Cryptanalysis of an Implementation of TTM Cryptosystems Based on Q_2^k -module*

Hongwei Tao

State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, China
China National Digital Switching System Engineering and Technological Research Center, Zhengzhou, China
tthhww 811@163.com

Abstract - TTM cryptosystems proposed by T.Moh are very fast due to the properties of tame automorphisms and small finite fields. The success of the first implementation of this system relies on the construction of Q_8-module. Unfortunately, Jintai Ding and Timonthy Hodges have defeated it by decomposing function Q_8 into terms S, T_1, T_2. Later Chunyen Chou, D. J. Guan and Jiunming Chen gave a systematic way to construct Q_2^k-module. In this paper, we describe an implementation of TTM cryptosystems based on this Q_2^k-module, then with method similar to Ding-Hodges, we break this implementation. For any given ciphertext, we can derive the corresponding plaintext within $O((n+r)^6)$ F_2^m-operations, where n+r is the number of ciphertext variables.

Index Terms - Multivariate public key cryptosystems, TTM, high order linearization equations.

I . Introduction

In the last twenty years, public key cryptography is an important tool for nowadays information society. Unfortunately traditional public key cryptosystems rely on either factoring (RSA) or discrete logarithms (ElGamal). However polynomial time quantum algorithms can be used to solve both problems [1]. Hence it is widely believed that research on new schemes based on other classes of problem is necessary.

Multivariate public key cryptosystem (MPKC) is one of the promising alternatives. This method is based on the proven theorem that solving a set of randomly chosen nonlinear polynomial equations over a finite field is NP-hard [2], and so far quantum computers have not yet been shown to be able to solve a set of multivariate polynomial equations efficiently. Moreover in general Multivariate public key schemes are much more computationally efficient than number theoretic based schemes.

T.Moh proposed TTM cryptosystems [3]. It is very fast due to its special design. Goubin and Courtois presented the MinRank attack on the TTM cryptosystems and claimed to have defeated this system [4]. However J. Chen and T.Moh refuted this claim and they presented another construction to support their claim [5]. But Ding and Schmidt extended the linearization method to attack this new implementation [6]. The success of this system relies on the construction of Q_8-type modules. Some constructions of Q_k-module are known, such as the systematic way to construct Q_2^k-module proposed by Chou et al. [7].

In this paper we describe an implementation of TTM cryptosystems based on Q_2^k -module proposed by Chou et al.. With the high order linearization equations (HOLE) attack proposed by Jintai Ding and Timonthy Hodges in [8], we attack this implementation. For any given ciphertext y′, we can find an affine subspace V containing the corresponding plaintext x′ in the plaintext space and all the polynomials in the public key polynomials derived from Q_2^k -module become constants on V. Then the public key polynomials restricting on V become de Jnquiere type which are easily inverted.

The paper is organized as follows. We present the systematic way to construct Q_2^k-module proposed by chou et al. in section 2. In section 3, we give an implementation of TTM cryptosystems based on this Q_2^k-module, and we propose the cryptanalysis of this implementation in section 4. In the last section, we describe the conclusion.

II. The Systematic Way to Construct Q_{2^k} -module Proposed by Chou et al.

Definition 1

[3] Let $L=\{p_1,\cdots,p_s\}$ be a set of polynomials in $x_1,\cdots,x_t$, and $f(x_1,\cdots,x_t)$ be a polynomial. If $Q(p_1(x_1,\cdots,x_t),\cdots,p_s(x_1,\cdots,x_t))=f(x_1,\cdots,x_t)$, then Q is called a generating polynomial of f over L . Furthermore if it is the minimal degree among all possible generating polynomials of f over L , then it is called a minimal generating polynomial of f over L .

