On the Signature Scheme TTMs

T. Moh*

March 16, 2006

Abstract

Since the paper [13] introducing the public-key encryption system TTM was published, there are attempts to realize the signature scheme of TTM as described in [13]. One series of papers published in [2], [3], [4], [19], the authors claimed that they have used TTM to create a scheme named TTS. In the abstract of [2], the authors stated: "*The commercial use of TTS is protected under the patent of TTM.*". There are several other ways of the implementation of the signature scheme of TTM. In this article, we will present the original ideas with clarity and with several implementations of security strengths $\geq 2^{93}$.
.

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. In Matsumoto-Imai theory ([10]), 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 [16]. Its decryption involves solving equations, and hence the process is slow.

The TTM cryptosystem (cf [13],[14]) 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

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 $h_{i,j}$,

$$(1) : \phi_{i,1}(x_1, \cdots, x_m) = x_1 = y_1$$
$$(2) : \phi_{i,2}(x_1, \cdots, x_m) = x_2 + h_{i,2}(x_1) = y_2$$
$$\cdots\cdots\cdots$$

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

$$(j) : \phi_{i,j}(x_1, \cdots, x_m) = x_j + h_{i,j}(x_1, \cdots, x_{j-1}) = y_j \tag{1}$$
$$\cdots\cdots\cdots$$
$$(m) : \phi_{i,m}(x_1, \cdots, x_m) = x_m + h_{i,m}(x_1, \cdots, x_{m-1}) = y_m$$

Many multivariate encryption systems use "searching" or "solving equations" to decode, i.e., find $\{x_j\}$ with giving $\{y_j\}$. Even if the system of equations are made to be quadratic, it still slows down the decryption process. An important property of tame mapping Φ_i is that not only we may find the values of $\{y_1, \cdots, y_m\}$ from the values of $\{x_1, \cdots, x_m\}$ by substitutions, but also the values of $\{x_1, \cdots, x_m\}$ from the values of $\{y_1, \cdots, y_m\}$ 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.

Note that the public-key is the map $\pi = (\pi_1, \cdots, \pi_n)$, that means to keep the public-key, we have to store all coefficients of $(\pi_1, \cdots, \pi_n)$. Hence the size of the public key depends exponentially on the *degree* of the map π which is defined as the maximum of the degrees of all coordinate polynomials $\{\pi_i : i = 1, \cdots, n\}$. Let Φ_1, Φ_2 be two maps. It is easy to see that $\deg(\Phi_2\Phi_1) \leq \deg(\Phi_2)\deg(\Phi_1)$. The following example shows that in some cases, we may have $\deg(\Phi_2\Phi_1) = \max\ (\deg(\Phi_2), \deg(\Phi_1))$.

An Baby Example

As in the case of TTM (cf [13], [14],[15]), the degrees of mappings 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

$$(1) : \phi_{1,1}(x_1, \cdots, x_8) = x_1$$
$$(2) : \phi_{1,2}(x_1, \cdots, x_8) = x_2$$
$$(3) : \phi_{1,3}(x_1, \cdots, x_8) = x_3 + x_1^2$$
$$(4) : \phi_{1,4}(x_1, \cdots, x_8) = x_4 + x_1x_2$$
$$(5) : \phi_{1,5}(x_1, \cdots, x_8) = x_5 + x_2^2$$
$$(6) : \phi_{1,6}(x_1, \cdots, x_8) = x_6 + x_2x_3$$
$$(7) : \phi_{1,7}(x_1, \cdots, x_8) = x_7 + x_1x_5$$
$$(8) : \phi_{1,8}(x_1, \cdots, x_8) = x_8 + x_1^2$$

and

$$(1) : \phi_{2,1}(x_1, \cdots, x_8) = x_1$$
$$(2) : \phi_{2,2}(x_1, \cdots, x_8) = x_2$$
$$(3) : \phi_{2,3}(x_1, \cdots, x_8) = x_3$$
$$(4) : \phi_{2,4}(x_1, \cdots, x_8) = x_4$$
$$(5) : \phi_{2,5}(x_1, \cdots, x_8) = x_5$$

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

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 $\pi = \Phi_2\Phi_1$ stays 2. ■

In general, we may select $\{\Phi_i : i = 1,\cdots,s\}$ such that all of them are of degree 2 and their composition is of degree 2. This intrinsic property can be used to keep the sizes of public keys down. The interested reader is referred to [13],[14],[15].

In [13], there is a description of the signature scheme of TTM. Let us quote from [13]:

The map $\hat{\pi}$ is not an onto map. However, we may restrict the map to a suitable subspace. $\cdots$. Clearly $\tau\hat{\pi}$ is an one to one and onto map $\cdots$. Moreover, the map is tame and its inverse at a point $(y_1',\cdots,y_j')$ can be found. The inverse at $(y_1',\cdots,y_j')$ forms a signature.

We shall give some mathematical formulations of the above statement. Let us consider only the ground field $K = F_{2^8}$, an $n-$dimensional affine space K^n and three maps Φ_1, Φ_2, Φ_3 with the map $\pi = \Phi_3\Phi_2\Phi_1$ where Φ_1 is an affine linear automorphism map of K^n to itself. We may restrict to a (secret) linear subspace of K^n of dimension $n-\ell$, i.e., using the principal of *minus* of Shamir of delete ℓ of the polynomials. Therefore we only require that Φ_3 is an affine linear automorphism map of $K^{n-\ell}$ to itself. The map Φ_2 as presented in [13] is a composition of two (or finitely many) *tame* maps. Then could every automorphic polynomial map be decomposed as a composition of finitely many tame maps? This is an open mathematical problem. For simplicity, we shall assume that Φ_2 is *any* polynomial map, *tame* or *not*. Let us look at the map Φ_2, which can be expressed as

$$
\Phi_2 := \begin{cases} y_{\ell+1} = \alpha_{\ell+1}(x_1,\cdots,x_n) + \beta_{\ell+1}(x_1,\cdots,x_n)\\ \cdots\\ y_n = \alpha_n(x_1,\cdots,x_n) + \beta_n(x_1,\cdots,x_n)\end{cases} \qquad (2)
$$

where $\{\alpha_i\}$ is a linear independent set of linear polynomials in $\{x_1,\cdots,x_n\}$ and β_i's are homogeneous quadratic polynomials. The above quoted statement requires that we skillfully select an affine linear subspace, such that the restriction of the above map Φ_2 to the linear subspace will become a *tame* map. For the time being, we shall set aside the problem of *skillfully selecting an affine linear subspace*, and present the other parts mathematically.

