Cryptanalysis of Yasuda, Takagi and Sakurai's Signature Scheme Using Invariant Subspaces

Wenbin Zhang and Chik How Tan

Temasek Laboratories
National University of Singapore
tslzw@nus.edu.sg and tsltch@nus.edu.sg

Abstract. In PQCrypto 2013 Yasuda, Takagi and Sakurai proposed an interesting signature scheme of efficiency $O(n^2)$ with parameter $(q = 6781, n = 121)$ claimed to have 140-bit security level. Later on almost at the same time two independent and different attacks were then proposed by Y. Hashimoto in PQCrypto 2014 and by the authors in ICISC 2014. Hashimoto's attack has complexity $O(n^4)$ and breaks $(q = 6781, n = 121)$ in several minutes. In this paper, we make an essential extension of our work in ICISC 2014. We develop for the our previous method a thorough and rigorous mathematical theory by applying intensively the theory of invariant subspaces, then work out a much better attack with complexity $O(n^4)$, and especially implement it successfully. Our new attack efficiently recovers equivalent private keys of many randomly generated instances, especially breaking $(q = 6781, n = 121)$ in only about 14.77 seconds, much faster than Y. Hashimoto's attack. The approach developed here might have further applications.

Keywords: post-quantum cryptography, multivariate public key cryptosystem, invariant subspace

1 Introduction

The threat of quantum computers has forced great efforts to search for new cryptosystems that could survive in the future quantum era. One of those candidates is multivariate public key cryptography (MPKC) whose public key is represented by multivariate polynomial maps. Current standard construction for the public key of MPKC is to compose a polynomial map $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$ at the two ends with two invertible affine maps $L : \mathbb{F}_q^n \to \mathbb{F}_q^n$ and $R : \mathbb{F}_q^m \to \mathbb{F}_q^m$, i.e., $\bar{F} = L \circ F \circ R : \mathbb{F}_q^n \to \mathbb{F}_q^m$. The theoretical foundation of the security of MPKC is the well known fact that solving a system of general polynomial equations (even with degree two only) over finite fields is NP-hard. A specific multivariate cryptosystem may also have certain weaknesses on its structure so that it could be attacked using special methods. Since 1980' the development of MPKC has been active and fast, and various interesting schemes as well as attacking methods have been developed. Overview of this area may be found in [WP05b, DGS06, DY09].

Recently a new interesting multivariate signature scheme was proposed by Yasuda, Takagi and Sakurai in PQCrypto 2013 [YTS13]. Their scheme has a special structure different from all previous schemes. They construct the public key from the classification of quadratic forms over finite fields of odd characteristic which claims that there are only two equivalence classes of quadratic forms

$$f : \mathbb{F}_q^r \to \mathbb{F}_q, \quad f(x_1, \ldots, x_r) = \sum_{1 \le i \le j \le r} a_{ij} x_i x_j,$$

cf. Theorem 3.8 of Chapter 2 of [Sch85]. Correspondingly their public key consists of two polynomial maps

$$F_1, F_2 : \mathbb{F}_q^n \to \mathbb{F}_q^m, \quad n = r^2, m = r(r+1)/2,$$

rather than one as other schemes. A great advantage of their scheme is on the efficiency of generating a signature which was claimed to be eight to nine times faster than Rainbow signature scheme [DS05] under certain parameters. On the security side, they claim that the best attack (at the time of PQCrypto 2013) is the MinRank attack with complexity $O(q^r) = O(q^{\sqrt{n}})$. In addition, two sets of parameters, $(q = 2053, n = 64)$ and $(q = 6781, n = 121)$ are proposed and claimed to be of at least 88-bit and 140-bit security respectively against MinRank attack. However a disadvantage of their scheme is that the public key size may be big; for instance, the above two sets of parameters have public key size 224.6kB and 1,583.2kB respectively.

However, the specific structure of Yasuda, Takagi and Sakurai's (YTS' for short) scheme is soon found to have strong weaknesses. Later on two independent and different attacks are then proposed to break YTS' scheme by Y. Hashimoto in PQCrypto 2014 [Has14] and by the authors in ICISC 2014 [ZT15]. The two attacks both explore weaknesses of the specific structure of YTS' scheme but in different ways. In [Has14], the public key of YTS' scheme is first expressed in terms of certain extension of matrices and then a complicated algebraic approach is worked out to recover the private key, which is somehow similar to the diagonalization process of a matrix. His attack is claimed to have complexity $O(n^4)$ only and implemented to recover the private key of YTS' scheme with parameter $(q = 6781, n = 121)$ in several minutes with running time varies from 240 to 450 seconds.

In [ZT15], a simple matrix expression, different from Hashimoto's, of the public key is given by the authors in terms of the private key. Then motivated by Kipnis and Shamir's attack [KS98, KPG99, CHDY11] to the (unbalanced) oil-vinegar signature scheme [Pat97, KPG99], this expression is converted to another one which clearly exposes the hidden geometric structure of YTS' scheme. Consequently the problem of finding an equivalent private key [WP05a] of YTS' scheme becomes a geometric problem, i.e. decomposing the whole space into a direct sum of certain invariant subspaces and finding an appropriate basis for each of them. Two closely related algorithms are then sketched using the theory of invariant subspaces [Cla] to solve this geometric problem and compute an equivalent key. Complexity of the two algorithms is estimated to be bounded by $O(n^{\frac{11}{2}} q^d)$ where d is expected generally to be 1. Implementation result is not given in [ZT15] as it was still in progress when the paper was published.

This paper is an essential extension of the authors' work [ZT15] introduced above. It carries over most basic settings, the matrix expression of the public key and the key idea in [ZT15], but the core part of this paper is a significant improvement and enhancement of [ZT15] on three important aspects. Firstly a thorough and rigorous theory is developed to completely uncover the structures of YTS' scheme and then to recover the secret information from the public key. Secondly based on this theory, a better algorithm is proposed with lower complexity $O(n^4)$, same as Hashimoto's, which is only square of the efficiency of signature generation. Thirdly this new algorithm is implemented successfully and recovers equivalent keys for various parameter sets. Especially, it breaks the parameter set $(q = 6781, n = 121)$ mentioned above in only about 14.77 seconds with running time varies from 7.91 to 26.73 seconds which is much faster than Hashimoto's result. Therefore this paper contributes a powerful approach to efficiently break Yasuda, Takagi and Sakurai's scheme. This approach might also have applications to the cryptanalysis of some other cryptosystems.