Theorem 1

[7] For any $k\geq 3$, $Q_{2^k}(z_1,\cdots,z_{3k+6})$ is a minimal generating polynomial of $x_{t_1}^2$ over $U=\{q_1,\cdots,q_{3k+6}\}$ where

$$q_i = x_{t_i}+x_{t_{i+1}}^2,\ i=1,\cdots,k-1 \qquad q_k = x_{t_k}+x_{t_{k+1}}x_{t_{k+2}}$$

$$q_{k+1}=x_{t_{k+1}}^2+x_{t_{k+3}}x_{t_{k+4}} \qquad q_{k+2}=x_{t_{k+2}}^2+x_{t_{k+3}}x_{t_{k+4}}$$

$$\cdots \qquad \cdots$$

* This work is partially supported by from China's 863 Program (No 2009AA012201) and the NSFC (No. 91118007).

$$q_{3k-1}=x_{t_{3k-1}}^2+x_{t_{3k+1}}x_{t_{3k+2}} \qquad q_{3k}=x_{t_{3k}}^2+x_{t_{3k+3}}x_{t_{3k+4}}$$
$$q_{3k+1}=x_{t_{3k-1}}x_{t_{3k+3}} \qquad q_{3k+2}=x_{t_{3k-1}}x_{t_{3k+4}}$$
$$q_{3k+3}=x_{t_{3k}}x_{t_{3k+1}} \qquad q_{3k+4}=x_{t_{3k}}x_{t_{3k+2}}$$
$$q_{3k+5}=x_{t_{3k+1}}x_{t_{3k+3}} \qquad q_{3k+6}=x_{t_{3k+2}}x_{t_{3k+2}}$$

$$Q_{2^k}(z_1,\cdots,z_{3k+6})=z_1^2+z_2^4+\cdots+z_k^{2k}+$$
$$\{z_{k+1}^{2^{k-1}}+\{z_{k+3}^{2^{k-2}}+\{\cdots+C_1\}\cdots\}\square\{z_{k+4}^{2^{k-2}}+\{\cdots+C_1\}\cdots\}\}$$
$$\{z_{k+2}^{2^{k-1}}+\{z_{k+3}^{2^{k-2}}+\{\cdots+C_1\}\cdots\}\square\{z_{k+4}^{2^{k-2}}+\{\cdots+C_1\}\cdots\}\}$$

With

$$C_1=S^2\left[z_{3k-4}^4+T_1T_2\right],\ S(z_1,\cdots,z_{3k+6})=z_{3k-5}^2+C_2$$
$$T_1(z_1,\cdots,z_{3k+6})=z_{3k-3}^2+C_2,\ T_2(z_1,\cdots,z_{3k+6})=z_{3k-2}^2+C_2$$
$$C_2=z_{3k-1}z_{3k}+z_{3k+1}z_{3k+2}+z_{3k+3}z_{3k+4}+z_{3k+5}z_{3k+6}$$

III. An Implementation of TTM Cryptosystems Based on this Q_{2^k} -module

Let K be a finite field of 2^m elements. The encryption map F of this implementation is the composition $F=\phi_4\circ\phi_3\circ\phi_2\circ\phi_1\circ e$, where

1) $e: K^n \to K^{n+r}$
$(x_1,\cdots x_n)\mapsto(x_1,\cdots x_n,0,\cdots 0)$

2) $\phi_1=(\phi_{1,1},\cdots,\phi_{1,n+r})$ is an invertible linear transformation, where
$\phi_{1,i}=\sum_{j=1}^{n+r}a_{i,j}x_j+b_i, i=1,2,\cdots,n+r$, such that

a) For $i=1,2,\cdots,n$, we always have $b_i\neq 0, a_{i,j}=0$, for $j=n+1,\cdots,n+r$ and at least half of the remaining $a_{i,j}$ are nonzero.

b) For $i=n+1,\cdots,n+r$, we always have $\phi_{1,i}=x_i$.

3) ϕ_2 is a De Jonquiere map from K^{n+r} to K^{n+r} such that
$\phi_{2,1}=x_1,\phi_{2,2}=x_2,$
$\phi_{2,t_i}(x_1,\cdots,x_{n+r})=x_{t_i}+q_i(x_{u_1},\cdots,x_{u_{3k+4}}),$
$\phi_{2,s_i}(x_1,\cdots,x_{n+r})=x_{s_i}+q_i(x_{v_1},\cdots,x_{v_{3k+4}}), i=1,\cdots,3k+6$
where s_i,t_i are distinct positive integers and all of them are bigger than n.

4) The map ϕ_3 is defined as
$\phi_{3,1}=x_1+Q_{2^k}(x_{t_1},\cdots,x_{t_{3k+6}}),\phi_{3,2}=x_2+Q_{2^k}(x_{s_1},\cdots,x_{s_{3k+6}}),$
$\phi_{3,i}=x_i, i=3,\cdots,n+r.$

5) ϕ_4 is an invertible affine linear map with
$F=\phi_4\circ\phi_3\circ\phi_2\circ\phi_1\circ e(0,\cdots,0)=(0,\cdots,0)$.
$e,\phi_1,\phi_2,\phi_3,\phi_4$ are taken as private key.

