High Order Linearization Equation (HOLE) Attack on Multivariate Public Key Cryptosystems

Jintai Ding[1⋆], Lei Hu[2⋆⋆], Xuyun Nie[2], Jianyu Li[2], John Wagner[1]

[1] Department of Mathematical Sciences, University of Cincinnati, Cincinnati, OH, 45220, USA
[2] State Key Laboratory of Information Security, Graduate School of Chinese Academy of Sciences, Beijing 100049, China
ding@math.uc.edu, {hu, nxy04b, ljy}@is.ac.cn, wagnerjh@email.uc.edu

Abstract. In the CT-track of the 2006 RSA conference, a new multivariate public key cryptosystem, which is called the Medium Field Equation (MFE) multivariate public key cryptosystem, is proposed by Wang, Yang, Hu and Lai. We use the second order linearization equation attack method by Patarin to break MFE. Given a ciphertext, we can derive the plaintext within 2^{23} $\mathbb{F}_{2^{16}}$-multiplications, after performing once for any given public key a computation of complexity less than 2^{52}. We also propose a high order linearization equation (HOLE) attack on multivariate public key cryptosystems, which is a further generalization of the (first and second order) linearization equation (LE). This method can be used to attack extensions of the current MFE.

Keywords: multivariate public key cryptosystem, quadratic polynomial, algebraic cryptanalysis, high order linearization equation.

1 Introduction

For the last three decades, public key cryptosystems, as a revolutionary breakthrough in cryptography, have developed into an indispensable element of our modern communication system. For RSA and other number theory based cryptosystems, their security depends on the assumption about the difficulty of certain number theory problems, such as the Integer Prime Factorization Problem or the Discrete Logarithm Problem. However, due to the quantum computer attack by Shor [Sho99] and the demand for more efficient cryptosystems for small devices, there is a great challenge to build new public key cryptosystems, in particular ones that could survive future attacks utilizing quantum computers [PQ].

⋆ The work of this author is partially supported by the Charles Phelps Taft Research Center and the Alexander von Humboldt Foundation.
⋆⋆ The work of this author is supported by NSFC (60573053) and National 863 Project of China (2006AA01Z416).

One such research direction utilizes a set of multivariate polynomials over a finite field, in particular, quadratic polynomials, as the public key of the cipher, which are called multivariate public key cryptosystems (MPKC). This method is based on the proven theorem that solving a set of multivariate quadratic polynomial equations over a finite field generally is an NP-complete problem. Note, however, this does not guarantee that these new cryptosystems are secure. In the last decade, there has been tremendous amount of work devoted to this area. In 2004, one such cryptosystem, Sflash [ACDG03] [PCG01a], was accepted as one of the final selections in the New European Schemes for Signatures, Integrity, and Encryption: IST-1999-12324. A more efficient family of Rainbow signature schemes was also proposed in the last years [DS05] [YC05] [WHLCY05].

In the development of MPKC, one particular interesting and important new area is the development of the so-called algebraic attack. This new attack method started from the linearization equation (LE) attack by Patarin [Pat95], which is used to break Matsumoto-Imai cryptosystems. A linearization equation is an equation in the form: $\sum a_{ij}u_iv_j + \sum b_iu_i + \sum c_jv_j + d = 0$, where the u_i are components of the plaintext and the v_j are components of the ciphertext.

Later, Patarin, Courtois, Shamir, and Kipnis generalized this method by multiplying high order terms $u_1^{\alpha_1} \cdots u_n^{\alpha_n}$ of the plaintext variables but using only linear terms of ciphertext variables (v_j), which is called the XL method [CKPS00]. The method is closely related to the new Gröbner basis method by Faugere [Fau99] [AFIKS04]. Furthermore, this new algebraic method was used to attack symmetric ciphers like AES and others [CPi02]. One can see that algebraic attacks are becoming increasingly important in cryptography.

Another generalization of LE also by Patarin [Pat96,PCG01a,C00], which is not as well-known, is the type of equations in the form:

$$\sum a_{ijk}u_iv_jv_k + \sum b_{ij}u_iv_j + \sum c_iu_i + \sum d_{jk}v_jv_k + \sum e_jv_j + f = 0.$$

As a further extension, we propose to call the equations that use high order terms of the ciphertext variables (v_j) while using only linear terms of plaintext variables (u_i), high order linearization equations (HOLE). The total degree of the highest order of the ciphertext variables (v_j) is called the order of the HOLE and the equation above is thus called a second order linearization equation (SOLE). For any MPKC, if we can derive such equations, then for any given ciphertext, we can insert it into the HOLEs, producing linear equations satisfied by the plaintext and these equations can be used to attack the system.

It turns out that the SOLEs can be used efficiently to break the Medium Field Equation (MFE) multivariate public key cryptosystem proposed by Wang, Yang, Hu and Lai in the CT-track of the 2006 RSA conference [WYH06].

MFE is an encryption scheme. Many encryption schemes of MPKC have been proposed, and many of them have been broken, for example, the TTM cryptosystem family [Moh99] [GC00] [CM01] [DS03a] [DS03b] [MCY04]. A very different direction goes along the idea started by Matsumoto and Imai [MI88], which can be generally called the "Big Field" idea.

Given a multivariate public key cryptosystem, the public key is defined as a map over the vector space $\mathbb{K}^n$, where $\mathbb{K}$ is a small finite field with q elements. However from the theory of finite fields, $\mathbb{K}^n$ can also be identified with a "big" finite field $\mathbb{E}$, which is a degree n extension of $\mathbb{K}$. That is, there is a standard $\mathbb{K}$-linear vector space isomorphism that identifies $\mathbb{E}$ with $\mathbb{K}^n$. The idea of the "Big Field" is that we can find a map, say ϕ_2, that is easy to invert on $\mathbb{E}$. Under the isomorphism we can build a map $\tilde{\phi_2}$: $\mathbb{K}^n \to \mathbb{K}^n$ as:

$$\tilde{\phi_2}(u_1, ..., u_n) \mapsto (g_1(u_1, ..., u_n), \cdots, g_n(u_1, ..., x_n)).$$

Then we use ϕ_1 and ϕ_3, two randomly chosen invertible affine linear maps over $\mathbb{K}^n$ which are the key part of the private key to "hide" ϕ_2. The public key is given by

$$\begin{aligned} &\bar{\phi_2}(u_1, ..., u_n) = \phi_3 \circ \tilde{\phi_2} \circ \phi_1(u_1, ..., u_n) \\ &= (h_1(u_1, ..., u_n), h_2(u_1, ..., u_n), \cdots, h_n(u_1, ..., u_n)). \end{aligned}$$