Analytically, we have the following presentation. Let Φ_1 be an invertible *affine* linear transformation which sends $[w_1, \cdots, w_n]$ to $[x_1, \cdots, x_n]$ as follow,

$$\Phi_1 : \begin{bmatrix} a_{1,1}, & a_{1,2}, & a_{1,3}, & \cdots, & \cdots, & a_{1,n} \\ a_{2,1}, & a_{2,2}, & a_{2,3}, & \cdots, & \cdots, & a_{2,n} \\ a_{3,1}, & a_{3,2}, & a_{3,3}, & \cdots, & \cdots, & a_{3,n} \\ \cdots, & \cdots, & \cdots, & \cdots, & \cdots, & \cdots \\ \cdots, & \cdots, & \cdots, & \cdots, & \cdots, & \cdots \\ a_{n,1}, & a_{n,2}, & a_{n,3}, & \cdots, & \cdots, & a_{n,n} \end{bmatrix} \times \begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ \cdot \\ \cdot \\ w_n \end{bmatrix} + \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ \cdot \\ \cdot \\ b_n \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \cdot \\ \cdot \\ x_n \end{bmatrix}$$

The above analytic form can be rewritten as the vector and matrix form as the follow,

$$\Phi_1(w) = A \times w + b = x$$

where A is an invertible matrix. The mapping Φ_3 can be written as,

$$\Phi_3 : \begin{bmatrix} b_{1,1}, & b_{1,2}, & b_{1,3}, & \cdots, & \cdots, & b_{1,n-\ell} \\ b_{2,1}, & b_{2,2}, & b_{2,3}, & \cdots, & \cdots, & b_{2,n-\ell} \\ b_{3,1}, & b_{3,2}, & b_{3,3}, & \cdots, & \cdots, & b_{3,n-\ell} \\ \cdots, & \cdots, & \cdots, & \cdots, & \cdots, & \cdots \\ \cdots, & \cdots, & \cdots, & \cdots, & \cdots, & \cdots \\ b_{n-\ell,1}, & b_{n-\ell,2}, & b_{n-\ell,3}, & \cdot, & \cdot, & b_{n-\ell,n-\ell} \end{bmatrix} \times \begin{bmatrix} y_{\ell+1} \\ y_{\ell+2} \\ y_{\ell+3} \\ \cdot \\ \cdot \\ y_n \end{bmatrix} + \begin{bmatrix} c_{\ell+1} \\ c_{\ell+2} \\ c_{\ell+3} \\ \cdot \\ \cdot \\ c_n \end{bmatrix} = \begin{bmatrix} z_{\ell+1} \\ z_{\ell+2} \\ z_{\ell+3} \\ \cdot \\ \cdot \\ z_n \end{bmatrix}$$

The above analytic form can be rewritten as the vector and matrix form as the follows,

$$\Phi_3(y) = B \times y + c = z$$

where B is an invertible matrix.

In the above equations, the vector b is randomly selected and the vector c is determined by the requirement $\pi([0, \cdots, 0]^T) = \Phi_3\Phi_2\Phi_1([0, \cdots, 0]^T) = [0, \cdots, 0]^T$. The map π is a many to one map, so it is not an encryption map, while it serves as a *hash* map.

Let us fix the notation as follows,

$$\pi := \begin{cases} z_{\ell+1} = \pi_{\ell+1}(w_1, \cdots, w_n), \\ \cdots, \\ z_n = \pi_n(w_1, \cdots, w_n) \end{cases} \tag{3}$$

We may rewrite the above using the vector notations as follows,

$$\begin{aligned} [z_{\ell+1}, \cdots, z_n]^T &= \pi([w_1, \cdots, w_n]^T) = \Phi_3\Phi_2\Phi_1([w_1, \cdots, w_n]^T) \\ [y_{\ell+1}, \cdots, y_n]^T &= \Phi_3^{-1}([z_{\ell+1}, \cdots, z_n]^T) \\ &= \Phi_2\Phi_1([w_1, \cdots, w_n]^T) \\ [w_1, \cdots, w_n]^T &= \Phi_1^{-1}([x_1, \cdots, x_n]^T) \end{aligned}$$

The functions of Φ_1, Φ_3 are used to (1) creating a large number of public-keys, and (2) hidding the variables x_i and functions y_j. The question for the implementations of the signature scheme is how to skillfully select an affine linear space or assign values to a part of $\{x_1, x_2, \cdots, x_n\}$ such that Φ_2 becomes a tame map $\bar{\Phi}_2$ at the point $[y_{\ell+1}, \cdots, y_n]^T$.

We will further discuss the questions of *skillfully selecting an affine linear subspace* in § 5 for the implementations TTMs. We shall discuss several issues before we talk about the details of TTMs.

2 Minrank

Several attacks on multivariate encryption systems involve the concepts of the *rank* of the map Φ_2 which is defined for quadratic polynomials as follows,

Definition The *rank* of a quadratic homogeneous polynomial $g \neq 0$ is the minimal number of variables which generate the non-square part of g, in symbol, $rank(g)$. The *rank* of the quadratic map Φ_2, $rank(\Phi_2)$, is the min $\{rank(g) : g$ is quadratic and in the vector space spanned by $\{\beta_i\}$ as in (2). ■

The *minrank attack* was formulated in [6]. The minrank attack of Goubin-Courtois' has a complexity $q^{\lceil \frac{m}{n} \rceil r} m^3$ where q is the number of elements in the field K and $r = rank(\Phi_2)$ (the paper [6] is full of errors, while the conclusion might be correct). Note that the rank r appears exponentially. The simple way to protect the signature system from minrank attack is to make r large enough.

We have the following theorem which is a theorem in [9] of H.Hironaka in characteristic 0 and later rediscovered by Patarin. For characteristic 2, the proof is identical with Hironaka's original proof [9]. We have.

Lemma 1 *: Let $g(x_1, \cdots, x_s)$ be a homogeneous polynomial of degree 2. Let ∂_i be the derivative with respect to x_i. Then the vector space dimension of the subspace generated by all $\partial_i(g)$ is independent of the set of variables $\{x_1, \cdots, x_s\}$.*

Proof. It follows by the chain rule of Calculus. ■

Theorem 2 *: Let $g(x_1, \cdots, x_s)$ be a homogeneous polynomial of degree 2. Let $\partial_i(g)$ be its derivative with respect to x_i. Then the rank(g)= the vector space dimension of the subspace generated by all $\partial_i(g)$.*

Proof. It follows form Lemma 1 that we may assume that $\{x_1, \cdots, x_t\}$ is a minimal set of variables which express the non-square part of g, then clearly $\partial_i(g) \in$ the vector space spanned by $\{x_1, \cdots, x_t\}$. So we have the t=rank$(g) \geq$ the vector space dimension of the subspace generated by all $\partial_i(g)$.

We note that if $s = 1$, then $g = 0 \; mod(x_1^2)$ and the theorem is trivially true. If $s > 1$, and the rank(g) = the vector space dimension of the subspace generated by all $\partial_i(g)$, then there is nothing to be proved. Thus if all $\partial_i(g)$ are linearly independent, then the preceding is true. Let us assume that they are linearly dependent. If $\partial_i(g) = 0$ for some $1 \leq i \leq t$, then we may delete x_i from the list of variables $\{x_1, \cdots, x_t\}$ and produce a contradiction, the proof is completed.

