On the Goubin-Courtois Attack on TTM

T. Moh*and Jiun-Ming Chen

Abstract

In the paper [1] published in "Asiacrypt 2000", L. Goubin and N.T. Courtois propose an attack on the TTM cryptosystem. In paper [1], they mispresent TTM cryptosystem. Then they jump an attack from an example of TTM to the general TTM cryptosystem. Finally they conclude:"There is very little hope that a secure triangular system (Tame transformation system in our terminology) will ever be proposed". This is serious challenge to many people working in the field.

In this paper, we will show that their attack is full of gaps in section 5. Even their attack on one implementation of TTM is questionable. We write a lengthy introduction to restate TTM cryptosystem and point out many possible implementations. It will be clear that their attack on one implementation can not be generalized to attacks on other implementations. As one usually said: "truth is in the fine details", we quote and analysis their TPM system at the end of the introduction and § 2. We further state one implementations of TTM cryptosystem in § 3. We analysis their MiniRank(r) attack in § 4 and show that is infeasible.

We conclude that the attack of [1] on the TTM cryptosystem is infeasible and full of gaps. There is no known attacks which can crack the TTM cryptosystem.

1 Introduction

In the past the most successful public-key encryption systems, such as RSA and ElGamal systems, are one dimensional. Their speeds might have to be accelerated by using hardware, and their applications become expensive. From a mathematical point of view, it will be natural to try higher dimensional methods, i.e., multivariate public-key encryption systems. As Kipnis and Shamir stated in [10]: "The RSA public key cryptosystem is based on a single modular equation in one variable. A natural generalization of this approach is to consider system of several modular equations in several variables." In Matsumoto-Imai theory ([5]), a polynomial of one variable (i.e., one dimensional) is expressed with respect to a field basis to achieve an expression of several variables (i.e., higher dimensional). Their attempt is noble, however, unsuccessful, since it has been cracked by Patarin. Patarin proposed another public-key system using "Hidden Field Equations (HFE)" in [8]. Its decryption involves solving equations, and hence the process is slow.

The TTM cryptosystem (cf [6],[7]) is a truly higher dimensional method. It is given by the composition of *tame* mappings $\pi(=\prod_i \Phi_i)$ from K^n to K^m where K is a finite field and $n \leq m$. The public key is the composition π while the private key is the set of mappings $\{\Phi_i\}$. The *tame* mappings, which are commonly known in mathematics, are defined as

*Math Department, Purdue University, West Lafayette, Indiana 47907-1395. tel: (765)-494-1930, e-mail ttm@math.purdue.edu

Definition: We define a *tame* mapping $\phi_i = (\phi_{i,1}, \cdots, \phi_{i,n})$ as either a linear transformation, or of the following form in any *order* of variables $x_1, \cdots, x_n$ with polynomials $h_{i,j}$,

$$\begin{aligned}
&(1): \phi_{i,1}(x_1, \cdots, x_n) = x_1 = y_1 \\
&(2): \phi_{i,2}(x_1, \cdots, x_n) = x_2 + h_{i,2}(x_1) = y_2 \\
&\cdots\cdots\cdots \\
&(j): \phi_{i,j}(x_1, \cdots, x_n) = x_j + h_{i,j}(x_1, \cdots, x_{j-1}) = y_j \\
&\cdots\cdots\cdots \\
&(m): \phi_{i,n}(x_1, \cdots, x_n) = x_n + h_{i,n}(x_1, \cdots, x_{n-1}) = y_n
\end{aligned}$$

An important property of tame mapping ϕ_i is that not only we may find the values of $\{y_1, \cdots, y_n\}$ from the values of $\{x_1, \cdots, x_n\}$ by substitutions, but also the values of $\{x_1, \cdots, x_n\}$ from the values of $\{y_1, \cdots, y_n\}$ by finding Φ_i^{-1} if it is linear or if it is not linear as in the above definition by finding the value of x_1 (which is y_1), and then the value of x_2 (which is $y_2 - h_{i,2}(y_1)$), and so on. This property makes the decoding extremely fast with the help of the private key (i.e, each individual mapping Φ_i). In TTM system, the speed of the deciphering process is in general faster than the encrypting process. In many past multivariate public-key encryption systems, it is inevitable to use "searching" or "solving equations" to decipher, and thus slow down the speed to almost unbearable. We will see that is what happens to the TPM system [1] (see below).

It can be done for a composition of mappings, as in the case of TTM, that the degrees of mappings (which is defined for every mapping ϕ_i to be the maximum of the degrees of all coordinate polynomials $\{\phi_{i,j}\}$) may not increase after compositions, i.e., say, if all $\phi_{i,j}$'s are of degree two or less, then their composition $\prod \phi_i$ may have coordinate polynomials of degree two or less. For instance, let $\phi_i = (\phi_{i,1}, \cdots, \phi_{i,8})$ for $i = 1, 2$ be defined as

$$\begin{aligned}
&(1): \phi_{1,1}(x_1, \cdots, x_8) = x_1 \\
&(2): \phi_{1,2}(x_1, \cdots, x_8) = x_2 \\
&(3): \phi_{1,3}(x_1, \cdots, x_8) = x_3 + x_1^2 \\
&(4): \phi_{1,4}(x_1, \cdots, x_8) = x_4 + x_1 x_2 \\
&(5): \phi_{1,5}(x_1, \cdots, x_8) = x_5 + x_2^2 \\
&(6): \phi_{1,6}(x_1, \cdots, x_8) = x_6 + x_2 x_3 \\
&(7): \phi_{1,7}(x_1, \cdots, x_8) = x_7 + x_1 x_5 \\
&(8): \phi_{1,8}(x_1, \cdots, x_8) = x_8 + x_1^2
\end{aligned}$$

