

A MORE SECURE MFE MULTIVARIATE PUBLIC KEY ENCRYPTION SCHEME*

Xin Wang[†]

*School of Telecommunications Engineering, Xidian University
Xi'an, 710071, China
wangxin@mail.xidian.edu.cn*

Feng Feng

*Department of Applied Mathematics and Applied Physics, Xi'an Institute of Posts and Telecommunications
Xi'an, 710121, China
fengf@xiyou.edu.cn*

Xinmei Wang

*State Key Lab. of Integrated Service Networks State, Xidian University
Xi'an, 710071, China
xmwang@xidian.edu.cn*

Qi Wang

*College of Electrical Engineering, Guangxi University
Nanning, 530004, China
314421549@qq.com*

In 2007 PKC conference, Ding, et al use the second order linearization equation attack method to break what be called MFE multivariate public key encryption scheme, and also proposed a high order linearization equation attack on multivariate public key cryptosystems. To resist high order linearization equation attack, we present an enhanced MFE encryption scheme in this article. The improved scheme has public key polynomials of degree four and operates on smaller field. Then we give some discussion, and security analysis show that the new scheme is more security.

Keywords: Public Key Cryptography; Multivariate; Cryptanalysis; MFE; HOLE.

1. Introduction

The problem of developing new public key cryptosystem had occupied the cryptographic research fields for the last thirty decades. Several recent public key systems use multivariate polynomial systems of equations, particularly quadratic polynomials, instead of number-theoretic constructions. The public operation in such a system is to evaluate the system output when given an input value. The private operation is to compute the pre-

* This paper is a revised and extended version of the paper presented in ICCIT08, November 11-13, 2008 at Busan, South Korea.

[†] Correspondence should be addressed to this author.

image of a given value. This research is based the observation that solving a system of modular multivariate polynomial equations over any finite field is NP-complete [Garay and Johnson (1979)]. And no quantum polynomial algorithm has been found to solve it.

In the development of multivariate public key cryptosystems, algebraic attack is an important area of research, which comes from the linearization equation attack by Patarin [Patarin (1995)]. This attack method refers to any technique that ends with a solving system. A linearization equation is an equation of such form: $\sum a_{ij}u_i v_j + \sum b_i u_i + \sum c_j v_j + d = 0$, where u_i are plaintext variables and v_j are ciphertext variables. Another generalization of linearization equation [Patarin et al. (2001)] has the following form: $\sum a_{ijk}u_i v_j v_k + \sum b_{ij}u_i v_j + \sum c_i u_i + \sum d_{jk}v_j v_k + \sum e_j v_j + f = 0$. As a further extension, Ding, et al propose to call the equations with high order terms of the ciphertext variables while only linear terms of plaintext variables "high order linearization equation (HOLE)" [Ding et al. (2007)]. The total degree of the highest order of the ciphertext variables is called the order of the HOLE; the equation above is thus called a second order linearization equation (SOLE). And they use the SOLEs to break the MFE multivariate public key cryptosystem proposed by Wang et al in the CT-track of the 2006 RSA conference [Wang et al. (2006)].

In this article, we modify the central map of the MFE and present an improved scheme. Substitute for a system of quadratic polynomials which operated in a big extension field, we improve the degree properly over a smaller extension field. Security analysis show the enhanced scheme is more secure, and we also make comparison between the two schemes. In addition, since the enhanced scheme has public key polynomials of degree four, which will lead larger size of public key, then we present a slight and immature idea to alleviate this problem.

2. MFE Public Key Cryptosystem

Let K be a finite field and L be its degree r extension field, generally $r = 4$ or 5 , which is so-called the "Medium Field". In MFE, we identify L with K^r by a K -linear isomorphism $\pi : L \rightarrow K^r$. Take a basis $(\theta_1, \dots, \theta_r)$ of L over K , and define $\pi(a_1\theta_1 + \dots + a_r\theta_r) = (a_1, \dots, a_r)$ for any $a_1, \dots, a_r \in K$. Then it is natural to extend π to two K -linear isomorphism $\pi_1 : L^{12} \rightarrow K^{12r}$ and $\pi_2 : L^{15} \rightarrow K^{15r}$.