The Matsumoto-Imai (MI) cryptosystem was broken by Patarin [Pat95], and later Patarin developed the HFE cryptosystem [Pat96]. The only difference between HFE and the MI is that they choose different ϕ_2. Currently the more promising cryptosystems are new variants of the MI and the HFE through Oil-Vinegar constructions and internal perturbations [Din04a] [FGS05] [DG05] [DS04a]. The idea to put several "big fields" together to build a cryptosystem is also used [MI88] [Pat96]. The new MFE cryptosystem [WYH06] uses what the designers call "Medium Field Encryption". The non-linear critical part of the public key is a function over an extension of the base field $\mathbb{K}$ of degree smaller than what would be called the "big field". Another key difference between MFE and HFE is that MFE uses functions derived from a matrix structure while the MI and the HFE use only polynomials of a single variable.

In the attack on MFE, we first use second order linearization equations (SOLEs), which we derive from the special algebraic structure of the crucial nonlinear map in MFE. This is the most essential step in our attack. Any given ciphertext can be inserted into the SOLEs to produce a set of equations linear in the plaintext variables. Solutions to these equations are finally plugged back into the original public key polynomial equations, providing a set of new quadratic equations that could be easily solved. The complexity of our break is less than 2^{52} one-time multiplications over $\mathbb{K}$ for any given public key, and the practical complexity of recovering a ciphertext is less than 2^{23} $\mathbb{K}$-operations.

The current MFE is based on matrices of size 2×2 and one may extend it to a construction using matrices of bigger size. The HOLEs of higher order can be extended to attack such an extension of the current MFE and the order of HOLE corresponds exactly to the size of the matrices.

We organize the paper as follows. We introduce the MFE cryptosystem in Section 2, and present our attack in Section 3. In Section 4, we discuss the connection of HOLE with the XL method. In the final section, we present the conclusion.

2 MFE Public Key Cryptosystem

Let $\mathbb{K}$ be a finite field, generally $\mathbb{F}_{2^{16}}$. Let $\mathbb{L}$ be its degree r extension field; $\mathbb{L}$ is considered the "Medium Field". In MFE, we always identify $\mathbb{L}$ with $\mathbb{K}^r$ by a $\mathbb{K}$-linear isomorphism $\pi : \mathbb{L} \to \mathbb{K}^r$. Namely we take a basis of $\mathbb{L}$ over $\mathbb{K}$, $\{\theta_1, \cdots, \theta_r\}$, and define π by $\pi(a_1\theta_1 + \cdots + a_r\theta_r) = (a_1, \cdots, a_r)$ for any $a_1, \cdots, a_r \in \mathbb{K}$. It is natural to extend π to two $\mathbb{K}$-linear isomorphisms $\pi_1 : \mathbb{L}^{12} \to \mathbb{K}^{12r}$ and $\pi_2 : \mathbb{L}^{15} \to \mathbb{K}^{15r}$.

A private key of MFE consists of two invertible affine transformations ϕ_1 and ϕ_3; and ϕ_1 is defined on $\mathbb{K}^{12r}$, and ϕ_3 on $\mathbb{K}^{15r}$. Let $\phi_2 : \mathbb{L}^{12} \to \mathbb{L}^{15}$ be the central nonlinear quadratic map of MFE. Note ϕ_2 is fixed except for the three components Q_1, Q_2, and Q_3, which have randomly chosen coefficients. The corresponding public key is $15r$ quadratic polynomials $h_1(u_1, ..., u_{12r}), h_2(u_1, ..., u_{12r}), \cdots$, and $h_{15r}(u_1, ..., u_{12r})$ given by

$$(h_1(u_1, ..., u_{12r}), \cdots, h_{15r}(u_1, ..., u_{12r})) = \phi_3 \circ \pi_2 \circ \phi_2 \circ \pi_1^{-1} \circ \phi_1(u_1, ..., u_{12r}). \quad (1)$$

Let $\phi_2(X_1, \cdots, X_{12}) = (Y_1, \cdots, Y_{15})$. The expressions of the Y_i are given by

$$\begin{cases} Y_1 = X_1 + X_5X_8 + X_6X_7 + Q_1; \\ Y_2 = X_2 + X_9X_{12} + X_{10}X_{11} + Q_2; \\ Y_3 = X_3 + X_1X_4 + X_2X_3 + Q_3; \\ Y_4 = X_1X_5 + X_2X_7; \qquad Y_5 = X_1X_6 + X_2X_8; \\ Y_6 = X_3X_5 + X_4X_7; \qquad Y_7 = X_3X_6 + X_4X_8; \\ Y_8 = X_1X_9 + X_2X_{11}; \qquad Y_9 = X_1X_{10} + X_2X_{12}; \\ Y_{10} = X_3X_9 + X_4X_{11}; \qquad Y_{11} = X_3X_{10} + X_4X_{12}; \\ Y_{12} = X_5X_9 + X_7X_{11}; \qquad Y_{13} = X_5X_{10} + X_7X_{12}; \\ Y_{14} = X_6X_9 + X_8X_{11}; \qquad Y_{15} = X_6X_{10} + X_8X_{12}. \end{cases} \quad (2)$$

Here Q_1, Q_2, and Q_3 form a triple (Q_1, Q_2, Q_3) which is a triangular map from $\mathbb{K}^{3r}$ to itself as follows. Let $\pi(X_1) = (x_1, \cdots, x_r)$, $\pi(X_2) = (x_{r+1}, \cdots, x_{2r})$, $\pi(X_3) = (x_{2r+1}, \cdots, x_{3r})$, and let $q_i \in \mathbb{K}[x_1, \cdots, x_{i-1}]$ for $2 \le i \le 3r$. Then

$$\begin{cases} Q_1(X_1) = \sum_{i=2}^{r} q_i(x_1, \cdots, x_{i-1})\theta_i, \\ Q_2(X_1, X_2) = \sum_{i=r+1}^{2r} q_i(x_1, \cdots, x_{i-1})\theta_{i-r}, \\ Q_3(X_1, X_2, X_3) = \sum_{i=2r+1}^{3r} q_i(x_1, \cdots, x_{i-1})\theta_{i-2r}. \end{cases}$$

The q_i can be any randomly chosen quadratic polynomials. A specific "tower"-structural choice for them is given in §5 of [WYH06].

