Breaking Instance II of New TTM Cryptosystems

Xuyun Nie[1], Xin Jiang[2], Lei Hu[2], Jintai Ding[3] and Zhiguang Qin[1]
[1]School of Computer Science and Engineering
University of Electronic Science and Technology of China
Chengdu 610054, China
[2]State Key Laboratory of Information Security
Graduate University of Chinese Academy of Sciences
Beijing 100049, China
[3]Department of Mathematical Sciences
University of Cincinnati
Cincinnati, OH, 45220, USA
xynie@uestc.edu.cn, {xjiang, hu}@is.ac.cn, ding@math.uc.edu

Abstract

TTM (Tame Transformation Method) is a type of multivariate public key cryptosystem. In 2007, the inventor of TTM proposed two new instances of TTM to resist the existing attacks, in particular, the Nie et al attack. The two instances are claimed to achieve a security of 2^{109} against Nie et al attack. Through computation, we found that the instance II satisfied First Order Linearization Equations. After finding all linearization equations, we can perform a ciphertext-only attack to break it.

1. Introduction

Due to quantum computer attack by Shor [1], traditional PKC, such as RSA and ElGamal, would be insecure in the future. There is a need to search for alternatives which are based on other classes of problems. Multivariate public key cryptosystem (MPKC) is a promising alternative.

The general form of MPKC is as follows. Let k be a finite field, n and m be two integers. Let L_1 and L_2 be randomly chosen invertible affine maps on k^n and k^m, respectively. ϕ is a non-linear map from k^n to k^m called central map of MPKC, which can be easily inverted. Let

$$\begin{aligned} Y &= (y_1, \cdots, y_m) \\ &= F(x_1, \cdots, x_n) \\ &= L_2 \circ \phi \circ L_1(x_1, \cdots, x_n), \end{aligned}$$

where F is a map from k^n to k^m. The expression of F is the public key of MPKC, which is a set of multivariate polynomials. The secret key consists of L_1 and L_2.

TTM (Tame Transformation Method) is a type of triangular MPKC, proposed by T. T. Moh originally in 1999 [2]. Maybe it is one of the fast cryptosystem of MPKC due to its specific structure. Its design idea comes from algebraic geometry, and its central map is the so-called tame transformation which is a core concept in algebraic geometry and is closely related to the famous Jacobian conjecture.

TTM has gone through several cycles of attack and defense. There are many instances of TTM proposed these year[2][3][4], but all instances of TTM are insecure, refer to [5], [6], [7]. In 2006, we broke an instance[4] proposed in 2004 by the inventors of TTM[7]. We found that there exist second order linearization equations (SOLEs) satisfied by the cipher, and utilizing this defect, we found a method to "unlock" the lock polynomials, and then we proposed a ciphertext-only attack on the instance, i.e., we can recover the corresponding plaintext for any given ciphertext.

In 2007, the inventor of TTM proposed two instances of TTM[8] to resist our attack. In this paper, the author of TTM did not give the detail of decryption process. This means we do not know how the lock polynomials were designed.

Through theoretical analysis on the central maps of the instances II in [8], we find the cipher of this instance satisfy first order linearization equations (FOLES) of form

$$\sum_{i=0}^{n-1} a_i \bar{x}_i + \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} b_{ij} \bar{x}_i F_j + \sum_{j=0}^{m-1} c_j F_j + d = 0,$$

while for the previous version of TTM, only second order linearization equations can be used in the beginning stage

978-0-7695-3278-3/08 $25.00 © 2008 IEEE
DOI 10.1109/IIH-MSP.2008.246

of the attack. This means this instance do not achieve a better design than the previous version. First order linearization equation attack method[9] can be traced back to Patarin in 1995 who defeated the original Matsemoto-Imai scheme [10]. We can find all linearizations equations in 2^{44} $\mathbb{F}_{2^8}$-computations which is precomputation for any given public key. Then for a given valid ciphertext, via three eliminations, we can find the corresponding plaintext in 2^{26} operations. Our experiments confirmed this point. Note that our attack is a ciphertext-only attack.

