Cryptanalysis of Novel Extended Multivariate Public Key Cryptosystem with Invertible Cycle

Gang Lu[1], Linyuan Xue[1], Xuyun Nie[1,2,3] and Zhiguang Qin[1,3]

(Corresponding author: Xuyun Nie)

School of Information and Software Engineering & University of Electronic Science and Technology of China[1]

Section 2, North Jianshe Road, Chengdu 610054, China

(Email: xynie@uestc.edu.cn)

State Key Laboratory of Information Security & Institute of Information Engineering[2]

Network and Data Security Key Laboratory of Sichuan Province[3]

(Received Dec. 1, 2016; revised and accepted Mar. 31, 2017)

Abstract

In 2016, Qiao *et al.* proposed a novel extended multivariate public key cryptosystem (EMC) to enhance the security of multivariate public key cryptosystem. They applied it on Matsumoto-Imai (MI) encryption scheme and claimed that the enhanced MI scheme can be secure against Linearization Equation (LE) attack. Through analysis, we found that the enhanced MI scheme satisfied Quadratization Equations (QE). After finding all the quadratization equations, we can recover the plaintext corresponding to a valid ciphertext of the enhanced MI scheme.

Keywords: Extended Multivariate Public Key Cryptosystem; Invertible Cycle; Multivariate Cryptography; Quadratization Equation

1 Introduction

In recent years, more and more researches have been made on the quantum computer. Once large-scale quantum computers are successfully built, the traditional public key cryptosystems such as RSA and ElGamal were no longer secure [19, 25]. The study of Post-quantum cryptography is urgent. Multivariate public key cryptosystem (MPKC) is one of promising alternative public key cryptosystem. The security of the MPKC is depended on the difficulty of solving systems of randomly chosen multivariate nonlinear polynomial equations over finite fields. Up to now, quantum computers do not appear to have advantage over the traditional computers to handle with this problem.

From 1988, many cryptosystems have been proposed in MPKCs, such as Matsumoto-Imai (MI) cryptosystem[15], Oil-Vinegar signature scheme [14, 22], Hidden Field Equation cryptosystem (HFE) [21], Tamed Transformation Method (TTM) [16], Medium Field Equation (MFE) cryptosystem [26] etc. But most of them are not secure. Hence, many security enhancement methods have been put forward, for example, Plus/Minus [23], Internal perturbation [4, 6], Piece in Hand method [13] etc. All of these methods are subjected to different levels of attacks [7, 8, 11, 12, 17, 18].

In 2016, Qiao *et al.* [24] proposed an idea named novel Extended Multivariate public key Cryptosystems(EMCs), which introduce nonlinear invertible transformations to enhance the security of defective MPKCs. They used three different nonlinear invertible transformations, invertible cycle, tame transformation and special oil and vinegar, and applied them on MI scheme. The original MI scheme was broken by Patarin [20] using Linearization Equation(LE) attack. Three enhanced MI schemes can resist LE attack.

In this paper, we focus on the enhanced MI scheme with invertible cycle. MI scheme satisfied LEs of form

$$\sum a_{ij}x_iy_j + \sum b_ix_i + \sum c_jy_j + d = 0, \qquad (1)$$

where x_i are the plaintext variables and y_j are the ciphertext variables. In the enhanced MI scheme with invertible cycle, they only applied a quadratic map on plaintext variables before performing MI encryption function. So, this scheme would satisfied a type of equation named Quadratization Equation(QE) of form

$$\sum a_{ijk}x_ix_jy_k + \sum b_{ij}x_iy_j + \sum c_iy_i + \sum d_{ij}x_ix_j + \sum e_ix_i + f = 0.$$

After finding all QEs for a given public key, substitute a valid ciphertext into these QEs, we can derive a set of quadratic equations on plaintext variables. Combining these quadratic equations with the public key and the valid ciphertext, we can recover the corresponding plaintext easily by Gröbner bases method.

This paper is organized as follows. In Section 2, we give some necessary fundamental notion and a brief description of the EMC with invertible cycle. Then, we present theoretical analysis and experimental results of our QE attack in Section 3. Finally, a conclusion was made in Section 4.