The encryption of MFE is the evaluation of public key polynomials, namely given a plaintext $(u_1, \cdots, u_{12r})$, its ciphertext is

$$(v_1, \cdots, v_{15r}) = (h_1(u_1, \cdots, u_{12r}), \cdots, h_{15r}(u_1, \cdots, u_{12r})).$$

Given a valid ciphertext $(v_1, \cdots, v_{15r})$, the decryption of MFE is to calculate in turn $\phi_1^{-1} \circ \pi_1 \circ \phi_2^{-1} \circ \pi_2^{-1} \circ \phi_3^{-1}(v_1, \cdots, v_{15r})$. Here the point is how to invert ϕ_2, its basic idea is to use the triangular structure of ϕ_2. Relating to our cryptanalysis, the method of computing ϕ_2^{-1} is listed as follows, see §4.2 and Appendix B of [WYH06].

Write $X_1, \cdots, X_{12}, Y_4, \cdots, Y_{15}$ as six 2×2 matrices:

$$\begin{aligned} &M_1 = \begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix}, M_2 = \begin{pmatrix} X_5 & X_6 \\ X_7 & X_8 \end{pmatrix}, M_3 = \begin{pmatrix} X_9 & X_{10} \\ X_{11} & X_{12} \end{pmatrix}, \\ &Z_3 = M_1 M_2 = \begin{pmatrix} Y_4 & Y_5 \\ Y_6 & Y_7 \end{pmatrix}, Z_2 = M_1 M_3 = \begin{pmatrix} Y_8 & Y_9 \\ Y_{10} & Y_{11} \end{pmatrix}, \\ &Z_1 = M_2^T M_3 = \begin{pmatrix} Y_{12} & Y_{13} \\ Y_{14} & Y_{15} \end{pmatrix}. \end{aligned} \tag{3}$$

Then

$$\begin{cases} \det(M_1) \cdot \det(M_2) = \det(Z_3), \\ \det(M_1) \cdot \det(M_3) = \det(Z_2), \\ \det(M_2) \cdot \det(M_3) = \det(Z_1). \end{cases}$$

When M_1, M_2, and M_3 are all invertible, we can get values of $\det(M_1)$, $\det(M_2)$, and $\det(M_3)$ from $\det(Z_1)$, $\det(Z_2)$, and $\det(Z_3)$, for instance, $\det(M_1) = \big(\det(Z_2) \cdot \det(Z_3)/\det(Z_1)\big)^{1/2}$. The square root operation is easy to handle over a field of characteristic 2.

With values of $\det(M_1)$, $\det(M_2)$, and $\det(M_3)$, we solve the following triangular map over $\mathbb{K}^{3r}$

$$\begin{cases} Y_1 = X_1 + Q_1 + \det(M_2) \\ Y_2 = X_2 + Q_2 + \det(M_3) \\ Y_3 = X_3 + Q_3 + \det(M_1) \end{cases} \tag{4}$$

to get in turn $x_1, \cdots, x_r, x_{r+1}, \cdots, x_{2r}, x_{2r+1}, \cdots$, and x_{3r}. Thus, we recover X_1, X_2, and X_3. From $X_1X_4 + X_2X_3 = \det(M_1)$ we then get X_4 provided $X_1 \neq 0$. The $X_5, \cdots, X_{12}$ are consequently solved from the 4th to 11th equations of (2). Appendix B of [WYH06] presents a method of computing the X_i in the case when $X_1 = 0$. It is slightly easier than the case of $X_1 \neq 0$.

If there is a non-invertible matrix among M_1, M_2, and M_3, then the decryption mentioned above will not work. This decryption failure exists in MFE [WYH06]. We call a plaintext **singular** if its corresponding M_1, M_2, and M_3 are not all invertible, otherwise it is called **nonsingular.** The ciphertext of a nonsingular plaintext is called a nonsingular ciphertext.

It is easy to prove that the ratio of singular plaintexts to all possible plaintexts is at most $4|\mathbb{L}|^{-1}$; when $\mathbb{L} = \mathbb{F}_{2^{64}}$, the ratio is at most 2^{-62}, which is quite small. In the next section we only consider how to recover nonsingular ciphertext.

There are two typical instances of MFE proposed by the designers of MFE.

1) MFE-1, where $\mathbb{K} = \mathbb{F}_{2^{16}}$ and $r = 4$. The public key has 60 polynomials with 48 variables.

2) MFE-1′, where $\mathbb{K} = \mathbb{F}_{2^{16}}$ and $r = 5$. The public key has 75 polynomials and 60 variables.

There is also a mini-version of MFE (MFE-0) using $\mathbb{K} = \mathbb{F}_{2^8}$ and $r = 4$, which has the same number of polynomials and variables as MFE-1.

3 Cryptanalysis on MFE

The designers of MFE noted they should avoid the linearization attack of Patarin (§6.2 of [WYH06]), and this is indeed the case. In the design of MFE, the last equations of (2) in MFE are defined such that $Z_1 = M_2^T M_3$ (see (2)), instead of $Z_1 = M_2 M_3$. Otherwise we would have $Z_3 M_3 = M_1 Z_1$ $(= M_1 M_2 M_3)$; this would have produced linearization equations for the cryptosystem. However we can use the HOLE, in particular the SOLE, to attack this cryptosystem.

3.1 Second Order Linearization Equations

First, we will show algebraically why the MFE has second order linearization equations. Denote by M^* the associated matrix of a square matrix; for $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, its associated matrix is $M^* = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. From (3), we have

$$Z_3 = M_1 M_2, \qquad Z_2 = M_1 M_3. \tag{5}$$

From these, we can derive

$$M_3 M_3^* M_1^* M_1 M_2 = M_3 (M_1 M_3)^* (M_1 M_2) = M_3 Z_2^* Z_3,$$

$$M_3 M_3^* M_1^* M_1 M_2 = (M_3 M_3^*)(M_1 M_1^*) M_2 = \det(M_3)\det(M_1) M_2 = \det(Z_2) M_2,$$

and hence,

$$M_3 Z_2^* Z_3 = \det(Z_2) M_2, \tag{6}$$

that is,

$$\begin{pmatrix} X_9 & X_{10} \\ X_{11} & X_{12} \end{pmatrix} \begin{pmatrix} Y_{11} & -Y_9 \\ -Y_{10} & Y_8 \end{pmatrix} \begin{pmatrix} Y_4 & Y_5 \\ Y_6 & Y_7 \end{pmatrix} = (Y_8 Y_{11} - Y_9 Y_{10}) \begin{pmatrix} X_5 & X_6 \\ X_7 & X_8 \end{pmatrix}. \tag{7}$$

