Int. J. Inf. Secur. (2006) 5(4): 231–240
DOI 10.1007/s10207-006-0003-9

REGULAR CONTRIBUTION

Jintai Ding · Dieter Schmidt · Zhijun Yin

Cryptanalysis of the new TTS scheme in CHES 2004

Published online: 4 April 2006

Abstract We combine the method of searching for an invariant subspace of the unbalanced Oil and Vinegar signature scheme and the Minrank method to defeat the new TTS signature scheme, which was suggested for low-cost smart card applications at CHES 2004. We show that the attack complexity is less than 2^{50}.

Keywords Public key · Multivariate · Quadratic polynomials · Minrank · Tame transformation

1 Introduction

The subject we deal with is the new TTS authentication system presented at CHES 2004. This new system belongs to the family of TTS multivariate signature schemes [23]. The main achievement of our work is to show how the combination of several different attack methods can be used to defeat the new TTS system, and more generally how combining known attacks on multivariate schemes can be a powerful tool.

In the last few years, new methods have been invented to construct multivariate cryptosystems, which use multivariate functions instead of functions of a single variable. The security of this type of cryptosystems is based on the fact that solving modular polynomial equations with many variables is an NP-complete problem [10].

In 2003, *Sflash* [18], a multivariate signature scheme was selected by NESSIE, the New European Schemes for Signatures, Integrity, and Encryption project within the Information Society Technologies (IST) Programme of the European Commission, as one of the security standards for low-cost smart-card applications. Sflash is a variant of the Matsumoto–Imai encryption cryptosystem [14], and is derived from it by applying the minus method, which was originally suggested by Shamir [20]. The minus method amounts to taking out (minus) a few components of a given multivariate map. After Patarin defeated the original Matsumoto–Imai encryption cryptosystem [16], several variants and extensions of the Matsumoto–Imai cryptosystem [5, 6, 17, 19], including Sflash, were constructed.

Another interesting family of cryptosystems is the TTM system [15]. The basic idea of this construction in some way originated from the famous Jacobian Conjecture in mathematics. For the TTM construction, the key building block are the nonlinear invertible de Jonquières maps $J(z_1, \ldots, z_m)$ over an m dimensional vector space on a field k, which maps an element $X = (z_1, \ldots, z_m)$ in k^m according to:

$$J(z_1, \ldots, z_m) = (z_1 + g_1(z_2, \ldots, z_m), \\ z_2 + g_2(z_3, \ldots, z_m), \ldots, z_{m-1} + g_{m-1}(z_m), z_m)$$

where the g_i are polynomial functions. The de Jonquières maps belong to the family of so-called tame transformations from algebraic geometry.

Although the inventor of TTM argued that the system is very secure against all known standard attacks, Courtois and Goubin [11] claimed that they could defeat the TTM schemes. The inventor of TTM refuted this claim in [1], and presented a new implementation scheme to support their case. In [7] another method was found to defeat the original TTM schemes in [15] and all other schemes suggested in [3]. Later Ding and Schmidt [8, 9] also defeated the new schemes in [1], and pointed out that all existing TTM schemes share a common defect that makes them insecure. Thus, at this moment all variants of TTM remain insecure.

The original TTM schemes were intended for the purpose of public key encryption. Attempts were made to apply a similar but simpler idea for signatures, the result being called the TTS (tamed transformation signature) scheme. It is essentially the result of an application of the minus method in [20] to a tame transformation. A few systems were suggested by Chen and his collaborators in [2, 22] and the security and efficiency of these systems were claimed to rival that of Sflash. The inventors of the first TTS schemes later admitted in [23] that they had been careless about their

J. Ding · D. Schmidt (✉) · Z. Yin
University of Cincinnati, Cincinnati, OH 45220, USA
E-mail: dschmidt@ececs.uc.edu

security claims, and they showed that all schemes in [22] could be defeated easily. New schemes were suggested in [23] and again were claimed to have the security and efficiency rivaling those of Sflash. One scheme in particular was carefully studied in terms of its practical implementation on low cost smart-card, and was presented at CHES 2004 [24]. They concluded that the system is indeed very efficient.

In this paper, we will present an attack method that defeats the new TTS scheme studied in [24] with a complexity of less than 2^{50} computations in a finite field of size 2^8. Our attack method is a combination of the method suggested in [12] used to attack the unbalanced Oil and Vinegar scheme, with the Minrank attack. The attack is successful, despite the claim of the authors in [23, 24] that the new scheme is totally secure from the Minrank attack.

This paper contains three main sections in addition to the introduction. In Sect. 2 we will introduce the original TTS schemes, give a brief cryptanalysis, and then review the new TTS signature schemes. In Sect. 3 we will present the cryptanalysis of the new TTS scheme, which was given in [24]. We will present our conclusions in the last section.

2 TTS and the new TTS schemes

2.1 The original TTS scheme and its cryptanalysis

The original TTS scheme [2, 22] combines Shamir's idea of Minus [20] with the basic idea of TTM. This combination was first implicitly pointed out in [11], where it was called a Triangular–Minus system.

For the case of such a TTS scheme [2, 22], the public key $\bar{T}$ is made of m quadratic polynomials in n variables over a finite field, $\bar{T}(x_1, \ldots, x_n) = (y_1(x_1, \ldots, x_n), \ldots, y_m(x_1, \ldots, x_n))$, where $m < n$. The m polynomials y_i, are made public for verifying the authenticity of the signature. We will limit our discussion to finite fields with characteristic 2, since this was used in all TTS schemes, although their construction would work for finite fields with odd characteristics.

The map $\bar{T}$ from k^n to k^m is derived as $\bar{T} = \bar{L}_1 \circ \mathfrak{J}^- \circ \bar{L}_2$, where $\circ$ denotes the composition of maps, $\bar{L}_1$ is an invertible affine linear map on a space of dimension m, $\bar{L}_2$ is an invertible affine linear map on a space of dimension n and $\bar{L}_1$, $\bar{L}_2$ are randomly chosen. The map

$$\begin{aligned}\mathfrak{J}^-(z_1, \ldots, z_n) &= (z_{n-m+1} + g_{n-m+1}(z_1, \ldots, z_{n-m}),\\ &z_{n-m+2} + g_{n-m+2}(z_1, \ldots, z_{n-m+1}), \ldots, z_n + g_n(z_1,\\ &\ldots, z_{n-1})) = (\bar{y}_1(z_1, \ldots, z_{n-m+1}), \ldots, \bar{y}_m(z_1, \ldots, z_n)),\end{aligned}$$

which is derived from the upper-triangular de Jonquières map

$$\begin{aligned}\mathfrak{J}(z_1, \ldots, z_n) = (&z_1, z_2 + g_2(z_1), \ldots,\\ &z_{n-m+1} + g_{n-m+1}(z_1, \ldots, z_{n-m}),\\ &z_{n-m+2} + g_{n-m+2}(z_1, \ldots, z_{n-m+1}), \ldots,\\ &z_n + g_n(z_1, \ldots, z_{n-1}))\end{aligned}$$

by removing the first $n-m$ components (the minus method). One can see that $\bar{T} = \bar{L}_1 \circ U^{-1} \circ U \circ \mathfrak{J}^- \circ \bar{L}_2$, where U is a randomly chosen lower-triangular invertible linear transformation from k^m to k^m such that