Remark: From the construction of map ϕ_1, we can obtain that $\phi_1\circ e(x_1,\cdots,x_n)=\phi_1(x_1,\cdots,x_n,0,\cdots,0)\overset{def}{=}e\circ\tilde{\phi}_1(x_1,\cdots,x_n)$ here $\tilde{\phi}_{1,i}(x_1,\cdots,x_n)=\phi_{1,i}(x_1,\cdots,x_n,0,\cdots,0), i=1,\cdots,n.$, Hence $\tilde{\phi}_1: K^n\to K^n$ is an invertible affine linear function.

IV. Cryptanalysis of the Implementation Described Above

Define

$\rho_1(x_1,\cdots,x_{n+r})=(x_{t_1},\cdots,x_{t_{3k+6}}),$
$\rho_2(x_1,\cdots,x_{n+r})=(x_{s_1},\cdots,x_{s_{3k+6}}),$
$\pi_1(x_1,\cdots,x_n)=(x_{u_1},\cdots,x_{u_{3k+4}}),$
$\pi_2(x_1,\cdots,x_n)=(x_{v_1},\cdots,x_{v_{3k+4}}),$
$q(x_{t_1},\cdots,x_{t_{3k+6}})=(q_1(x_{t_1},\cdots,x_{t_{3k+6}}),\cdots,q_{3k+6}(x_{t_1},\cdots,x_{t_{3k+6}}))$

For brevity, we set $\hat{\phi}_1=\phi_1\circ e,\ \hat{\phi}_2=\phi_2\circ e,\ \hat{\phi}_{21}=\phi_2\circ\phi_1\circ e,\ \hat{\phi}_{32}=\phi_3\circ\phi_2\circ e,\ \hat{\phi}_{321}=\phi_3\circ\phi_2\circ\phi_1\circ e,$ It is easily verified that $\rho_i\circ\hat{\phi}_2=\rho_i\circ\hat{\phi}_{32}=q\circ\pi_i, i=1,2.$ Set $(y_1,\cdots,y_{n+r})=F(x_1,\cdots,x_n)$. Let L denote the subspace of linear functions in $x_1,\cdots,x_n$, R denote the K-linear space of $K[x_1,\cdots,x_n]$ generated by $\{y_i^{2^{m-2}}y_j^{2^{m-2}}, y_i^{2^{m-2}}, y_j^{2^{m-1}}, 1 | 1\le i,j\le n+r\}$ and T denote the K-linear space of $K[x_1,\cdots,x_n]$ generated by $\{y_i^{2^{k-1}}, y_i^{2^{k-2}},\cdots,y_i,1 | 1\le i\le n+r\}$.

In the following we describe the attack procedure and its computational complexity. This attack is ciphertext-only attack.

Step 1 of the attack.

It is easily verified that $S(q_1,\cdots,q_{3k+6})=x_{t_{3k-5}}^4$, $T_1(q_1,\cdots,q_{3k+6})=x_{t_{3k-3}}^4$, $T_2(q_1,\cdots,q_{3k+6})=x_{t_{3k-2}}^4$. Notice that $S\circ\rho_1\circ\hat{\phi}_2(x_1,\cdots,x_n)=S\circ q\circ\pi_1(x_1,\cdots,x_n)=x_{u_{3k-5}}^4$, hence $S^{2^{m-2}}\circ\rho_1\circ\hat{\phi}_2(x_1,\cdots,x_n)=(x_{u_{3k-5}}^4)^{2^{m-2}}=x_{u_{3k-5}}$. But $S^{2^{m-2}}\circ\rho_1\circ\hat{\phi}_{21}=S^{2^{m-2}}\circ\rho_1\circ\hat{\phi}_2\circ\tilde{\phi}_1$ and both $\tilde{\phi}_1$ and