Expanding (7), we get four equations of the form

$$\sum a'_{ijk} X_i Y_j Y_k = 0, \tag{8}$$

which hold for any corresponding pair $(X_1, \cdots, X_{12}, Y_1, \cdots, Y_{15})$. For any non-singular plaintext, if we substitute all the Y_i by its corresponding value in the four equations of the form (8) derived from (7), we would get four linear equations with X_i as its . These four equations are linearly independent, since the matrices $\begin{pmatrix} Y_{11} & Y_9 \\ Y_{10} & Y_8 \end{pmatrix}$ and $\begin{pmatrix} Y_4 & Y_5 \\ Y_6 & Y_7 \end{pmatrix}$ are invertible.

Substituting $(X_1, \cdots, X_{12}) = \pi_1^{-1} \circ \phi_1(u_1, \cdots, u_{12r})$ and $(Y_1, \cdots, Y_{15}) = \pi_2^{-1} \circ \phi_3^{-1}(v_1, \cdots, v_{15r})$ into (8), we get $4r$ equations of the form

$$\sum_i u_i \left(\sum_{j \le k} a_{ijk} v_j v_k + \sum_j b_{ij} v_j + c_i \right) + \sum_{j \le k} d_{jk} v_j v_k + \sum_j e_j v_j + f = 0, \quad (9)$$

where the coefficients $a_{ijk}, b_{ij}, c_i, d_{jk}, e_j, f \in \mathbb{K}$, and the summations are respectively over $1 \le i \le 12r$, $1 \le j \le k \le 15r$ and $1 \le j \le 15r$. These equations, which are linear in plaintext components u_i and quadratic in ciphertext components v_j, are **second order linearization equations (SOLEs)**. It is easy to show that when all the v_j are substituted by any nonsingular ciphertext, the $4r$ SOLEs derived from (9) become linearly independent linear equations in u_i.

Similarly to (6), we can deduce from (5) another equation

$$M_2 Z_3^* Z_2 = \det(Z_3) M_3, \quad (10)$$

or in its matrix form,

$$\begin{pmatrix} X_5 & X_6 \\ X_7 & X_8 \end{pmatrix} \begin{pmatrix} Y_7 & -Y_5 \\ -Y_6 & Y_4 \end{pmatrix} \begin{pmatrix} Y_8 & Y_9 \\ Y_{10} & Y_{11} \end{pmatrix} = (Y_4 Y_7 - Y_5 Y_6) \begin{pmatrix} X_9 & X_{10} \\ X_{11} & X_{12} \end{pmatrix}. \quad (11)$$

The $4r$ SOLEs resulted from (11) are clearly different from the ones corresponding to (9). Furthermore, we can show that the $8r$ SOLEs obtained from (9) and (11) are all linearly independent. However, we note that when the v_i in these $8r$ SOLEs derived from (7) and (11) are assigned any nonsingular ciphertext, we will get only $4r$ linearly independent linear equations in u_i. In other words, once the values of v_i are given, as linear equations in X_i, (10) is completely equivalent to (6), and one can deduce (10) directly from (6) and vice versa. One can see this by the fact that multiplying from the right the both sides of (6) by $Z_3^* Z_2 / \det(Z_2)$ (this is a constant invertible matrix if the y_i values are given) gives (10).

Now, it is obvious that there are more SOLEs. We apply the above trick that results (6) and (10) from (5) to obtain

$$M_2 (Z_1^T)^* Z_2^T = \det(Z_1) M_1^T, \quad (12)$$

$$M_1^T (Z_2^T)^* Z_1^T = \det(Z_2) M_2, \quad (13)$$

from $Z_2 = M_1 M_3$ and $Z_1 = M_2^T M_3$. We can also obtain

$$M_1^T (Z_3^T)^* Z_1 = \det(Z_3) M_3, \quad (14)$$

$$M_3 (Z_1)^* Z_3^T = \det(Z_1) M_1^T, \quad (15)$$

from $Z_3 = M_1 M_2$ and $Z_1 = M_2^T M_3$. It is not hard to check that the polynomial equations derived from (6), (10), and (12)-(15) in terms of X_i and Y_j are all linearly independent. Thus, we get at least $24r$ linearly independent SOLEs in u_i and v_i over $\mathbb{K}$.

To find all SOLEs, we need to evaluate sufficiently many plain/cipher-texts in (9) to get a system of linear equations on the $a_{ijk}, b_{ij}, \cdots, f$. Let s be the dimension of its solution space and $(a_{ijk}^{(l)}, b_{ij}^{(l)}, \cdots, f^{(l)})$, $1 \leq l \leq s$, be its s linearly independent solutions. As mentioned above, we know $s \geq 24r$. For attack purposes, we only need to do the computation to get all the SOLEs once for any given public key.

Similarly to the relation between (6) and (10), as linear equations in X_i, (12) is equivalent to (13), and (14) is equivalent to (15) provided that the Y_i are assigned a nonsingular ciphertext value.

In addition, we can show that if we are given the values of v_i of a nonsingular ciphertext, from the $24r$ linearly independent SOLEs we derived above, we will produce only $8r$ linearly independent linear equations in u_i. Write (12) in its matrix form:

$$\begin{pmatrix} X_5 & X_6 \\ X_7 & X_8 \end{pmatrix} \begin{pmatrix} Y_{15} & -Y_{14} \\ -Y_{13} & Y_{12} \end{pmatrix} \begin{pmatrix} Y_8 & Y_{10} \\ Y_9 & Y_{11} \end{pmatrix} = (Y_{12}Y_{15} - Y_{13}Y_{14}) \begin{pmatrix} X_1 & X_3 \\ X_2 & X_4 \end{pmatrix}, \quad (16)$$

which results in $4r$ SOLEs. Given the values of Y_i of a nonsingular ciphertext, the eight linear equations in X_i derived from (16) and (7) are linearly independent, because the coefficient matrix corresponding to the set of eight linear equations, with the four equations from (16) as the first four ones, is in the form $\begin{pmatrix} I * 0 \\ 0 \; I * \end{pmatrix}$, where each row is scaled by a factor $Y_8Y_{11} - Y_9Y_{10}$ or $Y_{12}Y_{15} - Y_{13}Y_{14}$ correspondingly, and I and 0 are respectively the identity matrix and the zero matrix of order 4. This matrix is clearly of rank 8. This shows that the s' introduced in the next subsection is at least $8r$. The reason that the other SOLEs will not produce any new linear equations on u_i for any given values of v_i of a nonsingular ciphertext is that when the Y_i are assigned a nonsingular value, (14) can be easily deduced from (6) and (12).

