1171.