The paper is organized as follows. In Section 2 we introduce the instance II in reference [8]. Then we give the details of our attack on this instance in Section 3. Finally in Section 4, we conclude the paper.

2. TTM Cryptosystems

Let $\mathbb{K}$ be a small finite field with 2^8 elements, n and m are two integers. Generally, TTM systems are constructed by four maps ϕ_1, ϕ_2, ϕ_3, and ϕ_4. Their composition $F = \phi_4 \circ \phi_3 \circ \phi_2 \circ \phi_1 : \mathbb{K}^n \to \mathbb{K}^m$ is designed to be a set of quadratic polynomials, which is taken as the public key in a TTM system, and the linear maps ϕ_1 and ϕ_4 are taken as the corresponding secret key.

Here the encryption map $F : \mathbb{K}^n \to \mathbb{K}^m$ is a composition of the four maps, namely $F = \phi_4 \circ \phi_3 \circ \phi_2 \circ \phi_1$:

$$F : \mathbb{K}^n \xrightarrow{\phi_1} \mathbb{K}^n \xrightarrow{\phi_2} \mathbb{K}^m \xrightarrow{\phi_3} \mathbb{K}^m \xrightarrow{\phi_4} \mathbb{K}^m.$$

ϕ_1 and ϕ_4 are invertible affine linear maps, ϕ_2 is a tame quadratic transformation, and ϕ_3 is a high degree map using lock polynomials.

We use $\bar{x}_0, \cdots, \bar{x}_{n-1}$ and $\bar{y}_0, \cdots, \bar{y}_{m-1}$ to denote plaintext and ciphertext components, respectively. The input and output components of the central map are denoted by $x_0, \cdots, x_{n-1}$ and $y_0, \cdots, y_{m-1}$. That is,

$$\begin{array}{ll} (x_0, \cdots, x_{n-1}) & = \phi_1(\bar{x}_0, \cdots, \bar{x}_{n-1}), \\ (y_0, \cdots, y_{m-1}) & = \phi_3 \circ \phi_2(x_0, \cdots, x_{n-1}), \\ (\bar{y}_0, \cdots, \bar{y}_{m-1}) & = \phi_4(y_0, \cdots, y_{m-1}). \end{array}$$

As usual in many multivariate systems, ϕ_1 and ϕ_4 are taken as the private key, while the polynomial expression of the map $(\bar{y}_0, \cdots, \bar{y}_{m-1}) = F(\bar{x}_0, ..., \bar{x}_{n-1})$ is the public key. To encrypt a plaintext $(\bar{x}_0, ..., \bar{x}_{n-1})$ is to evaluate F at it.

The paper [8] did not provide the detail of the decryption process and the construction of lock polynomials. Only the expressions of the composed map $\phi_3 \circ \phi_2$ are given, please see [8] or Appendix A in the present paper.

For the instance I of the two new instances of TTM, $n = 103$ and $m = 210$; while for the second, $n = 112$ and $m = 215$ [8]. Our work focus on instance II.

3. Cryptanalysis of Instance II

For a given valid ciphertext $\bar{Y}' = (\bar{y}'_0, \bar{y}'_1, \cdots, \bar{y}'_{214})$, our goal is finding its corresponding plaintext $\bar{X}' = (\bar{x}'_0, \cdots, \bar{x}'_{111})$, namely, we want solve the following system of equations:

$$\left\{ \begin{array}{c} F_0(\bar{x}_0, \cdots, \bar{x}_{111}) = \bar{y}'_0; \\ F_1(\bar{x}_0, \cdots, \bar{x}_{111}) = \bar{y}'_1; \\ \vdots \\ F_{214}(\bar{x}_0, \cdots, \bar{x}_{111}) = \bar{y}'_{214}. \end{array} \right. \quad (1)$$

The main idea of our attack is to find linearization equations and use them to do eliminations on equation system (1).

3.1. Finding Linearization Equations

First, we show algebraically why this instance satisfies first order linearization equations.