and

$$\begin{aligned}
&(1): \phi_{2,1}(x_1, \cdots, x_8) = x_1 \\
&(2): \phi_{2,2}(x_1, \cdots, x_8) = x_2 \\
&(3): \phi_{2,3}(x_1, \cdots, x_8) = x_3 \\
&(4): \phi_{2,4}(x_1, \cdots, x_8) = x_4
\end{aligned}$$

$$
\begin{aligned}
(5) &: \phi_{2,5}(x_1, \cdots, x_8) = x_5 \\
(6) &: \phi_{2,6}(x_1, \cdots, x_8) = x_6 \\
(7) &: \phi_{2,7}(x_1, \cdots, x_8) = x_7 \\
(8) &: \phi_{2,8}(x_1, \cdots, x_8) = x_8 + x_3x_5 + x_4^2 + x_1x_7 + x_2x_6
\end{aligned}
$$

It is clear that with $\pi = \phi_2\phi_1 = (\pi_1, \cdots, \pi_8)$, we have the following,

$$
\begin{aligned}
(1) &: \pi_1(x_1, \cdots, x_8) = x_1 \\
(2) &: \pi_2(x_1, \cdots, x_8) = x_2 \\
(3) &: \pi_3(x_1, \cdots, x_8) = x_3 + x_1^2 \\
(4) &: \pi_4(x_1, \cdots, x_8) = x_4 + x_1x_2 \\
(5) &: \pi_5(x_1, \cdots, x_8) = x_5 + x_2^2 \\
(6) &: \pi_6(x_1, \cdots, x_8) = x_6 + x_2x_3 \\
(7) &: \pi_7(x_1, \cdots, x_8) = x_7 + x_1x_5 \\
(8) &: \pi_8(x_1, \cdots, x_8) = x_8 + x_1^2 + x_3x_5 + x_4^2 + x_1x_7 + x_2x_6
\end{aligned}
$$

The degree of $\phi_2\phi_1$ stays 2. This intrinsic property can be used to keep the sizes of public keys down.

The other interesting property of compositions of tame mappings is that many highest homogeneous parts of the coordinate polynomials can be created. Thus the system is protected from many known attacks using the exact vector spaces generated by the highest homogeneous parts, the dimensions of the said vector spaces, etc. .

It is a common feeling among mathematicians that it is much harder to factor polynomial (i.e., non-linear) mappings than to factor integers. It is known among algebraic geometers that it is extremely hard with a given mapping π (i.e., the public-key) to find its *tame* decomposition (the private key).

What is the **General Principle** of TTM? To avoid further confusions, let us quote from [6] or [7],

Principle (of TTM): Let m, n, r, s be positive integers. Let $n + r \geq 3$, and $\mathbf{K}$ a field of 2^m elements. Let the user select k tame automorphism $\phi_k, \cdots, \phi_2, \phi_1$ of $\mathbf{K}^{n+r}$. Let $\pi = \phi_k \cdots \phi_2\phi_1 = (\pi_1, \cdots, \pi_{n+r})$. Let $\hat{\pi} = (\pi_1(x_1, \cdots, x_n, 0, \cdots, 0), \cdots, \pi_{n+r}(x_1, \cdots, x_n, 0 \cdots, 0))$, and $f_i(x_1, \cdots, x_n) = \pi_i(x_1, \cdots, x_n, 0, \cdots, 0)$ for $i = 1, \cdots, n + r$.

The user will announce the map $\hat{\pi} = (f_1, \cdots, f_{n+r})$: $\mathbf{K}^n \mapsto \mathbf{K}^{n+r}$ and the field $\mathbf{K}$ of 2^m elements as the public key.

Given a plaintext $(x'_1, \cdots, x'_n) \in \mathbf{K}^n$. The sender evaluates $y'_i = f_i(x'_1, \cdots, x'_n)$. Then the ciphertext will be $(y'_1, \cdots, y'_{n+r}) \in \mathbf{K}^{n+r}$.

The legitimate receiver (i.e., the user) recovers the plaintext by $(x'_1, \cdots, x'_n, 0, \cdots, 0) = \phi_1^{-1} \cdots \phi_k^{-1}(y'_1, \cdots, y'_{n+r})$ (see **Corollaries** 2 & 3). The private key is the set of maps $\{\phi_1, \cdots, \phi_k\}$. ∎

It goes without saying that the above principle is different from the **General Principle** stated in § 2.4 of [1]. It is doubtful that their have read [6] or [7] (which are in the reference of [1]). No wonder that they confused the TTM cryptosystem with some implementations of TTM cryptosystem. It is easy to see that RSA is not some examples (say smooth integers) of RSA, and ECC is not some examples (say supersymmetric EC) of ECC. The only way to crack TTM is to attack the principle as above (cf [6] and [7]). As for the implementations of TTM, there are millions possibilities. Some may cut too much corner to speed up, these are common problems of any cryptosystem. Therefore, "crack" any particular implementation without a sound theoretical reason does not mean too much.