Take $12 X_i$ and $15 Y_i$ on extension field L , and arrange $X_1, X_2, \dots, X_{12}, Y_4, Y_5, \dots, Y_{15}$ into 2×2 matrices:

$$M_1 = \begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix}, M_2 = \begin{pmatrix} X_5 & X_6 \\ X_7 & X_8 \end{pmatrix}, M_3 = \begin{pmatrix} X_9 & X_{10} \\ X_{11} & X_{12} \end{pmatrix}.$$

Define

$$M_1 M_2 = \begin{pmatrix} Y_4 & Y_5 \\ Y_6 & Y_7 \end{pmatrix}, M_1 M_3 = \begin{pmatrix} Y_8 & Y_9 \\ Y_{10} & Y_{11} \end{pmatrix}, M_2^T M_3 = \begin{pmatrix} Y_{12} & Y_{13} \\ Y_{14} & Y_{15} \end{pmatrix}.$$

Then let $\phi_2(X_1, \dots, X_{12}) = (Y_1, \dots, Y_{15})$. The expressions of Y_i are represented by

$$\begin{aligned} Y_1 &= X_1 + X_5 X_8 + X_6 X_7 + Q_1; \\ Y_2 &= X_2 + X_9 X_{12} + X_{10} X_{11} + Q_2; \\ Y_3 &= X_3 + X_1 X_4 + X_2 X_3 + Q_3; \\ Y_4 &= X_1 X_5 + X_2 X_7; \quad Y_5 = X_1 X_6 + X_2 X_8; \\ Y_6 &= X_3 X_5 + X_4 X_7; \quad Y_7 = X_3 X_6 + X_4 X_8; \\ Y_8 &= X_1 X_9 + X_2 X_{11}; \quad Y_9 = X_1 X_{10} + X_2 X_{12}; \\ Y_{10} &= X_3 X_9 + X_4 X_{11}; \quad Y_{11} = X_3 X_{10} + X_4 X_{12}; \\ Y_{12} &= X_5 X_9 + X_7 X_{11}; \quad Y_{13} = X_5 X_{10} + X_7 X_{12}; \\ Y_{14} &= X_6 X_9 + X_8 X_{11}; \quad Y_{15} = X_6 X_{10} + X_8 X_{12}. \end{aligned}$$

The $\phi_2 : \mathbb{L}^{12} \rightarrow \mathbb{L}^{15}$ is called the central quadratic map, and is fixed except for three components Q_1, Q_2, Q_3 , which are randomly chosen quadratic polynomials. The triple (Q_1, Q_2, Q_3) form a triangular map from \mathbb{K}^{3r} to itself. The private key of MFE is composed of two invertible affine transformations $\phi_1 : w \rightarrow x = M_1 w + c_1$ and $\phi_3 : y \rightarrow z = M_3 y + c_3$, which are randomly chosen invertible affine transformations respectively defined on \mathbb{K}^{12r} and \mathbb{K}^{15r} , plus parameters in Q_i needed for taking its inverse. The public key is composed of the three maps as $\overline{\phi_2} = \phi_3 \circ \phi_2 \circ \phi_1 : \mathbb{K}^n \rightarrow \mathbb{K}^m$. The corresponding $15r$ public key quadratic polynomials are expressed by $(h_1(u_1, \dots, u_{12r}), \dots, h_{15}(u_1, \dots, u_{12r})) = \phi_3 \circ \pi_2 \circ \phi_2 \circ \pi_1^{-1} \circ \phi_1(u_1, \dots, u_{12r})$. This process can also be written as $\overline{\phi_2} : x \in K^n \xrightarrow{\phi_1} x' \xrightarrow{\phi_2} y' \xrightarrow{\phi_3} y \in K^m$

Given a plaintext (u_1, \dots, u_{12r}) , the encryption of MFE is to evaluate the public key polynomials. The decryption is to calculate in turn $\phi_1^{-1} \circ \pi_1 \circ \phi_2^{-1} \circ \pi_2^{-1} \circ \phi_3^{-1}$ for a valid ciphertext (u_1, \dots, u_{15r}) . Here the critical point is invert ϕ_2^{-1} , which can be solved by using the triangular structure of ϕ_2 . The method of computing the X_i is presented by Appendix B of [Wang et al. (2006)].