$$\begin{aligned}&U(z_1, \ldots, z_m)\\ &\quad= \left(a_{11}z_1, \sum_{j=1}^{2} a_{2j}z_j, \ldots, \sum_{j=1}^{i} a_{ij}z_j, \ldots, \sum_{j=1}^{m} a_{mj}z_j\right),\end{aligned}$$

where each $a_{jj} \neq 0$ for $j = 1, \ldots, m$. Then we have

$$\begin{aligned}&U \circ \mathfrak{J}^-(z_1, \ldots, z_a n)\\ &\quad= \left(a_{11}\bar{y}_1(z_1, \ldots, z_{n-m+1}), \sum_{j=1}^{2} a_{2j}\bar{y}_j(z_1, \ldots, z_{n-m+j}),\right.\\ &\quad\ldots, \sum_{j=1}^{i} a_{ij}\bar{y}_j(z_1, \ldots, z_{n-m+j}),\\ &\quad\left.\ldots, \sum_{j=1}^{m} a_{mj}\bar{y}_j(z_1, \ldots, z_{n-m+j})\right)\\ &\quad= (\bar{w}_1(z_1, \ldots, z_{n-m+1}), \ldots, \bar{w}_m(z_1, \ldots, z_n)).\end{aligned}$$

Therefore $U \circ \mathfrak{J}^-$ is an equivalent choice for $\mathfrak{J}^-$. In this case, we can associate the standard bilinear form to the quadratic part of $\bar{w}_i$. The ranks of those bilinear forms will be in ascending order, although not necessarily strictly ascending. This means that any such scheme cannot work, as the Minrank method [11] can be used due to this property of the ranks. This is a much more efficient attack method than the one of [23], where an idea suggested in [4] was used. The conclusion is that no matter what parameters one chooses, the old TTS systems as given in [2, 22] are insecure.

2.2 The new TTS scheme

The authors admitted in [23] that their previous constructions led to insecure schemes. They also suggested some new schemes and made claims about their security and their efficiency. The fundamental problem of their constructions seems to be that they are very much concerned about the efficiency in order to beat Sflash, so that their constructions are given in terms of specific formulas, rather than following from basic general principles. This is why our attack method relies on the specific form of these formulas, and not on some general structure.

The paper [23] suggests four families of formulas and one of them is carefully studied for its practical implementations on low cost smart-cards. It was presented at CHES-2004. In this paper, we will attack this family, which appears on page 373 of [24] and is called there TTS(20,28).

According to the claim in [23, 24] the system is secure with at least a complexity of 2^{80} (a minimum security requirement by NESSIE). This specific construction depends

on a map $f(x_0, x_1, \ldots, x_{27}) = (f_1, \ldots, f_{20})$ from $k^n = k^{28}$ to $k^m = k^{20}$, where k is a finite field of size 2^8. The map is given in the Appendix. The public key for the new TTS system is F and given by

$$F = L_1 \circ f \circ L_2.$$

L_1 is an invertible affine linear transformation over k^{20}. L_2 is an invertible affine linear transformation over k^{28}. These two transformations make up the secret key.

In order to sign a document $P = (p_1, \ldots, p_{20})$, which is an element of k^{20}, one needs to find a solution of the equation

$$F(x_0, \ldots, x_{27}) = P. \tag{2.1}$$

The reason that one can find a solution is due to the triangular type structure of the f_i.

From the formulas, it is clear that the constructed f_i can be divided into three groups.

$$\text{(I)} = \{f_i \mid i = 1, \ldots, 9\}, \quad \text{(II)} = \{f_i \mid i = 10, 11\},$$
$$\text{(III)} = \{f_i \mid i = 12, \ldots, 20\}.$$

First, we notice that the quadratic part of Group (I) elements are all in the form of

$$\sum_{i=1,\ldots,7;\, j=8,\ldots,16} a_{ij} x_i x_j, \tag{2.2}$$

and if we form any linear combination of those elements, the rank of the associated quadratic form stays at 14. Second, the Group (II) elements come from a de Jonquières construction and if we add Group (I) elements to the Group (II) elements, the rank of the corresponding bilinear form increases, but the rank cannot exceed 16. Third, we notice that the quadratic parts of Group (III) elements are all in the form of

$$\sum_{i=1,\ldots,18;\, j=19,\ldots,27} a_{ij} x_i x_j + \sum_{i,\, j=8,\ldots,18} b_{ij} x_i x_j + \sum_{j=19,\ldots,27} c_j x_0 x_j, \tag{2.3}$$

and if we add any Group (III) elements to any linear combination of Group (I) and (II) elements, the rank of the corresponding bilinear form also increases and a random linear combination of all f_i would produce a non-degenerate quadratic form.

In order to sign a document P one needs to solve the equation

$$f \circ L_2(x_0, \ldots, x_{27}) = L_1^{-1}(P).$$

One first solves $f(x_0, \ldots, x_{27}) = L_1^{-1}(P)$, and then applies L_2^{-1}.

To solve any equation in the form of $f(x_0, \ldots, x_{27}) = (\bar{p}_1, \ldots, \bar{p}_{20})$, because of (2.2), one first randomly fixes the values of $x_1, \ldots, x_7$. This allows the polynomials from Group (I) to produce nine linear equations, whose solution gives the values of $x_8, \ldots, x_{16}$. Then we plug the values of $x_1, \ldots, x_{16}$ into Group (II) and Group (III). Due to the de Jonquières type triangular structure, f_{10} produces first one linear equation, which gives the value of x_{17}. Then one once more plugs the value of x_{17} into f_{11}, which gives a linear equation to find the value of x_{18}. Then we substitute the values of x_{17}, x_{18} into Group (III), and randomly choose a value of x_0. This, due to (2.3), produces again nine linear equations, whose solution gives us the values of $x_{19}, \ldots, x_{27}$. Then one can apply L_2^{-1} to find a solution, which produces a signature vector.

To forge a signature, we need to know how to find a (not THE) solution for the equation $F(x_0, \ldots, x_{27}) = P$.

3 Cryptanalysis of the new TTS scheme

Our attack method is a combination of searching for invariant subspaces [12], of Minrank [11] and of other general methods for bilinear forms.

Let $L_2(x_0, \ldots, x_{27}) = (L_{2,0}(x_1, \ldots, x_{27}), \ldots, L_{2,27}(x_1, \ldots, x_{27}))$. Let $\tilde{F} = f \circ L_2$, and $\tilde{F}(x_0, x_1, \ldots, x_{27}) = (\tilde{F}_1, \ldots, \tilde{F}_{20})$.

Similar we define $(\tilde{\text{I}}) = \{\tilde{F}_i \mid i = 1, \ldots, 9\}$, $(\tilde{\text{II}}) = \{\tilde{F}_i \mid i = 10, 11\}$, and the third part $(\tilde{\tilde{\text{III}}}) = \{\tilde{F}_i \mid i = 12, \ldots, 20\}$. They have properties similar to those described in (2.2) and (2.3) for Groups (I), (II) and (III).