Simplified Version: We consider only four maps $\Phi_1, \Phi_2, \Phi_3, \Phi_4$ with the map $\pi = \Phi_4\Phi_3\Phi_2\Phi_1$ where Φ_1 is an affine linear map of K^n to the subspace of K^m with the last $m-n$ coordinates zeroes, Φ_2, Φ_3 non-linear tame maps and Φ_4 an affine linear map of K^m to K^m. Let us look at the composition $\Phi_3\Phi_2$, after we set $x_{n+1} = \cdots = x_m = 0$, which can be expressed as

$$\Phi_3\Phi_2 = \begin{cases} y_1 = x_1 + P_1(y_{i+1}, \cdots, y_m) = x_1 + P_1(x_{i+1} + f_{i+1}(x_1, \cdots, x_{i-1}), \cdots, f_m(x_1, \cdots, x_n)) \\ y_2 = x_2 + P_2(y_{i+1}, \cdots, y_m) = x_2 + P_2(x_{i+1} + f_{i+1}(x_1, \cdots, x_{i-1}), \cdots, f_m(x_1, \cdots, x_n)) \\ \cdots \\ y_i = x_i + P_i(y_{i+1}, \cdots, y_m) = x_i + P_i(x_{i+1} + f_{i+1}(x_1, \cdots, x_{i-1}), \cdots, f_m(x_1, \cdots, x_n)) \\ y_{i+1} = x_{i+1} + f_{i+1}(x_1, \cdots, x_i) \\ \cdots \\ y_n = x_n + f_n(x_1, \cdots, x_{n-1}) \\ y_{n+1} = 0 + f_{n+1}(x_1, \cdots, x_n) \\ \cdots \\ y_m = 0 + f_m(x_1, \cdots, x_n) \end{cases}$$

■

Note that in [6] or [7], only examples with $i = 2$ are given, while it is trivial to consider any i. Thus the simplified version of TTM cryptosystem is more general than the **General Principle** of § 2.4 of [1].The functions of Φ_1, Φ_4 are used to (1) creating a large number of public-keys, and (2) hidding the variables x_i and functions y_j.

Since the simplified TTM cryptosystem have speeds of tens of millions bit per second for both encryption and decryption([4], http://www.usdsi.com), and with a reasonable small public-key (about 4k bytes) and an even smaller private key (about 500 bytes) which can be used as a public key by simply composed the mappings $\prod \Phi_i$, concerned people shall provide "attacks" on the simplified version.

In [1] L. Goubin and N.T. Courtois introduce TPM as

"- n, u, r integers such that $r \leq n$. We also systematically put $m = n + u - r$.

"- $K = GF(q)$ a finite field.

"We first consider a function $\Psi : K^n \to K^{n+u-r}$ such that $(y_1, \cdots, y_{n+u-r}) = \Psi(x_1, \cdots, x_n)$

is defined by the following system of equations:

$$
\begin{cases}
y_1 = x_1 + g_1(\qquad\qquad\qquad\qquad x_{n-r+1}, \cdots, x_n) \\
y_2 = x_2 + g_2(x_1; \qquad\qquad\qquad\quad x_{n-r+1}, \cdots, x_n) \\
y_3 = x_3 + g_3(x_1, x_2; \qquad\qquad\quad x_{n-r+1}, \cdots, x_n) \\
\cdots \\
y_{n-r} = x_{n-r} + g_{n-r}(x_1, \cdots, x_{n-r-1}; x_{n-r+1}, \cdots, x_n) \\
y_{n-r+1} = g_{n-r+1}(x_1, \cdots, x_n) \\
\cdots \\
y_{n-r+u} = g_{n-r+u}(x_1, \cdots, x_n)
\end{cases}
$$

with each $g_i (1 \leq i \leq n + u - r)$ being a randomly chosen quadratic polynomial."

For later references, we will state the following trivial lemma:

Lemma 1 *For a TPM system as above, we always have $r \geq$ co-dimension of the vector subspace generated by the linear parts of $\{y_i\}$ in the vector space of all 1-forms in $\{x_i\}$.*

■

2 On the TPM system and the Searching Process

Their presentation of TPM system is unclear from our point of view. To clarify the issue involved, let us define,

Definition A partial tame series of length n-r is the last n-r part of a tame transformation, i.e.,

$$
\begin{aligned}
&(r+1) : \phi_{i,r+1}(x_1, \cdots, x_n) = x_{r+1} + h_{i,r+1}(x_1, \cdots, x_r) = y_{r+1} \\
&\cdots\cdots\cdots \\
&(n) : \phi_{i,n}(x_1, \cdots, x_n) = x_n + h_{i,n}(x_1, \cdots, x_{n-1}) = y_n
\end{aligned}
$$

Then we have the following simple lemmas for future uses:

Lemma 2 *The so-called MiniRank(r) attack part (cf § 2.1 of [1]) of a TPM system, the block of first n-r equations, is a partial tame series of length n-r.*

Proof. We simply re-order the variables as $\{x_{n-r+1}, \cdots, x_n, x_1, \cdots, x_{n-r}\}$. ■

Lemma 3 *For the so-called MiniRank(r) attack part (cf § 2.1 of [1]) of a TPM system, the block of first n-r equations, we always have $r =$ co-dimension of the vector subspace generated by the linear parts of $\{y_i\}$ in the vector space of all 1-forms in $\{x_i\}$.*

In [1] the authors spend pages to describe their proposed TPM system. Finally, they show that their system is "insecure" because they designed an a MiniRank(r) attack to crack it.

We like to point out a main problem, using searching process to decrypt, of many multivariate cryptosystems. The TPM cryptosystem is one of them. Let us examine it.