This paper is organized as follows. Section 2 is a brief review of YTS' scheme mostly following the setting in [ZT15]. Section 3 is an overview of our attack and it includes the matrix expression of the public key and the key idea in [ZT15] as its first two subsections but its third subsection is new and is an essential enhancement. Section 4 is detailed analysis of the technical issues and is also essential enhancement of the technical analysis in [ZT15]. In Section 5 our new algorithm is proposed and its complexity is estimated. This section is significant improvement of the corresponding part of [ZT15]. Section 6 is the presentation and discussion of implementation result which is lacked in [ZT15]. Section 7 is a comparison with Hashimoto's work and extends the corresponding part in [ZT15]. Section 8 is the concluding section. In addition, a brief introduction of the theory of invariant subspaces is included in Appendix A for easy reference. Appendix B shows how to attack the affine parts if the central map is quadratic homogeneous which should be already known to many experts in MPKC.

2 Yasuda, Takagi and Sakurai's Signature Scheme

In this section, we shall review Yasuda, Takagi and Sakurai's signature scheme following their paper [YTS13] but in a clearer way.
Let q be a power of an *odd* prime p and δ a non-square element in $\mathbb{F}_q$. Moreover let $I_{n,\delta} = \begin{pmatrix} I_{n-1} & \\ & \delta \end{pmatrix}$, and I_{n-1} the $(n-1) \times (n-1)$ identity matrix. Then there is the following two possible decompositions of a symmetric matrix over $\mathbb{F}_q$, corresponding to the well known classification of quadratic forms over $\mathbb{F}_q$, cf. Theorem 3.8 in Chapter 2 of [Sch85].

Theorem 1. *For any $n \times n$ symmetric matrix A over $\mathbb{F}_q$, there exists an $n \times n$ matrix X over $\mathbb{F}_q$ satisfying either $A = X^T X$ or $A = X^T I_{n,\delta} X$.*

It is known how to compute such a matrix X in linear algebra and an algorithm is sketched in [YTS13]. This result can be applied to construct a signature scheme in the following way.
Let $n = r^2$ and $m = r(r+1)/2$. Choose two one-one correspondences

$$\phi_1 : \text{the set of } r \times r \text{ matrices over } \mathbb{F}_q \overset{1-1}{\longleftrightarrow} \mathbb{F}_q^n,$$

$$\phi_2 : \text{the set of } r \times r \text{ symmetric matrices over } \mathbb{F}_q \overset{1-1}{\longleftrightarrow} \mathbb{F}_q^m.$$

Then a vector $x \in \mathbb{F}_q^n$ corresponds to the $r \times r$ matrix $X = \phi_1^{-1}(x)$, and $X^T X$ is a symmetric matrix corresponding to the vector $\phi_2(X^T X) \in \mathbb{F}_q^m$. Roughly speaking, $\phi_2(X^T X)$ is formed by the entries of the upper triangular part of $X^T X$ according to the specified order ϕ_2. Define two maps

$$F, F_\delta : \mathbb{F}_q^n \to \mathbb{F}_q^m, \quad F(x) = \phi_2(X^T X), \quad F_\delta(x) = \phi_2(X^T I_{r,\delta} X).$$

Then F, F_δ are two multivariate quadratic polynomial maps. Neither F nor F_δ is surjective but the union of their images can cover $\mathbb{F}_q^m$. The pair (F, F_δ) can serve as the central map of a multivariate signature scheme.
Let $R_1, R_2 : \mathbb{F}_q^n \to \mathbb{F}_q^n$ and $L : \mathbb{F}_q^m \to \mathbb{F}_q^m$ be three randomly chosen invertible affine transformations and

$$\bar{F} = L \circ F \circ R_1, \quad \bar{F_\delta} = L \circ F_\delta \circ R_2.$$

Yasuda, Takagi and Sakurai's (YTS' for short) scheme can be described as follows.

Public Key $\bar{F}$, $\bar{F}_\delta$.

Private Key R_1, R_2, L.

Signature Generation For a message $y \in \mathbb{F}_q^m$, first compute $y' = L^{-1}(y)$ and the corresponding symmetric matrix $Y = \phi_2^{-1}(y')$, then compute an $r \times r$ matrix X such that $Y = X^T X$ or $Y = X^T I_{r,\delta} X$, and the corresponding vector $x' = \phi_1(X)$, finally compute $x = R_1^{-1}(x')$ or $x = R_2^{-1}(x')$ correspondingly.

Verification A signature x is accepted if $\bar{F}(x) = y$ or $\bar{F}_\delta(x) = y$, otherwise rejected.

We remark that the chosen non-square element δ is unnecessary to keep secret as any non-square element can also work. In addition, we list some features of YTS' scheme in the following assuming that R_1, R_2, L are all linear.

Public Key Size By representing the quadratic parts of $\bar{F}$, $\bar{F}_\delta$ in terms of symmetric matrices, there are $\frac{1}{2}r^3(r+1)(r^2+1)$ elements of $\mathbb{F}_q$ in total. Noting that each $\mathbb{F}_q$ element has $\frac{1}{8}(\log_p q)\lceil \log_2 p \rceil$ Bytes, thus the public key size may be calculated as $\frac{1}{16}r^3(r+1)(r^2+1)(\log_p q)\lceil \log_2 p \rceil$ Bytes.

Efficiency of Signature Generation Generation of a signature needs $O(r^4) = O(n^2)$ $\mathbb{F}_q$ multiplications [YTS13].

Security The security level against Min-Rank attack is at least $O(q^r) = O(q^{\sqrt{n}})$ [YTS13] or more accurately $O(n^3 q^{\sqrt{n}})$ [Has14] for recovering L.

3 Attacking YTS' Scheme Using Invariant Subspaces

In this section we shall first give a simple and elegant matrix expression for YTS' public map in terms of the private key. This expression is important for our attack as it leads to a geometric interpretation by invariant subspaces. The starting point of our attack is motivated by Kipnis and Shamir's idea of attacking the oil-vinegar signature scheme [KS98]. Namely we shall apply their trick

$$A_k = R^T(\cdots)R \Longrightarrow A_l^{-1}A_k = R^{-1}(\cdots)R \Longrightarrow (A_l^{-1}A_k)R^{-1} = R^{-1}(\cdots)$$

to convert our matrix expression into another form. We find that this new form has clear geometric meaning in terms of invariant subspaces and converts the problem of finding a correct key into a geometric problem of finding certain invariant subspaces. We then propose a method to solve this resulted geometric problem by applying the theory of invariant subspaces, and thus break YTS' signature scheme.

To help understanding, we explain here why it is helpful in principle to use invariant subspaces. Invariant subspaces have nice structures and may be computed easily by the well studied theory of invariant subspaces. For example,

1. An invariant subspace which is invariant under a few linear maps $F_1, \ldots, F_k$ may be generated by very few or even only one vector and may be computed easily by computing the linear subspace spanned by some vectors of these forms $F_i(\mathbf{v})$, $F_i(F_j(\mathbf{v}))$, etc.
2. Some typical invariant subspaces of a linear map can be computed from its characteristic polynomials.