First we know that for $l = 1, \ldots, 9$,

$$\tilde{F}_l = \sum_{i=1,\ldots,7;\, j=8,\ldots,16} a_{lij} L_{2,i} L_{2,j}. \tag{3.1}$$

Therefore, if we could find the space of the linear combinations of the linear parts (no constant term) of $L_{2,i}$, $i = 1, \ldots, 7$, then we could do a linear substitution using any linear equation, whose linear part is defined by elements from this space. The solution is not unique, as can be seen in [13, 21], but for our purpose it suffices to work with a basis for the subspace. According to algebraic geometry, substitution of a linear equation is equivalent to the evaluation on a linear variety. Here the substitution by linear equations is equivalent to substituting all the $L_{2,i}$, $i = 1, \ldots, 7$, by constants.

F_i and $\tilde{F}_i$ are just linear combinations of each other with additional constant terms due to the invertibility of L_1. Through a search for linear equations by linear combination, we could find nine linear independent equations, whose solution gives the values of $L_{2,j}$, $j = 8, \ldots, 16$. Then due to the de Jonquières structure of Group (II), through substitution, the whole system will be reduced to solving a set of equations coming from linear combinations of Group $(\tilde{\tilde{\text{III}}})$ with all values of $L_{2,j}$, $j = 1, \ldots, 18$ given. This can be handled easily and it is the final step of our attack.

Our attack strategy actually is first to find the linear span of $(\tilde{\mathrm{I}})$ then to find the linear span of both $(\tilde{\mathrm{I}})$ and $(\tilde{\mathrm{II}})$, and then the linear span of the linear part of $L_{2,i}$, $j = 1, \ldots, 7$, in order to break the system.

3.1 Step 1: The unbalanced Oil and Vinegar attack

In preparation for Proposition 1 below we define the following set of variables.

- Let S be the set of all variables $\{x_0, \ldots, x_{27}\}$.
- Let $O = \{x_1, x_3, x_5, x_7, x_{19}, \ldots, x_{27}\}$ be the set of the so called Oil variables. The Vinegar variables make up the set $V = S - O$.
- Let $X = (x_0, x_1, \ldots, x_{27}) = \sum_{i=0}^{27} x_i E_i$, where $E_i = (0, 0, 0, \ldots, 1, 0, \ldots 0)$ is the vector whose component at position $i + 1$ is 1 and the rest are zero.
- Let $\bar{O}$ denote the space of the span of the vectors corresponding to the Oil variables, namely

  $$\bar{O} = \mathrm{Span}(E_1, E_3, E_5, E_7, E_{19}, \ldots, E_{27}),$$

- Let $\bar{V}$ denote the space of the span of the vectors corresponding to the Vinegar variables, namely

  $$\bar{V} = \mathrm{Span}(E_0, E_2, E_4, E_6, E_8, \ldots, E_{18}).$$

  Here we must be very careful about the difference between the variables and the corresponding space. The variables are just the coordinates of a vector in terms of the standard basis. They are functions from k^n to k, which actually are elements in the dual space of k^n. Therefore, these two are the dual of each other.
- Let $L_1(x_1, \ldots, x_{20}) = (x_1, \ldots, x_{20}) \times A_1 + (\alpha_1, \ldots, \alpha_{20})$ where A_1 is an $m \times m$ invertible matrix. Let $L_1^0(x_1, \ldots, x_{20}) = (x_1, \ldots, x_{20}) \times A_1 = (L_{1,1}^0, \ldots, L_{1,20}^0)$, be the linear part of L_1.
- Let $L_2(x_0, \ldots, x_{27}) = (x_0, \ldots, x_{27}) \times A_2 + (a_0, a_1, \ldots, a_{27})$, where A_2 is a $n \times n$ invertible matrix. Let $L_2^0(x_0, \ldots, x_{27}) = (x_0, \ldots, x_{27}) \times A_2$, and $L_{2,i}^0$ is the linear part of $L_{2,i}$. We can also see that for any fixed i,

  $$L_{2,i} = x_i \circ L_2(x_0, \ldots, x_{27}), \tag{3.2}$$

  namely $L_{2,i}$ can be derived as a composition of x_i by L_2 from the right.
- Let $\tilde{O} = L_2^0(\bar{O})$ be the image of $\bar{O}$ under L_2^0.
- Let ${f^0}_i$ denote the quadratic part of polynomial f_i.
- Let $f^0(x_0, \ldots, x_{27}) = ({f^0}_1, \ldots, {f^0}_{20})$.
- Let ${F^0}_i$ denote the quadratic part of polynomial F_i.
- Let $F^0(x_0, \ldots, x_{27}) = ({F^0}_1, \ldots, {F^0}_{20})$, so that $F^0 = L_1^0 \circ f^0 \circ L_2^0$.

For each quadratic polynomial ${f^0}_l = \sum_{i \geq j} (f_l)_{ij} x_i x_j$, we can use the standard method to associate an $n \times n$ symmetric matrix m_l to it such that $(m_l)_{ii} = 0$ and $(m_l)_{ij} = (m_l)_{ji} = (f_l)_{ij}$, if $i > j$. For each m_l, we can associate a bilinear form as $\langle X, X' \rangle_l = X m_l (X')^t$ and its quadratic form $\langle X, X \rangle_l = X m_l X^t$. Here $X' = (x'_0, \ldots, x'_{27})$. (Remark: When a field with odd characteristic is used the definition of these matrices has to be modified accordingly.)

Similarly for each quadratic polynomial ${F^0}_l = \sum_{i \geq j} (F_l)_{ij} x_i x_j$, we can associate an $n \times n$ symmetric matrix M_l. For each M_l, we can also associate a bilinear form as $\langle X, X' \rangle^l = X M_l (X')^t$ and its quadratic form $\langle X, X \rangle^l = X M_l X^t$.

Then we have that, for any fixed l,

$$M_l = \sum_{i=1}^{20} (A_1)_{il} \left(A_2 m_i A_2^t \right), \tag{3.3}$$

where $(A_1)_{il}$ are entries of the matrix A_1.

Our first observation is that

Proposition 1

$${f^0}_l(x_0, \ldots, x_{27}) = \sum_{i \in O, j \in V} \alpha_{i,j,l} x_i x_j + \sum_{i,j \in V} \beta_{i,j,l} x_i x_j, \tag{3.4}$$

for any fixed l.

Let $o = |O|$ and $v = |V|$. In terms of this description, these polynomials are just some unbalanced Oil and Vinegar polynomials [12] and all the matrices m_l can be rewritten in the corresponding form if we choose a coordinate system as

$$\bar{X} = (x_1, x_3, x_5, x_7, x_{19}, \ldots, x_{27}, x_0, x_2, x_4, x_6, x_8, x_9, \ldots, x_{18}).$$

Here we choose the basis of the oil space as the first o components and the basis of the vinegar space as the last v components, and we have that $\langle X, X \rangle_i = \bar{X} \bar{m}_i \bar{X}^t$,

$$\bar{m}_i = \begin{pmatrix} 0 & b_i \\ b_i^t & d_i \end{pmatrix}, \tag{3.5}$$

where b_i is an $o \times v$ matrix and d_i is a symmetric $v \times v$ matrix. This follows directly from (3.4).

Let Z be the 28×28 permutation matrix such that $X = \bar{X} \times Z$.

Because those polynomials are unbalanced Oil and Vinegar polynomials, we can apply the attack method in [12] to find the hidden Oil space $\tilde{O}$. According to [12], the computation complexity is roughly $(2^8)^{v-o-1} o^4 < 2^{23}$.

Now, let us assume that we have found $\tilde{O}$. Then we can choose a new coordinate system such that the first o components are from $\tilde{O}$ and rewrite the matrix M_i.