3.2 Ciphertext-only Attack

Now assume we have found a basis of the linear space of all SOLEs.
Given a ciphertext $(v'_1, \cdots, v'_{15r})$, our aim is to recover its plaintext $(u'_1, \cdots, u'_{12r})$. We plug the values of ciphertext $(v'_1, \cdots, v'_{15r})$ into the basis SOLEs:

$$\begin{cases} \sum\limits_i u_i \left(\sum\limits_{j \leq k} a_{ijk}^{(l)} v'_j v'_k + \sum\limits_j b_{ij}^{(l)} v'_j + c_i^{(l)} \right) + \sum\limits_{j \leq k} d_{jk}^{(l)} v'_j v'_k + \sum\limits_j e_j^{(l)} v'_j + f^{(l)} = 0 \\ 1 \leq l \leq s \end{cases} \quad (17)$$

giving us a linear system on $u_1, \cdots, u_{12r}$. Assume it has s' linearly independent solutions. From the previous subsection, we know $8r \leq s' \leq 12r$. We can represent s' of the variables $u_1, \cdots, u_{12r}$ by linear affine expressions of the remaining $t := 12r - s'$. Let $w_1, \cdots, w_t$ be these t variables.

Substitute these s' linear expressions into the original public key polynomials to get $15r$ new quadratic polynomials $\widetilde{h_1}(w_1, ..., w_t), \widetilde{h_2}(w_1, ..., w_t), \cdots$, and $\widetilde{h_{15r}}(w_1, ..., w_t)$.

Let S be the solution space of (17). Let Y'_i and Z'_i be components and matrices corresponding to the given $(v'_1, \cdots, v'_{15r})$, namely

$$(Y'_1, \cdots, Y'_{15}) = \pi_2^{-1} \circ \phi_3^{-1}(v'_1, \cdots, v'_{15r}),$$

$$Z'_3 = \begin{pmatrix} Y'_4 & Y'_5 \\ Y'_6 & Y'_7 \end{pmatrix}, Z'_2 = \begin{pmatrix} Y'_8 & Y'_9 \\ Y'_{10} & Y'_{11} \end{pmatrix}, Z'_1 = \begin{pmatrix} Y'_{12} & Y'_{13} \\ Y'_{14} & Y'_{15} \end{pmatrix}.$$

We have found a basis of all SOLEs and each SOLE is a linear combination of this basis. This fact holds when the variables v_i in the equations are substituted by v'_i. Applying this fact to (7), we know the four resulting equations in u_i from

$$M_3(Z'_2)^* \cdot Z'_3 = \det(Z'_2) M_2 \tag{18}$$

are all linear combinations of the equations in (17). In other words, (18) holds on S. Let $P_{23} = \det(Z'_2)\,((Z'_2)^* \cdot Z'_3)^{-1}$; then $M_3 = M_2 P_{23}$. P_{23} is a constant matrix dependent only on the ciphertext.

Now we have that $M_2^T M_3 = Z_1$ always holds on $\mathbb{K}^{12r}$; therefore, we have that $M_3^T M_3 = M_3^T M_2 P_{23} = Z_1 P_{23}$ holds on S. That is,

$$\begin{pmatrix} X_9^2 + X_{11}^2 & X_9X_{10} + X_{11}X_{12} \\ X_9X_{10} + X_{11}X_{12} & X_{10}^2 + X_{12}^2 \end{pmatrix} = \begin{pmatrix} Y_{12} & Y_{13} \\ Y_{14} & Y_{15} \end{pmatrix} P_{23} \tag{19}$$

holds on S. Comparing the diagonal entries of the matrices in both sides of (19), we find $X_9^2 + X_{11}^2$ and $X_{10}^2 + X_{12}^2$ are linear combinations of the Y_i. Applying ϕ_1 and ϕ_3 to these combinations and utilizing the fact that squaring is a linear operation on a field of characteristic 2, we have, on S, the $2r$ expressions corresponding to $X_9^2 + X_{11}^2$ and $X_{10}^2 + X_{12}^2$ are of the form $\sum a'_i u_i^2 + b'$ and $\mathbb{K}$-linear combinations of $h_1(u_1, ..., u_{12r}), h_2(u_1, ..., u_{12r}), \cdots, h_{15r}(u_1, ..., u_{12r})$ and 1 (constant).

Thus, of linear combinations of $\widetilde{h_1}(w_1, ..., w_t), \cdots, \widetilde{h_{15r}}(w_1, ..., w_t)$ and 1, there must exist $2r$ which contain only squaring terms and a constant term and correspond to $X_9^2 + X_{11}^2$ and $X_{10}^2 + X_{12}^2$.

It is easy to solve the following linear system on the $\widetilde{a_i}$ and $\widetilde{b_j}$:

$$\begin{cases} \sum\limits_{i=1}^{15r} \widetilde{a_i} \widetilde{h_i}(w_1, ..., w_t) + \sum\limits_{j=1}^{t} \widetilde{b_j} w_j^2 + \widetilde{c} = 0 \\ \forall w_1, ..., w_t \in \mathbb{K} \end{cases} \tag{20}$$

Essentially, this is to solve a linear equation system whose coefficients are the coefficients of the cross-terms and linear terms of the $\widetilde{h_i}(w_1, ..., w_t)$.

Let $(\widetilde{a_1}^{(l)}, \cdots, \widetilde{a_{15r}}^{(l)}, \widetilde{b_1}^{(l)}, \cdots, \widetilde{b_t}^{(l)})$, $1 \le l \le p$, be a basis of the solutions of (20). Set

$$\begin{cases} \sum\limits_{j=1}^{t} \left(\widetilde{b_j}^{(l)}\right)^{1/2} w_j + \left(\sum\limits_{i=1}^{15r} \widetilde{a_i}^{(l)} v'_i + \widetilde{c}^{(l)}\right)^{1/2} = 0. \\ 1 \le l \le p \end{cases} \tag{21}$$

For each $(u_1, ..., u_{12r}) \in S$, its corresponding $(w_1, ..., w_t)$ satisfies (21). From (21) we can represent p of the variables $w_1, ..., w_t$ by the remaining $t-p$ linearly. Totally, $s'+p$ components of the plaintext vector $(u'_1, ..., u'_{12r})$ are represented linearly by the remaining $12r - s' - p$.