2 Preliminaries

2.1 General Structure of MPKC

Let m, n are two positive integers and $k = GF(q)$ is a finite filed. $\bar{F} : k^n \rightarrow k^m$ is built as a composition of three maps:

$$\bar{F} = L_1 \circ F \circ L_2$$

where $F : k^n \rightarrow k^m$, named central map, is an invertible map. $L_1 : k^m \rightarrow k^m$ and $L_2 : k^n \rightarrow k^n$ are two invertible affine maps used to hide the structure of F.

The public key of MPKC consists of a set of multivariate quadratic polynomials over a finite field, which is the expression of map $\bar{F}$, that is

$$\begin{aligned} (y_1, \cdots, y_m) &= \bar{F}(x_1, \cdots, x_n) \\ &= L_1 \circ F \circ L_2(x_1, \cdots, x_n) \\ &= (\bar{f}_1, \cdots, \bar{f}_m), \end{aligned}$$

where $\bar{f}_1, \cdots, \bar{f}_n \in k[x_1, \cdots, x_n]$ are a set of nonlinear polynomials. The private keys are L_1 and L_2.

2.2 Direct attack

The direct attack to recover plaintext is to find a solution by solving the following system

$$\begin{cases} y'_1 = \bar{f}_1(x_1, \ldots, x_n) \\ \vdots \\ y'_m = \bar{f}_m(x_1, \ldots, x_n) \end{cases} \quad (2)$$

where $\bar{f}_i$ $(1 \leq i \leq m)$ are the components of a given public key $\bar{F}$ and $\boldsymbol{y'} = (y'_1, \ldots, y'_m)$ is a ciphertext under this public key. A straightforward way to solve this system is Gröbner basis [1] method and its variants $\mathbf{F}_4$ [9] and $\mathbf{F}_5$ [10]. According to [2], the complexity of $\mathbf{F}_5$ is bounded by

$$O\left(\binom{n + d_{reg}}{n}^{\omega}\right)$$

where n is the number of the plaintext variables, d_{reg} is the degree of regularity in Gröbner basis method and $2 \leq \omega \leq 3$.

2.3 Matsumoto-Imai Scheme

MI [15] scheme was proposed by Matsumoto and Imai in 1988. Let $k = GF(q)$ is a finite filed with characteristic 2, and K is a degree n extension of k. Let $\phi : K \rightarrow k^n$ is a standard k-linear isomorphism between K and k^n as follow:

$$\phi(a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}) = (a_0, a_1, \cdots, a_{n-1}).$$

Choose θ $(0 < \theta < n)$ such that $gcd(q^\theta + 1, q^n - 1) = 1$ and define the map $\widetilde{F}$ over K by $\widetilde{F}(X) = X^{q^\theta + 1}$.

The condition of θ ensure that $\widetilde{F}$ is an invertible map. Indeed, if t is an integer such that $t(1 + q^\theta) = 1 \bmod (q^n - 1)$, then $\widetilde{F}^{-1}$ is simply $\widetilde{F}^{-1} = X^t$.

The MI scheme uses $F(x_1, \cdots, x_n) = \phi \circ \widetilde{F} \circ \phi^{-1}(x_1, \cdots, x_n) : k^n \rightarrow k^n$ as its central map. Let L_1 and L_2 be two invertible affine transformations over k^n. The MI encryption map was defined as follows

$$\bar{F}(x_1, \cdots, x_n) = L_1 \circ F \circ L_2(x_1, \cdots, x_n) = (\bar{f}_1, \cdots, \bar{f}_n).$$

where $\bar{f}_1, \cdots, \bar{f}_n \in k[x_1, \cdots, x_n]$.

The public keys of MI are n polynomials, $(\bar{f}_1, \cdots, \bar{f}_n)$, and private keys are (L_1, L_2, θ).

2.4 Linearization Equation

The linearization equation(LE) is put forward by Patarin in 1995 [20] to break MI scheme.

In general, the form of a linearization equation given by

$$\sum_{i=1}^{n} a_i x_i A_i(y_1, \cdots, y_m) + B(y_1, \cdots, y_m) + c = 0,$$

where $x_i, (1 \leq i \leq n)$ are plaintext variables, $y_i, (1 \leq i \leq n)$ are ciphertext variables, $A_i, (1 \leq i \leq n)$ and B are polynomial functions with respect to the ciphertext variables.

