# CRYPTANALYSIS OF AN IMPLEMENTATION SCHEME OF THE TAMED TRANSFORMATION METHOD CRYPTOSYSTEM

JINTAI DING, TIMONTHY HODGES

Abstract. A Tamed Transformation Method (TTM) cryptosystem was proposed by T.T.Moh in 1999. We describe how the first implementation scheme of the TTM system can be defeated. The computational complexity of our attack is $2^{33}$ computations on the finite field with $2^8$ elements.

## 1. Introduction

During the last twenty years, public key cryptosystems have been developed to become an important part of our modern communication system. A number of different authors have constructed multivariable public key cryptosystems – cryptosystems based on multivariable functions instead of single variable functions. The safety of such systems rely on the difficulty of solving systems of polynomial equations with many variables. Recently, Matsumoto and Imai [MI] proposed a method that was later defeated by Patarin in [P]. Another method is the Tamed Transformation Method (TTM) proposed by Moh [M]. Goubin and Courtois claimed to have defeated this system in [CG], but Chen and Moh refuted this claim in [CM]. In this article, we use a completely different method to show that the implementation scheme suggested in [M] and also the ones suggested in [CGC] are not secure. Our approach is inspired by the work of Patarin on the Matsumoto-Imai scheme [P].

The basic idea of the TTM systems is that it is computationally difficult to decompose compositions of multi-variable functions. Let $K$ be a field, let $K^m = K \times K \cdots \times K$ and let $\bar{F}(x_1, \ldots, x_m) : K^m \to K^m$ be a bijection. Suppose that $\bar{F}(x_1, \ldots, x_m)$ is a composition of several maps $\phi_i(x_1, \ldots, x_m)$, $i = 1, \ldots, k$, such that:

(I) The function $\bar{F}(x_1, \ldots, x_m)$ can be evaluated quickly and easily for any specific value of $(x_1, \ldots, x_m)$.

(II) The $\phi_i(x_1, \ldots, x_m)$ are individually easy to invert but it is difficult to invert the product $\bar{F} = \phi_1 \circ \phi_2 \circ \cdots \circ \phi_k$, without knowing this decomposition.

An open key cryptosystem can be established as following: Assume party B intends to send party A a secret message in an open channel.

1. Party A first chooses such a pair $\bar{F}(x_1, \ldots, x_m)$ and a field $K$.
2. Party A publicizes the pair, $\bar{F}(x_1, \ldots, x_m)$ and $K$.
3. Party B obtains in public channel $\bar{F}(x_1, \ldots, x_m)$ and $K$.
4. A message $M = (a_1, \ldots, a_m)$ from party B is enciphered as $\bar{F}(a_1, \ldots, a_m)$ and is sent to party A in an open channel.
5. The message M is recovered by Party A using

$$(a_1, \ldots, a_m) = \bar{F}^{-1} \circ \bar{F}(a_1, \ldots, a_m)$$

*Key words and phrases.* Tamed Transformation Method, Composition of Functions, Inverse Map.

One can see that this works in a very similar way as RSA system, except that the security of RSA has nothing to do with property (I) and (II). The security of RSA relies on the difficulty of factorizing a product of two primes, $pq$.

In [M], Moh proposes constructing such a $\bar{F}(x_1, \ldots, x_m)$ over a finite field $K$ by choosing the $\phi_i$ to be the following two types of functions:

a) Affine Linear functions.

An invertible affine linear function is a function of the form $f(x) = L(x) + b$, where $L$ is a linear function and $b \in K^m$.

b) De Jonquiere Type.

A polynomial function $J : K^m \to K^m$ is said to be a de Jonquiere map if there is a basis of $K^m$ with respect to which

$$J(x_1, \ldots, x_m) = (x_1 + f_1(x_2, \ldots, x_m), x_2 + f_2(x_3, \ldots, x_m), \ldots, x_{m-1} + f(x_m), x_m)$$

for some polynomial functions $f_i : K^m \to K$.