$S^{2^{m-2}} \circ \rho_1 \circ \hat{\phi}_2$ are linear. Therefore $S^{2^{m-2}} \circ \rho_1 \circ \hat{\phi}_{21} \in L.$ Now observe that

$$S^{2^{m-2}} \circ \rho_1 \circ \hat{\phi}_{21} = S^{2^{m-2}} \circ \rho_1 \circ \hat{\phi}_{321} =$$
$$S^{2^{m-2}} \circ \rho_1 \circ \phi_4^{-1} \circ F(x) = S^{2^{m-2}} \circ \rho_1 \circ \phi_4^{-1}(y).$$

Since $\rho_1 \circ \phi_4^{-1}(y)$ is linear, and

$$S^{2^{m-2}}(z_1, \cdots, z_{3k+6}) = z_{3k-5}^{2^{m-1}} + z_{3k-1}^{2^{m-2}} z_{3k}^{2^{m-2}} + z_{3k+1}^{2^{m-2}} z_{3k+2}^{2^{m-2}} + z_{3k+3}^{2^{m-2}} z_{3k+4}^{2^{m-2}} + z_{3k+5}^{2^{m-2}} z_{3k+6}^{2^{m-2}}$$

It is clear $S^{2^{m-2}} \circ \rho_1 \circ \hat{\phi}_{21} = S^{2^{m-2}} \circ \rho_1 \circ \phi_4^{-1} \circ F \in R$. Therefore $S^{2^{m-2}} \circ \rho_1 \circ \hat{\phi}_{21} \in L \cap R$. Similarly $S^{2^{m-2}} \circ \rho_2 \circ \hat{\phi}_{21}$, $T_1^{2^{m-2}} \circ \rho_i \circ \hat{\phi}_{21}$, $T_2^{2^{m-2}} \circ \rho_i \circ \hat{\phi}_{21}, i = 1, 2$ all lie in $L \cap R$.This implies there exist equations in the form

$$\sum_{1 \le i \le j \le n+r} a_{ij} y_i^{2^{m-2}} y_j^{2^{m-2}} + \sum_{k=1}^{n+r} b_k y_k^{2^{m-2}} + \sum_{l=1}^{n+r} c_l y_k^{2^{m-1}} + \sum_{o=1}^{n} d_o x_o + f = 0 \quad (1)$$

where $a_{ij}, b_k, c_l, d_o, f \in K$. Let V denote the K-linear space composing of all the equations in the form (1). Notice that the number of unknown coefficients a_{ij}, b_k, c_l, d in (1) is equal to $c = 1/2(n+r)(n+r+3) + 2(n+1)$. To find all equations in V is equivalent to find a basis of V.To find a basis of ,we just randomly select slightly more than c, say $c + 1000$, plaintexts and substitute them in (1), the probability that we will not find the complete solution is essentially zero. Therefore we get a system $c + 1000$ of linear equations and solve it. The computational complexity to solve this system is $O((n+r)^6)$. Let $\dim V = D$. Let $\{a_{ij}^{(\rho)}, b_k^{(\rho)}, c_l^{(\rho)}, d_o^{(\rho)}, f^{(\rho)} \mid 1 \le \rho \le D\}$ be the coefficient vectors corresponding to a basis of V. Without loss of generality, we assume $(d_1^{(\rho)}, \cdots, d_n^{(\rho)}), 1 \le \rho \le l$ are linearly independent and the other vectors $(d_1^{(\rho)}, \cdots, d_n^{(\rho)})$, $l+1 \le \rho \le D$ are their linear combinations. The computational complexity of rearranging the resulting basis vectors is less than $O((n+r)^5)$. Let $E_\rho (1 \le \rho \le D)$ denote the equation $\sum_{1 \le i \le j \le n+r} a_{ij}^{(\rho)} y_i^{2^{m-2}} y_j^{2^{m-2}} + \sum_{k=1}^{n+r} b_k^{(\rho)} y_k^{2^{m-2}} + \sum_{l=1}^{n+r} c_l^{(\rho)} y_l^{2^{m-1}} + \sum_{o=1}^{n} d_o^{(\rho)} x_o + f^{(\rho)} = 0$. Let's assume we have a valid ciphertext $y' = (y_1', \cdots, y_{n+r}')$, our goal is to find its corresponding plaintext $x' = (x_1', \cdots, x_n')$ .Substituting $y = y'$ into $E_\rho (1 \le \rho \le l)$, we derive l linearly independent linear equations and denote them by $E_\rho' (1 \le \rho \le l)$. Solving $E_\rho' (1 \le \rho \le l)$ by Gaussian elimination, we can find two disjoint subsets of $\{1, \cdots, n\}$: $A_1' = \{v_1', \cdots, v_l'\}$ and $A_1 = \{v_1, \cdots, v_{n-l}\}$, and linear function in $x_{v_1}, \cdots, x_{v_{n-l}}$