By the central map of instance II, we have

$$\left\{ \begin{array}{l} y_{100} = x_{95}x_{89} + x_{91}x_{93} + x_{100}; \\ y_{102} = x_{90}x_{95} + x_{91}x_{94} + x_{102}; \\ y_{103} = x_{92}x_{94} + x_{90}x_{96} + x_{103}; \\ y_{104} = x_{92}x_{93} + x_{89}x_{96} + x_{104}. \end{array} \right. \quad (2)$$

From them we can derive

$$\left\{ \begin{array}{l} x_{96}y_{100} = x_{96}x_{95}x_{89} + x_{96}x_{91}x_{93} + x_{96}x_{100}; \\ x_{92}y_{102} = x_{92}x_{90}x_{95} + x_{92}x_{91}x_{94} + x_{92}x_{102}; \\ x_{91}y_{103} = x_{91}x_{92}x_{94} + x_{91}x_{90}x_{96} + x_{91}x_{103}; \\ x_{95}y_{104} = x_{95}x_{92}x_{93} + x_{95}x_{89}x_{96} + x_{95}x_{104}. \end{array} \right. \quad (3)$$

Adding the four above equations, we get

$$\begin{array}{rl} & x_{96}x_{100} + x_{92}x_{102} + x_{91}x_{103} + x_{95}x_{104} \\ = & x_{96}y_{100} + x_{92}y_{102} + x_{91}y_{103} + x_{95}x_{104} \\ & +(x_{90} + x_{93})(x_{91}x_{96} + x_{92}x_{95}). \end{array} \quad (4)$$

Since

$$y_1 + x_1 = x_{96}x_{100} + x_{92}x_{102} + x_{91}x_{103} + x_{95}x_{104},$$

and

$$y_{213} = x_{91}x_{96} + x_{92}x_{95},$$

equation (4) can be changed into

$$\begin{array}{rl} y_1 + x_1 = & x_{96}y_{100} + x_{92}y_{102} + x_{91}y_{103} \\ & +x_{95}x_{104} + (x_{90} + x_{93})y_{213}. \end{array} \quad (5)$$

This equation is a first order linearization equation.

Since F is derived from the central map by composing from the inner and outer sides by invertible affine linear maps ϕ_1 and ϕ_4, i.e., $x_i = \phi_{1,i}(\bar{x}_0, \cdots, \bar{x}_{111})$ and

$y_j = \phi_{4,j}^{-1}(F_0, \cdots, F_{214})$, each of the FOLEs on x_i and y_i can be changed into an identical equation of the form:

$$\sum_{i=0}^{111} a_i \bar{x}_i + \sum_{i=0}^{111}\sum_{j=0}^{214} b_{ij}\bar{x}_i F_j + \sum_{j=0}^{214} c_j F_j + d = 0, \quad (6)$$

which is satisfied by any $(\bar{x}_0, \cdots, \bar{x}_{111}) \in \mathbb{K}^{112}$.

To continue our attack, we must find all first order linearization equations satisfied by the cipher. To find all FOLEs is to find a basis of $\mathbb{K}$-linear space spanned by all unknown vector $(a_0, \ldots, a_{111}, b_{0,0}, \ldots, b_{111,214}, c_0, \ldots, c_{214}, d)$. Let D be the dimension of this linear space.

The number of unknown coefficients a_i, b_{ij}, c_j, and d in equation (6) is equal to

$$112 + 112 \times 215 + 215 + 1 = 24408.$$

To find all FOLEs, we randomly select slightly more than 24408, say 24500, plaintexts $(x_0, \cdots, x_{111})$ and substitute them in (6) to get a system of 24500 linear equations in 24008 unknowns, and then solve it. Its computational complexity (by a native Gaussian elimination) is less than 2^{44}.

We performed our experiment on a DELL PowerEdge 7250, a minicomputer with 4 Itanium2 CPU and 32GB ECC fully buffered DIMM memory. The operating system we used was 64-bit Windows Server 2003. We programmed the attack using VC++. In our experiment, we used four threads to deal with Gaussian elimination.

Our experiments showed that about 53 hours (2 days and 5 hours) were required for this Gaussian elimination phase (concretely, 53 hours and 7 minutes for one of 10 public keys). Our experiments show that $D = 242$, namely, we find 242 linearly independent linearization equations.