Such functions can be inverted by iteratively defining

$$J^{-1}(y_1, \ldots, y_m) = (J_1^{-1}(y_1, \ldots, y_m), \ldots, J_m^{-1}(y_1, \ldots, y_m))$$

where $J_m^{-1}(y_1, \ldots, y_m) = y_m$ and

$$J_k^{-1}(y_1, \ldots, y_m) = y_k - f_k(J_{k+1}^{-1}(y_1, \ldots, y_m), \ldots, J_m^{-1}(y_1, \ldots, y_m)).$$

However, if the degree of the polynomials involved is too high, this procedure will not be practical since computation of $J^{-1}(y_1, \ldots, y_m)$ will be too slow. Therefore, ideally the $f_i$ should be quadratic polynomials. To achieve this Moh proposes [M] an implementation scheme in which

(i) The field $K$ is taken to be a finite field of characteristic 2 and $m = 100$. The map $\bar{F}$ is constructed as the composition of four functions,

$$\bar{F} = \phi_4 \circ \phi_3 \circ \phi_2 \circ \phi_1,$$

where $\phi_2$ and $\phi_3$ are of de Jonquiere Type and $\phi_1$ and $\phi_4$ are affine linear;

(ii) The final encryption map is a map $F : K^{64} \to K^{100}$ of the form $F = \bar{F} \circ e$ where $e : K^{64} \to K^{100}$ is the embedding $e(x_1, \ldots, x_{64}) = (x_1, \ldots, x_{64}, 0, 0, \ldots, 0)$.

The key component of this construction is a multivariable polynomial $Q_8(z_1, \ldots, z_{30})$ of degree 8 and thirty quadratic polynomials $q_i(z_1, \ldots, z_{19})$ such that $Q_8(q_1, \ldots, q_{30})$ is quadratic.

We show in this article that the code may be defeated in the following fashion. Let $x'$ be a plaintext and $y' = F(x')$ be the associated ciphertext. Using particular properties of $Q_8$ and the $q_i$, we are able to show that there exists a linear subspace of $K^{64}$ on which the encryption function $F$ coincides with another function of the form $F' = \phi_4 \circ \phi_3' \circ \phi_2 \circ \phi_1 e$ where $\phi_3'$ is an affine linear map. In this case $F'$ is essentially of de Jonquiere type and can be "inverted". Moreover the finding of the linear subspace, and the construction and inversion of $F'$ can all be done in a computationally efficient fashion.

## 2. Cryptanalysis of the first TTM Scheme

Let us begin by reviewing the scheme proposed in [M]. From now on, we assume that $R$ is the finite field with $2^8$ elements, which we denote by $F_{2^8}$. The encryption map $F$ is the composition $F = \phi_4 \circ \phi_3 \circ \phi_2 \circ \phi_1 \circ e$ where $e : K^{64} \to K^{100}$ and the maps $\phi_i : K^{100} \to K^{100}$, for $i = 1, 2, 3, 4$ are defined in the following way.

Let $[j] = j \bmod 8$, and $0 < [j] < 9$. Define $\phi_2 = (\phi_{2,1}, \ldots, \phi_{2,100})$ and $\phi_3 = (\phi_{3,1}, \ldots, \phi_{3,100})$ to be maps of de Jonquiere type defined by:

$$
\begin{aligned}
\phi_{2,i} &= x_i, && i = 1, 2; \\
\phi_{2,i} &= x_i + x_{i-1}x_{i-2}, && i = 3, \ldots, 9; \\
\phi_{2,i} &= x_i + x_{[i-1]}^2 + x_{[i]}x_{[i-5]} + x_{[i+1]}x_{i+6}, && i = 10, \ldots, 17; \\
\phi_{2,i} &= x_i + x_{[i-1]}x_{[i+1]} + x_{[i]}x_{[i+4]}, && i = 18, \ldots, 25; \\
\phi_{2,i} &= x_i + x_{[i-1]}x_{[i+1]} + x_{[i+2]}x_{[i+5]}, && i = 26, \ldots, 30; \\
\phi_{2,i} &= x_i + x_{i-10}^2, && i = 31, \ldots, 60; \\
\phi_{2,61} &= x_{61} + x_9^2, && \\
\phi_{2,62} &= x_{62} + x_{61}^2, && \\
\phi_{2,63} &= x_{63} + x_{10}^2, && \\
\phi_{2,64} &= x_{64} + x_{63}^2, && \\
\phi_{2,i} &= x_i + q_{i-64}(x_9, x_{11}, \quad, x_{16}, x_{51}, x_{52}, \ldots, x_{62}), && i = 65, \ldots, 92; \\
\phi_{2,i} &= x_i + q_{i-92}(x_{10}, x_{17}, \ldots, x_{20}, x_{15}, x_{16}, x_{51}, \ldots, x_{60}, x_{63}, x_{64}), && i = 93, \ldots, 100;
\end{aligned}
$$