In terms of matrix notation, we can find an invertible $n \times n$ matrix A_3 such that

$$A_3 M_i A_3^t = \bar{M}_i = \begin{pmatrix} 0 & B_i \\ B_i^t & D_i \end{pmatrix}, \tag{3.6}$$

which follows from (3.5) and (3.4).

Let $L_3(x_0, \ldots, x_{27}) = (x_0, \ldots, x_{27}) \times A_3$. Then we know that the subspace $\bar{O}$ is invariant under the linear transformation $L_2^0 \circ L_3$ or equivalently

$$A_{32} = A_3 \times A_2 = Z^{-1} \times \begin{pmatrix} Q_1 & 0 \\ R & Q_2 \end{pmatrix} = Z^{-1} \times Q. \tag{3.7}$$

Remark 1 One important thing that we must be careful with is that A_{32} preserves the oil space, however in terms of coordinate system it actually preserves the vinegar coordinates, which is exactly due to the dual relationship mentioned at the beginning of this section.

Proposition 2 *Let Q be as defined above in (3.7). Then*
(1) the space spanned by E_i, $i = 0, \ldots, 12$, is invariant under the action of Q from the right;
(2) the space spanned by $x_i, i = 13, \ldots, 27$, is the same as the space spanned by $x_i \circ Q(x_0, \ldots, x_{27})$, where $Q(x_0, \ldots, x_{27}) = X \times Q$.

This is to say that

$$\begin{aligned} &\text{Span } \left\{L_{2,i}^0(x_0, \ldots, x_{27}), i \in V\right\} \\ &\quad = \text{Span}\{L_{3,i}^-(x_0, \ldots, x_{27}), i = 13, \ldots, 27\}, \end{aligned}$$

where

$$\begin{aligned} &(L_{3,0}^-(x_0, \ldots, x_{27}), \ldots, L_{3,27}^-(x_0, \ldots, x_{27})) \\ &\qquad = (x_0, \ldots, x_{27}) \times A_3^{-1} Z^{-1}. \end{aligned}$$

This can be seen easily from

$$A_2 = A_3^{-1} Z^{-1} \times \begin{pmatrix} Q_1 & 0 \\ R & Q_2 \end{pmatrix} = A_3^{-1} Z^{-1} Q.$$

This allows us to find the space spanned by the image of the linear parts of the vinegar variables composed from the right by L_2.

This finishes the first step of our attack, which is a simple application of the attack method for the unbalanced Oil and Vinegar scheme.

3.2 Step 2: The Minrank attack

Any bilinear form $\langle , \rangle_i$ on $k^n \times k^n$ can be restricted to the subspace $\bar{O} \times k^n$ and has then the form

$$\langle X_o, X' \rangle_i = \bar{X}_o (m_s)_i (\bar{X}')^t = X_o m_i (\bar{X}')^t = f^s{}_i \tag{3.8}$$

where

$$\begin{aligned} X_o &= (0, x_1, 0, x_3, 0, x_5, 0, x_7, 0, \ldots, 0, x_{19}, \ldots, x_{27}), \\ \bar{X}' &= (x_1', x_3', x_5', x_7', x_{19}', \\ &\qquad \ldots, x_{27}', x_0', x_2', x_4', x_6', x_8', x_9', \ldots, x_{18}') \\ \bar{X}_o &= (x_1, x_3, x_5, x_7, x_{19}, \ldots, x_{27}). \end{aligned}$$

and

$$(m_s)_i = (0 \; b_i), \tag{3.9}$$

where 0 denotes an $o \times o$ matrix and b_i an $o \times v$ matrix.

This implies that if we restrict the bilinear from $\langle , \rangle^i$ to the space $\tilde{O} \times k^n$, then the associated matrix $(M_s)_i$ under the coordinate system defined by A_3 should be exactly $\begin{pmatrix} 0 & B_i \end{pmatrix}$, and

$$B_i = \sum_{j=1,\ldots,20} (A_1)_{ji} \left(Q_1 b_j Q_2^t\right), \tag{3.10}$$

because

$$\begin{aligned} &\begin{pmatrix} Q_1 & 0 \\ R & Q_2 \end{pmatrix} \times \begin{pmatrix} 0 & b_j \\ b_j^t & d_j \end{pmatrix} \times \begin{pmatrix} Q_1 & 0 \\ R & Q_2 \end{pmatrix}^t \\ &\quad = \begin{pmatrix} 0 & Q_1 b_j Q_2^t \\ Q_2 b_j^t Q_1^t & Q_2 b_j^t R^t + R b_j Q_2^t + Q_2 d_j Q_2^t \end{pmatrix} \end{aligned}$$

Now let us look at all the b_i. Our key observation is that

$$\begin{aligned} f^s{}_{10} &= x_1 x_6' p_{17,1} + x_5 x_2' p_{17,2} + x_3 x_4' p_{17,3}, \\ f^s{}_{11} &= x_7 x_2' p_{18,1} + x_3 x_6' p_{18,2} + x_5 x_4' p_{17,3}. \end{aligned}$$

We find that the rank of the corresponding matrices $(m_s)_i$ or to say b_i is exactly 3 for $i = 10, 11$, since the bilinear form is restricted to a product of two different subspaces. The rank of the other matrices are all higher. One can also see clearly that in the space of all possible linear combinations of b_i, these two matrices and their constant multiples are the only matrices of the lowest rank 3.

In this case, we can use the Minrank method to search for both b_{10} and b_{11} in $Q_1 b_{10} Q_2^t$, $Q_1 b_{11} Q_2^t$ through linear combinations of B_i, because A_1 is invertible. We have a total of 20 matrices of size 13×15 and the Minrank is 3. From the complexity analysis in [11], we know to find one of them takes no more than a complexity of $(2^8)^{2\times 3} = 2^{48}$.

Now, let us assume that we have found two rank 3 matrices $H_i, i = 10, 11$, and that

$$H_i = \sum_{j=1}^{20} h_{ij} B_j. \tag{3.11}$$

Because of the uniqueness of the space of linear combinations of matrices B_j, we have that

$$\sum_{j=1}^{20} h_{10,j} {F^0}_j = \beta_1 \tilde{F^0}_{11}, \quad \sum_{j=1}^{20} h_{11,j} {F^0}_j = \beta_2 \tilde{F^0}_{10} \tag{3.12}$$

or

$$\sum_{j=1}^{20} h_{10,j} {F^0}_j = \beta_1 \tilde{F^0}_{10}, \quad \sum_{j=1}^{20} h_{11,j} {F^0}_j = \beta_2 \tilde{F^0}_{11}. \tag{3.13}$$

where β_1 β_2 are non-zero constants in k and

$$\big(\tilde{F^0}_1, \ldots, \tilde{F^0}_{20}\big) = f^0 \circ L_2^0, \quad f^0 = \big({f^0}_1, \ldots, {f^0}_{20}\big).$$

The quadratic polynomials ${f^0}_i$ are linearly independent, the linear and constant terms are, therefore, determined by the quadratic terms. This means that we could find constant multiples of both $\tilde{F}_{10}$, $\tilde{F}_{11}$ by applying formula (3.12) or (3.13), namely

$$\sum_{j=1}^{20} h_{10,j} F_j = \beta_1 \tilde{F}_{11}, \quad \sum_{j=1}^{20} h_{11,j} F_j = \beta_2 \tilde{F}_{10} \tag{3.14}$$

or

$$\sum_{j=1}^{20} h_{10,j} F_j = \beta_1 \tilde{F}_{10}, \quad \sum_{j=1}^{20} h_{11,j} F_j = \beta_2 \tilde{F}_{11}. \tag{3.15}$$

Here $(\tilde{F}_1, \ldots, \tilde{F}_{20}) = F \circ L_2$, and $\tilde{F}_{10}, \tilde{F}_{11}$ are essentially f_{10}, f_{11} but with a substitution of variables.