Note that we surely have $s'+p \geq 10r$, since the matrix of the coefficients on $X_1, X_2, \cdots, X_{12}$ of ten expansions in (16), (7), $(X_9^2+X_{11}^2)^{1/2}$, and $(X_{10}^2+X_{12}^2)^{1/2}$ is $\begin{pmatrix} I * 0 \\ 0\ I\ * \\ 0\ 0\ A \end{pmatrix}$, where $A = \begin{pmatrix} 1\,0\,1\,0 \\ 0\,1\,0\,1 \end{pmatrix}$, and the matrix is obviously of rank 10. In other words, solving two systems (17) and (21) eliminates at least $10r$ variables of the plaintext components. If $p = 0$, i.e., there is no nonzero linear combination of the $\widetilde{h_i}(w_1, ..., w_t)$ being of the form $\sum a'_i w_i^2 + b'$, then we must have $s' \geq 10r$ and after the first elimination (i.e., via (17)), the expressions corresponding to $X_9^2 + X_{11}^2$ and $X_{10}^2 + X_{12}^2$ are constants.

3.3 Finding the Plaintext

We substitute these linear expressions that result from solving (21), into $\widetilde{h_1}(w_1, ..., w_t), \cdots, \widetilde{h_{15r}}(w_1, ..., w_t)$ to get $15r$ new quadratic polynomials on $12r - s' - p\ (\leq 2r)$ variables. Denote them by $\widehat{h_1}, \cdots, \widehat{h_{15r}}$. Since $12r - s' - p$ is very small (at most 8 and 10 for MFE-1 and MFE-1′, respectively), in principle, we can use the Gröbner basis method to solve the system

$$\widehat{h_i} = v'_i, \quad \forall\ i = 1, \cdots, 15r \tag{22}$$

very easily to find the plaintext finally.

However, we know here that we start from $15r$ equations; therefore we expect to get many more than $2r$ (the number of variables) equations. This means we can solve it easily, for example, using the XL method [CKPS00]. In our experiments, this set of equations does turn out to be very easy to solve.

3.4 A Practical Attack Procedure, Its Complexity and Experimental Verification

Our attack can be divided into the following four steps:

Step 1 of the attack: *Find a basis of the linear space of the coefficient vectors* $(a_{ijk}, b_{ij}, \cdots, f)$ *of all SOLEs.*

As mentioned in §3.1, this is solving a system of linear equations obtained by evaluating sufficiently many plain/cipher-texts in (9). There are $\binom{12r+1}{1}\binom{15r+2}{2}$ monomials of the form $u_i^\alpha v_j^\beta v_k^\gamma$ on u_i and v_j $(\alpha, \beta, \gamma = 0$ or $1)$. This number is 92659 and 178486 for $r = 4$ and 5, respectively, and is somewhat large. Choosing a number of plain/cipher-text pairs slightly more than the number of unknowns, say 1000, we can completely find the solution space in general. The complexity is respectively $\frac{1}{2} \cdot 92659^3 \approx 2^{48.5} < 2^{49}$ and $\frac{1}{2} \cdot 178486^3 \approx 2^{51.34} < 2^{52}$ $\mathbb{F}_{2^{16}}$-multiplications using a naive Gaussian elimination.

This step is an one-time computation for any given public key. Let $(a_{ijk}^{(l)}, b_{ij}^{(l)}, \cdots, f^{(l)})$, $1 \leq l \leq s$, be a basis of the equation system.

Our computer experiments confirm that the dimension of SOLE is exactly $24r$, which is performed on the level of the Medium field $\mathbb{L}$ not on the small field K.

Step 2 of the attack: *Given a valid ciphertext* $(v'_1, \cdots, v'_{15r})$*, we plug it into (17) and solve the system of linear equations to obtain linear expressions of the remaining* $12r - s'$ *in terms of the other* s' *variables of the plaintext components.*

The complexity of this step is $15rs^2 < (15r)^3$, and is less than 2^{19}.

Substitute these linear expressions into the original public key polynomials to get new quadratic polynomials $\widetilde{h_1}(w_1, ..., w_t), \cdots$, and $\widetilde{h_{15r}}(w_1, ..., w_t)$.

Step 3 of the attack: *Solve the system (20) and obtain its solution basis* $(\widetilde{a_1}^{(l)}, \cdots, \widetilde{a_{15r}}^{(l)}, \widetilde{b_1}^{(l)}, \cdots, \widetilde{b_t}^{(l)})$, $1 \leq l \leq p$*. Then solve the system (21) to find expression of the* p *components of the plaintext by the remaining* $12r - s' - p$ *linearly.*

The complexity of solving (20) is $(15r+t)^3 < (30r)^3 < 2^{22}$, and that for (21) is $pt^2 < (15r)^3 < 2^{19}$.

Our computer experiments show that s' is indeed 8r and p is $2r$.

Step 4 of the attack: *Derive new public key polynomials* $(\widehat{h_1}, \cdots, \widehat{h_{15r}})$ *from the solutions of (21), solve the system (22) and finally obtain the value of* p *components of the plaintext by using a Gröbner base or a linearization method. Then we use the linear expressions on the remaining plaintext components derived in steps 2 and 3 to find the eliminated components.*

In 1000 experimental samples we have done, we find that after Step 3, the number of linearly independent quadratic equations are actually 20 for MFE-1. We solve them by finding a set of $2r$ linearly independent linear equations inside the space spanned by these equations. It takes almost no time.

Therefore the total attack complexity is less than 2^{52}. The complexity of the attack recovering the plaintext (steps 2, 3 and 4) is less than 2^{23}.

3.5 Experimental Results

We chose 10 different pairs of ϕ_1 and ϕ_3, for each of which we chose 100 different valid ciphertext for experiments. For all chosen ciphertexts, the attack successively found their corresponding plaintexts.