Let us consider the commonly useful situation $K = GF(2^8)$, i.e., $q = 2^8$. If $r = n$, then all useful equations are discarded with only "random" type equations left. The legitimate user is on the same footing as the attacker. No one will dream such a nightmare. If r is not really "small" as $0, 1, 2, 3$, the decrypting process as described in § 2.2 of [1] with searching through K^r for the correct values of $\{x_{n-r+1}, \cdots, x_n\}$ will be painfully slow. If $r \geq 9$, then there are $2^{8\times 9} = 2^{72}$ possibilities for searching, i.e., it will be physically impossible to find the correct plaintext for the legitimate user. Even if $r = 4, 5, 6, 7, 8$, the legitimate user still has to search through $2^{32}, 2^{40}, 2^{48}, 2^{56}, 2^{64}$ possibilities, the decrypting process will be impractical. Assume that we have a computer with speed 10^{10} operations per second, it will take thirty years to search through 2^{64} possibilities, with the improbable assumption that it takes only one operation to verify one possibility which includes loading data, performing computations and checking the result to see if it is "meaningful". In other words, it will take at least thirty years to decrypt just one block. On the other hand, for $r = 0, 1, 2, 3$, according to their analysis if true, the system can be cracked with a complexity $q^{\lceil \frac{m}{n} \rceil r} \times m^3 \leq 2^{68}$ if $q = 2^8, m \leq 100$ and $\lceil \frac{m}{n} \rceil = 2$. Therefore, the hypothetic TPM cryptosystem is either too slow (slower than one bit per second for decrypting) or insecure in the cases we have discussed.

Many multivariate cryptosystems fall into the same traps of searching, and only can be used for signatures. The TTM cryptosystem applies a subtle mathematical phenomenon; it is very fast to use the decomposition of the map π into the product $\prod_i \Phi_i$, where every Φ_i is *tame*, to decrypt the ciphertext. There is no "searching" as used in the TPM system. The speed of TTM encryption system can easily reach tens of million bits per second ([4], http://www.usdsi.com) which is very close to the fast modern secret key system AES.

Why the useless TPM system is introduced? Clearly, for the purpose to state unsubstantially that "TTM belongs to TPM(64,38,2,GF(256))" as in [1], and then "crack" TTM by "crack "TPM(?,?,2,GF(256)).

3 An example of TTM

The cryptanalysis of TTM has been studied in [6], [7]. A new attack is proposed in [1] which will be answered by the present article. For the sake of attacking TTM system, one may simply apply the analysis of their TPM system to the TTM system. We should use their main conclusion (while disregard their arguments to reach it, after all the conclusion is the only useful result) of a formula of $q^{\lceil \frac{m}{n} \rceil r} \times m^3$ to the TTM, where q is the number of elements in the ground field, m is the length of the ciphertexts and n is the length of the plaintexts. What is the significant number r? It has never been discussed in [1]. We are simply told r is 2 for TTM cryptosystems. Why?

Maybe we have to do their work. Let us give an example to show that this number may easily be 4 or more, and the cryptosystem is strong.

The kernel construction of an implementation of the TTM cryptosystem is to construct polynomials $P_1, \cdots, P_i$ which are essentially copies of a **component** $\mathbf{Q}_8$ in [6][7]. Every

component $\mathbf{Q}_8$ will generate a huge number of public keys. The construction of **component** $\mathbf{Q}_8$ is highly technical and quite mathematical. One of the main purposes of the present article is to present a new **component** $\mathbf{Q}_8$ to the readers to illustrate that mathematically there are many possible ways to implement TTM.

Example of component $\mathbf{Q}_8$: Let us define a $\mathbf{Q}_8$ as follows,

$\mathbf{Q}_8$: Let the field $\mathbf{K}$ be of 2^8 elements, and $a_i \neq 0$ for $i = 1, 2, 3$. Let