In other words, if the problem to be solved involves some invariant subspaces, then there may be practical methods to compute them and thus help solve the problem. For easy reference, we include an appendix, see Appendix A, briefly introducing the theory of invariant subspaces, referring to [Cla] for a more complete theory.

Recall that $n = r^2$, $m = r(r+1)/2$.

3.1 Our Expression of YTS' Public Map

We consider only the first map of the public key

$$\bar{F} = L \circ F \circ R.$$

Here we simply assume that both L, R are linear in the following as their affine parts can be recovered or illuminated easily, cf. Appendix B. Write $\bar{F} = (\bar{f}_1, \dots, \bar{f}_m)$. Since F is quadratic homogeneous and both L, R are assumed linear, $\bar{f}_k$ is quadratic homogeneous and can be written as

$$\bar{f}_k(x) = x^T A_k x, \quad x \in \mathbb{F}_q^n$$

where A_k is an $n \times n$ symmetric matrix publicly known.
We next compute these $\bar{f}_k$ in terms L, R. Choose for ϕ_1, ϕ_2 the following two one-one correspondences

$$x = \phi_1(X) = (x_{11}, \dots, x_{1r}, x_{21}, \dots, x_{2r}, \dots, x_{r1}, \dots, x_{rr}) \in \mathbb{F}_q^n, \qquad (1)$$

$$y = \phi_2(Y) = (y_{11}, y_{12}, y_{22}, \dots, y_{1r}, \dots, y_{rr}) \in \mathbb{F}_q^m, \qquad (2)$$

where $X = (x_{ij})_{r\times r}$ is an $r \times r$ matrix and $Y = (y_{ij})_{r\times r}$ an $r \times r$ symmetric matrix. Let $x' = Rx$ and $X' = (x'_{ij})_{r\times r} = \phi_1^{-1}(x')$. Then

$$\phi_2^{-1}(F(x')) = X'^T X' = (f_{ij})_{r\times r}$$

$$= \begin{pmatrix} x'^2_{11} + \cdots + x'^2_{r1} & x'_{11}x'_{12} + \cdots + x'_{r1}x'_{r2} & \dots & x'_{11}x'_{1r} + \cdots + x'_{r1}x'_{rr} \\ x'_{11}x'_{12} + \cdots + x'_{r1}x'_{r2} & x'^2_{12} + \cdots + x'^2_{r2} & \dots & x'_{12}x'_{1r} + \cdots + x'_{r2}x'_{rr} \\ \vdots & \vdots & \ddots & \vdots \\ x'_{11}x'_{1r} + \cdots + x'_{r1}x'_{rr} & x'_{12}x'_{1r} + \cdots + x'_{r2}x'_{rr} & \dots & x'^2_{1r} + \cdots + x'^2_{rr} \end{pmatrix}$$

where $f_{ij} = x'_{1i}x'_{1j} + \cdots + x'_{ri}x'_{rj}$, and thus

$$F(x') = (f_{11}, f_{12}, f_{22}, \dots, f_{1r}, \dots, f_{rr}).$$

Accordingly write the $m \times m$ matrix L in the following form

$$\begin{pmatrix} l_{1;1,1} & l_{1;1,2} & l_{1;2,2} & \dots & l_{1;1,r} & \dots & l_{1;r,r} \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ l_{m;1,1} & l_{m;1,2} & l_{m;2,2} & \dots & l_{m;1,r} & \dots & l_{m;r,r} \end{pmatrix}.$$

For each $1 \le k \le m$, the kth component of $L \circ F$ is

$$(L \circ F)_k(x') = \sum_{1 \le i \le j \le r} l_{k;i,j} f_{ij} = \sum_{1 \le s \le r} \sum_{1 \le i \le j \le r} l_{k;i,j} x'_{si} x'_{sj}$$

which can be written in the following matrix form

$$(L \circ F)_k(x') = x'^T \begin{pmatrix} L_k & & \\ & \ddots & \\ & & L_k \end{pmatrix} x'$$

with r L_k on the diagonal, where L_k is the following symmetric matrix corresponding to the kth row of L,

$$L_k = \begin{pmatrix} l_{k;1,1} & \frac{1}{2} l_{k;1,2} & \cdots & \frac{1}{2} l_{k;1,r} \\ \frac{1}{2} l_{k;1,2} & l_{k;2,2} & \cdots & \frac{1}{2} l_{k;2,r} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{2} l_{k;1,r} & \frac{1}{2} l_{k;2,r} & \cdots & l_{k;r,r} \end{pmatrix}.$$

Substitute $x' = Rx$, then we have the following simple matrix representation for the public map

$$\bar{f}_k(x) = (L \circ F \circ R)_k(x) = x^T R^T \begin{pmatrix} L_k & & \\ & \ddots & \\ & & L_k \end{pmatrix} Rx.$$

In particular, the representing matrix A_k of $\bar{f}_k(x) = x^T A_k x$ has the following simple expression

$$A_k = R^T \begin{pmatrix} L_k & & \\ & \ddots & \\ & & L_k \end{pmatrix} R, \quad \text{for } 1 \leq k \leq m. \tag{3}$$

For convenience, write $A \oplus B = \begin{pmatrix} A & \\ & B \end{pmatrix}$ and $A^{\oplus r} = \overbrace{A \oplus \cdots \oplus A}^{r}$, for matrices A, B. We thus rewrite equation (3) as

$$A_k = R^T L_k^{\oplus r} R.$$

If an invertible $m \times m$ matrix L and an invertible $n \times n$ matrix R together satisfy equation (3), then they give the public map $\bar{F}$ and thus the pair (L, R) is a correct key, i.e., equivalent to the original private key which is kept secret.

3.2 Geometric Interpretation by Invariant Subspaces

Here we show how our expression (3) for the public map leads to a geometric interpretation by invariant subspaces which uncovers the underlying geometric structure of YTS' scheme.
First of all we need to consider the invertibility of A_k and L_k. Among all L_k, $1 \leq k \leq m$, the probability that at least one of them is invertible, is obviously higher than the probability of a random symmetric matrix being invertible. The latter probability is known to be almost one [Car54, Mac69] so that the probability that no L_k is invertible is negligible. In addition, A_k and L_k obviously share the same invertibility by equation 3. We hence make the following assumption from now on.

Assumption 1 *There is an l such that A_l is invertible.*

Remark 1. It should be noted that this assumption is not compulsory. Even if all A_k (L_k), $1 \leq k \leq m$, are singular, there is always a nonsingular linear combination of A_k (L_k) due to the following reason. Since L is invertible, its m rows are linearly independent, so are the corresponding L_k, $1 \leq k \leq m$. Notice that each L_k is an $r \times r$ symmetric matrix and $m = r(r+1)/2$. Thus L_k, $1 \leq k \leq m$, form a basis for the space of $r \times r$ symmetric matrices. Hence there is always a nonsingular linear combination of L_k, $1 \leq k \leq m$, and thus of A_k, $1 \leq k \leq m$. Therefore if all A_k are singular, we can just pick a nonsingular linear combination of them, and the attack in this paper still works.