3.3 Step 3: The search for the null subspace

Now let us take a careful look at both f_{11}^0, f_{10}^0 in terms of their related bilinear forms. Through computation, we know that both m_{11}, m_{10} are of rank 14 and therefore the corresponding bilinear form is of rank 14 and the null spaces N_{11}, N_{10} (the space of vectors perpendicular to the whole space) for both bilinear forms have dimension 14. We can see and show by calculation that

$$N_{10} = \text{Span}(E_0, E_7, E_8, E_{17}, E_{18}, E_{19}, \ldots, E_{27})$$
$$N_{11} = \text{Span}(E_0, E_1, E_8, E_9, E_{18}, E_{19}, \ldots, E_{27})$$

We observe that

$$N_{10} \cap N_{11} \cap \bar{O} = \text{Span}(E_{19}, \ldots, E_{27}) = \bar{O}_1$$

Because of (3.11), we know that the null spaces of the bilinear form associated to $M_i, i = 10, 11$ should give us exactly $L_2^0(N_i) = \tilde{N}_i, i = 10, 11$. Here $\tilde{N}_i$ denotes the null space for the bilinear form defined by M_i. This can be done by solving a set of n linear equations with n variables:

$$X \times M_i = 0.$$

This means that we can find

$$\tilde{O}_1 = L_2^0(\bar{O}_1)$$
$$= \tilde{N}_{10} \cap \tilde{N}_{11} \cap \tilde{O} = \text{Span}\big(L_2^0(x_{19}), \ldots, L_2^0(x_{27})\big).$$

Now, let us assume that we have found $\tilde{O}_1$, then we can choose a new coordinate system such that the first o_1 components are from $\tilde{O}_1$, where o_1 is the dimension of $\tilde{O}_1$ and rewrite the matrix M_i.

In terms of matrix notation, we can find an invertible $n \times n$ matrix A_4 such that

$$A_4 M_i A_4^t = \tilde{M}_i = \begin{pmatrix} 0 & \tilde{B}_i \\ \tilde{B}_i^t & \tilde{D}_i \end{pmatrix}. \tag{3.16}$$

This follows from the specific formulas of f_i, where there is no $x_i x_j$ term if $19 \le i, j \le 27$. The size of the matrix 0 is $o_1 \times o_1$.

Let $L_4(x_0, \ldots, x_{27}) = (x_0, \ldots, x_{27}) \times A_4$. Then we know that the subspace $\bar{O}_1$ is invariant under the linear transformation $L_2^0 \circ L_4$

3.4 Step 4: The search for the subspace of the linear span of both (Ĩ) and (Ĩ̃)

In terms of the coordinate system $\tilde{X} = (x_{19}, \ldots, x_{27}, x_0, x_1, \ldots, x_{18})$, m_i will become a different matrix $\tilde{m}_i$. We observe that

$$\tilde{m}_i = \begin{pmatrix} 0 & 0 \\ 0 & U_i \end{pmatrix}, \tag{3.17}$$

for $i = 1, \ldots, 11$ and U_i is of the size $19 \times 19 = (n - o_1) \times (n - o_1)$. This is due to the fact that the polynomials in the Groups (I) and (II) contain no $x_i x_j$ for $i \in \{19, \ldots, 27\}$ and $j \in \{0, \ldots, 18\}$.

This implies that in the coordinate system defined by A_4, we can find a set of 19 linearly independent matrices $\hat{M}_j$ which are linear combinations of $\tilde{M}_i$ such that

$$\hat{M}_j = \sum_{i=1}^{19} \gamma_{ij} \tilde{M}_i = \begin{pmatrix} 0 & 0 \\ 0 & \hat{U}_j \end{pmatrix}. \tag{3.18}$$

This set of matrices can be found easily by solving a small set of linear equations.

From the formula (3.17) as for the case of (3.12), (3.13), we know that

$$\text{Span}\left\{\sum_{i=1}^{19}\gamma_{ij}F_i \mid , i=1,\ldots,11\right\} = \text{Span}\{\tilde{F}_i \mid i=1,\ldots,11\} \tag{3.19}$$

We will denote this space $\tilde{G}_{12}$.

3.5 Step 5: The search for the subspace of the linear span of the elements in Group ($\tilde{\text{I}}$)

Let us denote this space of the linear span of the elements in Group ($\tilde{\text{I}}$) by $\tilde{G}_1$.

We know that

(1) $\tilde{G}_1$ is a subspace of $\tilde{G}_{12}$, whose dimension is $dim(\tilde{G}_{12})-2$;
(2) if we take any polynomial in $\tilde{G}_{12}$ not in $\tilde{G}_1$ it has the property that the quadratic form corresponding to the quadratic part of this polynomial is of rank 18 (bigger than 14). On the other hand for any elements inside $\tilde{G}_1$ the corresponding rank is exactly 14.

This means that we can find a basis of $\tilde{G}_1$ by choosing three polynomials q_1, q_2 and q_3 from any basis of $\tilde{G}_{12}$ and search for all $q_1+u_1q_2+u_2q_3$ whose corresponding quadratic form is of rank 14, where $u_1,u_2 \in k$. This will definitely produce one element in $\tilde{G}_1$ because a dimension 3 subspace must non-trivially intersect a dimension 9 subspace in a space of total dimension 11. Using this procedure on the corresponding matrices of the bilinear form for the polynomials by looking for matrix of rank 14, we can find a basis of $\tilde{G}_1$ by at most searching 10 times. The complexity of this step is less than $(2^8)^2\times 18^3\times 10/6 < 2^{30}$.

3.6 Step 6: Reformulation of $\tilde{G}_1$

Let $G_{12} = \text{Span}\{f_i \mid i=1,\ldots,11\}$ and $G_1 = \text{Span}\{f_i \mid i=1,\ldots,9\}$. Let N_i denote the null space for each bilinear form $\langle , \rangle_i$. Then we observe and prove by calculation that

$$\bar{N} = \bigcap_{i=1,\ldots,9} N_i = \text{Span}(E_0, E_{17}, E_{18}, E_{19}, \ldots, E_{27}).$$

This implies that we could find a basis of the space, which consists of a basis of the subspace of the intersection of all the null spaces of the bilinear forms defined by the quadratic parts of the polynomials in $\tilde{G}_1$. This gives us a matrix A_5 such that

$$A_5 B A_5^t = \begin{pmatrix} 0 & \tilde{b}_i \\ \tilde{b}_i^t & \tilde{d}_i \end{pmatrix},$$

where B is any symmetric matrix of the bilinear form corresponding to the quadratic part of any polynomial in $\tilde{G}_1$.