where $q_i(z_1, \ldots, z_{19})$, i=1,...,30, are degree two polynomials of 19 variables $z_1, \ldots, z_{19}$.

$$
\begin{aligned}
q_1 &= z_1 + z_2z_6, & q_2 &= z_2^2 + z_3z_7, \\
q_3 &= z_3^2 + z_4z_{10}, & q_4 &= z_3z_5, \\
q_5 &= z_3z_{11}, & q_6 &= z_4z_7, \\
q_7 &= z_4z_5, & q_8 &= z_7^2 + z_5z_{11}, \\
q_9 &= z_6^2 + z_8z_9, & q_{10} &= z_8^2 + z_{12}z_{13}, \\
q_{11} &= z_9^2 + z_{14}z_{15}, & q_{12} &= z_7z_{10}, \\
q_{13} &= z_{10}z_{11}, & q_{14} &= z_{12}^2 + z_7z_8, \\
q_{15} &= z_{13}^2 + z_{11}z_{16}, & q_{16} &= z_{14}^2 + z_{10}z_{12}, \\
q_{17} &= z_{15}^2 + z_{11}z_{17}, & q_{18} &= z_{12}z_{16}, \\
q_{19} &= z_{11}z_{12}, & q_{20} &= z_8z_{13}, \\
q_{21} &= z_7z_{13}, & q_{22} &= z_8z_{16}, \\
q_{23} &= z_{14}z_{17}, & q_{24} &= z_7z_{11}, \\
q_{25} &= z_{12}z_{15}, & q_{26} &= z_{10}z_{15}, \\
q_{27} &= z_{12}z_{17}, & q_{28} &= z_{11}z_{14}, \\
q_{29} &= z_{18} + z_1^2, & q_{30} &= z_{19} + z_{18}^2.
\end{aligned}
$$

The map $\phi_3$ is defined as:

$$
\begin{aligned}
\phi_{3,1} &= x_1 + Q_8(x_{65}, x_{66}, \ldots, x_{92}, x_{61}, x_{62}) \\
\phi_{3,2} &= x_2 + Q_8(x_{93}, \ldots, x_{100}, x_{73}, \ldots, x_{92}, x_{63}, x_{64}) \\
\phi_{3,i} &= x_i, \quad i = 3, \ldots, 100;
\end{aligned}
$$

where $Q_8 : R^{30} \to R$ is given by:

$$Q_8(z_1, \ldots, z_{30}) = z_1^8 + [z_2^4 + z_3^4 + z_3^2 z_8^2 + z_4^2 z_5^2 + z_6^2 z_{12}^2 + z_7^2 z_{13}^2] \times$$
$$[z_9^4 + (z_{10}^2 + z_{14}z_{15} + z_{18}z_{19} + z_{20}z_{21} + z_{22}z_{24})(z_{11}^2 + z_{16}z_{17} + z_{23}z_{28} + z_{25}z_{26} + z_{13}z_{27})] + z_{29}^4 + z_{30}^2.$$

The map $\phi_1$ is an affine linear map satisfying certain other restrictions [M] that imply in particular that $\phi_1$ is a trivial extension of an affine linear map $\tilde{\phi}_1 : K^{64} \to K^{64}$. The most important consequence of these restrictions for what follows is that $\phi_1 \circ e = e \circ \tilde{\phi}_1$. Finally $\phi_4$ is an arbitrary affine linear map.