By Assumption 1, we have inverses A_l^{-1}, L_l^{-1}. Then write $A_{lk} = A_l^{-1} A_k$ and $L_{lk} = L_l^{-1} L_k$. Then by equation (3),

$$A_{lk} = (R^{-1}(L_l^{-1})^{\oplus r} R^{-T})(R^T L_k^{\oplus r} R) = R^{-1}((L_l^{-1})^{\oplus r} L_k^{\oplus r}) R = R^{-1} L_{lk}^{\oplus r} R,$$

$$A_{lk}R^{-1} = R^{-1}L_{lk}^{\oplus r} = R^{-1}\begin{pmatrix} L_{lk} & & \\ & \ddots & \\ & & L_{lk} \end{pmatrix}.$$

We observe that this has the following geometric meaning in terms of invariant subspaces, referring to Appendix A for a brief introduction of the theory of invariant subspaces. For $1 \leq s \leq r$, let V_s denote the linear subspace of $\mathbb{F}_q^n$ spanned by $R_{r(s-1)+1}$, ..., R_{rs} where R_i the ith column vector of R^{-1}.

Theorem 2. *If (L, R) is a correct key, then V_s is an r-dim invariant subspace of A_{lk} for all $k \neq l$, and*

$$A_{lk}(R_{r(s-1)+1}, \ldots, R_{rs}) = (R_{r(s-1)+1}, \ldots, R_{rs})L_{lk}.$$

Moreover, $\mathbb{F}_q^n$ is a direct sum of these r invariant subspaces,

$$\mathbb{F}_q^n = V_1 \oplus \cdots \oplus V_r.$$

Proof. This follows obviously from $A_{lk}R^{-1} = R^{-1}L_{lk}^{\oplus r}$.

This observation suggests that, to find a correct key (L, R), we may decompose inductively $\mathbb{F}_q^n$ into a direct sum of r-dim invariant subspaces $\mathbb{F}_q^n = V_1 \oplus \cdots \oplus V_r$ such that each V_s is of dimension n and invariant under all A_{lk}, and compute a basis of V_s such that the representing matrix of A_{lk} to V_s is L_{lk} with respect to this basis. Then the matrix of these bases may give R^{-1}, and thus all L_k from $R^{-T}A_kR^{-1} = L_k^{\oplus r}$ by equation (3), hence R, L.

3.3 Strategy of Finding a Correct Key

We find, however, that Theorem 2 is not sufficient to guarantee a correct key; satisfaction of equation (3) indeed has more subtle restrictions to these invariant subspaces V_s as given below.

Proposition 1. *If (L, R) is a correct key, then the basis $(R_{r(s-1)+1}, \ldots, R_{rs})$ of V_s satisfies*

$$(R_{r(s-1)+1}, \ldots, R_{rs})^T A_k (R_{r(s-1)+1}, \ldots, R_{rs}) = L_k \tag{4}$$

for $1 \leq k \leq m$. In addition, if $s \neq s'$, V_s and $V_{s'}$ are orthogonal to each other with respect to A_k, i.e. $\mathbf{u}^T A_k \mathbf{v} = 0$ for $\mathbf{u} \in V_s$, $\mathbf{v} \in V_{s'}$ and $1 \leq k \leq m$.

Proof. By equation (3), we have $R^{-T}A_kR^{-1} = L_k^{\oplus r}$. Then the claim follows obviously.

These additional restrictions make the situation much complicated. Fortunately we find that it is unnecessary to consider so many restrictions but only a few of them will do.

Lemma 1. *(L, R) is a correct key, i.e., satisfying*

$$R^{-T}A_kR^{-1} = L_k^{\oplus r}, \quad \textit{for } 1 \leq k \leq m,$$

if and only if

$$A_{lk}R^{-1} = R^{-1}L_{lk}^{\oplus r} \quad \textit{for } k \neq l \quad \textit{and} \quad R^{-T}A_lR^{-1} = L_l^{\oplus r}.$$

Proof. The "only if" direction is already given above. For the "if" direction, $A_{lk}R^{-1} = R^{-1}L_{lk}^{\oplus r}$ implies $A_kR^{-1} = A_lR^{-1}L_{lk}^{\oplus r}$, thus

$$R^{-T}A_kR^{-1} = R^{-T}(A_lR^{-1}L_{lk}^{\oplus r}) = (R^{-T}A_lR^{-1})L_{lk}^{\oplus r} = L_l^{\oplus r}L_{lk}^{\oplus r} = L_k^{\oplus r}$$

since $R^{-T}A_lR^{-1} = L_l^{\oplus r}$.

Translating the above sufficient and necessary conditions into geometric language, we have:

Theorem 3. *(L, R) is a correct key if and only if the following three conditions are all satisfied:*

1. *Each V_s is an r-dim invariant subspace of A_{lk} with its basis satisfying*

$$A_{lk}(R_{r(s-1)+1}, \dots, R_{rs}) = (R_{r(s-1)+1}, \dots, R_{rs})L_{lk}, \quad \textit{for } k \neq l. \tag{5}$$

2. *If $s \neq s'$, V_s and $V_{s'}$ are orthogonal to each other with respect to A_l, i.e. $\mathbf{u}^TA_l\mathbf{v} = 0$ for $\mathbf{u} \in V_s$, $\mathbf{v} \in V_{s'}$.*
3. *The basis of V_s satisfies*

$$(R_{r(s-1)+1}, \dots, R_{rs})^TA_l(R_{r(s-1)+1}, \dots, R_{rs}) = L_l. \tag{6}$$

Proof. The claim is true because $A_{lk}R^{-1} = R^{-1}L_{lk}^{\oplus r}$ is equivalent the first condition and $R^{-T}A_lR^{-1} = L_l^{\oplus r}$ is equivalent to the second and third conditions.

Based on this theorem, our strategy of finding a correct key is to find inductively invariant subspaces $V_1, \dots, V_r$ which are mutually orthogonal with respect to A_l and whose bases satisfy equations (5) and (6). The first step is to practically find invariant subspaces of dimension r. We might randomly pick a vector $\mathbf{v}$ and compute the invariant subspace generated by $\mathbf{v}$ under all A_{lk}; repeat doing so until one with dimension r is found. We then need to test if an r-dim invariant subspace generated is a correct invariant subspace according to Theorem 3. If it is not a correct one, we need to try another random vector again. Once the first correct invariant subspace V_1 is found, its basis will determine not only L_l by equation (6) but also other L_k by equation (4), and thus all L_{lk}. All these L_k then give one part of the private key, i.e., L. Next, to find the second correct invariant subspace, we search from vectors orthogonal to V_1 to generate an r-dim invariant subspace and then compute its basis by equation (5). We repeat doing so until this basis satisfies equation (6), then this invariant subspace will be V_2. The rest may be found similarly and inductively. Finally the matrix of all the bases computed will be R^{-1} and thus R is found.