$$x_{v_j'} = h_j(x_{v_1}, \cdots, x_{v_{n-l}}), 1 \le j \le l. \quad (2)$$

The computational complexity of substitution and Gaussian elimination is $O((n+r)^2 2^{m-2} l)$. Let

$$W = \{(x_1, \cdots, x_n) \mid x_{v_j'} = h_j(x_{v_1}, \cdots, x_{v_{n-l}}), 1 \le j \le l\}$$

then for any $(x_1, \cdots, x_n) \in W$, it satisfies $\sum_{o=1}^{n} d_o^{(\rho)} x_o = r^{(\rho)}$, $1 \le \rho \le l,$ where $r^{(\rho)} = \sum_{1 \le i \le j \le n+r} a_{ij}^{(\rho)} (y_i')^{2^{m-2}} (y_j')^{2^{m-2}} + \sum_{k=1}^{n+r} b_k^{(\rho)} (y_k')^{2^{m-2}} + \sum_{l=1}^{n+r} c_l^{(\rho)} (y_l')^{2^{m-1}} + f^{(\rho)}$. Since $S^{2^{m-2}} \circ \rho_1 \circ \hat{\phi}_{21} \in L \cap R$. Then there exist $a_i (1 \le i \le n), a_i \in K$ such that

$$S^{2^{m-2}} \circ \rho_1 \circ \hat{\phi}_{21} + \sum_{i=1}^{n} a_i x_i + a = 0 \in V \quad (3)$$

Therefore (3) is a linear combination of E_ρ, $1 \le \rho \le D$, $\sum_{i=1}^{n} a_i x_i$ at $x \in W$ is a linear combination of $\sum_{o=1}^{n} d_o^{(\rho)} x_o, 1 \le \rho \le l,$ that is, it is a linear combination of constants $r^{(\rho)}, 1 \le \rho \le l,$. Hence $S^{2^{m-2}} \circ \rho_1 \circ \hat{\phi}_{21}$ is a constant on W, so is $S \circ \rho_1 \circ \hat{\phi}_{21}$. Similarly, we can derive that $S \circ \rho_2 \circ \hat{\phi}_{21}$, $T_1 \circ \rho_i \circ \hat{\phi}_{21}$, $T_2 \circ \rho_i \circ \hat{\phi}_{21}$ are all constants on W. Now substitute (2) into $y_i(x_1, \cdots, x_n)$ and derive $\tilde{y}_i(x_{v_1}, \cdots, x_{v_{n-l}}), i = 1, \cdots, n+r$. The computational complexity of this step is $O((n+r)(n-l+2)^2(l+3))$.

Since $m \ll n+r$ and $l \ll n+r$. Then the computational complexity of this step is less than $O((n+r)^6)$.

Step 2 of the attack.

Notice that $Q_{2^k} \circ \rho_1 \circ \hat{\phi}_2(x_1, \cdots, x_n) = Q_{2^k} \circ q \circ \pi_1(x_1,$