This implies that we can define a linear transformation L_5 as

$$L_5(x_0,\ldots,x_{27}) = (x_0,\ldots,x_{27})\times A_5,$$

for any $\tilde{F}_i$ in $\tilde{G}_1$, and we have

$$\tilde{F}_i \circ L_5(x_0,\ldots,x_{27}) = \sum_{i\geq j=1}^{16}\tilde{\alpha}_{i,j}x_ix_j + \sum_{i=1}^{16}\tilde{\alpha}_i x_i + \tilde{\alpha}.$$

Therefore, by composing with L_5, all the polynomials in $\tilde{G}_1$ become a set of polynomials with only 16 variables. We will call this new set of polynomials $\tilde{GL}_1$.

From the above procedure and by solving a set of linear equations, we find an affine linear transformation L_6 on k^{16} such that the space $\tilde{GL}_1$ is derived from composition of the elements in G_1 from the right by L_6.

Now we treat all elements in G_1 and $\tilde{GL}_1$ as a polynomial of only 16 variables and ignore the other variables.

Again we associate the quadratic part of each G_1 with a bilinear form and we can see that all those forms are exactly of rank 14. Let us pick randomly nine linearly independent polynomials $\hat{F}_i$ from $\tilde{GL}_1$ Let $\langle , \rangle_i^s$ denote the bilinear form corresponding to the quadratic part of $\hat{F}_i$ over k^{16}. Let $N^s{}_i$ denote the null space for each bilinear form $\langle , \rangle_i^s$.

Through observation and computation simulations, we find

$$\text{Span}\big(N_i^s, i=1,\ldots,9\big) = \text{Span}\big(E_i^s, i=8,\ldots,16\big).$$

Using the same argument from Remark 1, we can find the image of the space spanned by the the image of $L_{6,i}(x_1,\ldots,x_{16}), i=1,2,3,4,5,6,7$, where

$$L_6(x_1,\ldots,x_{16}) = (L_{6,1}(x_1,\ldots,x_{16}),\ldots,L_{6,16}(x_1,\ldots,x_{16})).$$

So we find the image of the linear parts of the seven variables $\{x_1,\ldots,x_7\}$ composed by L_6.

Again following the same argument of Remark 1, by combining L_5 and L_6, for any basis of the space spanned by $L_{6,i}(x_1,\ldots,x_{16})$, $i=1,2,3,4,5,6,7$, if we compose each by L_5^{-1} from the right, they give us a basis of the image space of the span of the linear parts of seven variables $\{x_1,\ldots,x_7\}$ composed by L_2. We will denote a basis we find for this space by $k_i(x_0,\ldots,x_{27}), i=1,\ldots,7$.

3.7 Step 7: Completing the attack

Assume we have a message P to be signed. We first randomly choose r_i and solve the equation $k_1(x_0,\ldots,x_{27})=r_i$ by Gaussian elimination and substitute the final results into the polynomial equations coming form a basis of $\tilde{G}_1$ found

in Step 5. From the point of algebraic geometry, this is equivalent to giving specific values to $x_1, \ldots, x_7$ for f_i. This should produce nine linearly independent equations, which we again solve by Gaussian elimination. This is equivalent to finishing the polynomials from Group (I).

Then again we substitute it into the remaining two polynomial equations from $\tilde{G}_{12}$, whose linear combination would produce one linear equation, and then we substitute again, the remaining equations should produce another linear equation. This finishes the polynomials from Group (II).

When we substitute again, we will only have nine nonlinear equations left from (2.1). They are all coming from linear combinations of polynomials from Group (III), but with all $x_1, \ldots, x_{18}$ replaced by given values and the variables $x_0, x_{19}, \ldots, x_{27}$ have undergone an invertible affine linear transformation.

Let us choose a random set of values v_i and choose $x_1 = v_1, \ldots, x_{18} = v_{18}$ and let

$$f^e{}_i(x_0, x_{19}, \ldots, x_{27}) = f_i(x_0, v_1, \ldots, v_{18}, x_{19}, \ldots, x_{27}),$$

for $i = 12, \ldots, 20$. Let

$$f^e(x_0, x_{19}, \ldots, x_{27}) = (f^e_{12}(x_0, x_{19}, \ldots, x_{27}), \ldots, f^e_{20}(x_0, x_{19}, \ldots, x_{27})).$$

Let

$$F^e(x_0, x_{19}, \ldots, x_{27}) = L^e_1 \circ f^e \circ L^e_2(x_0, x_{19}, \ldots, x_{27}),$$

where L^e_1 and L^e_2 are invertible affine linear transformations. Our problem now is actually to solve a set of equations in the form: $F^e(x_0, x_{19}, \ldots, x_{27}) = P_e$, where P_e belongs to k^9.

To do so, the only thing we need to know is how to find the image of the linear part of x_0 under the composition from the right by L^e_2, which is a linear combination of other variables. The observation is that all quadratic parts of the f^e_i is in the form $x_0 \times x_j$ with no other quadratic terms, and the corresponding quadratic form has rank 2.

Let f^e_a and f^e_b be two linearly independent elements in the space spanned by f^e_i.

Let N^e_a and N^e_b denote the null space for each bilinear form derived from the quadratic part of f^e_a and f^e_b

Through computer simulations and direct proof, we have

$$\mathrm{Span}\big(N^e_a, N^e_b\big) = \mathrm{Span}\big(E^e_i, i = 1, \ldots, 9\big),$$

where $E^e_i = (0, 0, \ldots, 1, \ldots, 0)$ is the standard basis in k^{10}.

Using the same argument from Remark 1, this implies we could find the image of the space spanned by $L^e_2(x_0, \ldots, x_{27})$, where

$$L^e_2(x_0, x_{19}, \ldots, x_{27}) = \big(L^e_{2,0}(x_0, x_{19}, \ldots, x_{27}), \ldots, L^e_{2,9}(x_0, x_{19}, \ldots, x_{27})\big).$$

This is done by finding the corresponding dimension two space of the invariant variables for both f^e_a and f^e_b as described in Remark 1. The intersection of the two spaces has exactly dimension one and it is proportional to the linear part of $L^e_{2,0}(x_0, \ldots, x_{27})$.

Then we choose a random value for $L^e_{2,0}(x_0, \ldots, x_{27})$ and we substitute it into the nonlinear equations, which is equivalent to the case of giving x_0 a specific value in addition to $x_1, \ldots, x_{27}$ to all the f_i. This will produce again 9 linear independent equations. Then we collect all the linear independent equations whose solution will give a forgery of a signature.

For each of the seven steps we gave the computational complexity, except for those steps, where only simple systems of linear equations have to be solved, which can be done easily. The complexity of our procedure is mainly determined by Step 2. All other steps have a much lower complexity, and we conclude therefore, that the complexity of the entire attack is less than 2^{50}.

4 Conclusion

We combined a few different methods to break the TTS scheme of [24]. One can see that we go through a very complicated procedure, but computationally it is not difficult. The reason for this is that this new family of schemes uses specialized sparse polynomials. This introduced a chain of weaknesses. Each weakness can then be attacked with a different tool.

We believe that our attack can be made to work against all other TTS schemes, which were published in the February 2004 version of [23]. Of course, one can immediately suggest new formulas, as was done in the revised version of [23], which our method as given cannot defeat. But we think, one must be extremely careful when using specific sparse polynomials.