4 Technical Analysis

In this section, we shall execute the strategy described in the preceding section, elaborate all the technical details and resolve the technical issues. There will be three major parts:

1. Practical method to search for r-dim invariant subspaces.
2. Finding criteria for an r-dim invariant subspace to be the first correct invariant subspace V_1 according to Theorem 3.
3. Generating the rest correct r-dim invariant subspaces according to Theorem 3.

4.1 Practical Method of Searching for r-dim Invariant Subspaces

When generating an r-dim invariant subspace from a random vector, the first natural searching range is $\mathbb{F}_q^n$, but this is too big making it impractical. In this subsection, we shall find a practical method to significantly reduce the searching range of r-dim invariant subspaces from the whole space $\mathbb{F}_q^n$ to a much smaller subspace. This is the key to make our attack very efficient. We shall first consider generating proper invariant subspaces and then r-dim invariant subspaces.

To find a proper invariant subspace of $\mathbb{F}_q^n$, we may pick a nonzero vector $\mathbf{u} \in \mathbb{F}_q^n$, and then compute the invariant subspace $\langle \mathbf{u} | A_{lk}, k \neq l \rangle$ generated by $\mathbf{u}$ under all A_{lk}, $k \neq l$, cf. Appendix A for the notation. For convenience, we simplify the notation $\langle \mathbf{u} | A_{lk}, k \neq l \rangle$ as $\langle\!\langle \mathbf{u} \rangle\!\rangle$. There will be two cases: 1) $\dim \langle\!\langle \mathbf{u} \rangle\!\rangle = n$, i.e. $\langle\!\langle \mathbf{u} \rangle\!\rangle = \mathbb{F}_q^n$, and 2) $\dim \langle\!\langle \mathbf{u} \rangle\!\rangle < n$. In the second case we shall call $\mathbf{u}$ a *proper vector*. If it is the first case, then we pick another nonzero vector and repeat this process until a proper invariant subspace is obtained.

If only one linear map is considered, the chance to get a proper vector would be large, but here we are considering $m-1$ linear maps together. We give the following rough estimation on the chance.

Proposition 2. *The probability of a random vector in $\mathbb{F}_q^n$ being proper is greater than q^{-r}.*

Proof. Given an invariant decomposition $\mathbb{F}_q^n = V_1 \oplus \cdots \oplus V_r$ with $\dim V_i = r$, picking randomly a vector $\mathbf{v} \in \mathbb{F}_q^n$ is equivalently to picking randomly r vectors $\mathbf{v}_i \in V_i$. If there is one $\mathbf{v}_i = 0$, then $\mathbf{v}$ is proper. The probability that at least one $\mathbf{v}_i = 0$ is $1 - (1 - q^{-r})^r$. Thus the probability that a random vector is proper is no less than $1 - (1 - q^{-r})^r$. Then the claim follows from the following inequality

$$q^{-r} < 1 - (1 - q^{-r})^r = q^{-r}[1 + (1 - q^{-r}) + \cdots + (1 - q^{-r})^{r-1}] < rq^{-r}.$$

We remark that if there is no $\mathbf{v}_i = 0$ for a decomposition $\mathbb{F}_q^n = V_1 \oplus \cdots \oplus V_r$, there may be other such decomposition having it. Or even if there is no decomposition with some $\mathbf{v}_i = 0$, $\mathbf{v}$ may still be proper. Hence the probability that a random vector being proper is expected much higher than $1 - (1 - q^{-r})^r$. Nevertheless, this probability may still be too small if q^r is too large. To increase the chance of getting proper vectors, we propose the following method to reduce the searching range significantly.

From the theory of invariant subspaces, referring to Appendix A or [Cla], invariant subspaces are essentially related with the characteristic polynomial of a linear map. By $A_{lk} = R^{-1} L_{lk}^{\oplus} R$, A_{lk} and L_{lk} share the same minimum polynomial and the characteristic polynomial of A_{lk} is the rth power of the one of L_{lk}. Denote the characteristic polynomial of L_{lk} by ϕ_{lk}. From Appendix A, for each prime i.e., irreducible factor ψ of ϕ_{lk}, $\ker \psi(A_{lk})$ is a prime invariant subspace of A_{lk} and any nonzero vector of it has the irreducible ψ as its local minimal polynomial. In addition, it has the following important decomposition.

Theorem 4. *All $V_s \cap \ker \psi(A_{lk})$, $1 \leq s \leq r$, are isomorphic and*

$$\ker \psi(A_{lk}) = \bigoplus_{s=1}^{r} (V_s \cap \ker \psi(A_{lk})).$$

Consequently $r | \dim \ker \psi(A_{lk})$.

Proof. Recall for all s,

$$A_{lk}(R_{r(s-1)+1},\ldots,R_{rs}) = (R_{r(s-1)+1},\ldots,R_{rs})L_{lk}.$$

Namely the restriction $A_{lk}|_{V_s}$ of A_{lk} to V_s is given by L_{lk}, and thus all $A_{lk}|_{V_s}$, $1 \le s \le r$, are equivalent and share the same properties. Hence all $\ker\psi(A_{lk}|_{V_s})$, $1 \le s \le r$, are isomorphic. Since $\psi(A_{lk}|_{V_s})(v) = \psi(A_{lk})(v)$ for $v \in V_s$, we have

$$\ker\psi(A_{lk}|_{V_s}) = V_s \cap \ker\psi(A_{lk}).$$

Thus all $V_s \cap \ker\psi(A_{lk})$, $1 \le s \le r$, are isomorphic.
It is obvious that

$$\ker\psi(A_{lk}) \supseteq \bigoplus_{s=1}^{r}(V_s \cap \ker\psi(A_{lk})).$$

On the other hand, since $\mathbb{F}_q^n = \bigoplus_{s=1}^{r} V_s$, each nonzero $v \in \ker\psi(A_{lk})$ has a unique decomposition

$$v = v_1 + \cdots + v_r, \quad v_s \in V_s.$$

Applying $\psi(A_{lk})$ to both sides, we have $\psi(A_{lk})(v_s) \in V_s$ since V_s is invariant under A_{lk}, and

$$0 = \psi(A_{lk})(v) = \psi(A_{lk})(v_1) + \cdots + \psi(A_{lk})(v_r).$$

By the uniqueness of the decomposition, $\psi(A_{lk})(v_s) = 0$, i.e., $v_s \in V_s \cap \ker\psi(A_{lk})$. Hence

$$\ker\psi(A_{lk}) \subseteq \bigoplus_{s=1}^{r}(V_s \cap \ker\psi(A_{lk})).$$

Therefore both sides are equal.