We shall consider the remaining cases, i.e., there is a non-trivial linear relation among 2 or more $\partial_i(g)$. We should change variables to delete one of them. Let

$$\sum_{i=1}^{m} b_i \partial_i(g) = 0$$

be a non-trivial relation among them. For our convenience, after changing the order of variables, we may assume all $b_i \neq 0$ for $i = 1, \cdots, m \leq t$. We define a new set of variables

$\{y_1, \cdots, y_s\}$ as

$$\begin{aligned}
&b_1 y_1 = x_1 \\
&y_2 = (b_2/b_1)x_1 + x_2, \qquad \text{or } x_2 = b_2 y_1 + y_2 \\
&\cdots \\
&y_m = (b_m/b_1)x_1 + x_m, \qquad \text{or } x_m = b_m y_1 + y_m \\
&y_{m+1} = x_{m+1} \\
&\cdots \\
&y_s = x_s
\end{aligned}$$

Let us define ∂_i^* to be the derivative with respect to y_i. Then we have

$$\partial_1^*(g) = \sum_{i=1}^{s} \partial_i(g) \frac{\partial(x_i)}{\partial(y_1)} = \sum_{i=1}^{m} b_i \partial(g) = 0$$

Therefore we produce a contradiction as before, and complete our proof. ∎

Example: Let us consider $xy + yz + xz \in K[x, y, z]$. The partial derivatives, $y+z, x+z, x+y$ spannes a two dimensional vector space as

$$(y+z) + (x+z) + (x+y) = 0$$

We defined

$$\begin{aligned}
x' &= x \\
y' &= x + y \\
z' &= x + z
\end{aligned}$$

Then we have $xy + yz + xz \equiv (x+y)(x+z)$ mod $K[x^2, y^2, z^2]$. So its minrank=2. ∎

Corollary 3 *Let* $g = p_{1,2}x_1x_2 + p_{3,4}x_3x_4 + \cdots + p_{2n-1,2n}x_{2n-1}x_{2n}$ *where* $p_{2i-1,2i}$*'s are non-zero numbers. Then* $rank(g) = 2n$*.*

∎

The situation of our corollary is general. Let us define

Definition : Let $\{x_1, \cdots, x_s\}$ be a set of variables. Let $g \in K[x_1, \cdots, x_s]$ be a quadratic homogeneous polynomial. If $g = x_1x_2 + x_3x_4 + \cdots + x_{2n-1}x_{2n}$ mod $K[x_1^2, \cdots, x_s^2]$. Then g is in the *standard form* with respect to $\{x_1, \cdots, x_s\}$. ∎

We have the following proposition,

Proposition 4 *: Let* $g \in K[x_1, \cdots, x_s]$ *be a quadratic homogeneous polynomial. Then there is a new set of variables* $\{y_1, \cdots, y_s\}$ *such that* g *is in the standard form with respect to* $\{y_1, \cdots, y_s\}$*. Especially, the minrank is an even number.*

Proof. We may assume that minrank(g)=t. Let $\partial_1(g) = y_2 = ax_2 + \cdots$ with $a \neq 0$ (re-order the variables $\{x_1, \cdots, x_s\}$ if necessary). Replacing x_2 by y_2, we have a new set of variables $\{x_1, y_2, \cdots, x_s\}$. The partial derivative of g with respect to y_2 will be $ax_1 + \cdots$, name it y_1. Note that $g = g^*(x_1, y_2, x_3, \cdots, x_s) = (x_1 + \cdots)y_2 + h(x_3, \cdots, x_s)$ mod $K[x_1^2, y_2^2, x_3^2, \cdots, x_s^2]$. Then it is easy to see that

$$g = y_1 y_2 + h(x_3, \cdots, x_s) \ mod \ k[y_1^2, y_2^2, x_3^2, \cdots, x_s^2]$$

Now we make an induction for h. ∎

Proposition 5 *: Let g be a homogeneous quadratic polynomial. If g mod $K[x_1^2, \cdots, x_n^2] \in (x_1, \cdots, x_\ell)$, the ideal generated by $\{x_1, \cdots, x_\ell\}$, let $g = \sum_{i=1}^{\ell} h_i x_i$, then the minrank(g)= 2ℓ if $\{x_1, \cdots, x_\ell, h_1, \cdots, h_\ell\}$ is a linearly independent set, otherwise minrank(g)< 2ℓ.*

Proof. We make an induction on ℓ. If $\ell = 1$, and if $\{x_1, h_1\}$ is a linearly independent set, then we may extend it to a set of variables, and our proposition follows from a preceding Corollary. If it is a linearly dependent set, then $g = ax_1^2 = 0$ mod $K[x_1^2, \cdots, x_n^2]$, and minrank(g)= $0 < 2$. Our proposition follows.

In general, let $\ell > 1$. The first conclusion follows routinely. Let us assume that $\{x_1, \cdots, x_\ell, h_1, \cdots, h_\ell\}$ is a linearly dependent set with the following equation,

$$\sum_{i=1}^{\ell} (a_i x_i + b_i h_i) = 0$$

Let $L = \{i : b_i \neq 0\}$. Then the above equation can be re-written as,

$$\sum_{i \in L} (a_i x_i + b_i h_i) + \sum_{i \notin L} (a_i x_i) = 0$$

Without losing generality, we may assume that $b_\ell = 1$. It is easy to see that

$$g = \sum h_i x_i = \sum_{i \in L} (h_i + (a_i/b_i)x_i)x_i + \sum_{i \notin L} h_i x_i \ mod \ K[x_1^2, \cdots, x_n^2]$$

Let $h_i^* = h_i + (a_i/b_i)x_i \ \forall i \in L$ and $h_i^* = h_i \ \forall i \notin L$. Then we have

$$g = \sum h_i^* x_i \ mod \ K[x_1^2, \cdots, x_n^2]$$

and the linear relation between $\{x_1, \cdots, x_\ell, h_1, \cdots, h_\ell\}$ can be re-written as

$$\sum_{i \in L} (b_i h_i^*) + \sum_{i \notin L} (a_i x_i) = 0$$

Or

$$b_\ell h_\ell^* = \sum_{i \in L, i \neq \ell} (b_i h_i^*) + \sum_{i \notin L} (a_i x_i)$$

Replacing h_ℓ in the expression of g by the above equation and collect terms, we have

$$g = \sum_{i \in L, i \neq \ell}^{\ell-1} (x_i + b_i x_\ell) h_i^* + \sum_{i \notin L} (h_i + a_i x_\ell) x_i \ mod \ K[x_1^2, \cdots, x_n^2]$$