Appendix

The map f in terms of the formula on page 373 in [24] uses randomly chosen none zero elements $p_{i,j}$ from the field k and is given as:

$$\begin{aligned}
f(x_0, \ldots, x_{27}) &= (f_1(x_0, \ldots, x_{27}), \ldots, f_{20}(x_0, \ldots, x_{27})),\\
f_1 &= x_8 + x_1x_8p_{8,1} + x_2x_9p_{8,2} + x_3x_{10}p_{8,3}\\
&\quad + x_4x_{11}p_{8,4} + x_5x_{12}p_{8,5} + x_6x_{13}p_{8,6} + x_7x_{14}p_{8,7},\\
f_2 &= x_9 + x_1x_9p_{9,1} + x_2x_{10}p_{9,2} + x_3x_{11}p_{9,3}\\
&\quad + x_4x_{12}p_{9,4} + x_5x_{13}p_{9,5} + x_6x_{14}p_{9,6} + x_7x_{15}p_{9,7},\\
f_3 &= x_{10} + x_1x_{10}p_{10,1} + x_2x_{11}p_{10,2} + x_3x_{12}p_{10,3}\\
&\quad + x_4x_{13}p_{10,4} + x_5x_{14}p_{10,5} + x_6x_{15}p_{10,6}\\
&\quad + x_7x_{16}p_{10,7},\\
f_4 &= x_{11} + x_1x_{11}p_{11,1} + x_2x_{12}p_{11,2} + x_3x_{13}p_{11,3}\\
&\quad + x_4x_{14}p_{11,4} + x_5x_{15}p_{11,5} + x_6x_{16}p_{11,6}\\
&\quad + x_7x_8p_{11,7},\\
f_5 &= x_{12} + x_1x_{12}p_{12,1} + x_2x_{13}p_{12,2} + x_3x_{14}p_{12,3}\\
&\quad + x_4x_{15}p_{12,4} + x_5x_{16}p_{12,5}\\
&\quad + x_6x_8p_{12,6} + x_7x_9p_{12,7},
\end{aligned}$$

$$
\begin{aligned}
f_6 &= x_{13} + x_1x_{13}p_{13,1} + x_2x_{14}p_{13,2} + x_3x_{15}p_{13,3} \\
&\quad + x_4x_{16}p_{13,4} + x_5x_8p_{13,5} \\
&\quad + x_6x_9p_{13,6} + x_7x_{10}p_{13,7}, \\
f_7 &= x_{14} + x_1x_{14}p_{14,1} + x_2x_{15}p_{14,2} + x_3x_{16}p_{14,3} \\
&\quad + x_4x_8p_{14,4} + x_5x_9p_{14,5} \\
&\quad + x_6x_{10}p_{14,6} + x_7x_{11}p_{14,7}, \\
f_8 &= x_{15} + x_1x_{15}p_{15,1} + x_2x_{16}p_{15,2} + x_3x_8p_{15,3} \\
&\quad + x_4x_9p_{15,4} + x_5x_{10}p_{15,5} \\
&\quad + x_6x_{11}p_{15,6} + x_7x_{12}p_{15,7}, \\
f_9 &= x_{16} + x_1x_{16}p_{16,1} + x_2x_8p_{16,2} + x_3x_9p_{16,3} \\
&\quad + x_4x_{10}p_{16,4} + x_5x_{11}p_{16,5} \\
&\quad + x_6x_{12}p_{16,6} + x_7x_{13}p_{16,7}, \\
f_{10} &= x_{17} + x_1x_6p_{17,1} + x_2x_5p_{17,2} + x_3x_4p_{17,3} \\
&\quad + x_9x_{16}p_{17,4} + \\
&\quad x_{10}x_{15}p_{17,5} + x_{11}x_{14}p_{17,6} + x_{12}x_{13}p_{17,7}, \\
f_{11} &= x_{18} + x_2x_7p_{18,1} + x_3x_6p_{18,2} + x_4x_5p_{18,3} \\
&\quad + x_{10}x_{17}p_{18,4} + x_{11}x_{16}p_{18,5} \\
&\quad + x_{12}x_{15}p_{18,6} + x_{13}x_{14}p_{18,7}, \\
f_{12} &= x_{19} + x_8x_{10}p_{19,0} + x_0x_{19}p_{19,1} + x_{18}x_{20}p_{19,2} \\
&\quad + x_{17}x_{21}p_{19,3} + x_{16}x_{22}p_{19,4} \\
&\quad + x_{15}x_{23}p_{19,5} + x_{14}x_{24}p_{19,6} + x_{13}x_{25}p_{19,7} \\
&\quad + x_{12}x_{26}p_{19,8} + x_{11}x_{27}p_{19,9}, \\
f_{13} &= x_{20} + x_9x_{11}p_{20,0} + x_2x_{19}p_{20,1} + x_0x_{20}p_{20,2} \\
&\quad + x_{18}x_{21}p_{20,3} + x_{17}x_{22}p_{20,4} \\
&\quad + x_{16}x_{23}p_{20,5} + x_{15}x_{24}p_{20,6} + x_{14}x_{25}p_{20,7} \\
&\quad + x_{13}x_{26}p_{20,8} + x_{12}x_{27}p_{20,9}, \\
f_{14} &= x_{21} + x_{10}x_{12}p_{21,0} + x_4x_{19}p_{21,1} + x_2x_{20}p_{21,2} \\
&\quad + x_0x_{21}p_{21,3} + x_{18}x_{22}p_{21,4} + x_{17}x_{23}p_{21,5} \\
&\quad + x_{16}x_{24}p_{21,6} + x_{15}x_{25}p_{21,7} + x_{14}x_{26}p_{21,8} \\
&\quad + x_{13}x_{27}p_{21,9}, \\
f_{15} &= x_{22} + x_{11}x_{13}p_{22,0} + x_6x_{19}p_{22,1} + x_4x_{20}p_{22,2} \\
&\quad + x_2x_{21}p_{22,3} + x_0x_{22}p_{22,4} + x_{18}x_{23}p_{22,5} \\
&\quad + x_{17}x_{24}p_{22,6} + x_{16}x_{25}p_{22,7} + x_{15}x_{26}p_{22,8} \\
&\quad + x_{14}x_{27}p_{22,9}, \\
f_{16} &= x_{23} + x_{12}x_{14}p_{23,0} + x_8x_{19}p_{23,1} + x_6x_{20}p_{23,2} \\
&\quad + x_4x_{21}p_{23,3} + x_2x_{22}p_{23,4} + x_0x_{23}p_{23,5} \\
&\quad + x_{18}x_{24}p_{23,6} + x_{17}x_{25}p_{23,7} + x_{16}x_{26}p_{23,8} \\
&\quad + x_{15}x_{27}p_{23,9}, \\
f_{17} &= x_{24} + x_{13}x_{15}p_{24,0} + x_{10}x_{19}p_{24,1} + x_8x_{20}p_{24,2} \\
&\quad + x_6x_{21}p_{24,3} + x_4x_{22}p_{24,4} + x_2x_{23}p_{24,5} + x_0x_{24}p_{24,6} \\
&\quad + x_{18}x_{25}p_{24,7} + x_{17}x_{26}p_{24,8} + x_{16}x_{27}p_{24,9}, \\
f_{18} &= x_{25} + x_{14}x_{16}p_{25,0} + x_{12}x_{19}p_{25,1} + x_{10}x_{20}p_{25,2} \\
&\quad + x_8x_{21}p_{25,3} + x_6x_{22}p_{25,4} + x_4x_{23}p_{25,5} + x_2x_{24}p_{25,6} \\
&\quad + x_0x_{25}p_{25,7} + x_{18}x_{26}p_{25,8} + x_{17}x_{27}p_{25,9}, \\
f_{19} &= x_{26} + x_{15}x_{17}p_{26,0} + x_{14}x_{19}p_{26,1} + x_{12}x_{20}p_{26,2} \\
&\quad + x_{10}x_{21}p_{26,3} + x_8x_{22}p_{26,4} + x_6x_{23}p_{26,5} + x_4x_{24}p_{26,6} \\
&\quad + x_2x_{25}p_{26,7} + x_0x_{26}p_{26,8} + x_{18}x_{27}p_{26,9}, \\
f_{20} &= x_{27} + x_{16}x_{18}p_{27,0} + x_{16}x_{19}p_{27,1} + x_{14}x_{20}p_{27,2} \\
&\quad + x_{12}x_{21}p_{27,3} + x_{10}x_{22}p_{27,4} + x_8x_{23}p_{27,5} + x_6x_{24}p_{27,6} \\
&\quad + x_4x_{25}p_{27,7} + x_2x_{26}p_{27,8} + x_0x_{27}p_{27,9},
\end{aligned}
$$