It is obvious that LE is linear on plaintext variables. In other words, given a valid ciphertext $(y_1, \cdots, y_m)$ and substituted it into LE, LE will become a linear polynomial equation on plaintext variables.

We usually refer to the maximum degree of ciphertext variables as the order of the LE.

For example, the first order linearization equation (FOLE) is given by

$$\sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} x_i y_j + \sum_{i=1}^{m} b_i y_i + \sum_{i=1}^{n} c_i x_i + d = 0.$$

And the second order linearization equation (SOLE) is of form

$$\sum_{i=1}^{n} \sum_{j=i}^{m} \sum_{k=j}^{m} a_{ijk} x_i y_j y_k + \sum_{i=1}^{m} \sum_{j=i}^{m} b_{ij} y_i y_j + \sum_{i=1}^{n} \sum_{j=i}^{m} c_{ij} x_i y_j + \sum_{i=1}^{m} d_i y_i + \sum_{i=1}^{n} e_i x_i + f = 0.$$

Linearization Equation can help us to do elimination on the system (2). For more information about LE attack, please refer to [5] and [17].

2.5 Quadratization Equation

The quadratization equation attack is proposed by Cao *et al.* [3] in 2010. The general form of a quadratization equation is

$$\sum_{i=1}^{n}\sum_{j=i}^{n} a_{ij}x_ix_jA_{ij}(y_1,\cdots,y_m)+\sum_{i=1}^{n} b_ix_iB_i(y_1,\cdots,y_m) +C(y_1,\cdots,y_m)+c=0$$

where $x_i,(1 \leq i \leq n)$ are plaintext variables, $y_i,(1 \leq i \leq n)$ are ciphertext variables, $A_{ij}(y_1,\cdots,y_m), B_i(y_1,\cdots,y_m)$ and $C(y_1,\cdots,y_m)$ are polynomial functions in the ciphertext variables.

We can find that substituting a valid ciphertext $(y_1,\cdots,y_m)$ into a QE, the QE will become a quadratic equation on plaintext variables. If we can derive a set of QEs, we will derive a set of quadratic equations on plaintext variables for a valid ciphertext. Combine these equations with the system (2), the degree of regularity might be lower down in solving the system (2) by Gröbner basis method. Hence, the complexity of solving the system (2) will be smaller. Similar to the LE, we can also define the order of the QE as the maximum degree of ciphertext variables.

The first order quadratization equation (FOQE), an example of QE, is given by

$$\sum_{i=1}^{n}\sum_{j=i}^{n}\sum_{k=j}^{m} a_{ijk}x_ix_jy_k+\sum_{i=1}^{n}\sum_{j=i}^{m} b_{ij}x_iy_j + \sum_{i=1}^{m} c_iy_i+\sum_{i=1}^{n}\sum_{j=i}^{n} d_{ij}x_ix_j+\sum_{i=1}^{n} e_ix_i+f=0.$$

2.6 The Novel EMC

The Novel EMC, designed by Qiao *et al.* [24], may serve as an security enhancement method both on encryption system and signature system. The main idea of the novel EMC is that they introduced a nonlinear invertible transformation L_3 and applied it on the plaintext variables before the original encryption map work, namely, as in Equation (3):

$$\begin{aligned}\widetilde{F}(x_1,\cdots,x_n) &= \bar{F}\circ L_3(x_1,\cdots,x_n)\\ &= L_1\circ F\circ L_2\circ L_3(x_1,\cdots,x_n).\end{aligned} \quad (3)$$

where $(x_1,\cdots,x_n)\in k^n$, $k=GF(q)$.

The public key of the novel EMC is the expression of map $\widetilde{F}$ and the private keys are L_1, L_2 and L_3.

In [24], they chose three types of nonlinear invertible transformation L_3, invertible cycle, tame transformation and special oil and vinegar. In the following parts of this paper, we only give cryptanalysis of the novel EMC with invertible cycle.

The L_3 as invertible cycle is described as follows.