If the set $\{h_i^* : i \in L.i \neq \ell\} \cup \{x_i : i \notin L\}$ is a linear dependent set, then we may further reduce the number of elements in the union of two sets. Our induction process is completed. ■

Proposition 6 *: Let I be an ideal generated by 1-forms (i.e., homogeneous polynomials of degree 1) in $K[x_1, x_2, \cdots, x_n]$. We always have $rank(h\ mod\ I) \leq rank(h)$.*

Proof. Let $\{x_1, \cdots, x_s\}$ be a minimal set of variables which express g, then clearly with $\bar{x_i} = x_i\ mod\ I$, the set $\{\bar{x_1}, \cdots, \bar{x_s}\}$ will be a set of variables which express $h\ mod\ I$. ■

3 Oil and Vinegar Attack

J. Patarin proposed an "*Oil and Vinegar Algorithm for Signatures*". As presented in [11] for a generalization of it, the *Unbalanced Oil and Vinegar Algorithm for Signature* (with notations slightly modified by us), the scheme is to have a **Secrete Key** made of two parts,

1. A bijective and affine linear transformation s of K^{o+v} to itself. .
2. A set (S) of o equations of the following form

$$\forall i, 1 \leq i \leq o,\ y_i = \sum \gamma_{ijk} x_j x'_k + \sum \lambda_{ijk} x'_j x'_k + \sum \xi_{ij} x_j + \xi'_{ij} x'_j + \delta_i \qquad (S)$$

Note that these equations (S) contains no terms in $x_i x_j$. The variables $\{x_i : i = 1, \cdots, o\}$ are called the *oil* variables and the variables $\{x'_j : j = o+1, \cdots, o+v\}$ are called the *vinegar* variables. Let $w = s^{-1}(x)$ where $x = [x_1, \cdots, x_o, x'_{o+1}, \cdots, x'_{o+v}]^T$. Then then the **Public Key** is the following set of equations

$$\forall i, 1 \leq i \leq o,\ y_i = P_i(w) \qquad (P)$$

The Computation of a Signature (with the Secret Key):

Step 1: Assign random values to the vinegar variables. The set of equations (S) becomes linear in the oil variables. Solve the linear set of equations in the oil variables. If the set of linear equations is inconsistent, then assign a set of new random values to the vinegar variables. One can show that there is a fixed and > 0 probability for the system of equations to be consistent. Therefore after certain number of trying, the probability will be good to solve the system of equations.

Step 2:We compute $w = s^{-1}(x)$. Then w is a signature.

The **cryptanalysis**: According to [11], we define the *oil subspace* to be the linear subspace of all vectors in K^{o+v} whose last v coordinates are zeroes. The *vinegar space* to be the linear subspace of all vectors whose first o coordinates are zeroes. Let O be the image of the oil subspace by s^{-1}.

Given a set of equations (S), we may delete the constants and the linear parts to form a set of homogeneous polynomials (S^*). For any homogeneous quadratic polynomial h, we may associate with it a square matrix B. Consider the matrix $A = B + B^T$, one may formulate an analysis of h by studying A.

Translating to the matrix form, if we list the oil variable first, the the matrix will be of the following form,

$$A = \begin{bmatrix} 0, & b_i \\ b_i^T, & d_i \end{bmatrix}$$

where b_i is an $o \times v$ matrix and d_i is a symmetric $v \times v$ matrix.

The problem of finding common invariant subspace of the set of matrices is studied in [10]. With a twist of probability theory [11], we find O with good probability, and take any complement subspace V of dimension v, we have $O{+}V{=}K^{o+v}$. The number of steps to finish the above process is $q^{v-o-1}o^4$. Now we may assign random values to V as in the Step 1 of the Computation of a Signature, we may forge a signature. ■

Remark: In the above Signature Scheme, it is very important to have the number of equations equal o, the number of *oil variables*, and the equations (S) be random enough. Otherwise, there will be two problems. In either cases, we may consider $m(< v)$ random polynomials as follows,

$$\forall i, o < i \leq o + m,\ y_i = \sum \lambda_{ijk} x'_j x'_k + \sum \xi'_{ij} x'_j + \delta_i \qquad (S')$$

Then (1): According to [11], to find a solutions set of $\{x'_j : j = 0+1, \cdots, o+v\}$ is NP-Hard. Therefore, it is inefficient to use the **Secret Key**. (2). Similarly, it is inefficient to assign values to the vinegar variables to forge a signature.

In the other parts, § 5,7, of [11], the authors always assume that the number of quadratic equations are small comparing with the number of variables (either $n^2/2 \leq v$ *or* $n^2 \leq n + v$ where n is the number of equations and $n + v$ is the number of variables). Their conclusions are of little use for our considerations in this article.

On the other hand, for any signature scheme the method of [11] is meaningful to separate the oil variables and the vinegar variables with a complexity of $q^{v-0-1}o^4$. This step by itself may not break the signature scheme, however, may serve as the first step of a successive cryptanalysis as indicated by [8]. The best way of stopping a similar cryptanalysis, from our point of view, is to manipulate the numbers v and o so that for a signature scheme we always have

$$q^{v-0-1}o^4 \geq 2^{93}$$

■

We have

Proposition 7 *: The set $\{x'_{o+1}, \cdots, x'_{o+v}\}$ is a set of vinegar variables iff the set of homogeneous quadratic polynomials $(S^*) \subset$ the ideal $(x'_{o+1}, \cdots, x'_{o+v})$, where*

$$\forall i, 1 \leq i \leq o,\ y_i^* = \sum \gamma_{ijk} x_j x'_k + \sum \lambda_{ijk} x'_j x'_k \qquad (S^*)$$

Proof. Trivial. ■

Definition : Let S be a set of homogeneous quadratic polynomials. Let $o(S)$ be the maximal number of oil variables with respect to all linear variables, and $v(S)$ be the minimal number of all vinegar variables. Note that $o(S) + v(S) = n$. ∎

For our usage later on, we need some special kind of generators of a linear ideal (i.e., an ideal generated by linear forms in $x_1, \cdots, x_m$) with respect to an ordering $x_1, \cdots, x_m$.