The time-consuming step of our attack is the first step. In our experiments, we randomly selected 92800 plain/cipher-text pairs and substituted them into the public key. Then the main work we will do is a Gaussian elimination on a 92800×92659 matrix on $\mathbb{F}_{2^{16}}$. The complexity of this process is less than 2^{52}. We estimate the time to do this Gaussian elimination will be about two years on a standard PC.

So, we performed our experiment on a DELL PowerEdge 7250, a mincom with 4 Itanium2 CPU and 32GB ECC fully buffered DIMM memory. The operating system we used was 64-bit Windows Server2003. We programmed the attack using VC++. Multiple threads can improve the efficiency of programs on a

computer with multiple CPU. In our experiments, we used four threads to deal with Gaussian elimination. And we designed a method which will be patented to speed up the multiplication on $\mathbb{F}_{2^{16}}$.

Our experiments showed that 282 hours and 6 minutes (11 days and 18 hours and 6 minutes) were required for the first step, which is an one time computation for any given public key. Only about 2 seconds were needed to execute the remaining steps.

For MFE-1, our experiments confirm that we can find 96 linearly independent SOLEs for a given valid public key in step 1. And we can eliminate 32 plaintext variables in step 2 and 8 plaintext variables in step 3, namely, $s' = 32$ and $p = 8$.

One more important point of our experiments is the fact that we actually used parallel computation (4 Itanium2 CPU) to speed up and accomplish the computation in a reasonable time, which, we thought, was impossible at the very beginning. This demonstrated that parallel computation, in particular, large scale parallel computation, could extend much further the limit of our computation capacity. We believe this is a direction that deserves serious consideration especially in practical attacks.

3.6 Extension of MFE and High Order Linearization Attack

The construction of MFE relies on the multiplicative structure of 2×2 matrices and it is not difficult to see that one can extend this construction in a straightforward way by using matrices of larger sizes $m \times m$, for example, 3×3 or 4×4, to build new MFE cryptosystems. For any such an construction using matrix of $m \times m$, it is not difficult to see that the m-th order LE can be applied to attack the cryptosystem. The fundamental reason behind is the formula that for any matrix Q of size $m \times m$, we know that

$$Q^{-1} = \frac{1}{det(Q)} Q^*,$$

where Q^* is the associated matrix of Q. In terms of algebraic formulas for $det(Q)$ and Q^*, we know that $det(Q)$ can be expressed as a degree m polynomial of the components Q_{ij} of Q and each component of Q^* can be expressed in terms of a degree $(m-1)$ polynomial of the components Q_{ij} of Q. With this and the formulas (6) and (10) and other similar formulas, we can see that, for such a case, the order m linearization equations exists and they can be used to attack such a system. Therefore the current design of MFE needs to increase m substantially to avoid such an attack.

4 The Connection of HOLE with XL

One important point we want to make is that the HOLE method is closely related to the XL method [CKPS00]. In particular one may also explore the possibility of combining these two algebraic methods together to develop additional techniques.

Assume we are given a system of equations $f_i(u_1, \cdots, u_n) = v'_i,\ 1 \le i \le m$. Let $U = (u_1, \cdots, u_n)$ and $g_i(U) = f_i(U) - v'_i$. For any nonnegative integral vector $\alpha = (\alpha_1, \cdots, \alpha_n)$, denote $u_1^{\alpha_1} \cdots u_n^{\alpha_n}$ by U^α. Similarly, for $\beta = (\beta_1, \cdots, \beta_m)$, denote $f_1^{\beta_1} \cdots f_m^{\beta_m}$ by F^β and $g_1^{\beta_1} \cdots g_m^{\beta_m}$ by G^β.

A variant of the XL method first translates the equation system above into another system of equations of the form: $\sum a_{\alpha,i} U^\alpha g_i(U) = 0$, where $1 \le i \le m$ and α are nonnegative integral vectors with small component sum (upper-bounded by some small integer D). Then define all terms $U^\alpha U^\gamma$ as new unknowns and solve the resulting linear equation system.

On the other hand, the HOLE method attempts to solve a system of equations of the form: $\sum_{i,\beta} a_{i,\beta} u_i G^\beta = 0$, where $1 \le i \le n$ and β are chosen small vectors. Since the $f_i(U)$ are equivalent to the $g_i(U)$ under affine transformations, the above system is equivalent to the form: $\sum_{i,\beta} b_{i,\beta} u_i F^\beta = 0$. Our attack presented in the previous section actually finds **identical** equations with the form above, and hence we can substitute F^β by $v_1'^{\beta_1} \cdots v_m'^{\beta_m}$ and get a linear system that the plaintext satisfies.

As a comparison, we find that if a HOLE with order D could be used to successfully attack a system by finding linear equations, then one should expect that the XL method should work as well. But the order of XL should be of degree $2D - 1$ (the total degree is $2D + 1$), because the v_i in general are of degree 2. From this consideration, we conclude that though HOLE definitely cannot be a replacement for the XL method. Yet there could be cases that the HOLE method would be much more efficient than XL. In one case we consider polynomials of degree $D+1$ (HOLE), while in the other case, we consider polynomials of degree $2D+1$ (XL). Another critical point is that when we use the HOLE method, the computation of HOLEs is performed only once for a given public key, then the HOLEs are used for any ciphertext; while the general XL algorithm needs to run its main part each time for different values of ciphertext. Thus one should think HOLE as a possibly more efficient alternative to XL, if it can work; and there would be cases that HOLE can work practically while the XL cannot.

More importantly, one may consider unifying the XL and HOLE methods. We may expect to efficiently solve the system of equations of the form:

$$\sum_{\alpha,\beta} a_{\alpha,\beta} U^\alpha G^\beta = 0. \tag{23}$$

From the point view of algebraic geometry, this definitely makes sense. But at this moment, we have not yet found any example where such a method could indeed be more efficient in an attack. Furthermore, one can expect that this method may be useful to attack other cryptosystems, such as symmetric ciphers.

5 Conclusion

In this paper, we use an extension of the linearization equation attack method of Patarin, which we call the high order linearization equation method, to break the

MFE multivariate public key cryptosystem in CT-RSA 2006. This shows that the high order linearization equation method is indeed an important algebraic attack method. For any multivariate public key cryptosystem, one should take into account this new method.

References

[ACDG03] Mehdi-Laurent Akkar, Nicolas T. Courtois, Romain Duteuil, and Louis Goubin. A fast and secure implementation of Sflash. In *PKC-2003, LNCS*, volume 2567, pages 267–278. Springer, 2003.