As $\ker\psi(A_{lk})$ is much smaller than $\mathbb{F}_q^n$, it is a better space to search for proper vectors. Among all $\ker\psi(A_{lk})$ for all $k \neq l$ and irreducible factors ψ, we can choose one of them which is of minimum dimension and denote it V_0. Since $r|\dim V_0$, write $\dim V_0 = dr$. Using V_0 to search for proper vectors, the chance of getting a proper vector increases significantly as estimated below.

Proposition 3. *The probability of a random vector in V_0 being proper is greater than q^{-d}.*

We further consider the probability distribution of d and the probability of generating an r-dim invariant subspace from a random vector in V_0. It seems that there is no obvious mathematical method to deduce them. So we tested 1,500 instances covering various primes and dimensions to see what would happen. From our test result we have the following surprising findings:

1. If $r > 2$, it is almost always $d = 1$ and a random nonzero vector in V_0 almost always generate an r-dim invariant subspace. In fact each of them does not appear only 5 times among a thousand instances.
2. If $r = 2$, $d = 1$ appears 364 times among 500 instances, as well as that a random nonzero vector in V_0 generates an r-dim invariant subspace.
3. Wherever $r > 2$ or $r = 2$, $d = 1$ appears or does not appear simultaneously with that a random nonzero vector in V_0 generates an r-dim invariant subspace among all 1,500 instances.

From these findings, we make the following assumption.

Assumption 2 *1) If $d = 1$, then a random nonzero vector $\mathbf{u} \in V_0$ almost always generates an r-dim invariant subspace. 2) When $r > 2$, the probability of $d = 1$ is almost 1, as well as the probability of $\dim\langle\langle\mathbf{u}\rangle\rangle = r$; in other words, the probabilities of $d > 1$ and of $\dim\langle\langle\mathbf{u}\rangle\rangle \neq r$ both are negligible. 3) If $r = 2$, both probabilities of $d = 1$ and of $\dim\langle\langle\mathbf{u}\rangle\rangle = r$ are generally no less than $\frac{1}{2}$.*

4.2 Finding the First Correct Invariant Subspace

In this subsection, we shall find the first correct invariant subspace V_1 in $\mathbb{F}_q^n = \bigoplus_{s=1}^r V_s$.

After reducing the searching range from $\mathbb{F}_q^n$ to V_0, we may search for an r-dim invariant subspace by picking randomly a nonzero vector $\mathbf{u} \in V_0$, and then computing the invariant subspace $\langle\!\langle \mathbf{u} \rangle\!\rangle$, generated by $\mathbf{u}$ under all A_{lk}, $k \neq l$. To compute $\langle\!\langle \mathbf{u} \rangle\!\rangle$, we may compute the linear subspace spanned by $\mathbf{u}$, $A_{lk}\mathbf{u}$, …, $A_{lk}^n\mathbf{u}$ for all $k \neq l$, and some $A_{lk}^i A_{lk'}^j \mathbf{u}$ — if necessary, add more vectors of this form $A_{lk}^i A_{lk'}^{i'} A_{lk''}^{i''}\mathbf{u}$ etc. By Assumption 2, only one or two trials will generally give an r-dim invariant subspace $\langle\!\langle \mathbf{u} \rangle\!\rangle$.

After finding an r-dim invariant subspace U, we find that it may not be a correct invariant subspace. We analyze the situation and resolve this issue in the following. We note that by Theorem 3 an r-dim invariant subspace should have a basis $\mathbf{b}_1, \ldots, \mathbf{b}_r$ such that

$$(\mathbf{b}_1, \ldots, \mathbf{b}_r)^T A_l (\mathbf{b}_1, \ldots, \mathbf{b}_r) = L_l.$$

Note that the left hand side should be nonsingular according to Assumption 1. We remark that this condition is not dispensable as there exist linearly independent vectors $\mathbf{a}_1, \ldots, \mathbf{a}_r$ in $\mathbb{F}_q^n$ such that $(\mathbf{a}_1, \ldots, \mathbf{a}_r)^T A_l (\mathbf{a}_1, \ldots, \mathbf{a}_r)$ is singular in our implementation. In addition, according to Theorem 1, there are two types of square matrices over $\mathbb{F}_q^n$ with q odd:

1) with determinant a square, and
2) with determinant a non-square.

For convenience, we call them *square type* and *non-square type* respectively. Note that $A_l = R^T L_l^{\oplus r} R$. So if r is odd, A_l keeps the type of L_l, but if r is even, A_l is always of square type. Therefore, we should add this type condition to $\langle\!\langle \mathbf{u} \rangle\!\rangle$.

To summarize, the criteria for searching the first desired invariant subspace are:

1. $\mathbf{u} \in V_0$ and if a vector has been tried previously then discard the linear subspace spanned by it.
2. $\dim\langle\!\langle \mathbf{u} \rangle\!\rangle = r$.
3. $\langle\!\langle \mathbf{u} \rangle\!\rangle$ has a basis $\mathbf{b}_1, \ldots, \mathbf{b}_r$ such that $(\mathbf{b}_1, \ldots, \mathbf{b}_r)^T A_l (\mathbf{b}_1, \ldots, \mathbf{b}_r)$ is nonsingular.
4. If r is odd, $\langle\!\langle \mathbf{u} \rangle\!\rangle$ has a basis $\mathbf{b}_1, \ldots, \mathbf{b}_r$ such that $\det((\mathbf{b}_1, \ldots, \mathbf{b}_r)^T A_l (\mathbf{b}_1, \ldots, \mathbf{b}_r))$ is a square if $\det A_l$ is a square and non-square if $\det A_l$ non-square. If r is even, there is no such restriction on the type.

We will see in our experiments that only several trials or even only one will give such a $\langle\!\langle \mathbf{u} \rangle\!\rangle$. After finding one, let $V_1 = \langle\!\langle \mathbf{u} \rangle\!\rangle$ and denote its basis $\mathbf{u}_{11}, \ldots, \mathbf{u}_{1r}$ (in fact any basis will do). Compute

$$L_k = (\mathbf{u}_{11}, \ldots, \mathbf{u}_{1r})^T A_k (\mathbf{u}_{11}, \ldots, \mathbf{u}_{1r}), \quad 1 \leq k \leq m$$

and $L_{lk} = L_l^{-1} L_k$ for $k \neq l$. These L_k may not equal to the original ones, but they will be equivalent.