The work above depends only on any given public key, and it can be solved once for all cryptanalysis under that public key.

3.2. Eliminations

Now we have derived all SOLEs. Then given a valid ciphertext, we can do elimination on the system (1).

Substituting $(F_0, \cdots, F_{214}) = (\bar{y}'_0, \cdots, \bar{y}'_{214})$ into every FOLEs, we can obtain a set of linear equations in plaintext variables. Solving this system, we can represent l variables of $x_0, \cdots, x_{111}$ by linear combinations of other $112-l$. Our experiments show $l = 86$. Hence, we derive a new equation system of following form:

$$\begin{cases} \hat{F}_0(\bar{x}_{u_1}, \cdots, \bar{x}_{u_{26}}) = \bar{y}'_0; \\ \hat{F}_1(\bar{x}_{u_1}, \cdots, \bar{x}_{u_{26}}) = \bar{y}'_1; \\ \vdots \\ \hat{F}_{214}(\bar{x}_{u_1}, \cdots, \bar{x}_{u_{26}}) = y'_{214}. \end{cases} \quad (7)$$

where $\bar{x}_{u_1}, \cdots, \bar{x}_{u_{26}}$ are remainder variables.

Our computer experiments find, for these new quadratic polynomials $\hat{F}_j(\bar{x}_{u_1}, \cdots, \bar{x}_{u_{26}})$ $(0 \le j \le 214)$, there still exist identical equations of the form

$$\sum_{i=0}^{103-l} \hat{a}_i \bar{x}_{u_i} + \sum_{j=0}^{210} \hat{b}_j \hat{F}_j + \hat{d} = 0, \quad (8)$$

which are satisfied by all $(\bar{x}_{u_1}, \cdots, \bar{x}_{u_{26}}) \in K^{26}$ and the coefficients $(\hat{b}_0, \cdots, \hat{b}_{214}) \neq (0, \cdots, 0)$.

We can use the same method as before to do elimination on system (7). Our experiments show we can eliminate 22 variable in this step. So we get a system of equations with 4 variables and 215 equations. This system of equations can be solved easily. After getting the values of last four variables, we substitute them into the affine expressions to get the corresponding plaintext.

The computational complexity of these steps is less then 2^{26}, in our experiment, it is less than one minute.

For any given valid ciphertext, our experiments successfully find the corresponding plaintext.

4. Conclusion

Using first order linearization equations, we broke the instance II of two new instances of TTM public key cryptosystem recently proposed by Prof. T. T. Moh in the paper [8]. We have done experiments to confirm our attack of finding the corresponding plaintext for any given valid ciphertext. This instance does not achieve better design than the previous instance of TTM in 2004.

Acknowledgement

We would like to thank the anonymous reviewers for their valuable comments and suggestions. This work of the first author is supported by the National Natural Science Foundation of China under contract no. 60673075 and the National High Technology Research and Development Program of China (863) under contract no. 2006AA01Z428. The work of the third author is supported by National 863 Program (2006AA01Z416), National 973 Program (2007CB311201) and NSFC (60773134).

References

[1] Peter Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

[2] T. Moh. A Public Key System with Signature and Master Key Functions. *Communication in Algebra*, 27(5):2207–2222, 1999.

[3] J. Chen and T. Moh. On the Goubin-Courtois attack on TTM. 2001. http://eprint.iacr.org/2001/72.

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

[5] Louis Goubin and Nicolas Courtois. Cryptanalysis of the TTM Cryptosystem. In *ASIACRYPT2000*, pages 44–57, 2000.

[6] J. Ding and D. Schmidt. The New TTM Implementation is Not Secure. In *CCC2003*, pages 106–121, 2003. http://eprint.iacr.org/2003/86.

[7] Xuyun Nie, Lei Hu, Jianyu Li, Crystal Updegrove, and Jintai Ding. Breaking a New Instance of TTM Cryptosystems. In *ACNS2006*, pages 210–225, 2006.

[8] T. Moh. Two New Examples of TTM. 2007. http://eprint.iacr.org/2007/144.