$$
\begin{array}{ll}
q_1(a_1,a_2,a_3,x_1,\cdots,x_{11}) = x_4x_2 + a_1x_5; & q_2(a_1,a_2,a_3,x_1,\cdots,x_{11}) = x_3x_4 + a_1x_6; \\
q_3(a_1,a_2,a_3,x_1,\cdots,x_{11}) = x_2x_5 + a_1x_7; & q_4(a_1,a_2,a_3,x_1,\cdots,x_{11}) = x_4x_7 + a_1x_8; \\
q_5(a_1,a_2,a_3,x_1,\cdots,x_{11}) = x_1x_5 + a_1x_9; & q_6(a_1,a_2,a_3,x_1,\cdots,x_{11}) = x_1x_2 + a_2x_{10}; \\
q_7(a_1,a_2,a_3,x_1,\cdots,x_{11}) = x_9x_2 + a_2x_{11}; & q_8(a_1,a_2,a_3,x_1,\cdots,x_{11}) = x_9x_3 + a_1x_1; \\
q_9(a_1,a_2,a_3,x_1,\cdots,x_{11}) = x_1x_3; & q_{10}(a_1,a_2,a_3,x_1,\cdots,x_{11}) = x_1x_7 + a_1x_9; \\
q_{11}(a_1,a_2,a_3,x_1,\cdots,x_{11}) = x_9x_4 + a_1x_1; & q_{12}(a_1,a_2,a_3,x_1,\cdots,x_{11}) = x_9x_7 + a_1x_1; \\
q_{13}(a_1,a_2,a_3,x_1,\cdots,x_{11}) = x_3x_{11} + a_1x_{10}; & q_{14}(a_1,a_2,a_3,x_1,\cdots,x_{11}) = x_{10}x_5 + a_1x_{11}; \\
q_{15}(a_1,a_2,a_3,x_1,\cdots,x_{11}) = x_{10}x_3; & q_{16}(a_1,a_2,a_3,x_1,\cdots,x_{11}) = x_{10}x_2; \\
q_{17}(a_1,a_2,a_3,x_1,\cdots,x_{11}) = x_7x_8 + a_1x_7; & q_{18}(a_1,a_2,a_3,x_1,\cdots,x_{11}) = x_7x_5 + a_1x_2; \\
q_{19}(a_1,a_2,a_3,x_1,\cdots,x_{11}) = x_2x_3 + a_1x_7; & q_{20}(a_1,a_2,a_3,x_1,\cdots,x_{11}) = x_5x_8 + a_1x_5; \\
q_{21}(a_1,a_2,a_3,x_1,\cdots,x_{11}) = x_5x_4 + a_1x_6; & q_{22}(a_1,a_2,a_3,x_1,\cdots,x_{11}) = x_3x_8; \\
q_{23}(a_1,a_2,a_3,x_1,\cdots,x_{11}) = x_3x_5 + a_1x_8; & q_{24}(a_1,a_2,a_3,x_1,\cdots,x_{11}) = x_3x_7; \\
q_{25}(a_1,a_2,a_3,x_1,\cdots,x_{11}) = x_6x_8 + a_3x_5; & q_{26}(a_1,a_2,a_3,x_1,\cdots,x_{11}) = x_6x_2; \\
q_{27}(a_1,a_2,a_3,x_1,\cdots,x_{11}) = x_6x_5; & q_{28}(a_1,a_2,a_3,x_1,\cdots,x_{11}) = x_6x_7 + a_3x_2; \\
q_{29}(a_1,a_2,a_3,x_1,\cdots,x_{11}) = x_2x_{11}; & q_{30}(a_1,a_2,a_3,x_1,\cdots,x_{12}) = x_{11}x_4 + a_1x_{10}; \\
q_{31}(a_1,a_2,a_3,x_1,\cdots,x_{11}) = x_{10}x_7 + a_1x_{11}; & q_{32}(a_1,a_2,a_3,x_1,\cdots,x_{11}) = (x_3 + x_5)x_6 + a_1x_4; \\
q_{33}(a_1,a_2,a_3,x_1,\cdots,x_{11}) = x_{11}x_8; & q_{34}(a_1,a_2,a_3,x_1,\cdots,x_{11}) = x_{10}x_8; \\
q_{35}(a_1,a_2,a_3,x_1,\cdots,x_{11}) = x_{11}x_7 + a_1x_{10}; &
\end{array}
$$

Then the following Q_8 is a minimal generating polynomial of $a_1^{14}(x_1x_{11} + x_{10}x_9)$ with degree 8 in q_i,

$$
\begin{aligned}
Q_8 = \; & (q_5q_{13} + q_8q_{14})(q_{19}q_{32} + q_2(q_{18} + q_{24}))^2(q_{20}q_{19} + q_{23}q_{18})) + (q_{32}q_3 + (q_{18} + q_{24})q_{21})^2 \\
& (q_{22}q_{19} + q_{23}q_{24})(q_9q_{13} + q_8q_{15}) + a_1^8((q_{25}q_{26} + q_{27}q_{28})(q_6q_{29} + q_7q_{16}) \\
& +(q_{10}q_{30} + q_{11}q_{31})(q_{17}q_1 + q_{18}q_4)) + a_1^8a_2^4(q_6q_{33} + q_{34}q_7 + q_5q_{35} + q_{14}q_{12}) \\
& = a_1^{14}(x_1x_{11} + x_{10}x_9)
\end{aligned}
$$

■

By a trick of H. Hironaka [3] (and later, Patarin), it is easy to show that the expression $(x_1x_{11} + x_{10}x_9)$ needs four variables for any representation.

Lemma 4 *The maxima length of partial tame series of the above example is 7 and r=4.*

Proof. Note that $n = 11$ and x_3 is missing from all 1-forms. Moreover, if x_1 appears in some 1-form, then x_9 appears in the quadratic form, and if x_9 appears in some one 1-form, then x_1 appears in the quadratic form. Therefore x_1 and x_9 can not both appears in the 1-forms of any partial tame series. Same arguments hold for the pairs of $\{x_2, x_7\}, \{x_4, x_6\}$ (except q_{17} which can not appear in any partial tame series). We conclude that the maximal length of tame partial series is at most 11-4=7, while $q_1, \cdots, q_7$ is of length 7. ■

Implementation

We will give an implementation of TTM cryptosystem based on the above example. In this implementation, we will assume that $a_i = 1$ for simplicity.

We shall use the notations of above $\mathbf{Q}_8$, q_i. Let $K = GF(2^8)$, $n \geq 30$ and $m = n + 52$. We have four maps, $\Phi_1, \Phi_2, \Phi_3, \Phi_4$ with the map $\pi = \Phi_4\Phi_3\Phi_2\Phi_1$ where Φ_1 is an affine linear map of K^n to the subspace of K^m with the last 52 coordinates zeroes, Φ_2, Φ_3 tame maps and Φ_4 an affine linear map of K^m to K^m.

For readers convenient, we define polynomials P_1, P_2, P_3 as for $j = 1, 2, 3$.

$$\begin{aligned} P_j &= P_j(y_{m-58}, \cdots, y_{m-55}, y_{m+1-8j}, \cdots, y_{m+8-8j}, y_{m-46}, \cdots, y_{m-24}) \\ &= Q_8(y_{m-58}, \cdots, y_{m-55}, y_{m+1-8j}, \cdots, y_{m+8-8j}, y_{m-46}, \cdots, y_{m-24}) \end{aligned}$$

and P_4 as $P_4 = P_4(y_{m-58}, \cdots, y_{m-24}) = Q_8(y_{m-58}, \cdots, y_{m-24})$. Then we select suitable $\beta_{ij} \neq 0$ for $i, j = 1, \cdots, 4$ such that $R_i = \sum_j \beta_{ij} P_j$ are linearly independent.