To simplify the notation, we set

$$\hat{\phi}_1 = \phi_1 \circ e, \quad \hat{\phi}_{12} = \phi_2 \circ \phi_1 \circ e, \quad \hat{\phi}_{123} = \phi_3 \circ \phi_2 \circ \phi_1 \circ e, \quad \hat{\phi}_2 = \phi_2 \circ e, \quad \hat{\phi}_{23} = \phi_3 \circ \phi_2 \circ e$$

We assume that $F$, $\phi_2$ and $\phi_3$ are public, but $\phi_1$ and $\phi_4$ are private. The goal is to invert $F$ without knowledge of $\phi_1$ and $\phi_4$. To do this we find for any given ciphertext $y'$ a linear subspace $V$ of $K^{64}$ which contains the original and unknown plaintext $x'$ and on which the function $F$ coincides with a simpler function $\check{F} : K^{64} \to K^{100}$ which is computationally invertible.

To do this we find a linear subvariety of $K^{64}$ on which $\phi_3$ applied to the image of $\hat{\phi}_{21}$ is essentially linear. To see what this entails, define

$$\rho_1(x_1, \ldots, x_{100}) = (x_{65}, \ldots, x_{92}, x_{61}, x_{62})$$
$$\rho_2(x_1, \ldots, x_{100}) = (x_{93}, \ldots, x_{100}, x_{73}, \ldots, x_{92}, x_{63}, x_{64})$$

Note that

$$(\hat{\phi}_{321})_1(x) = \phi_3(z) = \hat{\phi}_{21}(x)_1 + Q_8 \circ \rho_1 \circ \hat{\phi}_{21}(x)$$
$$(\hat{\phi}_{321})_2(x) = \phi_3(z) = \hat{\phi}_{21}(x)_2 + Q_8 \circ \rho_2 \circ \hat{\phi}_{21}(x)$$
$$(\hat{\phi}_{321})_i(x) = \hat{\phi}_{21}(x)_i, \quad i = 3, \ldots, 100.$$

Thus it suffices to find a linear subvariety on which the functions $Q_8 \circ \rho_i \circ \hat{\phi}_{21}(x)$ are constant.

Define $q : K^{19} \to K^{30}$, $\pi_i : K^{64} \to K^{19}$ and $\rho_i : K^{100} \to K^{30}$ for $i = 1, 2$ by

$$q(x_1, \ldots, x_{19}) = (q_1(x_1, \ldots, x_{19}), \ldots, q_{30}(x_1, \ldots, x_{19}))$$
$$\pi_1(x_1, \ldots, x_{64}) = (x_9, x_{11}, \ldots, x_{16}, x_{51}, x_{52}, \ldots, x_{62})$$
$$\pi_2(x_1, \ldots, x_{64}) = (x_{10}, x_{17}, \ldots, x_{20}, x_{15}, x_{16}, x_{51}, \ldots, x_{60}, x_{63}, x_{64})$$

**Lemma 1.** *For $i = 1, 2$, $\rho_i \circ \hat{\phi}_2 = \rho_i \circ \hat{\phi}_{32} = q \circ \pi_i$.*

*Proof.* The fact that $\rho_i \circ \hat{\phi}_2 = q \circ \pi_i$ is a routine calculation. The remaining equality follows from the fact that $\rho_i \circ \phi_3 = \rho_i$. □

We now break the polynomial $Q_8$ into components:

$$Q_8(z_1, \ldots, z_{30}) = z_1^8 + S(z_1, \ldots, z_{30})^2[z_9^4 + T_1(z_1, \ldots, z_{30})T_2(z_1, \ldots, z_{30})] + z_{29}^4 + z_{30}^2.$$

where

$$S(z_1, \ldots, z_{30}) = z_2^2 + z_3^2 + z_3 z_8 + z_4 z_5 + z_6 z_{12} + z_7 z_{13}$$
$$T_1(z_1, \ldots, z_{30}) = z_{10}^2 + z_{14}z_{15} + z_{18}z_{19} + z_{20}z_{21} + z_{22}z_{24}$$
$$T_2(z_1, \ldots, z_{30}) = z_{11}^2 + z_{16}z_{17} + z_{23}z_{28} + z_{25}z_{26} + z_{13}z_{27}$$

It is easily verified that

$$S(q_1,\ldots,q_{30}) = z_2^4$$
$$T_1(q_1,\ldots,q_{30}) = z_8^4$$
$$T_2(q_1,\ldots,q_{30}) = z_9^4$$

and hence that $Q_8(q_1,\ldots,q_{30}) = z_{19}^2$.