References

1. Chen, J., Moh, T.: On the Goubin-Courtois attack on TTM. Cryptol. ePrint Arch. **72** (2001). http://eprint.iacr.org/2001/072
2. Chen, J., Yang, B., Peng, B.: Tame transformation signatures with topsy-yurvy hashes. In: IWAP'02, pp. 1–8 (2002). http://dsns.csie.nctu.edu.tw/iwap/proceedings/proceedings/sessionD/7.pdf
3. Chou, G., Guan, J., Chen, J.: A systematic construction of a q_{2^k}-model in TTM. Comm. Algebra **30**, 551–562 (2002)
4. Coppersmith, D., Stern, J., Vaudenay, S.: The security of the birational permutation signature schemes. J. Cryptol. **10**(3), 207–221 (1997)
5. Courtois, N., Goubin, L., Patarin, J.: Sflash^{v3}, a fast asymmetric signature scheme (2003). http://eprint.iacr.org/2003/211
6. Ding, J.: A new variant of the Matsumoto-Imai cryptosystem through perturbation. In: Bao, F., Deng, R., Zhou, J. (eds.) Public Key Cryptosystems, PKC 2004, vol. 2947, pp. 305–318. LNCS. Springer, Berlin Heidelberg New York (2004)
7. Ding, J., Hodges, T.: Cryptanalysis of an implementation scheme of TTM. J. Algebra Appl. **3**, 273–282 (2004). http://eprint.iacr.org/2003/084
8. Ding, J., Schmidt, D.: A common defect of the TTM cryptosystem. In: Proceedings of the Technical Track of the ACNS'03, pp. 68–78. ICISA Press (2003). http://eprint.iacr.org/2003/085
9. Ding, J., Schmidt, D.S.: The new TTM implementation is not secure. In: Niederreiter, H., Feng, K.Q., Xing, C.P. (eds.) Proceedings of International Workshop on Coding, Cryptography and Combinatorics (CCC 2003), pp. 106–121 (2003)
10. Garey, M.R., Johnson, D.S.: Computers and Intractability, A Guide to the Theory of NP-Completeness. W.H. Freeman (1979)
11. Goubin, L., Courtois, N.: Cryptanalysis of the TTM cryptosystem. In: Okamoto, T. (ed.) Advances in Cryptology – ASIACRYPT 2000, International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 3–7, 2000, vol. 1976 of LNCS, pp. 44–57. Springer, Berlin Heidelberg New York (2000)
12. Kipnis, A., Patarin, J., Goubin, L.: Unbalanced oil and vinegar signature schemes. In: Stern, J. (ed.) EUROCRYPT '99: International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2–6, 1999, vol. 1592 of LNCS, pp. 206–222. Springer, Berlin Heidelberg New York (1999)
13. Kipnis, A., Shamir, A.: Cryptanalysis of the oil & vinegar signature scheme. In: Krawczyk, H. (ed.) Advances in Cryptology – CRYPTO'98: 18th Annual International Cryptology Conference, Santa Barbara, California, USA, August 1998, vol. 1462 of LNCS, pp. 257–267. Springer, Berlin Heidelberg New York (1998)
14. Matsumoto, T., Imai, H.: Public quadratic polynomial-tuples for efficient signature verification and message encryption. In: Guenther, C.G. (ed.) Advances in Cryptology – EUROCRYPT '88, vol. 330 of LNCS, pp. 419–453. Springer, Berlin Heidelberg New York (1988)
15. Moh, T.T.: A fast public key system with signature and master key functions. Commun. Algebra **27**, 2207–2222 (1999). http://www.usdsi.com/ttm.html
16. Patarin, J.: Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88. In: Coppersmith, D. (ed.) Advances in Cryptology – Crypto '95, vol. 963 of LNCS, pp. 248–261 (1995)
17. Patarin, J.: Hidden Field Equations (HFE) and Isomorphism of Polynomials (IP): two new families of asymmetric algorithms. In: Maurer, U. (ed.) Eurocrypt'96, vol. 1070 of LNCS, pp. 33–48. Springer, Berlin Heidelberg New York (1996). Extended Version: http://www.minrank.org/hfe.pdf

18. Patarin, J., Courtois, N., Goubin, L.: Flash, a fast multivariate signature algorithm. In: Naccache, C. (ed.) Progress in Cryptology, CT-RSA, vol. 2020 of LNCS, pp. 298–307. Springer, Berlin Heidelberg New York (2001)
19. Patarin, J., Courtois, N., Goubin, L.: QUARTZ, 128-bit long digital signatures http://www.minrank.org/quartz/. In: Naccache, C. (ed.) Progress in Cryptology, CT-RSA, vol. 2020 of LNCS, pp. 282–297. Springer, Berlin Heidelberg New York (2001)
20. Shamir, A.: Efficient signature schemes based on birational permutations. In: Stinson, D.R. (ed.) Advances in Cryptology – CRYPTO '93 (Santa Barbara, CA, 1993), vol. 1462 of LNCS, pp. 257–266. Springer, Berlin Heidelberg New York (1993)
21. Wolf, C., Preneel, B.: Large superfluous keys in multivariate quadratic asymmetric systems. In: Vaudenay, S. (ed.) Public Key Cryptography – PKC 2005: 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets, Switzerland, January 23–26, 2005, vol. 3386 of LNCS, pp. 275–287. Springer, Berlin Heidelberg New York (2005)
22. Yang, B., Chen, J.: A more secure and efficacious TTS signature scheme. ICISC 2003 (2003). http://eprint.iacr.org/2003/160
23. Yang, B., Chen, J.: TTS: Rank attacks in tame-like multivariate PKCs. http://eprint.iacr.org/2004/061 (February 2004)
24. Yang, B., Chen, J., Chen, Y.: TTS: High-speed signatures on a low-cost smart card. In: Joye, M., Quisquater, J. (eds.) Cryptographic Hardware and Embedded Systems: CHES 2004, vol. 3156 of LNCS, pp. 371–385. Springer, Berlin Heidelberg New York (2004)