We should look at the composition $\Phi_3\Phi_2$ which can be expressed as

$$\Phi_3\Phi_2 = \begin{cases} y_1 = x_1 + R_1 \\ \quad = x_1 + \beta_{14}(x_{m-62}x_{m-52} + x_{m-53}x_{m-54}) + \sum_{j=1}^{j=3} \beta_{1j}(x_{m-62-2j}x_{m-52} + x_{m-61-2j}x_{53}) \\ y_2 = x_2 + f_2(x_1) + R_2 \\ \quad = x_2 + f_2(x_1) + \beta_{24}(x_{m-62}x_{m-52} + x_{m-53}x_{m-54}) \\ \qquad + \sum_{j=1}^{j=3} \beta_{2j}(x_{m-62-2j}x_{m-52} + x_{m-61-2j}x_{53}) \\ y_3 = x_3 + f_3(x_1, x_2) + R_3 \\ \quad = x_3 + f_3(x_1, x_2) + \beta_{34}(x_{m-62}x_{m-52} + x_{m-53}x_{m-54}) \\ \qquad + \sum_{j=1}^{j=3} \beta_{3j}(x_{m-62-2j}x_{m-52} + x_{m-61-2j}x_{53}) \\ y_4 = x_4 + f_4(x_1, x_2, x_3) + R_4 \\ \quad = x_4 + f_4(x_1, x_2, x_3) + \beta_{44}(x_{m-62}x_{m-52} + x_{m-53}x_{m-54}) \\ \qquad + \sum_{j=1}^{j=3} \beta_{4j}(x_{m-62-2j}x_{m-52} + x_{m-61-2j}x_{53}) \\ y_5 = x_5 + f_5(x_1, \cdots, x_4) \\ \cdots \\ y_{m-59} = x_{m-59} + f_{m-59}(x_1, \cdots, x_{m-60}) \\ y_{m-58} = q_1(x_{m-62}, \cdots, x_{m-52}) = x_{m-58} + x_{m-59}x_{m-61} \\ \cdots \\ y_{m-52} = q_7(x_{m-62}, \cdots, x_{m-52}) = x_{m-52} + x_{m-54}x_{m-61} \\ y_{m-51} = q_8(x_{m-62}, \cdots, x_{m-52}) \\ \cdots \\ y_{m-24} = q_{35}(x_{m-62}, \cdots, x_{m-52}) \\ y_{m-23} = q_5(x_{m-64}, x_{m-61}, \cdots, x_{m-55}, x_{m-63}, x_{m-53}, x_{m-52}) \\ \cdots \\ y_{m-16} = q_{12}(x_{m-64}, x_{m-61}, \cdots, x_{m-55}, x_{m-63}, x_{m-53}, x_{m-52}) \\ y_{m-15} = q_5(x_{m-66}, x_{m-61}, \cdots, x_{m-55}, x_{m-65}, x_{m-53}, x_{m-52}) \\ \cdots \\ y_{m-8} = q_{12}(x_{m-66}, x_{m-61}, \cdots, x_{m-55}, x_{m-65}, x_{m-53}, x_{m-52}) \\ y_{m-7} = q_5(x_{m-68}, x_{m-61}, \cdots, x_{m-55}, x_{m-67}, x_{m-53}, x_{m-52}) \\ \cdots \\ y_m = q_{12}(x_{m-68}, x_{m-61}, \cdots, x_{m-55}, x_{m-67}, x_{m-53}, x_{m-52}) \end{cases}$$

where f_i's are random quadratic polynomials such that the vector space dimension of all homogeneous degree 2 parts of the above system is m.

As usual we further require that $\pi(0, \cdots, 0) = (0, \cdots, 0)$. Then π is the public key, while $\{\Phi_1, \Phi_2, \Phi_3, \Phi_4\}$ is the private key. ∎

We have the following proposition:

Proposition 5 *The number r for the above implementation of the TTM cryptosystem (if to be treated as the TPM system) is 4.*

Proof. Clearly, the number of variables is $n = m - 52$, according to previous Lemmas, we have to show the maximal length of partial tame series is $n-4$. Therefore $r = n-(n-4) = 4$. Obviously $\{y_5, \cdots, y_n\}$ is a partial tame series of length $n - 4$. For any partial tame series not involving any of $\{y_1, y_2, y_3, y_4\}$, the dimension of the vector subspace generated by the linear parts $\leq n - 4$. For any partial tame series to involve any one of $\{y_1, \cdots, y_4\}$, the y_i corresponding to the variables in R_i (note that R_i involves 10 variables) must be in front of this particular y_j, then many y_s can not be in the partial tame series (let us consider x_{m-62}, then y_{m-62} can not be in the series. If x_{m-62} does appear in some 1-form of the series, then y_{m-48} or y_{m-57} is in the series, and x_{m-54} appears in the quadratic form. Since any y_s whose 1-form involves x_{m-54} is with quadratic form involving x_{m-62}, therefore x_{m-54} never appears in the 1-form of the series. Further note that $x_{m-62-2j}$ and $x_{m-61-2j}$ appears in pairs in many expressions.) By direct computation, it is easy to show that its length $\leq n-4$. ∎

4 A MiniRank(r) attack on TTM

Let us take $m = 100, n = 48$. Note that in this case, we have $\lceil \frac{m}{n} \rceil = 3$ with the expanding rate= 2.08. Maybe the expanding rate is too big for any storage device to somebody's taste (i.e., in [1] they insist to have $\lceil \frac{m}{n} \rceil \leq 2$). However, it is permissible for communication purposes. For storage devices, we may take $m = 104, n = 52$. Note that in this case, we have $\lceil \frac{m}{n} \rceil = 2 =$ the expanding rate.