4.3 Finding the Rest Correct Invariant Subspaces

We next show how to inductively find all the rest correct invariant subspaces $V_2, \ldots, V_r$. Suppose we have found $V_1, \ldots, V_i$, we find in the following those conditions that V_{i+1} should satisfy. Firstly $\dim V_{i+1} = r$. By the second condition of Theorem 3, V_{i+1} is orthogonal to $V_1, \ldots, V_i$ in the following sense:

$$\mathbf{u}^T A_k \mathbf{v} = 0, \quad \forall \mathbf{u} \in V_{i+1}, \mathbf{v} \in V_j, 1 \leq j \leq i, k \neq l.$$

By Theorem 2, V_{i+1} has a basis $\mathbf{b}_1, \ldots, \mathbf{b}_r$ such that

$$A_{lk}(\mathbf{b}_1, \ldots, \mathbf{b}_r) = (\mathbf{b}_1, \ldots, \mathbf{b}_r)L_{lk}.$$

Conversely, such a basis can be solved from this equation. Then by Equation 6 of Theorem 3, we test if this basis satisfies

$$(\mathbf{b}_1, \ldots, \mathbf{b}_r)^T A_l(\mathbf{b}_1, \ldots, \mathbf{b}_r) = t^2 L_l$$

for some $t \in \mathbb{F}_q$. There is t^2 on the right hand side since the type of L_l need to be taken into account.

To Summarize, we shall search for a vector $\mathbf{u}$ to generate V_{i+1} according to the following criteria:

1. $\mathbf{u} \in V_0$ and if a vector has been tried previously then discard the linear subspace spanned by it.
2. $\mathbf{u}^T A_k \mathbf{v} = 0$, $\forall \mathbf{v} \in V_j$, $1 \leq j \leq i$, $k \neq l$.
3. $\dim\langle\!\langle \mathbf{u} \rangle\!\rangle = r$.
4. The basis $\mathbf{b}_1, \ldots, \mathbf{b}_r$ of $\langle\!\langle \mathbf{u} \rangle\!\rangle$ solved from $A_{lk}(\mathbf{b}_1, \ldots, \mathbf{b}_r) = (\mathbf{b}_1, \ldots, \mathbf{b}_r)L_{lk}$ satisfies $(\mathbf{b}_1, \ldots, \mathbf{b}_r)^T A_l(\mathbf{b}_1, \ldots, \mathbf{b}_r) = t^2 L_l$ for some $t \in \mathbb{F}_q$.

With only several trials or even only one as shown in our experiments, we will find such a $\mathbf{u}$. Then let $V_{i+1} = \langle\!\langle \mathbf{u} \rangle\!\rangle$ and $\mathbf{u}_{i+1,j} = t\mathbf{b}_j$, $1 \leq j \leq r$. Continue this process until we find V_r. Then let

$$R^{-1} = (\mathbf{u}_{11}, \ldots, \mathbf{u}_{1r}, \ldots, \mathbf{u}_{r1}, \ldots, \mathbf{u}_{rr}),$$

and compute R from R^{-1} and L from all L_k. Finally verify Equation 3 to check if (L, R) is a correct key.

5 Algorithm and Complexity

In this section we shall first give our algorithm of attacking YTS' scheme based on the theory in preceding sections and analyze its complexity.

5.1 Algorithm

In preceding sections, we have developed a detailed theory of attacking YTS' scheme using invariant subspaces. We now summarize it as an algorithm of recovering a correct private key of YTS' scheme from its public map.

Algorithm 1 *Given the matrices $A_1, \ldots, A_m$ of the first part of the public map $\bar{F}$ of YTS' scheme, a correct private key, i.e., a pair of matrices (L, R) satisfying Equation 3, may be computed from the following steps.*

1. *Among all A_k, find an invertible A_l and then compute $A_{lk} = A_l^{-1} A_k$.*
2. *For each A_{lk}, compute its every primary factor ψ, then $\psi(A_{lk})$ and $\dim \ker \psi(A_{lk})$ until $\dim \ker \psi(A_{lk}) = r$ which means $d = 1$. Denote this $\ker \psi(A_{lk})$ as V_0 and continue to next step. If it is always $\dim \ker \psi(A_{lk}) \neq r$ which means $d > 1$, then exit and return "This algorithm is not applicable".*
3. *Pick a $\mathbf{u} \in V_0$ following the first criterion in Subsection 4.2, and compute the invariant subspace $\langle\!\langle \mathbf{u} \rangle\!\rangle$ by computing the linear subspace spanned by $\mathbf{u}$, some $A_{lk}^i \mathbf{u}$ and some $A_{lk}^i A_{lk'}^{i'} \mathbf{u}$ — add some $A_{lk}^i A_{lk'}^{i'} A_{lk''}^{i''} \mathbf{u}$ etc if necessary. Repeat this process until a $\langle\!\langle \mathbf{u} \rangle\!\rangle$ satisfying all the criteria in Subsection 4.2 is found, and let it be V_1.*

4. *Let* $\mathbf{u}_{11}, \dots, \mathbf{u}_{1r}$ *be a basis of* V_1*. Compute* $L_k = (\mathbf{u}_{11}, \dots, \mathbf{u}_{1r})^T A_k(\mathbf{u}_{11}, \dots, \mathbf{u}_{1r})$*,* $1 \leq k \leq m$*, and* $L_{lk} = L_l^{-1} L_k$ *for* $k \neq l$*.*
5. *Similar to Step 3, compute* V_{i+1} *and basis* $\mathbf{u}_{i+1,1}, \dots, \mathbf{u}_{i+1,r}$ *following the criteria in Subsection 4.3. Repeat this process until all* $V_2, \dots, V_r$ *are found.*
6. *Compute* R *from* $R^{-1} = (\mathbf{u}_{11}, \dots, \mathbf{u}_{1r}, \dots, \mathbf{u}_{r1}, \dots, \mathbf{u}_{rr})$ *and* L *from all* L_k*.*
7. *Verify Equation 3 to check if* (L, R) *is a correct key.*

Note that the condition $\dim \ker \psi(A_{lk}) = r$ at Step 2 implies that Algorithm 1 applies only when $d = 1$. It should be mentioned that the requirement $d = 1$ is just for easy implementation. If $d > 1$, an applicable algorithm can actually be obtained by modifying Algorithm 1 with not much effort. In that case, what we may get is a proper invariant subspace whose dimension is a multiple of r, but we can decompose it further into smaller invariant subspaces. In other words, we can inductively decompose the whole space into smaller and smaller invariant subspaces until a full decomposition into r-dim invariant subspaces is obtained. Then the rest are analogous to but more tedious than Algorithm 1. Nevertheless, Assumption 2 assures that Algorithm 1 is (almost) always applicable when $r > 2$ and often so when $r = 2$ as confirmed in our implementation.