[9] Jacques Patarin. Cryptoanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88. In *CRYPTO'95*, pages 248–261, 1995.

[10] Tsutomu Matsumoto and Hideki Imai. Public Quadratic Polynominal-Tuples for Efficient Signature-Verification and Message-Encryption. In *EUROCRYPT'88*, pages 419–453, 1988.

Appendix A: Description of Central Map

The expressions of $(y_0, \cdots, y_{214}) = \phi_3 \circ \phi_2(x_0, \cdots, x_{111})$ are listed as follows. Due to page limitation, we only give a part of expressions which produce linearization equations. The more details refer to [8]. In these expressions in the original paper [8], the expression of y_{108} is missed. So, in our experiments, we set $y_{108} = f(x_0, \cdots, x_{107}) + x_{108}$, where f is a randomly chosen quadratic polynomial.

$$
\begin{aligned}
y_0 &= x_1x_4 + x_2x_3 + x_0;\\
y_1 &= x_{96}x_{100} + x_{92}x_{102} + x_{91}x_{103} + x_{95}x_{104} + x_1;\\
y_2 &= x_{80}x_{85} + x_{76}x_{86} + x_{75}x_{87} + x_{79}x_{88} + x_2;\\
y_3 &= x_{64}x_{69} + x_{60}x_{70} + x_{59}x_{71} + x_{63}x_{72} + x_1x_2 + x_3;\\
y_4 &= x_{48}x_{53} + x_{44}x_{54} + x_{43}x_{55} + x_{47}x_{56} + x_1x_3 + x_2x_3 + x_4;\\
&\vdots\\
y_{52} &= x_{41}x_{46} + x_{42}x_{45} + x_{49} + x_{52};\\
y_{53} &= x_{41}x_{47} + x_{43}x_{45} + x_{53};\\
y_{54} &= x_{42}x_{47} + x_{43}x_{46} + x_{54};\\
y_{55} &= x_{44}x_{46} + x_{42}x_{48} + x_{55};\\
y_{56} &= x_{44}x_{45} + x_{41}x_{48} + x_{56};\\
&\vdots\\
y_{68} &= x_{57}x_{62} + x_{58}x_{61} + x_{65} + x_{68};\\
y_{69} &= x_{57}x_{63} + x_{59}x_{61} + x_{69};\\
y_{70} &= x_{58}x_{63} + x_{59}x_{62} + x_{70};\\
y_{71} &= x_{60}x_{62} + x_{58}x_{64} + x_{71};\\
y_{72} &= x_{60}x_{61} + x_{57}x_{64} + x_{72};\\
&\vdots\\
y_{84} &= x_{73}x_{78} + x_{74}x_{77} + x_{81} + x_{84};\\
y_{85} &= x_{73}x_{79} + x_{75}x_{77} + x_{85};\\
y_{86} &= x_{74}x_{79} + x_{75}x_{78} + x_{86};\\
y_{87} &= x_{76}x_{78} + x_{74}x_{80} + x_{87};\\
y_{88} &= x_{76}x_{77} + x_{73}x_{80} + x_{88};\\
&\vdots\\
y_{100} &= x_{95}x_{89} + x_{91}x_{93} + x_{100};\\
y_{101} &= x_{89}x_{94} + x_{90}x_{93} + x_{97} + x_{101};\\
y_{102} &= x_{90}x_{95} + x_{91}x_{94} + x_{102};\\
y_{103} &= x_{92}x_{94} + x_{90}x_{96} + x_{103};\\
y_{104} &= x_{92}x_{93} + x_{89}x_{96} + x_{104};\\
&\vdots\\
y_{175} &= x_{54}x_{56} + x_{53}x_{55};\\
y_{176} &= x_{54}x_{50} + x_{49}x_{55} + x_{48};\\
y_{177} &= x_{53}x_{50} + x_{49}x_{56} + x_{44};\\