3. HOLE Attack

Let

$$Z_3 = M_1 M_2, Z_2 = M_1 M_3,$$

we have

$$\begin{aligned} M_3 Z_2^* Z_3 &= M_3 (M_1 M_3)^* (M_1 M_2) \\ &= M_3 M_3^* M_1^* M_1 M_2 \\ &= (M_3 M_3^*) (M_1^* M_1) M_2 \\ &= \det(Z_2) M_2 \end{aligned}$$

that is,

$$M_3 Z_2^* Z_3 = \det(Z_2) M_2.$$

When both Z_i and M_i are replaced by X_i and Y_i , and expanded, four equations of the following form are given by

$$\sum l_{ijk} X_i Y_j Y_k = 0,$$

which hold for any corresponding pair $(X_1, \dots, X_{12}, Y_1, \dots, Y_{15})$. Substituting $(X_1, \dots, X_{12}) = (u_1, \dots, u_{12r})$ and $(Y_1, \dots, Y_{15}) = (v_1, \dots, v_{15r})$ into the above equation, then we can get $4r$ equations of the form

$$\sum_i u_i \left(\sum_{j \leq k} a_{ijk} v_j v_k + \sum_j b_{ij} v_j + c_i \right) + \sum_{j \leq k} d_{jk} v_j v_k + \sum_j e_j v_j + f = 0 \quad (1)$$

the coefficients $a_{ijk}, b_{ij}, c_i, d_{jk}, e_j, f \in \mathbb{K}$. These equations are SOLEs.

In ciphertext-only attack, we firstly evaluate sufficient many plain/cipher-texts to get a system of linear equations on the coefficients a_{ijk}, \dots, f and find linearly independent SOLEs linear in u_i . Then, given cipher components, we can reduce the plaintext variables u_i by Gauss Elimination method. Substitute these linear expressions into the original public key polynomials. When the number of the variables is small enough to solving the equations by using Gröbner basis method, we recover the plaintext finally.

4. Enhanced MFE scheme

4.1. Construction of Central Map

Similarly, \mathbf{K} is the base field ($\text{charF} = 2$), \mathbf{L} is the extension field, and two \mathbf{K} -linear isomorphism are π_1 and π_2 . The private key of the new scheme still are ϕ_1, ϕ_3 , and parameters in \mathcal{Q}_i .

Let

$$M_1 = \begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix}, M_2 = \begin{pmatrix} X_5 & X_6 \\ X_7 & X_8 \end{pmatrix}, M_3 = \begin{pmatrix} X_9 & X_{10} \\ X_{11} & X_{12} \end{pmatrix}.$$

$$X_2 X_3 M_1 M_2 = \begin{pmatrix} Y_4 & Y_5 \\ Y_6 & Y_7 \end{pmatrix}, X_1 X_2 M_1 M_3 = \begin{pmatrix} Y_8 & Y_9 \\ Y_{10} & Y_{11} \end{pmatrix}, \quad (2)$$

$$X_1 X_3 M_2^T M_3 = \begin{pmatrix} Y_{12} & Y_{13} \\ Y_{14} & Y_{15} \end{pmatrix},$$

then the corresponding central map $\phi_2 : \mathbf{L}^{12} \rightarrow \mathbf{L}^{15}$ is as follows:

$$\begin{aligned} Y_1 &= X_1 + X_1^2(X_9 X_{12} + X_{10} X_{11}) + \mathcal{Q}_1; \\ Y_2 &= X_2 + X_2^2(X_1 X_4 + X_2 X_3) + \mathcal{Q}_2; \\ Y_3 &= X_3 + X_3^2(X_5 X_8 + X_6 X_7) + \mathcal{Q}_3; \\ Y_4 &= X_2 X_3(X_1 X_5 + X_2 X_7); \quad Y_5 = X_2 X_3(X_1 X_6 + X_2 X_8); \\ Y_6 &= X_2 X_3(X_3 X_5 + X_4 X_7); \quad Y_7 = X_2 X_3(X_3 X_6 + X_4 X_8); \\ Y_8 &= X_1 X_2(X_1 X_9 + X_2 X_{11}); \quad Y_9 = X_1 X_2(X_1 X_{10} + X_2 X_{12}); \\ Y_{10} &= X_1 X_2(X_3 X_9 + X_4 X_{11}); \quad Y_{11} = X_1 X_2(X_3 X_{10} + X_4 X_{12}); \\ Y_{12} &= X_1 X_3(X_5 X_9 + X_7 X_{11}); \quad Y_{13} = X_1 X_3(X_5 X_{10} + X_7 X_{12}); \\ Y_{14} &= X_1 X_3(X_6 X_9 + X_8 X_{11}); \quad Y_{15} = X_1 X_3(X_6 X_{10} + X_8 X_{12}). \end{aligned}$$

4.2. Encryption and Decryption

4.2.1. Encryption

Encryption is to compute the value of public key polynomials by substituting the plaintext components.

4.2.2. Decryption

Step1: From (2) we have

$$\begin{aligned} X_2^2 X_3^2 \det M_1 \det M_2 &= Y_4 Y_7 + Y_5 Y_6; \\ X_1^2 X_2^2 \det M_1 \det M_3 &= Y_8 Y_{11} + Y_9 Y_{10}; \\ X_1^2 X_3^2 \det M_2 \det M_3 &= Y_{12} Y_{15} + Y_{13} Y_{14}. \end{aligned}$$

When M_1, M_2, M_3 are all invertible, none of X_1, X_2, X_3 is zero, and knowing Y_4, \dots, Y_{15} , we can get values of $X_1^2 \det M_3, X_3^2 \det M_2$, and $X_2^2 \det M_1$ as follows,

$$\begin{aligned} X_1^2 \det M_3 &= \sqrt{(Y_8 Y_{11} + Y_9 Y_{10})(Y_{12} Y_{15} + Y_{13} Y_{14})(Y_4 Y_7 + Y_5 Y_6)^{-1}}; \\ X_3^2 \det M_2 &= \sqrt{(Y_4 Y_7 + Y_5 Y_6)(Y_{12} Y_{15} + Y_{13} Y_{14})(Y_8 Y_{11} + Y_9 Y_{10})^{-1}}; \\ X_2^2 \det M_1 &= \sqrt{(Y_4 Y_7 + Y_5 Y_6)(Y_8 Y_{11} + Y_9 Y_{10})(Y_{12} Y_{15} + Y_{13} Y_{14})^{-1}}. \end{aligned}$$

The square root operation is easy to handle over a $\text{char} = 2$ field.

Step2: Then substitute $X_1^2 \det M_3, X_2^2 \det M_1$ and $X_3^2 \det M_2$ into

$$\begin{aligned} Y_1 &= X_1 + X_1^2 \det M_3 + Q_1; \\ Y_2 &= X_2 + X_2^2 \det M_1 + Q_2; \\ Y_3 &= X_3 + X_3^2 \det M_2 + Q_3, \end{aligned}$$

we can find X_1, X_2 and X_3 in a triangular manner.

Step3: From $X_2^2 \det M_1$, we can obtain $\det M_1$, then X_4 .