Definition Let a linear ideal I be given. A set of generators $r_1, \cdots, r_k$ with some indices i missing (or we may take the missing ones to be 0's), is said to be a standard generator set if (1), $r_1, \cdots, r_k$ form a linearly independent set, and $I = (r_1, \cdots, r_k)$. (2), with

$$r_j = x_j + \sum_{i=1}^{j-1} a_{ji} x_i$$

where j is not missing (or $r_j \neq 0$), and $a_{ji} = 0$ if i is not missing. ∎

We have

Proposition 8 *Given any linear ideal $I \subset K[x_1, \cdots, x_m]$ and any ordering of the variables $x_1, \cdots, x_m$, (1), there is a standard generator set of I with respect to the ordering. (2), let $i_1, \cdots, i_s$ be integers such that $r_j = 0$ iff $j \in \{i_1, \cdots, i_s\}$, then $K[x_1, \cdots, x_m]/I = K[x_{i_1}, \cdots, x_{i_s}]$. (3), let $\bar{x}_i = x_i$ mod I, and the vector space generated by $\bar{x}_1, \cdots, \bar{x}_m$ be s-dimensional, then $m = s+$ the minimal number of generators of I.*

Proof. It follows from Gaussian Elimination process, and the fundamental theorem of linear algebra ∎

Let $\Phi_i = (\phi_{i,1}, \cdots, \phi_{i,n})$ be a quadratic tame transformation with coefficients random and non-zeroes as in the **Introduction**. Let Φ_i^* be the quadratic homogeneous parts of Φ_i as follows,

$$\Phi_i^* := \begin{cases} h_{i,1} = 0 \\ h_{i,2} = 0 \\ h_{i,3}(x_1, x_2) \\ \cdots \\ h_{i,\ell}(x_1, \cdots, x_{\ell-1}) \\ \cdots \\ h_{i,m}(x_1, \cdots, x_{m-1}) \end{cases}$$

Then the following proposition will show that $v(\Phi_i^*) = m - 1$.

Proposition 9 *: Let Φ_i and Φ_i^* be as above. Let $m > 2$. Then we have the only vinegar variable set is of the form $[x_1, \cdots, x_{m-1}]$ and $v(\Phi_i^*) = m - 1$.*

Proof. We may assume that $h_{i,3}(x_1, x_2)$ has no linear factors. Then a vinegar variablem set I must contain x_1, x_2. Suppose up to ℓ steps, $[x_1, \cdots, x_{\ell-2}] \subset I$, we look at the polynomial $h_{i,\ell} \equiv a x_{\ell-1}^2 \; mod(x_1, \cdots, x_{\ell-2})$. Therefore $x_{\ell-1} \in I$. ∎

Proposition 10 *: Let Φ be a system of random homogeneous quadratic polynomials in $x_1, \cdots, x_n$, $y_1, \cdots, y_m$. If after we set $y_1 = \cdots = y_m = 0$, the set of polynomials Φ is restricted to $\bar{\Phi}$, then we have $v(\Phi) \geq v(\bar{\Phi})$.*

Proof. Let all polynomials of Φ be in $(z_1, \cdots, z_\ell)$ where $\ell = v(\Phi)$. After the reduction by setting $y_1 = \cdots = y_m = 0$, the set of polynomials in $\bar{\Phi}$ is a subset of $(\bar{z}_1, \cdots, \bar{z}_\ell)$ (some of $\bar{z}_i$ might be 0). Hence we have $v(\Phi) \geq v(\bar{\Phi})$. ■

The following Propositions will further reduce the bound on the parameter (see the § 6). Let us introduce the following notations: let the ring be $K[x_1, \cdots, x_n]$, ℓ be a positive integer, the ideal M_i be generated by variables $\{x_1, \cdots, x_{i-1}\}$. A polynomial f_i is a random (non-homogeneous) quadratic polynomial $\in M_i$,

Proposition 11 *: Let $\ell > 2$ and let us omit the first ℓ polynomials and modify the transformation Φ in Proposition 9 as follows,*

$$\Phi_2 := \begin{cases} y_{\ell+1} = x_{\ell+1} + f_{\ell+1} \\ \cdots \\ \cdots \\ y_m = x_m + f_m \end{cases}$$

We have (1), if $x_i \in I$ for $i = 1, \cdots, \ell - 2$, then $v(\Phi_2) = m - 1$. (2), let $\bar{x}_i = x_i$ mod I, if $\{\bar{x}_1, \cdots, \bar{x}_{\ell-2}\}$ generate an s-dimensional vector space, then $v(\Phi_2) = m - s - 1$.

Proof. (1), We set $x_1 = \cdots = x_{\ell-2} = 0$. Then our system of equations is reduced to the system of equations of Proposition 9. Therefore I needs $m - (\ell - 2) - 1 + (\ell - 2) = m - 1$ generators.

(2), Let $\{\bar{x}_1, \cdots, \bar{x}_{\ell-2}\}$ generate an s-dimensional vector space V. Let $\{r_1, \cdots, r_{m-1}\}$ be a standard generating set of I with respect to the natural ordering, note that some r_i may be 0. Then clearly $(r_1, \cdots, r_{\ell-2})$ generated an $\ell - 2 - s$ dimensional vector space. It follows from Proposition 9 that

$$v(\Phi_2) = m - (\ell - 2) - 1 + (\ell - 2) - s = m - s - 1$$

■

ng

Proposition 12 *: Let $\ell \geq 2$ and let us omit the first ℓ polynomials and modify the transformation Φ in Proposition 9 as follows,*

$$\Phi_2 := \begin{cases} y_{\ell+1} = x_{\ell+1} + f_{\ell+1} \\ \cdots \\ \cdots \\ y_m = x_m + f_m \end{cases}$$

with $m \geq 2\ell \geq 4$. Then we have $v(\Phi_2) \geq m - 3$.

Proof. If $\ell = 2$, then our Proposition follows from Proposition 10. If $v(\Phi_2) \geq m - 3$, then we have nothing to prove. Let us assume $\ell > 2$ and $v(\Phi_2) < m - 3$. Let us set $x_1 = 0$. Then there is a reduction of ℓ. Therefore $v(\bar{\Phi}_2) \geq m - 4$. If $v(\bar{\Phi}_2) \geq m - 3$, or the ideal I of minimal vinegar variables $\ni x_1$, then $v(\Phi_2) \geq m - 3$, and we are done. Otherwise (still with $r_1 = 0$) we expect to produce a contradiction. Let us form an Induction Hypothesis:

with $\{r_2, \cdots, r_{m-1}\}$ being a standard generating set of I with respect to the natural order $x_1, \cdots, x_{m-1}$ and at most two of the indices $2, \cdots, m-1$ are missing, say they are indices r, s. Note that if the Induction Hypothesis is true for all ℓ, m, then our statement follows from Proposition 11.