Let μ is an invertible map on positive integer, given by

$$\mu:\{1,\cdots,n\}\to\{1,\cdots,n\}:\mu(i)=\begin{cases}1 & \text{for } i=n\\ i+1 & \text{otherwise}\end{cases}$$

For $n\geq 2$, let $L_3:(x_1,\cdots,x_n)\to(t_1,\cdots,t_n)$ be a nonlinear transformation over k^n, defined as Equation (4):

$$\begin{cases} t_1=\begin{cases} c_1x_1x_2 & \text{for } n \text{ odd}\\ c_1x_1^qx_2 & \text{for } n \text{ even}\end{cases},\\ t_i=c_ix_ix_{\mu(i)} \text{ for } 2\leq i\leq n\end{cases} \quad (4)$$

Remark. *Due to* $(x_1,\cdots,x_n)\in k^n$ *and* $k=GF(q)$, $x_i^q=x_i$. *When* n *is an even,* L_3 *is not invertible because that from (4), we can derive* $x_1=\frac{c_2c_4\cdots c_nt_1t_3\cdots t_{n-1}}{c_1c_3\cdots c_{n-1}t_2t_4\cdots t_n}\cdot x_1$, *that is, we can not derive* x_1 *from* L_3. *Hence, the map* L_3 *is not invertible when* n *is an even. So we consider only the case* n *is an odd.*

The public keys of the novel EMC with invertible cycle are a set quartic polynomials. More detail about process of encryption and decryption please refer to [24].

Practical Parameters. In [24], the authors chose MI encryption scheme as the original MPKC and they recommended $k=GF(2^{16})$, and $n=27$.

3 Cryptanalysis of Novel EMC

Although the enhanced MI scheme with invertible cycle can resist linearization equations attack, the design of the L_3 based on "Invertible Cycle" will bring new security hazards to the scheme. Since it is vulnerable to quadratization equation attack, it appears that L_3, at some level, is not an appropriate method to raise the security of the original scheme.

3.1 Quadratization Equations

As we know, the original scheme MI satisfies the first order linearization equation. So the ciphertext variables $y_i,(1\leq i\leq n)$ and the intermedium variables $t_i,(1\leq i\leq n)$ satisfy the first order linearization equation, namely,

$$\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}t_iy_j+\sum_{i=1}^{n} b_iy_i+\sum_{i=1}^{n} c_it_i+d=0. \quad (5)$$

Substituting Equation (4) into Equation (5), Equation (5) will change into the following equation:

$$\sum_{i=1}^{n}\sum_{j=i}^{n}\sum_{k=1}^{n} a_{ijk}x_ix_jy_k+\sum_{i=1}^{n}\sum_{j=1}^{n} b_{ij}x_iy_j+\sum_{i=1}^{n} c_iy_i +\sum_{i=1}^{n}\sum_{j=i}^{n} d_{ij}x_ix_j+\sum_{i=1}^{n} e_ix_i+f=0 \quad (6)$$

Equation (6) is exactly a Quadratization Equation. To continues our attack, we need find out all quadratization equations. This can be done as follows.

To find all quadratization equations equivalent to find a basis of the space V spanned by all QEs.

The number of coefficients in Equation (6) is equal to $\frac{(n+1)^2(n+2)}{2}$. Then we can randomly generate slightly over $\frac{(n+1)^2(n+2)}{2}$ plaintext/ciphertext pairs from the public key and substitute them into Equation (6). It is clear that we obtain a system of linear equation on unknown coefficients($a_{ijk}, b_{ij}, c_{ij}, d_i, e_i, f \in k$). Solving this system, we can get a basis of the solution space of this system, namely denote by Equation (7).

$$\begin{cases} \sum_{i=1}^{n}\sum_{j=i}^{n}\sum_{k=1}^{n} a_{ijk}^{(\rho)} x_i x_j y_k + \sum_{i=1}^{n}\sum_{j=i}^{n} b_{ij}^{(\rho)} x_i x_j \\ + \sum_{i=1}^{n}\sum_{j=i}^{n} c_{ij}^{(\rho)} x_i y_j + \sum_{i=1}^{n} d_i^{(\rho)} x_i \\ + \sum_{i=1}^{n} e_i^{(\rho)} y_i + f^{(\rho)} = 0 \\ 1 \leq \rho \leq D \end{cases} \tag{7}$$

where D is the dimension of the space V.