Step4: Let $A = (X_1 X_2 X_3)^{-1} (\det M_1)^{-1}$, then

$$\begin{aligned}
 X_5 &= A(X_1 X_4 Y_4 + X_1 X_2 Y_6); \\
 X_6 &= A(X_1 X_4 Y_5 + X_1 X_2 Y_7); \\
 X_7 &= A(X_1 X_3 Y_4 + X_1^2 Y_6); \\
 X_8 &= A(X_1 X_3 Y_5 + X_1^2 Y_7); \\
 X_9 &= A(X_3 X_4 Y_8 + X_2 X_3 Y_{10}); \\
 X_{10} &= A(X_3 X_4 Y_9 + X_2 X_3 Y_{11}); \\
 X_{11} &= A(X_3^2 Y_8 + X_1 X_3 Y_{10}); \\
 X_{12} &= A(X_3^2 Y_9 + X_1 X_3 Y_{11}).
 \end{aligned}$$

5. Analysis and Comparison

5.1. Security Analysis

HOLE Attack: We show how the new MFE to resist the SOLE attack. Such as (1) in MFE, the equation has degree two in cipher components v_i while linear in plain components v_i . Hence, we consider the formula which include product of some two elements among Z_i , Z_i^* and Z_i^T . Without loss of generality, suppose the expression on left side of equality is Z_2^* and Z_3 . Expanding, we get $X_1^2 X_2 X_3 M_3^* M_1^* M_1 M_2$. Note the foot note goes all over from 1 to 3. If the right side only has Z_2 (or $\det Z_2, Z_2^*$, and Z_2^T), we should at least plus X_3 and M_2 . This will lead to non-linear in X_i . So, no SOLEs can be found.

Rank Attacks: Rank attacks contain the High Rank and Low Rank. These attacks are mainly against all TPM and some other tame-like systems [Yang and Chen(2005)]. In these attacks, the quadratic parts are associated with symmetric matrices. The attackers try to recover the private key by finding linear combinations of matrices with a given specific rank. However, the central and public polynomials in the enhanced MFE have degree four, which have not efficient expressions of symmetric matrices. Therefore these attacks are not feasible for our scheme.

Patarin Relations Attack for C^* : In original MFE, the matrix products are arranged $M_1 M_2$, $M_1 M_3$, and $M_2^T M_3$, which aims to avoid Patarin Relations. There is also no Patarin Relation in the enhanced system.

Gröbner Bases: Gröbner Bases is a well-known way of solving polynomials. The classical algorithm is Buchberger's algorithm for computing Gröbner bases [Courtois et al. (2000)]. The algorithm orders all the monomials and eliminates the top monomial by combining two equations with appropriate polynomial coefficients, and until only one

variable remains, then solves the univariate polynomial equation. Computing the Gröbner basis of a system of m polynomials equations of maximal degree d in n variables has time complexity $m^3 d^{o(n^3)}$ [Caniglia et al. (1988)]. Gröbner base techniques do not usually benefit from the fact that the number of equations exceeds the number of variables, since they proceed by sequentially eliminating a single monomial from a particular pair of equations. So, current Gröbner-based methods cannot be used to cryptanalyze the enhanced MFE effectively.

Patarin's IP Approach: Patarin et al proposed an attack method for fixed central map schemes in [Patarin (1996)]. Since there are variable parameters in the central equation, the IP attack is not applicable.

5.2. Size of Key

Let $n = 12r$ variables and $m = 15r$ equations in system of public key polynomials, the private key is the coefficients in ϕ_1, ϕ_3 and Q_i for a total of $n^2 + m^2$ elements of \mathbb{K} . The public key comprise about $(mn^4)/4!$ coefficients of $\overline{\phi_2}$ for the enhanced MFE, while about $mn^2/2$ for the original MFE. Unfortunately the size of public key of the new scheme is larger than that of the original MFE. However, besides we take smaller value of parameter r , if we can also manage to make the public key polynomials be sparse polynomials, then the size of public key can be reduced greatly. For example, whether can we set some restrictions on affine transformation parts?