We have the following proposition:

Proposition 6 *For $m = 100$ or $= 104$, the attack of [1] (if it is true) is infeasible on the example of implementation of TTM encryptosystem of § 3.*

Proof. Since the number r is at least 4 by the preceding proposition, then the complexity of the attack of [1] is at least (unproved, cf the section 5) $q^{\lceil \frac{m}{n} \rceil r} \times m^3 \geq 2^{84}$ where we take $q = 2^8$. ∎

We shall emphasize that there are many possible examples for practical usages.

5 Errors of Goubin-Courtois' Paper

In the attack [1] by Goubin and Courtois, the most important part of the article is "§ 3.3 Strategy of attack". The sequential sections "§ 4. Special case attacks on TPM", "§5.

The kernel attack on MiniRank(r) and TPM", and "§ 6. The degeneracy attack on TPM signature schemes" all refer to § 3.3 and are based on it. However, there are a number of wrong or questionable arguments in § 3.3 and the following sections. Here we concentrate on § 3.3 only.

(I) At p.6 of [1] (p.49 of Asiacrypt 2000 proceedings), the authors defined the matrices A_i's and M_i's in the beginning of § 3.3 as follows.
"In each equation $y_i = x_i + g_i(x_1, \ldots, x_{i-1}\,; x_{n-r+1}, \ldots, x_n)\ (1 \le i \le n-r)$, the homogeneous part is given by ${}^tXA_iX$, with ${}^tX = (x_1, \ldots, x_n)$, A_i being a (secret) matrix. Similarly, in each public equation $y'_i = P_i(x'_1, \ldots, x'_n)$ is given by ${}^tX'M_iX'$, with ${}^tX' = (x'_1, \cdots, x'_n)$, M_i being a (public) matrix."

(Existence): Indeed, for any square matrix A, we have

$$ {}^tXAX = (x_1, \ldots, x_n) \begin{pmatrix} A_{11} & \cdots & A_{1n} \\ \vdots & \ddots & \vdots \\ A_{n1} & \cdots & A_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \sum_j A_{jj}\, x_j^2 + \sum_{j<k} (A_{jk} + A_{kj})\, x_j x_k. $$

Every homogeneous quadratic polynomial can be written in the form of ${}^tXAX$.

(Uniqueness): In general the expression is *not* unique. For example,

$$ x_1^2 + x_2^2 + x_1x_3 + x_2x_3 = {}^tX \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} X = {}^tX \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix} X = {}^tX \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix} X. $$

The representation is unique if we restrict A to be upper-triangular ($A_{jk} = 0$ for $j > k$), lower-triangular ($A_{jk} = 0$ for $j < k$), or symmetric ($A_{jk} = A_{kj}$ for all j, k). Since the uniqueness is significant in the later arguments, the authors should specify the nature of A_i's and M_i's in the beginning.

(Non-symmetric): On the slide 9 of [9], the authors introduced a notion from "Basic linear algebra" in the following way: "The homogeneous part of a quadratic equation $y_i \rightsquigarrow$ a symmetric matrix M_i."

No. They can not be symmetric. Although TTM can be generalized to fields of any nonzero characteristic, like other multivariate cryptosystems, TTM is mainly designed for finite fields of characteristic 2. Actually, all implementations of TTM are working on $GF(2^8)$. Basic linear algebra also tells us that quadratic forms can *not* be represented by symmetric matrices over a field of characteristic 2. For example, if $n = 3$,

$$ \begin{aligned} {}^tX \begin{pmatrix} a_1 & b_1 & b_2 \\ b_1 & a_2 & b_3 \\ b_2 & b_3 & a_3 \end{pmatrix} X &= a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + 2b_1\, x_1x_2 + 2b_2\, x_1x_3 + 2b_3\, x_2x_3 \\ &= a_1x_1^2 + a_2x_2^2 + a_3x_3^2. \end{aligned} $$

There is no way to represent x_1x_2 by a symmetric matrix. The basic fact of linear algebra which states that in characteristic two a general quadratic homogeneous polynomial can not be represented by a symmetric matrix causes a severe consequence in [1].

(II) At p.7 of [1], the authors claimed:

$$ \text{" We thus have, for any } X' : \quad {}^tX'({}^tSA_iS)X' = {}^tX' \left(\sum_{j=1}^{m} t_{ij} M_j \right) X' $$

$$\text{so that:} \qquad \forall i,\ 1 \le i \le m,\ \sum_{j=1}^{m} t_{ij} M_j \ = \ {}^tSA_iS.\text{''}$$

The authors implicitly assume the *uniqueness* (cf I). Without any restriction on the square matrices, it is clearly wrong.

This statement is true if both ${}^tSA_iS$ and $\sum t_{ij}M_j$ are upper-triangular, lower-triangular, or symmetric. Notice that ${}^tSA_iS$ is symmetric if and only if A_i is, because $A_i = {}^tA_i \Leftrightarrow {}^tSA_iS = {}^tS\,{}^tA_iS \Leftrightarrow {}^tSA_iS = {}^t({}^tSA_iS)$. We have seen that none of M_i, A_i, or ${}^tSA_iS$ is symmetric all the time. As we pointed out before, it is impossible to require the matrices to be symmetric in characteristic two.