The process above relies merely on any given public key and it can be executed once for all cryptanalysis under that public key.

3.2 Ciphertext-only Attack

For a given cipheretext $\boldsymbol{y}' = (y_1', \cdots, y_n')$, substitute them into Equation (7) and do Gaussian elimination on it, we can get D' quadratic equations on variables, namely:

$$\begin{cases} \sum_{i=1}^{n}\sum_{j=i}^{n} \widetilde{a}_{ij}^{(\rho)} x_i x_j + \sum_{i=1}^{n} \widetilde{b}_i^{(\rho)} x_i + \widetilde{c}^{(\rho)} = 0 \\ 1 \leq \rho \leq D' \end{cases} \tag{8}$$

Combining these quadratic equations (8) with the system (2), we obtain a new system with $D' + n$ equations on plaintext variables. Then we solve the new system by Grönber basis algorithm. Experiments results show the corresponding plaintext can be recovered efficiently.

The algorithm of our attack can be seen in Algorithm 1.

Algorithm 1 Steps of QE Attack

1. **Input:** public key $\bar{F}$ of a MPKC, ciphertext $\boldsymbol{y}' \in k^n$
2. **Output:** corresponding plaintext $\boldsymbol{x}' \in k^n$
3. Determine the number of QE. It is $\frac{(n+1)^2(n+2)}{2}$;
4. Compute $N > \frac{(n+1)^2(n+2)}{2}$ plaintext/ciphertext pairs from the public key;
5. Substitute these plaintext/ciphertext pairs into Equation (6) and solve the resulted linear system;
6. Substitute the ciphertext $\boldsymbol{y}'$ into the quadratization equation found by last step and obtain D' quadratic equations on the plaintext variables.
7. Combine the quadratic equations with the system (2) to get a new system on plaintext variables. Solve the system directly via Gröbner Basis method.

3.3 Complexity and Experiments Results

In our attack, we set $k = GF(2^{16})$, $n = 27$, and the original MPKC is MI encryption scheme with $\theta = 4$. We chose randomly a valid ciphertext $\boldsymbol{y}' = (y_1', \cdots, y_n')$ and we want to find the corresponding plaintext $\boldsymbol{x}' = (x_1', \cdots, x_n')$.

In the first step, the number of coefficients in QE is equal to $\frac{(n+1)^2(n+2)}{2} = \frac{22736}{2} = 11368$. We computed 11370 plaintext/ciphertext pairs and substituted them into Equation (6) and did Gaussian Elimination on the resulted linear system. The complexity of $\frac{(n+1)^2(n+2)}{2}$ plaintext/ciphertext pairs generation is about $O(n^8)$. It is about 2^{38} for $n = 27$. And the complexity of the Gaussian Elimination is less than $(\frac{(n+1)^2(n+2)}{2})^3$, which is less than 2^{41} for $n = 27$. The dimension D of the space spanned by all QEs is equal to 26 in our experiments. This step is the most time consuming step in our attack. But this can be done once for a given public key.

In the second step, we substituted a valid ciphertext $\boldsymbol{y}' = (y_1', \cdots, y_n')$ into Equation (7) and we obtained 26 linear independent quadratic polynomials equation on plaintext variables.

In last step, combining the quadratic equations derived in step 2 with the system (2), we used Gröbner basis solving it and obtained the corresponding plaintext. Extensive experimental evidence has shown that the degree of regularity in solving the system is 3, hence the complexity of this step is $O\left(\binom{n+3}{n}^{\omega}\right)$, which is less than 2^{36} for $n = 27, 2 \leq \omega \leq 3$.

We performed our attack via Magma on a PC with Intel Core i5-3350P CPU 3.10 GHz and 4 GB of memory. In our experiments, we chose different parameters to illustrated our attack.

In Table 1, we showed the time of three stages under different parameters. T_1 indicates the time of generating $\frac{(n+1)^2(n+2)}{2}$ plaintext-ciphertext pairs from the public key. T_2 indicates the time of obtaining the quadratization equations. T_3 indicates the time of recovering the plaintext.