[AFIKS04] Gwénolé Ars and Jean-Charles Faugère and Hideki Imai and Mitsuru Kawazoe and Makoto Sugita Comparison between XL and Gröbner Basis Algorithms, *Asiacrypt 2004*, LNCS, V. 3329.

[MFSY05] M. Bardet, J-C. Fauge, B. Salvy and B-Y. Yang Asymptotic Behaviour of the Degree of Regularity of Semi-Regular Polynomial Systems MEGA 2005, Eighth International Symposium on Effective Methods in Algebraic Geometry, Porto Conte, Alghero, Sardinia (Italy), May 27th - June 1st, 2005, 15 pages.

[C00] Nicolas T. Courtois The security of hidden field equations (HFE) In C. Naccache, editor, Progress in cryptology, CT-RSA, LNCS, volume 2020, pages 266–281. Springer, 2001

[CKPS00] Nicolas Courtois, Alexander Klimov, Jacques Patarin, and Adi Shamir. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In B. Preenel, editor, *Advances in cryptology, Eurocrypt 2000, LNCS*, volume 1807, pages 392–407. Springer, 2000.

[CPi02] Nicolas Courtois, Josef Pieprzyk: Cryptanalysis of Block Ciphers with Overdefined Systems of Equations. ASIACRYPT 2002, LNCS 2501, 267-287, Springer 2002.

[CM01] J. Chen and T. Moh. On the Goubin-Courtois attack on TTM. *Cryptology ePrint Archive*, 72, 2001. http://eprint.iacr.org/2001/072.

[DH76] Whitfield Diffie and Martin Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[Din04a] Jintai Ding. A new variant of the Matsumoto-Imai cryptosystem through perturbation. In F. Bao, R. Deng, and J. Zhou, editors, *the 7th International Workshop on Practice and Theory in Public key Cryptography, Singapore, (PKC'04), LNCS*, volume 2947, pages 305–318. Springer, 2004.

[DG05] Jintai Ding and Jason Gower Inoculating Multivariate Schemes Against Differential Attacks. Accepted for PKC-2006, IACR eprint 2005/255.

[DS03a] J. Ding and D. S. Schmidt. A common defect of the TTM cryptosystem. In *Proceedings of the technical track of the ACNS'03, ICISA Press*, pages 68–78, 2003. http://eprint.iacr.org.

[DS03b] J. Ding and D. S. Schmidt. The new TTM implementation is not secure. In H. Niederreiter K.Q. Feng and C.P. Xing, editors, *Proceedings of International Workshop on Coding, Cryptography and Combinatorics (CCC 2003)*, pages 106–121, 2003.

[DS04a] Jintai Ding, and D. S. Schmidt Cryptanalysis of HFEV and the internal perturbation of HFE. The 8th International Workshop on Practice and Theory in Public key Cryptography, Jan. 2005, Switzerland (PKC'05), Lecture Notes in Computer Sciences, volume 3386, pages 288-301 Springer, 2005.

[DS05] Jintai Ding, and D. S. Schmidt Rainbow, a new multivariate public key signature scheme. The Third International Conference of Applied Cryptography and Network Security (ACNS 2005), New York, June 7-10, 2005, Lecture Notes in Computer Science 3531, Page 164-175, Springer, 2005.

[Fau99] Jean-Charles Faugère A new efficient algorithm for computing Gröbner bases (F_4), Journal of Pure and Applied Algebra, V. 139, P. 61-88, June 199.

[FGS05] P.-A. Fouque, L. Granboulan, and J. Stern. Differential Cryptanalysis for Multivariate Schemes Advances in Cryptology - EUROCRYPT 2005, Lecture Notes in Computer Science 3494 Springer 2005, Page 341-353.

[GC00] L. Goubin and N. Courtois. Cryptanalysis of the TTM cryptosystem. *LNCS, Springer Verlag*, 1976:44–57, 2000.

[KS99] Aviad Kipnis and Adi Shamir. Cryptanalysis of the HFE public key cryptosystem by relinearization. In M. Wiener, editor, *Advances in crytology – Crypto '99, LNCS*, volume 1666, pages 19–30. Springer, 1999.

[MI88] 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.

[Moh99] T. 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.

[MCY04] T.Moh and J.M.Chen and Boyin Yang Building Instances of TTM Immune to the Goubin-Courtois Attack and the Ding-Schmidt Attack. IACR eprint 2004/168, http://eprint.iacr.org.

[NES] NESSIE. European project IST-1999-12324 on New European Schemes for Signature, Integrity and Encryption. http://www.cryptonessie.org.

[Pat95] 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, 1995.

[Pat96] 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.

[Pat97] J. Patarin. The oil and vinegar signature scheme. *Dagstuhl Workshop on Cryptography, September 1997*, 1997.

[PCG01a] Jacques Patarin, Nicolas Courtois, and Louis Goubin. Flash, a fast multivariate signature algorithm. In *LNCS*, volume 2020, pages 298–307. Springer, 2001.

[PGC98] Jacques Patarin, Louis Goubin, and Nicolas Courtois. C^*_{-+} and HM: variations around two schemes of T. Matsumoto and H. Imai. In K. Ohta and D. Pei, editors, *ASIACRYPT'98, LNCS*, volume 1514, pages 35–50. Springer, 1998.

[PQ] PQCrypto 2006: International Workshop on Post-Quantum Cryptography http://postquantum.cr.yp.to/

[RSA78] Ronald Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public key cryptosystems. *ACM*, 21(2):120–126, 1978.

[Sho99] Peter Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.*, 41(2):303–332, 1999.

[WHLCY05] Lih-Chung Wang and Yuh-Hua Hu and Feipei Lai and Chun-Yen Chou and Bo-Yin Yang, Tractable Rational Map Signature, Public Key Cryptosystems 2005, LNCS 3386, Springer, P. 244-257.

[WYH06] Lih-Chung Wang, Bo-yin Yang, Yuh-Hua Hu and Feipei Lai, A Medium-Field Multivariate Public key Encryption Scheme, CT-RSA 2006: The Cryptographers' Track at the RSA Conference 2006, LNCS 3860, 132-149, Springer, 2006.

[YC05] B. Yang and J. Chen. Building Secure Tame-like Multivariate Public key Cryptosystems–The New TTS. Information Security and Privacy: 10th Australasian Conference–ACISP 2005, LNCS 3574, 2005, Springer, P. 518-531.