y_{178} &= x_{51}x_{56} + x_{53}x_{52} + x_{43};\\
y_{179} &= x_{51}x_{50} + x_{49}x_{52} + x_{42} + x_{45};\\
y_{180} &= x_{44}x_{47} + x_{43}x_{48};\\
y_{181} &= x_{51}x_{55} + x_{54}x_{52} + x_{47};\\
y_{182} &= x_{57}x_{70} + x_{58}x_{69} + x_{59}x_{65} + x_{60}x_{67} + x_{111} + x_{110} + x_{109}\\
&+x_4x_{110} + x_{108}x_{111} + x_3x_{109};\\
y_{183} &= x_{61}x_{71} + x_{62}x_{72} + x_{63}x_{66} + x_{64}x_{68};\\
y_{184} &= x_{61}x_{70} + x_{69}x_{62} + x_{65}x_{63} + x_{64}x_{67};\\
y_{185} &= x_{57}x_{71} + x_{58}x_{72} + x_{59}x_{66} + x_{60}x_{68};\\
y_{186} &= x_{70}x_{72} + x_{69}x_{71};\\
y_{187} &= x_{70}x_{66} + x_{65}x_{71} + x_{64};\\
y_{188} &= x_{69}x_{66} + x_{65}x_{72} + x_{60};\\
y_{189} &= x_{72}x_{67} + x_{69}x_{68} + x_{59};\\
y_{190} &= x_{67}x_{66} + x_{65}x_{68} + x_{58} + x_{61};\\
y_{191} &= x_{60}x_{63} + x_{59}x_{64};\\
y_{192} &= x_{67}x_{71} + x_{70}x_{68} + x_{63};\\
y_{193} &= x_{73}x_{86} + x_{74}x_{85} + x_{75}x_{81} + x_{76}x_{83} + x_{111} + x_{110} + x_{109}\\
&+x_4x_{110} + x_{108}x_{111} + x_3x_{109};\\
y_{194} &= x_{77}x_{87} + x_{78}x_{88} + x_{79}x_{82} + x_{80}x_{84};\\
y_{195} &= x_{77}x_{86} + x_{78}x_{85} + x_{79}x_{81} + x_{80}x_{83};\\
y_{196} &= x_{73}x_{87} + x_{74}x_{88} + x_{75}x_{82} + x_{76}x_{84};\\
y_{197} &= x_{86}x_{88} + x_{85}x_{87};\\
y_{198} &= x_{86}x_{82} + x_{81}x_{87} + x_{80};\\
y_{199} &= x_{85}x_{82} + x_{81}x_{88} + x_{76};\\
y_{200} &= x_{83}x_{88} + x_{85}x_{84} + x_{75};\\
y_{201} &= x_{83}x_{82} + x_{81}x_{84} + x_{74} + x_{77};\\
y_{202} &= x_{76}x_{79} + x_{75}x_{80};\\
y_{203} &= x_{83}x_{87} + x_{86}x_{84} + x_{79};\\
y_{204} &= x_{89}x_{102} + x_{90}x_{100} + x_{91}x_{97} + x_{92}x_{99} + x_{111} + x_{110} + x_{109}\\
&+x_4x_{110} + x_{108}x_{111} + x_3x_{109};\\
y_{205} &= x_{93}x_{103} + x_{94}x_{104} + x_{95}x_{98} + x_{96}x_{101};\\
y_{206} &= x_{93}x_{102} + x_{94}x_{100} + x_{95}x_{97} + x_{96}x_{99};\\
y_{207} &= x_{89}x_{103} + x_{90}x_{104} + x_{91}x_{98} + x_{92}x_{101};\\
y_{208} &= x_{102}x_{104} + x_{100}x_{103};\\
y_{209} &= x_{102}x_{98} + x_{97}x_{103} + x_{96};\\
y_{210} &= x_{100}x_{98} + x_{97}x_{104} + x_{92};\\
y_{211} &= x_{99}x_{104} + x_{100}x_{101} + x_{91};\\
y_{212} &= x_{99}x_{98} + x_{97}x_{101} + x_{90} + x_{93};\\
y_{213} &= x_{92}x_{95} + x_{91}x_{96};\\
y_{214} &= x_{99}x_{103} + x_{102}x_{101} + x_{95};
\end{aligned}
$$