In Table 2, we compared the efficiency of our attack with the direct attack on the EMC with invertible cycle. The results showed that the degree of regularity in Gröbner basis method is reduced, so as to the execution time. In Table 2, $Time_Q$ and $d_{reg}(Q)$ express the time of recovering the plaintext and the degree of regularity in our attack and $Time_D$ and $d_{reg}(D)$ express the time and the degree of regularity in direct attack. According to the results in our experiments, the complexity of direct attack is $O\left(\binom{n+6}{n}^{\omega}\right)$, which is greater than the complexity of our attack, $O\left(\binom{n+3}{n}^{\omega}\right)$.

4 Conclusions

In this paper, we presented the cryptanalysis of the novel EMC with invertible cycle by Quadratization Equation attack. The same method can also be applied on the novel EMC with tame transformation. The emergence of Quadratization Equation can damage the security of

Table 1: The time comparison of practical attack under different parameters

n	**q**	D	D'	T_1 [**s**]	T_2[**s**]	T_3[**s**]	d_{reg}
21	2^8	20	20	25.265	131.922	0.36	3
21	2^{16}	20	20	27.487	719.523	0.92	3
23	2^8	22	22	41.969	279.891	0.813	3
23	2^{16}	22	22	48.875	1720.364	2.262	3
25	2^8	24	24	67.328	563.907	1.625	3
25	2^{16}	24	24	81.619	333.726	4.914	3
27	2^8	26	26	105.39	1105.969	3.625	3
27	2^{16}	26	26	114.037	6771.333	17.503	3

Table 2: The efficiency comparison of Quadratization attack & Direct attack

n	**q**	$Time_Q$	$d_{reg}(Q)$	$Time_D$	$d_{reg}(D)$
21	2^8	0.36	3	8.219	6
23	2^8	0.813	3	17.922	6
25	2^8	1.625	3	34.828	6
27	2^8	3.625	3	54.515	6

MPKCs. We should avoid it in designing MPKCs.

Acknowledgments

This work was supported by the National Key Basic Research Program of China under grant 2013CB834203, Major International (Regional) Joint Research Project of China National Science Foundation under grant No.61520106007 and The science and technology foundation of Sichuan Province (No.2016GZ0065). The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] W. W. Adams and P. Loustaunau, "An introduction to gröbner bases," *Graduate Studies in Mathematics*, vol. 60, no. 1, p. 167–168, 1994.

[2] M. Bardet, J. C. Faugere, and B. Salvy, "On the complexity of gröbner basis computation of semi-regular overdetermined algebraic equations," in *Proceedings of the International Conference on Polynomial System Solving*, pp. 71–74, 2004.

[3] W. W. Cao, X. Y. Nie, L. Hu, X. L. Tang, and J. T. Ding, "Cryptanalysis of two quartic encryption schemes and one improved MFE scheme," in *International Workshop on Post-Quantum Cryptography*, pp. 41–60, 2010.

[4] J. T. Ding, "A new variant of the Matsumoto-Imai cryptosystem through perturbation," in *International Workshop on Public Key Cryptography*, pp. 305–318, 2004.

[5] J. T. Ding, L. Hu, X. Y. Nie, J. Y. Li, and J. Wagner, "High order linearization equation (HOLE) atttack on multivariate public key cryptosystems," in *International Workshop on Public Key Cryptography*, pp. 233–248, 2007.

[6] J. T. Ding and D. Schmidt, "Cryptanalysis of HFEv and internal perturbation of HFE," in *International Workshop on Public Key Cryptography*, pp. 288–301, 2005.

[7] V. Dubois, P. A. Fouque, A. Shamir, and J. Stern, "Practical cryptanalysis of SFLASH," in *Annual International Cryptology Conference*, pp. 1–12. Springer, 2007.

[8] V. Dubois, L. Granboulan, and J. Stern, "Cryptanalysis of HFE with internal perturbation," in *International Workshop on Public Key Cryptography*, pp. 249–265, 2007.

[9] J. C. Faugere, "A new efficient algorithm for computing gröbner bases (F_4)," *Journal of Pure and Applied Algebra*, vol. 139, no. 1, pp. 61–88, 1999.