$\cdots, x_n) = x_{u_1}^2$, hence $Q_{2^k}^{2^{m-1}} \circ \rho_1 \circ \hat{\phi}_2(x_1, \cdots, x_n) = (x_{u_1}^2)^{2^{m-1}} = x_{u_1}$. But $Q_{2^k}^{2^{m-1}} \circ \rho_1 \circ \hat{\phi}_{21} = Q_{2^k}^{2^{m-1}} \circ \rho_1 \circ \hat{\phi}_2 \circ \tilde{\phi}_1$ and both $Q_{2^k}^{2^{m-1}} \circ \rho_1 \circ \hat{\phi}_{21}$ and $\tilde{\phi}_1$ are linear. Therefore $Q_{2^k}^{2^{m-1}} \circ \rho_1 \circ \hat{\phi}_{21} \in L$. Now observe that $Q_{2^k}^{2^{m-1}} \circ \rho_1 \circ \hat{\phi}_{21}(x) = Q_{2^k}^{2^{m-1}} \circ \rho_1 \circ \hat{\phi}_{321}(x) = Q_{2^k}^{2^{m-1}} \circ \rho_1 \circ \phi_4^{-1} \circ F(x) = Q_{2^k}^{2^{m-1}} \circ \rho_1 \circ \phi_4^{-1}(y)$. Since $\rho_1 \circ \phi_4^{-1}(y)$ is linear, and $S \circ \rho_i \circ \hat{\phi}_{21}$, $T_1 \circ \rho_i \circ \hat{\phi}_{21}$, $T_2 \circ \rho_i \circ \hat{\phi}_{21}, i = 1, 2$ are all constants on W. It is clear that $Q_{2^k}^{2^{m-1}} \circ \rho_1 \circ \hat{\phi}_{21}|_W \in T$, Similarly $Q_{2^k}^{2^{m-1}} \circ \rho_2 \circ \hat{\phi}_{21}|_W \in T$. Therefore there exist equations in the form

$$\sum_{i=1}^{n+r} \tilde{a}_{i,k-1} \tilde{y}_i^{2^{k-1}} + \sum_{i=1}^{n+r} \tilde{a}_{i,k-2} \tilde{y}_i^{2^{k-2}} + \cdots + \sum_{i=1}^{n+r} \tilde{a}_{i,0} \tilde{y}_i + \tilde{d} + \sum_{i=1}^{n-l} \tilde{e}_i x_{v_i} = 0 \quad (4)$$

where $\tilde{a}_{i,k-1}, \cdots, \tilde{a}_{i,0}, \tilde{d}, \tilde{e}_i \in K$. Using the same method mentioned above, we can find a basis for K-linear space $\tilde{V}$ composing of all the equations in the form (4). Let $\dim \tilde{V} = D$ and $\{\tilde{a}_{i,k-1}^{(\rho)}, \tilde{a}_{i,k-2}^{(\rho)}, \cdots, \tilde{a}_{i,0}^{(\rho)}, \tilde{e}_i^{(\rho)}, \tilde{d}^{(\rho)} \mid 1 \le \rho \le D\}$ be the coefficient vectors corresponding to this basis of $\tilde{V}$. Without loss of generality, we assume $(\tilde{e}_1^{(\rho)}, \cdots, \tilde{e}_{n-l}^{(\rho)})$, $1 \le \rho \le k$ are linearly independent and the other vectors $(\tilde{e}_1^{(\rho)}, \cdots, \tilde{e}_{n-l}^{(\rho)}), 1 \le \rho \le \tilde{D}$ are their linear combinations. Let $\tilde{E}_\rho (1 \le \rho \le \tilde{D})$ denote equation

$$\sum_{i=1}^{n+r} \tilde{a}_{i,k-1}^{(\rho)} \tilde{y}_i^{2^{k-1}} + \sum_{i=1}^{n+r} \tilde{a}_{i,k-2}^{(\rho)} \tilde{y}_i^{2^{k-2}} + \cdots + \sum_{i=1}^{n+r} \tilde{a}_{i,0}^{(\rho)} \tilde{y}_i + \tilde{d} + \sum_{i=1}^{n-l} \tilde{e}_i^{(\rho)} x_{v_i} = 0$$

Substitute $\tilde{y} = y'$ into $\tilde{E}_\rho (1 \le \rho \le \tilde{D})$ and derive $\tilde{E}'_\rho (1 \le \rho \le \tilde{D})$. Doing a simple Gaussian elimination, from $\tilde{E}'_\rho (1 \le \rho \le \tilde{D})$, we can find two disjoint subsets of $\{v_1, \cdots, v_{n-l}\}$: $A'_2 = \{w'_1, \cdots, w'_{n-l-k}\}$ and $A_2 = \{w_1, \cdots, w_{n-l-k}\}$, and linear expressions

$$x_{w'_j} = \tilde{h}_j (x_{w_1}, \cdots, x_{w_{n-l-k}}), 1 \le j \le k. \quad (5)$$