5.3. Discussion

The character of field in MFE scheme is usually 2, and the extension of field is implemented as "tower" degree-two extensions. We have a recursive definition for $\text{GF}(2^8)^{2^i}$. With a proper choice of α , we have $\text{GF}(2^8)^{2^{i-1}} = \text{GF}(2^8)^{2^{i-1}}[x]/(x^2 + x + \alpha)$.

The multiplication and inversion are

$$\begin{aligned} (ax + b)(cx + d) &= [(a + b)(c + d) + bd]x + [ac\alpha + bd], \\ (ax + b)^{-1} &= (ax + a + b)(ab + b^2 + a^2\alpha), \end{aligned}$$

where the addition is the bitwise XOR, and the multiplication of expressions of a, b, c, d , and α are done in $\text{GF}(2^8)^{2^{i-1}}$. As the more the number of extensions, the higher the computation. $\text{GF}(2^8)$ multiplications are three times faster than $\text{GF}(2^{16})$ multiplications, twenty times faster than $\text{GF}(2^{32})$. For the original MFE, the suggested parameters are $r = 4$ or 5 , $\mathbb{K} = \text{GF}(2^8)$ or $\text{GF}(2^{16})$, then corresponding \mathbb{L} is at least $\text{GF}(2^{32})$. The public key polynomials of the enhanced MFE are of degree four, so

we can use even smaller base field \mathbf{K} and its extension field \mathbf{L} . For instance, we can take $r = 2$ or 3 , and $\mathbf{K} = \text{GF}(2^8)$ or even $\text{GF}(2^4)$.

By the way, since the enhanced MFE has public key polynomials of degree four, this will obviously increase the encryption time. However, after we actually test, we find it doesn't cost much more time comparing with the original MFE scheme with the same parameters.

6. Conclusion

MFE multivariate encryption scheme uses medium sized field extensions, which makes it faster than previous schemes. However, it suffers a major security weakness due to structure of itself. In this paper, we present a more secure MFE scheme to resist the HOLE attack. The enhanced system has a set of polynomials of degree four, hence a larger size of public key. While, we present some thoughts to alleviate this problem, besides take smaller value of parameters. Certainly researches for systems of higher degree are still far from enough. There still need amount of work devoted to this area.

Acknowledgments

The first author will wish to thank Prof. Xinmei Wang for his constant understanding and support. This work was supported by the National Natural Science Foundation of China (No.60503010) and the Education Department of Shaanxi Province of China (No.08JK432).

References

- Caniglia, L., Galligo, A. (1988). Some New Effectivity Bounds in Computational Geometry. *Lecture Notes in Computer Science*, 357: 131–151.
- Courtois, N., Klimov, A. (2000). Efficient algorithms for solving overdefined systems of multivariate polynomial equations. *Lecture Notes in Computer Science*, 1807: 392–407.
- Ding, J., Hu, L. (2007). High order linearization equation (hole) attack on multivariate public key cryptosystems. *Lecture Notes in Computer Science*, 4450: 233–248.
- Garay, M. and Johnson, D. (1979). *Computers and intractability—a guide to the theory of NP-Completeness*, 1st edn. W.H. Freeman and Company, San Francisco.
- Patarin, J. (1995). Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88. *Lecture Notes in Computer Science*, 963: 248–261.
- Patarin, J. (1996). Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. *Lecture Notes in Computer Science*, 1070: 33–48.
- Patarin, J., Courtois, N. (2001). Flash, a fast multivariate signature algorithm. *Lecture Notes in Computer Science*, 2020: 298–307.
- Wang, L. C., Yang, B. Y. (2006). A Medium-Field Multivariate Public key Encryption Scheme. *Lecture Notes in Computer Science*, 3860: 132–149.
- Yang, B. Y. and Chen, J. M. (2005). Rank Attacks and Defence in Tame-Like Multivariate PKC's. *Lecture Notes in Computer Science*, 3574: 518–531.