[10] J. C. Faugere, "A new efficient algorithm for computing gröbner bases without reduction to zero (F_5)," *Issac Proceedings of the International Symposium on Symbolic Algebraic Computation*, vol. 139, no. 1-3, pp. 75–83, 2004.

[11] J. C. Faugere, A. Joux, L. Perret, and J. Treger, "Cryptanalysis of the hidden matrix cryptosystem," in *International Conference on Cryptology and Information Security in Latin America*, pp. 241–254, 2010.

[12] P. A. Fouque, L. Granboulan, and J. Stern, "Differential cryptanalysis for multivariate schemes," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 341–353, 2005.

[13] R. Fujita, K. Tadaki, and S. Tsujii, "Nonlinear piece in hand perturbation vector method for enhancing security of multivariate public key cryptosystems," in *International Workshop on Post-Quantum Cryptography*, pp. 148–164, 2008.

[14] A. Kipnis, J. Patarin, and L. Goubin, "Unbalanced oil and vinegar signature schemes," in *International*

Conference on the Theory and Applications of Cryptographic Techniques, pp. 206–222, 1999.

[15] T. Matsumoto and H. Imai, "Public quadratic polynomial-tuples for efficient signature-verification and message-encryption," in *Workshop on the Theory and Application of of Cryptographic Techniques*, pp. 419–453. Springer, 1988.

[16] T. T. Moh, "A public key system with signature and master key functions," *Communications in Algebra*, vol. 27, no. 5, pp. 2207–2222, 1999.

[17] X. Y. Nie, P. Albrecht, B. Johannes, and F. G. Li, "Linearization equation attack on 2-layer nonlinear piece in hand method," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 97, no. 9, pp. 1952–1961, 2014.

[18] X. Y. Nie, C. Y. Hou, Z. H. Xu, and G. Lu, "Analysis of second order matrices construction in MFE public key cryptosystem," *International Journal of Network Security*, vol. 18, no. 1, pp. 158–164, 2016.

[19] V. Padmavathi, B. Vishnu Vardhan, A. V. N. Krishna, "Provably secure quantum key distribution by applying quantum gate," *International Journal of Network Security*, vol. 20, no. 1, pp. 88-94, 2018.

[20] J. Patarin, "Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt88," in *Annual International Cryptology Conference*, pp. 248–261, 1995.

[21] J. Patarin, "Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms," in *Advances in Cryptology (EUROCRYPT'96)*, pp. 33–48, 1996.

[22] J. Patarin, "The oil and vinegar signature scheme," in *Dagstuhl Workshop on Cryptography*, 1997.

[23] J. Patarin, L. Goubin, and N. Courtois, "C^*_{-+} and HM: Variations around two schemes of T. Matsumoto and H. Imai," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 35–50, 1998.

[24] S. T. Qiao, W. B. Han, Y. F. Li, and L. Y. Jiao, "Construction of extended multivariate public key cryptosystems," *International Journal of Network Security*, vol. 18, no. 1, pp. 60–67, 2016.

[25] M. S. Srinath, V. Chandrasekaran, "Isogeny-based quantum-resistant undeniable blind signature scheme," *International Journal of Network Security*, vol. 20, no. 1, pp. 9-18, 2018.

[26] L. C. Wang, B. Y. Yang, Y. H. Hu, and F. P. Lai, "A "Medium-Field" multivariate public-key encryption scheme," in *The Cryptographers' Track at the RSA Conference (CT-RSA'06)*, pp. 132–149, 2006.

Biography

Gang Lu is a PH.D candidate in University of Electronic Science and Technology of China now. His research interests include cryptography and security of big data.

Linyuan Xue is pursuing his Master degree from the Department of Information and Software Engineering, University of Electronic Science and Technology of China. His research interests include multivariate public key cryptosystems and network security.

Xuyun Nie received the Ph.D. degree in Information security from Graduate university of Chinese Academy of Sciences, Beijing, China, in 2007. He is presently an Associate Professor at University of Electronic Science and Technology of China (UESTC). His research interests include cryptography and information security.

Zhiguang Qin is a professor in the School of Information and Software Engineering, UESTC. He received his PH.D. degree from UESTC in 1996. His research interests include: information security and computer network.