Note that the vector space of 1-homogeneous forms in I is of dimension $m-4$. Then we have the following expressions,

$$r_i = x_i + a_i x_1 + b_i x_r + c_i x_s$$

Substitute

$$\begin{aligned} r_i &= x_i + a_i x_1 + b_i x_r + c_i x_s \\ x_1 &= a_1 x_1 \\ x_r &= b_r x_r \\ x_s &= c_s x_s \end{aligned}$$

into the above system of equations Φ_2, then the coefficients of $x_1^2, x_1x_r, x_1x_s, x_r^2, x_rx_s, x_s^2$ will produce $6(m-\ell) = 3m + 3(m-2\ell) \geq 3m$ homogeneous random non-zero equations in $3(m-3)+3 = 3m-6$ variables a_i, b_i, c_i. Note the number of equations is greater than the number of equations. Hence all $\{a_1\}, \{b_i\}, \{c_i\}$ must be zeros. Now it follows from Proposition 11 that $v(\Phi_2) = m-1 > m-4$. A contradiction. ■

Remark: In general, if we have set disjoint set of variables $\{x_i\}$ and $\{y_j\}$, and we have two reductions mod the two set of variables, we do not expect the number of vinegar variables to be additive. Let us consider,

$$g = (x_1 + y_1)(x_2 + y_2)$$

Then the numbers of vinegar variables are all 1's, before the reductions and after the reductions with respect to $\{x_1, x_2\}$ and $\{y_1, y_2\}$. ■

4 Linearization Attack

One of the way to crack a cryptosystem is to find the plaintext $\{x_i\}$ from the cyphertext $\{y_j\}$. The other attack based on an idea of Patarin which broke the scheme of Matsumoto-Imai and tailored by Ding and Schmidt ([7]) for an attack on an implementation of TTM is as follows, (quote from [7])

Linearization equation is an equation in the form of

$$\sum_{i=1,j=1}^{n,m} a_{ij} x_i y_j(x_1, \cdots, x_n) + \sum_{i=1}^{n} b_i x_i + \sum_{j=1}^{m} c_j y_j(x_1, \cdots, x_n) + d = 0$$

which is satisfied by the set of polynomials y_i of the cipher F and its variable x_i. (Our remark: Please note that the above equation becomes linear once the values of $\{y_j\}$ are known. A suitable system of linear equations of the above type will locate the values of $\{x_i\}$). Those equations were first used by Patarin successfully to attack the Matsumoto-Imai cryptosystems, which we call the linearization method.

which we will call the first order, since y_j appears only in the first order, Patarin-Ding-Schmidt attack. The second order, where y_j appears to the second order, attack is the following (see [7]),

A higher order type of linearization equation:

$$\sum a_{ij}y_iy_j + \sum b_{ij}y_ix_j + \sum c_ky_k + \sum d_\ell x_\ell + e = 0$$

$\cdots$. *To find all solutions for this case surely takes more time but not impossible.*

One may even go to order 3, allow y_j to appear in the third order, attacks. We have the following proposition,

Proposition 13 *: Let $K \subset K^*$ be two finite fields. If all polynomials are $\in K[x_1, \cdots, x_n]$, and if the linear attacks as above with coefficients $a_{ij}, \cdots, e$ in K^* are successive, then the linear attacks as above with coefficients $a_{ij}, \cdots, e$ in K will be successive.*

Proof. Note that the equations are all linear in the coefficients. ■

5 TTMs

Recall that an affine linear transformation is considered to be a tame transformation. For the signature scheme TTMs, we will introduce another variable x_{n+1}. Let we define the product of two vectors $v = (t_1, \cdots, t_m), u = (s_1, \cdots, s_m)$, where t_i, s_j are polynomials as

$$v \odot u = \sum t_is_i$$

Let σ be a cyclic permutation on vector $v = (t_1, \cdots, t_9)$ as

$$\sigma(t_1, \cdots, t_9) = (t_2, \cdots, t_9, t_1)$$

Then naturally we have for $0 \le i \le 8$, the following

$$\sigma^i(t_1, \cdots, t_9) = (t_{i+1}, \cdots, t_9, t_1, \cdots, t_i)$$

We shall define for $0 \le i \le 8$, the following

$$g_{n-i} = ((x_{n+1}, x_1, \cdots, x_7, x_8) \odot (\sigma^i(x_n, x_{n-1}, \cdots, x_{n-8}))$$

For instance, if $i = 5$, then we have

$$g_{n-5} = x_{n+1}x_{n-5} + x_1x_{n-6} + x_2x_{n-7} + x_3x_{n-8} + x_4x_n + x_5x_{n-1} + x_6x_{n-2} + x_7x_{n-3} + x_8x_{n-4}$$

In the following we shall have f_i a random quadratic polynomial in $K[x_1, \cdots, x_{i-1}]$ and h_{n-i} a random quadratic polynomial in $K[x_1, \cdots, x_{n-9}]$. We define the in-between quadratic transformation Φ_2 with ℓ a suitable positive integer as

$$\Phi_2 := \begin{cases} y_{\ell+1} = x_{\ell+1} + f_{\ell+1}(x_1, \cdots, x_\ell) \\ \cdots \\ y_{n-9} = x_{n-9} + f_{n-9}(x_1, \cdots, x_{n-10}) \\ y_{n-8} = x_{n-8} + h_{n-8} + g_{n-8} \\ \cdots \\ y_n = x_n + h_n + g_n \end{cases}$$

The map π will be announced by giving the $n-\ell$ polynomials $\{z_i = \pi_i(\{w_j\}) : for\ i = \ell+1, \cdots, n\}$.

For our usage, we will assume $\ell \geq 8$. It produces a signature in the following way. Given the vector z' (which is a numerical vector), the message the user intends to write, then the vector y' can be found at once (because B is known to the user and invertible, c is known to the user). We assign random values $x'_1, \cdots, x'_\ell$ to $x_1, \cdots, x_\ell$. Then it is easy to see that this new Φ_2 is a *tame transformation* up to $n-9$, and the values $x'_{\ell+1}, \cdots, x'_{n-9}$ can be found. After the substitution, the last nine equations become

$$
\begin{aligned}
&y'_{n-8} = x_{n-8} + x_{n+1}x_{n-8} + \cdots + x'_7 x_{n-6} + x'_8 x_{n-7} + \mu'_{n-8} \\
&\cdots \\
&y'_n = x_n + x_{n+1}x_n + x'_1 x_{n-1} + \cdots + x'_8 x_{n-8} + \mu'_n
\end{aligned}
$$

In the above system of equations, x'_i, y'_i, μ'_j are numbers. If we treat the above system of equations as linear in $x_{n-8}, \cdots, x_n$, the the determinant of the coefficient matrix is of the following form,

$$
det \begin{bmatrix}
x_{n+1}+1, & x'_8, & \cdots, & \cdots, & x'_2, & x'_1 \\
x'_1, & x_{n+1}+1, & \cdots, & \cdots, & x'_3, & x'_2 \\
\cdots, & \cdots, & \cdots, & \cdots, & \cdots, & \cdots \\
\cdots, & \cdots, & \cdots, & \cdots, & \cdots, & \cdots \\
x'_8, & x'_7, & \cdots, & \cdots, & x'_1, & x_{n+1}+1
\end{bmatrix}
$$

It is a monic polynomial of degree 9 in x_{n+1}. Now we will select a value x'_{n+1} for x_{n+1} such that the determinant is non-zero. Therefore, the values $x'_{n-8}, \cdots, x'_n$ of $x_{n-8}, \cdots, x_n$ are determined. We have a complete set of values $\{x'_1, \cdots, x'_{n+1}\}$. Furthermore, we find the values $\{w'_1, \cdots, w'_{n+1}\}$ which is the signature. This satisfies what was said in [13].