First we find a linear subvariety on which $S$, $T_1$ and $T_2$ are constant. To do this we introduce a little more notation. Let $\mathcal{O}[K^{64}]$ denote the polynomial functions on $K^{64}$ and let $\mathcal{L}$ denote the subspace of linear functions. Set $y_i = F(x_i)$. Denote by $\mathcal{S}$ the subspace of $\mathcal{O}[K^{64}]$ generated by the set $\{y_i^{2^6}y_j^{2^6}, y_i^{2^6}, y_i^{2^7}, 1 \mid 1 \leq i \leq 100\}$. Consider the space $\mathcal{L}\cap\mathcal{S}$. If $g \in \mathcal{L}\cap\mathcal{S}$, then we may write

$$g = \sum_{i,j} a_{ij}y_i^{2^6}y_j^{2^6} + \sum_k b_k y_k^{2^6} + \sum_l c_l y_l^{2^7} + d$$

for some $a_{ij}, b_k, c \in K$. For any specific ciphertext $y' \in K^{100}$, we may set $g(y') = \sum_{i,j} a_{ij}(y_i')^{2^6}(y_j')^{2^6} + \sum_k b_k(y_k')^{2^6} + \sum_l c_l(y_l')^{2^7} + d$. Define the linear subvariety $V_1$ by

$$V_1 = \mathcal{V}(g - g(y') \mid g \in \mathcal{L}\cap\mathcal{S})$$

The rationale for considering $V_1$ is that the functions $S\circ\rho_i\circ\hat{\phi}_2$, $T_1\circ\rho_i\circ\hat{\phi}_2$ and $T_2\circ\rho_i\circ\hat{\phi}_2$ are all constant on $V_1$. This fact is an immediate corollary of the following proposition.

**Proposition 1.** *The functions $S^{2^6}\circ\rho_i\circ\hat{\phi}_{21}$, $T_1^{2^6}\circ\rho_i\circ\hat{\phi}_{21}$ and $T_2^{2^6}\circ\rho_i\circ\hat{\phi}_{21}$ all lie in $\mathcal{L}\cap\mathcal{S}$.*

*Proof.* Notice that

$$S\rho_1\circ\hat{\phi}_2(x) = S\circ q\circ\pi_1(x) = x_{11}^4$$

Hence, $S^{2^6}\circ\rho_i\circ\hat{\phi}_2(x) = (x_{11}^4)^{2^6} = x_{11}$. But $S^{2^6}\circ\rho_i\circ\hat{\phi}_{21} = S^{2^6}\circ\rho_i\circ\hat{\phi}_2\circ\tilde{\phi}$ and both $S^{2^6}\circ\rho_i\circ\hat{\phi}_2$ and $\tilde{\phi}$ are linear. Hence $S^{2^6}\circ\rho_i\circ\hat{\phi}_{21} \in \mathcal{L}$. Now observe that

$$S^{2^6}\circ\rho_1\circ\hat{\phi}_{21}(x) = S^{2^6}\circ\rho_1\circ\hat{\phi}_{321} = S^{2^6}\circ\rho_1\circ\phi_4^{-1}\circ F(x) = S^{2^6}\circ\rho_1\circ\phi_4^{-1}(y)$$

Since $\rho_1\circ\phi_4^{-1}$ is linear and

$$S(z)^{2^6} = z_2^{2^7} + z_3^{2^7} + z_3^{2^6}z_8^{2^6} + z_4^{2^6}z_5^{2^6} + z_6^{2^6}z_{12}^{2^6} + z_7^{2^6}z_{13}^{2^6}$$

it is clear that $S^{2^6}\circ\rho_1\circ\hat{\phi}_{21} = S^{2^6}\circ\rho_1\circ\phi_4^{-1}\circ F \in \mathcal{S}$. An analogous argument works for the other five cases. $\square$

It is easily verified that the six functions described in the above proposition are linearly independent. Thus $\dim\mathcal{L}\cap\mathcal{S} \geq 6$. However we will not need this fact in what follows.