Let $\tilde{W} = \{(x_1, \cdots, x_n) \in W \mid x_{w'_j} = \tilde{h}_j (x_{w_1}, \cdots, x_{w_{n-l-k}}), 1 \le j \le k\}$ then by the similar analysis in the step 1 of the attack, we can get that $Q_{2^k} \circ \rho_i \circ \hat{\phi}_{21}, i = 1, 2$ are constants on $\tilde{W}$. Let $Q_{2^k} \circ \rho_1 \circ \hat{\phi}_{21}|_{\tilde{W}}$, $Q_{2^k} \circ \rho_2 \circ \hat{\phi}_{21}|_{\tilde{W}}$ be c_1, c_2 respectively. Substitute (5) into $\tilde{y}_i$ and derive $\hat{y}_i, i = 1, \cdots, n+r$. The computational complexity of this step is about $O((n+r)^3 k^3)$

Step 3 of the attack.

For any $(x_1, \cdots, x_n) \in \tilde{W}$, we have

$$\phi_{4,1}^{-1}(\hat{y}) = \hat{\phi}_{321,1}(x_1, \cdots, x_n) = \phi_{1,1}(x_1, \cdots, x_n, 0, \cdots, 0) + c_1$$

So there must exist equations of the form $\sum_{i=1}^{n-l-k} \hat{a}_i x_{w_i} + \sum_{i=1}^{n+r} \hat{b}_i \hat{y}_i + \hat{d} = 0$. Similarly to the step 1 of the attack, we can derive a subspace $\tilde{W}$ of $\hat{W}$ on which $\phi_{1,1}(x_1, \cdots, x_n, 0, \cdots, 0)$ is a constant. Repeating similar steps, we derive in turn smaller and smaller affine subspace of $\tilde{W}$. On these subspace we have in turn $\phi_{1,2}(x_1, \cdots, x_n, 0, \cdots, 0), \cdots, \phi_{1,n}(x_1, \cdots, x_n, 0, \cdots, 0)$ are constants. Therefore they are all constants on the last subspace. Since ϕ_1 is an invertible map, $(x_1, \cdots, x_n)$ is a constant vector on that subspace, which implies that this affine subspace is a point. This point is exactly the plaintext.

This procedure takes no significant time compared to that of step1.

Since $k < n + r$. Then the total computational complexity of the attack is at most $O((n+r)^6)$.

V. Conclusion

In this paper, we use HOLE attack to break an implementation based on Q_2^k -module proposed by Chou et al. The complexity of the computation needed to defeat this implementation is about $O((n+r)^6)$, where n+r is the number of the ciphertext variables. However it does not mean that all such type implementations are all insecure. For example the ones suggested in [9] seem different and we can't directly apply this method in this situation. As we have seen that linearization and its generalization HOLE all can be used to break some multivariate public key cryptosystems. For anyone who want to present an secure multivariate public key cryptosystem should take into account these methods.

References

[1] Shor, P., "Polynomial-time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", SIAM Journal on Computing, 1997, 26(5): 1484-1509.

[2] Patarin, J., Goubin, L., "Trapdoor One-Way Permutations and Multivariate Polynomials", in Proceedings of International Conference on Information Security and Cryptology 1997, LNCS 1334, Berlin: Springer, 1997, 356-368.

[3] Moh, T., "A Public Key System with Signature and Master Key Functions", Communications in Algebra, 1999, 27(5): 2207-2222.

[4] Goubin, L., Courtois, N., "Cryptanalysis of the TTM cryptosystem", in Proceedings of Asiacrypt'2000, LNCS 1976, Berlin: 2000, 44-57

[5] Chen, J., Moh, T., "On the Goubin-Courtois attack on TTM". Cryptology ePrint Archive, 72, 2001. http://eprint.iacr.org/2001/072.
[6] Ding, J. T., Schmidt, D., "The New TTM Implementation is not Secure", in Proceedings of International Workshop on Coding, Cryptography and Combinatorics (CCC 2003), 2003, 106-121.
[7] Chou, C. Y., Guan, D. J., Chen J. M., "A Systematic Construction of a Q2k -module in TTM", Comm. Algebra, 2002, 30(2): 551-562.
[8] Ding, J. T., Hodges, T., "Cryptanalysis of an Implementation of the Tamed Transformation Method Cryptosystem", J. Algebra Appl., 2004, 3: 273-282.
[9] Wang, L. C., Chang, F. H., "Square-free Qk Components in TTM", Taiwanese Journal of Mathematics, 2003, 7(4): 615-629.