The verifier may apply the public key to w', which is equivalent to find the unique x' then the unique $[y'_{\ell+1}, \cdots, y'_n]^T$ and then the unique z'.

We may call the signature scheme TTMs[n-ℓ,n+1].

We have the following proposition about the number of vinegar variables for TTMs[n-ℓ,n+1].

Proposition 14 *Let us assume that $n-9 \geq 2\ell$ and $\ell = 10$. Then the number of vinegar variables, $v(\Phi_2)$, is $\geq n-9$.*

Proof. Let $I = (r_1, \cdots, r_{n+1})$ be a linear ideal of vinegar variables with $r_1, \cdots, r_{n+1}$ a standard generator set with respect to the natural ordering. Note that some r_i may be zero. Let us separate the variables $x_1, \cdots, x_{n+1}$ into 3 categories, (1), $x_i \in I$, i.e, $x_i = 0 \bmod I$. (2), $x_i \notin I$ but $r_i \neq 0$, i.e., $(x_i \bmod I) \in K[x_1, \cdots, x_{i-1}]$. (3) $x_i \notin I$ and $r_i = 0$, i.e., $(x_i \bmod I) = x_i$. Note that for x_i to be in category (1) or (2), then the corresponding $r_i \neq 0$.

Clearly $(r_1, \cdots, r_{n-10})$ is a linear ideal of vinegar variables of the first $n-\ell-9$ polynomials. It follows from Proposition 12 that I contains at least $n-9-3$ terms. We wish to increase the lower bound by 3.

Let us consider the three possibilities, (1) x_{n+1} is of category 3, (2) x_{n+1} is of category 1, (3) x_{n+1} is of category 2.

(1). x_{n+1} is of category 3. If any one of $x_{n-8}, \cdots, x_n$ is in category 3, say x_{n-j}, then we may look at the following equation,

$$x_{n+1}x_{n-j} + x_1 x_{n-j+1} + \cdots = g_{n-j} + h_{n-j} \in I$$

Clearly, after mod out I, the first term is of the form $x_{n+1}x_{n-j}$ which will not be cancelled by any other term. Therefore it is a contradiction. We conclude that none of $x_{n-8}, \cdots, x_n$ is of category 3 or $r_{n-8} \neq 0, \cdots, r_n \neq 0$ and the lower bound will be raised by at least 9.

(2). x_{n+1} is of category 1. Note that $r_{n+1} \neq 0$. We need to raise the lower bound by 2. We want to show that either the lower bound can be raised by 2 or $x_j \in I$ for $j = 1, \cdots, 8$. Note that in the second case (i.e., $x_j \in I$ for $j = 1, \cdots, 8$), it follows from Proposition 11 that the lower bound is raised by 2. Therefore we may assume otherwise, i.e., there is a smallest i such that $x_j \in I$ for $j < i$ and $x_i \notin I$. Then by the definition of standard generator set, we have either x_i is in category 1 or 3. It follows from our assumption that x_i is in category 3. Let us look at the last two equations

$$\begin{aligned}
g_n + h_n &= x_{n+1}x_n + x_1 x_{n-1} + x_2 x_{n-2} + \cdots + x_i x_{n-i} + \cdots + x_8 x_{n-8} + h_n \\
g_{n-1} + h_{n-1} &= x_{n+1}x_{n-1} + x_1 x_{n-2} + x_2 x_{n-3} + \cdots + x_i x_{n-i-1} + \cdots + x_8 x_n + h_{n-1}
\end{aligned}$$

There are two possibilities for x_{n-i}, (a) it is in category 3, or (b) it is not in category 3. In the possibility (a), after we mod out I for the first equation above, there will be a term $x_i x_{n-i}$ which can not be cancelled by any other terms, and this contradicts the assumption that I is a vinegar ideal. We are left with the second possibility (b). Note that in this case we have $r_{n-i} \neq 0$. We only have to further raise the lower bound by 1. We may further assume that x_{n-k}'s are all in category 3 for all $k > i$ (otherwise the lower bound will be further raised by 1). Now we shall look at the second equation above. If x_n is in category 3, then $x_i x_{n-i-1}$ can not be cancelled mod I, which is impossible. Therefore x_n is not in category 3, and $r_n \neq 0$. We conclude that the lower bound is further raised by 1, just as required by the Proposition.

(3). x_{n+1} is of category 2. Note that $r_{n+1} \neq 0$. We need to raise the lower bound by 2. Further note that $x_{n+1} \neq 0 \bmod I$. If x_n is in category 3, then when we mod out I for the first equation in the previous paragraph, we will be left with a term of the form αx_n (which is induced by $x_{n+1}x_n$) where $\alpha \neq 0$ which can not be cancelled by any other terms. This is impossible. We conclude that x_n is not in category 3, or $r_n \neq 0$. Hence we raise the lower bound by 1 more. We are looking for a further raise and finish our task. We may assume that x_{n-i} are all in category 3 for $i = 1, \cdots, 8$. Otherwise our task is finished.

Let us consider if all x_i for $i = 1, \cdots, 8$ are in category 1 or 2. By the way of picking up standard generators with respect to the natural ordering, if all x_i for $i = 1, \cdots, 8$ are in category 1 or 2, then all x_i for $i = 1, \cdots, 8$ are in category 1. It then follows from Proposition 11 that our task is finished. Henceforth, we may assume that for some $i = 1, \cdots, 8$, x_i is in the category 3. We shall take the first i with this property and assume that $x_j \in I$ for $j < i$ and x_i is in category 3. The first equation above will be reduced to the following after mod out I

$$\begin{aligned}
&\bar{x}_{n+1}\bar{x}_n + \bar{x}_i \bar{x}_{n-i} + \cdots + \bar{x}_8 \bar{x}_{n-8} + \bar{h}_n(x_1, \cdots, x_{n-9}) \\
&= \bar{x}_{n+1}\bar{x}_n + x_i x_{n-i} + \cdots + \bar{x}_8 x_{n-8} + \bar{h}_n(x_1, \cdots, x_{n-9})
\end{aligned}$$

Let us think $\bar{x}_1, \cdots, \bar{x}_{n-9}$ as numbers and $x_{n-8}, \cdots, x_{n-1}$ as variables. Then the above equation is a linear equation. It is easy to see that at least one of $\bar{x}_{n+1}, \bar{x}_n$ must only involve

$\bar{x}_i, \cdots, \bar{x}_{n-9}$ and the other one is of the form $\overline{a_{n-i}x_{n-i} + \cdots}$. Comparing the coefficients of $x_{n-i}, \cdots, x_{n-8}$, we can conclude easily that $\overline{x_j - b_j x_i} = 0$ for $j = i-1, \cdots, n-8$ and some suitable numbers $\{b_j\}$. Therefore we conclude that $s = dim\ V = 1$ where V is the vector space generated by $\{\bar{x}_1, \cdots, \bar{x}_8\}$. Now it follows from Proposition 11 that the lower bound is raised by 1. ∎