We now repeat this procedure to restrict to a smaller linear subvariety. Denote by $\mathcal{T}$ the subspace of $\mathcal{O}[K^{64}]$ generated by the set $\{y_i^4, y_i^2, y_i, 1 \mid 1 \leq i \leq 100\}$. Consider the space $\mathcal{L}_{\mathcal{T}} = \{g \in \mathcal{L} \mid g|_{V_1} = h|_{V_1} \text{ for some } h \in \mathcal{T}\}$.

**Proposition 2.** *The functions $Q_8^{2^7}\circ\rho_i\circ\hat{\phi}_{21}$ belong to $\mathcal{L}_{\mathcal{T}}$.*

*Proof.* The fact that $Q_8^{2^7}\circ\rho_i\circ\hat{\phi}_{21} \in \mathcal{L}$ follows from the fact that $Q_8(q_1,\ldots,q_{30}) = z_{19}^2$. As in the proof of the previous proposition,

$$Q_8^{2^7}\circ\rho_1\circ\hat{\phi}_{21}(x) = Q_8^{2^7}\circ\rho_1\circ\hat{\phi}_{321}(x) = Q_8^{2^7}\circ\rho_1\circ\phi_4^{-1}\circ F(x) = Q_8^{2^7}\circ\rho_1\circ\phi_4^{-1}(y)$$

and $\rho_1 \circ \phi_4^{-1}$ is linear. Since

$$Q_8(z_1, \ldots, z_{30}) = z_1^8 + S(z_1, \ldots, z_{30})^2[z_9^4 + T_1(z_1, \ldots, z_{30})T_2(z_1, \ldots, z_{30})] + z_{29}^4 + z_{30}^2,$$

the previous proposition implies that $Q_8^{2^7} \circ \rho_i \circ \hat{\phi}_{21}$ coincides with an element of $\mathcal{T}$ on $V_1$. □

If $g \in \mathcal{T}$, then we may write

$$g = \sum_i a_i y_i^4 + b_i y_i^2 + c_i y_i + d$$

for some $a_i, b_i, c_i, d \in K$. For any specific ciphertext $y' \in K^{100}$, again set $g(y') = \sum_i a_i(y_i')^4 + b_i(y_i')^2 + c_i(y_i') + d$. Define the linear subvariety $V \subset V_1$ by

$$V = \mathcal{V}(g - g(y') \mid g \in \mathcal{L}_{\mathcal{T}}).$$

**Theorem 1.** *The functions $Q_8 \circ \rho_i \circ \hat{\phi}_{21}$ for $i = 1, 2$ are constant on the linear subvariety $V$.*

For a given plaintext $x'$ let $a_i = Q_8 \circ \rho_i \circ \hat{\phi}_{21}(x')$. Define $\phi_3'$ be the function:

$$\begin{aligned}
\phi_{3,1} &= x_1 + a_1 \\
\phi_{3,2} &= x_2 + a_2 \\
\phi_{3,i} &= x_i, \quad i = 3, \ldots, 100;
\end{aligned}$$

and let $F' = \phi_4 \circ \phi_3' \circ \phi_2 \circ \phi_1 \circ e$. Then $F$ and $F'$ coincide on the linear subvariety $V$ containing $x'$. Since $F'$ is evidently of de Jonquiere type, we can invert $F|_V$, using the procedure described below, thereby finding the ciphertext $x'$.

## 3. The attack procedure and its complexity

We perform three steps to derive the plaintext $(x_1', \ldots, x_{64}')$ from the ciphertext $(y_1', \ldots, y_{100}')$. The first step is a common step for any given ciphertext.