If we require both ${}^tSA_iS$ and $\sum t_{ij}M_j$ are upper-triangular (or lower-triangular), there is no guarantee that A_i is also upper-triangular (or lower-triangular respectively). For example,

$${}^tSA_iS = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} = \sum t_{ij}M_j$$

is upper-triangular, but A_i is not.

A bunch of counterexamples can be found, one of them comes from the above:

$${}^tX' \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} X' = {}^tX' \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix} X' \quad \text{for any } X',$$

$$\text{but} \quad \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

(III) Notice that even the ranks of the the last two matrices are different, since $\mathrm{Rank}({}^tSA_1S) = 2 < 3 = \mathrm{Rank}(\sum t_{ij}M_j)$. therefore, their sequential claim "We have $\mathrm{Rank}({}^tSA_1S) = \mathrm{Rank}(A_1) \le r$ and thus Rank $(\sum t_{ij}M_j) \le r$." is false.

(IV) The later argument "With a good probability, we can suppose that: $\sum_{j=1}^m \lambda_j M_j = \mu\,{}^tSA_1S$." (cf [1]) is doubtful, because $\sum t_{ij}M_j = {}^tSA_iS$ is not necessarily true. "With a good probability" is an interesting phrase. The authors didn't estimate how good it is, and they didn't take this into account while computing the complexity of their attack either.

(V) The subspaces V_0 and W_0 play an important role in the theory. The authors assured that they are obtained by $V_0 = \mathrm{Im}\left(\sum_{j=1}^m \lambda_j M_j A_1\right)$ and $W_0 = \mathrm{Ker}\left(\sum_{j=1}^m \lambda_j M_j A_1\right)$. However, let's recall that A_1 is secret by assumption, and one of our goals is to find it. It makes sense to compute $\mathrm{Im}(\sum \lambda_j M_j)$ or $\mathrm{Ker}(\sum \lambda_j M_j)$, but it is still not clear how to find $\mathrm{Im}(\sum \lambda_j M_j A_1)$ or $\mathrm{Ker}(\sum \lambda_j M_j A_1)$.

(VI) Also the authors claimed that $V_0 = S^{-1}(K^{n-r} \times \{0\}^r)$ and $W_0 = S^{-1}(\{0\}^{n-r} \times K^r)$. Let's try to find some relations among these sets. We have

$$\left(\sum \lambda_j M_j\right) V_0 = (\mu\,{}^tSA_1S)\, S^{-1}(K^{n-r} \times \{0\}^r) = \mu\,{}^tSA_1\,(K^{n-r} \times \{0\}^r) = \mu\,{}^tS\,\mathbf{0} = \mathbf{0}$$

where $\mathbf{0}$ denotes the zero space. Consequently $V_0 \subseteq \mathrm{Ker}\left(\sum_{j=1}^m \lambda_j M_j\right)$. On the other hand,

$$\mathrm{Im}\left(\sum \lambda_j M_j\right) = \left(\sum \lambda_j M_j\right) K^n = (\mu\,{}^tSA_1S)\,K^n = ({}^tSA_1)\,K^n \subseteq {}^tS\,(\{0\}^{n-r} \times K^r).$$

They are very different from the identities at p.7 of [1].

(VII) In the following paragraph, the description of their process to deduce V_1 and W_1 is vague. Since V_0, W_0, and the two deduced sequences of subspaces $V_0 \supseteq V_1 \supseteq V_2 \supseteq \ldots \supseteq V_{n-r-1}$ and $W_0 \subseteq W_1 \subseteq W_2 \subseteq \ldots \subseteq W_{n-r-1}$ are not the vector spaces as the authors claimed, therefore there is no sufficient reason to believe that the strategy of attack described in [1] leads to the complete determination of the secret functions s, t, and all g_i's as the conclusion in the end of § 3.3.

6 Conclusion

The attack of [1] on the TTM cryptosystem is infeasible and full of gaps. There is no known attacks which can crack the TTM cryptosystem.

References

[1] Goubin, L. and Courtois, N.T. *Cryptanalysis of the TTM Cryptosystem.* Accepted by Asiacrypt 2000, Dec 2000.

[2] Chou, C.Y. Guan, D.J. and Chen J.M. *A Systematic Construction of a Q_{2^k}-module in TTM.* Accepted by Communications in Algebra

[3] Hironaka, H. *Resolution of singularities of an algebraic variety over a field of characteristic zero.*Ann. Math Vol 79, 1964.

[4] Lucier, B. *Cryptography, Finite Fields, and AltiVec.* http://www.altivec.org/articles/

[5] Imai, H. Matsumoto *Algebraic methods for constructing asymmetric cryptosystems, Algebraic and Error-Correcting Codes.* Prod. Third Intern. Conf., Grenoble, France, Springer-Verlag, 108-119, 1985.

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

[7] Moh, T. *A Fast Public Key System With Signature And Master Key Functions.* CrypTEC'99 (Proc. International Workshop on Cryptographic Techniques & E-commerce), City University of Hong Kong Press, July, 1999.

[8] Patarin, J. *Hidden Field Equations (HFE) and Isomorphisms of Polynomials (IP): two new Families of Asymmetric Algorithms.* Eurocrypt'96, 1996.

[9] Goubin, L. Courtois, N.*Transparencies of "Cryptanalysis of TTM" presented at Asiacrypt 2000*, Available at http://www.cp8.bull.net/sct/uk/partners/index.html

[10] Kipnis, A. Shamir, A.*Cryptanasis of the HFE Public Key Cryptosystem by Relinearization* CRYPTO'99, 1999.,