6 The Cryptanalysis and the Parameters

We will select the parameters n, ℓ depending on the arts of cryptanalysis. At the present, the main tools the attackers use are (1) the Montgomery-Sathaye's attack of finding the linear terms without quadratic parts, (2) the Coppersmith-Stern-Vaudenay's attack on Shamir's birational permutation signature [1], which uses the common kernel space to find the variables not appearing sufficiently many times (currently 9 times) in the quadratic homogeneous forms, (3) the Patarin's linearization attack, (4) the Kipnis-Shamir's [10] oil-vinegar attack which breaks Patarin's *Oil and Vinegar signature scheme* by separating all variables into oil variable and vinegar variables. A Kipnis, J. Patarin, and L. Goubin generalized the method to *Unbalanced Oil and Vinegar Signature Scheme* [11] and show the number of steps of separating variables to oil and vinegar variables is $q^{v-o-1}o^4$. Ding, Schmidt and Yin [8][1] successively apply this technique as the first step of cryptanalysis to break a claimed *secured* case of TTS. (5) the Goubin-Courtois' *minrank* attack which breaks a learner's challenge of TTM and show that the security is $q^{r\lceil \frac{m}{n} \rceil} m^3$.

Let us handle the above mentioned attacks. We want to show that TTMs[20,31] is immune to the above mentioned attacks. In this case, we have $n = 30, \ell = 10$.

For (2) the Coppersmith-Stern-Vaudenay's attack, it suffices to require any variable appears in 9 equations. In TTMs[20,31], every variable x_i for $i \leq 21$ certainly appears in 9 equations. For $x_{22}, \cdots, x_{31}$, they certainly appear in the last nine equations.

For (4) the Kipnis-Patarin-Goubin's attack, it is follows from Proposition 14 that the number v of vinegar variables is at least 21 and the number o of oil variables is at most 10. According to the security formula,

$$o^4 q^{n+1-2o-1} \geq 2^{93}$$

An imitation of Ding-Schmidt-Yin's attack on TTS can not pass the first step and hence fail on TTMs.

For (5) the Goubin-Gourtois' minrank attack, then the minrank will be at least 10. According to their formula,

$$q^r (n-\ell)^3 > 2^{93}$$

the security will be at least 2^{93}. By the way, since the minrank attack fails, the Montgomery-Sathaye's attack fails too.

As for (3) the Patarin's attack, it fails after we run the program (written by B.Y. Yang) of linearization for TTMs[20,31] with coefficients in $\mathbf{F_2}$, and show that there is no equation

[1] In the paper [19], Yang-Chen show a formula which is claimed to be secure, in [8] Ding-Schmidt-Yin show the said formula is insecure, and in genral they mistrust any formula of similar kind, in [20] Yang-Chen give another formula which is claimed to be secure.

produced up to linearization attack of order 3. It follows from Proposition 13 that the same statement holds for $\mathbf{F}_{2^8}$. Therefore all mentioned attacks fail.

Similar to the above analysis, we have TTMs[m,m+11] for all $m \geq 20$. In case we need to include some m bytes hash function, we may select the proper m.

7 Performance

We may compare TTMs(20,31) with NESSIE (the New European Schemes for Signature, Integrity, and Encryption) round 2 candidate signature schemes (the winner is **Sflash**) for security standards for low-cost smart-card applications in the following table,

Scheme	Signature	Publ-key	Priv-key	Setup	Signing	Verifying
RSA-PSS	1024 bits	128 B	320 B	2.7 sec	84 ms	2.0 ms
ECDSA	326 bits	48 B	24 B	1.6 ms	1.9 ms	5.1 ms
ESIGN	1152 bits	145 B	96 B	0.21 sec	1.2 ms	0.74 ms
QUARTZ	128 bits	71.0 kB	3.9 kB	3.1 sec	11 sec	0.24 ms
SFLASH	259 bits	15.4 kB	2.4 kB	1.5 sec	2.8 ms	0.39 ms
TTMs(20,31)	248 bits	10.8 kB	1.4 kB	1.6 ms	20 μs	0.21 ms

Table 1: Performances on a 500 MHz PC

It is obvious that TTMs[20,31] is superior to SFLASH.

References

[1] Coppersmith, D.,Stern, J. and Vaudenay, S. *Attacks on the Birational Permutation Signature Scheme.* Crypto'93, LNCS 773, pp. 435-443.

[2] Chen, J.M., Yang, B.Y. and Peng, B.Y., *Tame Transformation Signatures With Topsy-Turvy Hashes.* pp 93-100, IWAP'2002.

[3] Chen, J.M., and Yang, B.Y., *TTS: Rank attacks in tame-like multivariate PKCs.* http://eprint.iacr.org/2004/061.

[4] Chen, J.M., Yang, B.Y. and Chen, Y., *TTS: High-speed signature on a low-cost smart card.* In Joye and Quisquater, editors, Cryptographic Hardware and Embedded System: CHES 2004, LNCS 3156, pp 371-385. Springer,2004.

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

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

[7] Ding,J. Schmidt, D.*A Defect Of The Implementation Schemes Of The TTM Cryptosystem* Cryptology ePrint Archiv (2003/086).

[8] Ding J., Schmidt. D., and Yin, Z., *Cryptanalysis of the new TTS Schemes in CHES-2004.* IWAP 2004.

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

[10] Imai, H. Matsumoto *Algebraic methods for constructing asymmetric cryptosystems, Algebraic and Error-Correcting Codes.* Prod. The 44th Intern. Conf., Grenoble, France, Springer-Verlag, 108-119, 1985.

[11] Kipnis, A., Patarin, J. and Goubin, L. *Unbalanced Oil and Vinegar Signature Scheme.* Eurocrypt'99, LNCS, vol 1592, pp. 206-222. springer 1999.

[12] Kipnis, A., Shamir, A. *Cryptanalysis of the Oil and Vinegar Signature Scheme.* Crypt'98, LNCS, vol 1462, pp. 257-266.

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

[14] 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.

[15] 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.

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

[17] Patarin, J. *The Oil and Vinegar Algorithm for Signatures.* presented at the Dagstuhl Workshop on Cryptography, Sept 1997

[18] Shamir, A. *Efficient signature schemes based on birational permutations.* In LNCS, advances in cryptology- CRYPTO'93, vol 1462, pp257-266. Springer, 1998.

[19] Yang. B.Y. and Chen, J.M. *TTS: High-Speed Signatures from Low-End Smartcard.* CHES'04, LNCS 3156, pp.371-383.

[20] Yang. B.Y. and Chen, J.M. *Building Secure Tame-Like Multivariate Public-Key Cryptosystem: the New TTS.* Pre-print, 2005.