*Step 1 of the attack*

*Find a basis for the space $W_1$ of solutions of the equations*

$$\sum_{i,j=1}^{100} a_{ij} y_i^{2^6} y_j^{2^6} + \sum_{k=1}^{100} b_k y_k^{2^6} + c + \sum_{m=1}^{64} d_m x_m = 0.$$

*in the unknowns $a_{ij}, b_k, c, d_m$.*

This system of equations involves $5215 = 100 + 50 \times 99 + 100 + 64 + 1$ variables and $812353 = 1 + 64 + (32 \times 63 + 48) + (48 + 32 \times 63 + (64 \times 63 \times 62/6)) + (48 + 32 \times 63 \times 3 + (64 \times 63 \times 62/6) \times 3 + (64 \times 63 \times 62 \times 61/24)$ equations. Since the number of equations far exceeds the number of variables, we do not need to use all of the equations to find the solution. In practice we can randomly choose 8000 equations; the probability that we will not find the complete solution is essentially zero. Solving these linear equations, involves row operations on an $8000 \times 5215$ matrix. However, because we are working over a finite field with only $2^8$ elements, the row operations corresponding to each column requires at most $2^8 - 1$ multiplication of any given row. Elimination of each variable takes, on average, $(2^8 - 1) \times 8000/2$ multiplications. Therefore the solution of these equations requires at most $5215 \times (2^8 - 1) \times 8000/2 \doteq 2^{33}$ computations on the finite field $K$. Moreover this step is independent of the value of the ciphertext $y'$

Because we are working over the fixed field $K$, we can perform the computation of multiplication on $K$ by first finding a generator $g$ of the multiplicative group of $K$, storing the table of elements of $K$ in the form $g^k$, then computing the multiplication by two searches and one addition. This will improve the speed by at least a factor of 2. Thus, this preliminary step takes at most $2^{32}$ computations.

*Step 2 of the attack*

*Step 1 yields a set of equations of $x$ of the form*

$$\sum_{m=1}^{64} d_m x_m = \sum_{i,j=1}^{100} a_{ij} y_i^{2^6} y_j^{2^6} + \sum_{k=1}^{100} b_k y_k^{2^6} + c.$$

*For a given ciphertext $(y'_1, .., y'_{100})$, we substitute these values into the right hand side to derive a set of linear equations in $x_i$. Solving this system by Gaussian elimination enables us to eliminate a certain set of, say, $s$ $x_i$'s by expressing them as linear expressions in the remaining variables. We may then substitute these expressions into the $y_i$ to produce a new set of functions, $\tilde{y}_i$ for $i = 1, \ldots, 100$, in the remaining $64 - m$ variables.*

This process corresponds to the identification as a vector space of the linear subvariety $V_1$ described in the previous section.

*Step 3 of the attack*

*Find a basis for the space of solutions of the system of equations*

$$\sum_{i=1}^{100} \tilde{a}_i \tilde{y}_i^4 + \sum_{i=1}^{100} \tilde{b}_i \tilde{y}_i^2 + \sum_{i=1}^{100} \tilde{c}_j \tilde{y}_j + \tilde{d} + \sum_{i=1}^{64-m} e_i x_{k_i} = 0.$$

*in the unknowns $\tilde{a}_i, \tilde{b}_i, \tilde{c}_j$ and $\tilde{d}$. We then repeat the procedure of step 2. Each element of this basis yields an equation of this form into which we can again substitute the ciphertext. this gives a system of linear equations, which we can again solve to eliminate a further set of say $\tilde{m}$ variables. Substituting for these variables in the $\tilde{y}_i$, $\hat{y}_i$.*

For the first part, the number of variables is 301 and the number of equations is $3 \times ((64 - m)(64 - m + 3)/2 < 5307$. The computation in this step takes no significant time compared to that of Step 1.

The span of the remaining $x_i$'s forms a vector space that we are identifying naturally with the linear subspace $V$ described above. We now proceed to "invert" $F|_V$. Since this map is essentially of de Jonquiere type, this procedure is fairly standard. We aim to solve the system of polynomial equations $\hat{y}_i - y'_i = 0$. Since the map $F|_V$ is of de Jonquiere type, the vector space spanned by the polynomial functions $\hat{y}_i - y'_i$ intersects $\mathcal{L}$ nontrivially; i.e., it contains a linear function of the $x_i$. This enables us to substitute for one of the $x_i$'s, thereby reducing the number of variables. The nature of a function of de Jonquiere type, then enables us to iterate this process.

