The Recent Attack of Nie et al On TTM is Faulty

T. Moh[*]

Nov 19.2006

Abstract

Recently there is a paper entitled "*Breaking a New Instance of TTM Cryptosystem*" by Xuyun Nie, Lei Hu, Jianyu Li, Crystal Updegrove and Jintai Ding [1] claiming a successive attack on the scheme of TTM presented in [3]. In the present article, we will show that their claim is a **misunderstanding**.

1 Introduction

The strength of a public key system is solely on the public key, i.e., with the public key known to the general public, the attacker tries to find the private key or its equivalences. Note that the attacker has no information about the private key nor how it is constructed.

The TTM cryptosystem (cf [2],[3]) 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 (which can be written as a sequence of quadratic polynomials) **while the private key is the set of mappings** $\{\phi_i\}$. The *tame* mappings, which are commonly known in mathematics, are defined as

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

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

In paper [3], an implementation of TTM is given. The public key is the composition of $\phi_4\phi_3\phi_2\phi_1$ which will be written as a sequence of quadratic polynomials. An attacker shall focus on them. The private keys $\phi_4, \phi_3, \phi_2, \phi_1$ are written as polynomials of degrees $1, 8, 2, 1$ respectively.

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

2 Legitimate Attack

There is only one type of *legitimate attacks*: Knowing only the public key π which is a sequence of quadratic polynomials, the attacker tries to decipher a coded message (an equivalent private key will suffice).

3 The fault of the said attack

Instead of attacking the public key, the authors of [1] assume that parts of the private key are known to the attackers. To be precise, they assume that the private keys ϕ_3 and ϕ_2 are known to them. Furthermore, they assume that the **constructions** of the private key ϕ_3 is known to them. Note that in no situation, we will let the construction of the public key and the private key be known to the legitimate users and the general public. The attacker has to work to find the algebraic properties and the construction of the pair of public key-private key, even if the part of the private key, ϕ_3, ϕ_2, is available. The construction is always hidden from the general public. For instance, in the famous RSA cryptosystem, an integer $n = pq$ is used where p, q are two large prime numbers. The construction $n = p \times q$ is always hidden from the general public. Note that by the preceding discussions on the legitimate attack, the attack is not legitimate.

The reasons that we publish the construction of the private key are manifold;

(1): To publish the end result of ϕ_3 as polynomials of degree 8 in y_j's will be to long and not elegant enough. To save the pages we publish the sequence of substitutions which could be used by the readers to verify the system. Clearly the sequence of 16 polynomials $R_1, \cdots, G_5$ is **not** for the attacker to manipulate.

(2): We provide some materials for scholars to think about. Maybe someone will find some ideas to solve a difficult mathematical problem, i.e., the following **ring membership problem**.

Ring membership problem: Suppose that we are given a polynomial $f(x_1, \cdots, x_n)$ of degree r (in our case $r = 8$). Can we find polynomials $h_1(x_1, \cdots, x_n), \cdots, h_n(x_1, \cdots, x_n)$ with $1 < max(degree(h_i)) < r$ such that $f \in K[h_1, \cdots, h_n]$ and $\text{degree}_{h_1, \cdots, h_n}(f) < r$? If not, how can we tell?

The point is although we provide the structure of the private key as the list of 110 quadratic polynomials for ϕ_2 and 16 polynomials $R_1, \cdots, G_5$ for ϕ_3, the attacker will not be allowed to use them directly. Even if the attacker knows part of the private key, i.e., ϕ_3 as polynomials of degrees 8 in y_j's, which is doubtful, and if the attacker want to use the structure of ϕ_3 as given by the 16 polynomials $R_1, \cdots, G_5$, then the attacker must show a way to search and detect them!

Even in this case, if the attacker want to use a general search of some kind to find the 16 polynomials $R_1, \cdots, G_5$, then he/she must be able to handle a general polynomial of degree 8 in 110 variables which calls for memory of the size 1.8×10^{14} which is beyond present day's technology. Only then the attacker may think of some way in solving a system of equations. One may increase the degree 8 to, say, degree 16, thus increase the memory to a size of 1.8×10^{22} to counter any development of technology. .

4 Summary

The authors of [1] bark up the wrong tree. Otherwise, the authors provide many interesting computations. We wish to commend them for their good work.

References

[1] Nie, Xuyun., Hu,lei., Li, Jianyu., Updegrove, Crystal., and Ding, Jintai *Breaking a New Instance of TTM Cryptosystems.* ACNS 2006, LNCS 3989, pp. 210-225, 2006.

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

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