*Step 4 of the attack*

*We now proceed to "invert" $F|_V$. Since this map is essentially of de Jonquiere type, this procedure is fairly standard. We aim to solve the system of polynomial equations $\hat{y}_i - y'_i = 0$.*

*Since the map $F|_V$ is of de Jonquiere type, the vector space spanned by the polynomial functions $\hat{y}_i - y'_i$ intersects $\mathcal{L}$ nontrivially; i.e., it contains a linear function of the $x_i$. This enables us to substitute for one of the $x_i$'s, thereby reducing the number of variables. The nature of a function of de Jonquiere type enables us to iterate this process. This elimination process enables us to find the coordinates $x'_i$ of the plaintext corresponding to the variables involved in the $\hat{y}_i$. We use the linear equations derived in the previous steps to find the remaining coordinates.*

Again, this procedure takes no significant time compared to that of Step 1. Thus the three steps together require at most $2^{33}$ computations.

## 4. Conclusion

We have shown that implementation scheme in [M] is not secure. The complexity of the computation needed to defeat the scheme is less than $2^{33}$.

The problem is to solve the system of equations $y'_i = F_i(x_1, \ldots, x_{64})$. We know there exists a set of polynomials $G_j$ such that the solution is given by $x_j = G_j(y'_1, \ldots, y'_{100})$. The standard method of attack is to look for polynomials $G_j(y_1, \ldots, y_{100})$ of low degree. However, this is often impossible. Instead we search for low degree polynomials $\bar{G}_j$ such that $\bar{G}_j(y_1^{2^6}, \ldots, y_{100}^{2^6})$ produces linear combinations of the $x_i$.

Recently a family of versions of the functions $Q_8$ with much higher degrees was described in [CGC]. These again decompose into terms analogous to the $S$, $T_1$ and $T_2$ above and hence can be defeated by an analogous approach. Thus the security of such systems depends crucially on the construction of the function that plays the role of $Q_8$.

We do not, however, claim that all such $Q_8$-type implementations make the system insecure. For example, a new suggestion in [CM] seems very different and we can not directly apply our method in this situation. However even for this case, it is possible that an extention of our method further could succeed in defeating this more complicated system.

The web site of the US Data Security poses a number of challenges concerning the TTM cryptosystem. Professor Moh informed us that the scheme defeated in this article is essentially Learner's Challenge I in the web site. In order to defeat this challenge we need to first find the functions $y_i$. Since these are not given explicitly, this requires the encoding of thousands of plaintexts. Because of the limited access to the cipher, we have not yet been able to compute the $y_i$ explicitly.

**Acknowledgment**

We would like to thank Professor T.T. Moh for comments on this paper.

## References


[CM] Chen, J., Moh, T., *On the Goubin-Courtois Attack on TTM* , Cryptology ePrint Archive (2001/72).

[CGC] Chou, G., Guan, J. Chen J. *A systematic Construction of a $Q_{2^k}$-model in TTM*, Comm. Algebra 30 (2002), no. 2, 551–562.

[CG] Goubin, L., Courtois, N., *Cryptanalysis of the TTM cryptosystem*, Asiacrypt2000, LNCS 1976, 44-57.

[D] Dickerson, Matthew, *The inverse of an automorphism in polynomial time.* J. Symbolic Comput. 13 (1992), no. 2, 209–220.

[MI] Matsumoto, T., Imai, H., *Public quadratic polynomial-tuples for efficient signature-verification and message-encryption*, Advances in cryptology—EUROCRYPT '88 (Davos, 1988), 419–453, Lecture Notes in Comput. Sci., 330, Springer, Berlin, 1988.

[M] Moh, T. T., *A fast public Key System with Signature and Master key functions*, Communications in Algebra, 27(5), (1999), 2207-2222 ( http://www.usdsi.com/ttm.html )

[P] Patarin, J., *Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88.*, Des. Codes Cryptogr. 20 (2000), no. 2, 175–209.



*E-mail address*: `ding@math.uc.edu, timothy.hodges@uc.edu`

Department of Mathematical Sciences, University of Cincinnati, Cincinnati, OH, 45221-0025 USA