5.2 Complexity

We shall estimate the complexity of Algorithm 1 by counting the number of $\mathbb{F}_q$ multiplications needed and by experimental method.

We first count the number of $\mathbb{F}_q$ multiplications needed for Steps 1, 4, 6 and 7 as these steps are relatively simple:

Step	1	4	6	7
# $\mathbb{F}_q$ multiplications	$O(r^8)$	$O(r^7)$	$O(r^6)$	$O(r^6)$

In theory the primary factors at Step 2 can be computed using Berlekamp's algorithm [Ber67, Ber70, vzGP01] or recent faster algorithms of Kedlaya and Umans [KU11]. Notice that the complexity estimation for these algorithms are for large parameters, but practical parameters used for YTS' scheme are rather small compared to them. Our numerous experiments and implementation show that not only this computation of primary factors but also the whole Step 2 is almost done immediately, so the complexity of Step 2 is too little to take into account.

For Steps 3 and 5, the first question is how many $\mathbb{F}_q$ multiplications are needed for the computation of the invariant subspace $\langle\langle \mathbf{u} \rangle\rangle$ generated by a vector $\mathbf{u}$. Notice that the dimension of $\dim\langle\langle \mathbf{u} \rangle\rangle$ is always r by Assumption 2 since $d = 1$ from Step 2. So to span $\langle\langle \mathbf{u} \rangle\rangle$, it should be enough to use these $(m-1)r = O(r^3)$ vectors $\mathbf{u}, A_{lk}\mathbf{u}, \dots, A_{lk}^r\mathbf{u}$ for all $k \neq l$ and some $A_{lk}^i A_{lk'}^j \mathbf{u}$. Note that each product $A_{lk}\mathbf{u}$ needs r^4 $\mathbb{F}_q$ multiplications and it is more efficient to compute the triple product $A_{lk}A_{lk'}\mathbf{u}$ in this order $A_{lk}(A_{lk'}\mathbf{u})$. Then computing $\langle\langle \mathbf{u} \rangle\rangle$ will need $O(r^3 r^4) = O(r^7)$ $\mathbb{F}_q$ multiplications.

The second question of Steps 3 and 5 is how many trials are needed to get a correct $\mathbf{u}$. As there seems no obvious accurate theoretical estimation on the number of trials, we conduct experiments to estimate the complexity of searching correct $\mathbf{u}$. Our experiment covers various p, q, r and includes 625 random instances in total with each one attacked twice. The results are presented in Tables 1 and 2, where "# trials" means the number of trials done to get a correct $\mathbf{u}$ and "# times" means the number of times that "# trials" appears among all the tests. From Table 1, we see that when $r > 2$ every attack is successful as expected in Assumption 2 and that almost always at most 5 trials can give a correct $\mathbf{u}$ and especially only 1 or 2 trials will be enough mostly. When $r = 2$, Table 2 also confirms the expectation in Assumption 2 that the success rate is no less than $\frac{1}{2}$, but it is surprising to find that only 1 trial is almost enough to get a correct $\mathbf{u}$ and no more than 2 trials are needed. From these experiment results, we thus can conclude that the complexity of searching correct $\mathbf{u}$ is rather small. Additionally recall that there are r correct $\langle\langle\mathbf{u}\rangle\rangle$ need to be computed to generate the r invariant subspaces. Therefore the complexity of Steps 3 and 5 is bounded by $O(r^7 \cdot r) = O(r^8)$.

Table 1. Searching Complexity ($r > 2$)

$r > 2$			
# instances	# attacks	# successful attacks	# success rate
400	800	800	100%

# trials	1	2	3	4	5	6	7	8	9	10	11	12	13	≥ 14
# times	2751	801	415	190	121	69	39	18	10	5	1	2	1	0
ratio (%)	62.20	18.11	9.38	4.30	2.74	1.56	0.88	0.41	0.23	0.11	0.00	0.00	0.00	0.00

Table 2. Searching Complexity ($r = 2$)

$r = 2$			
# instances	# attacks	# successful attacks	# success rate
225	450	330	73.33%

# trials	1	2	≥ 3
# times	655	5	0
ratio (%)	99.24	0.76	0.00

To summarize, we have the following estimation on the complexity.

Proposition 4. *The complexity of Algorithm 1 is $O(r^8) = O(n^4)$ $\mathbb{F}_q$ multiplications.*

Recall that the efficiency of signature generation is $O(r^4) = O(n^2)$ $\mathbb{F}_q$ multiplications [YTS13]. Namely the complexity of our attack is only square of the efficiency of signature generation. Therefore it is safe to claim that YTS' scheme is generally broken efficiently by our attack.

6 Implementation Results

In this section we shall present and discuss our implementation results. Our algorithm is implemented under the following computation environment:

- RAM: 24.0 GB
- Processor: Dual XEON Quad Core 2.27 GHz
- Operating System: RedHat Enterprise Linux 5.9 (64-bit)
- Magma V2.19-10

Due to the restriction of our computing power, we set the following limit: if the average computation time reaches around 500 seconds for a set of parameters, then we will stop testing bigger parameters.

Recall that all the parameters of YTS' scheme are p a prime, q a power of p, n the number of variables, $r = \sqrt{n}$ and $m = r(r+1)/2$, but (p, q, r) are the major ones. We shall present the average computation time and success rate of a few tests of a set of parameters (p, q, r). Along with them, we also calculate both the lower bound $q^{\sqrt{n}}$ on security against Min-Rank attack and the public key size as helpful references. According to Assumption 2, the cases that $r > 2$ and that $r = 2$ are different. In detail, when $r > 2$, d is expected generally 1 so that Algorithm 1 applies generally and thus its success rate is expected generally 1; but when $r = 2$ the probability of $d = 1$ is expected generally no less than $\frac{1}{2}$ so that the success rate of Algorithm 1 is expected generally no less than $\frac{1}{2}$ as well. Hence we shall separate our implementation into two parts accordingly.

When $r > 2$, our implementation always get a correct key; i.e., the success rate of our attack is 100%, so we shall omit it in the tables below. For the choice of parameters, we recall that in [YTS13] two sets of parameters $(p = 2053, q = p, r = 8)$ and $(p = 6781, q = p, r = 11)$ are chosen and claimed to have security level higher than 88-bit and 140-bit respectively. Thus we of course consider these two sets of parameters. In addition, we also consider other various sets of parameters, including the smallest odd prime 3 and picking randomly a prime between 3 and 2053 and a prime much bigger than 6781. For each set of parameters (p, q, r), we generate randomly 5 instances and attack each instance 5 times, then calculate the average computation time for the 25 attacks to a set of parameters. Our first implementation data are displayed in Tables 3, 4, 5, 6, 7. From these tables, we see that the computation time is small and increases slowly as both r and the extension degree $\log_p q$ increase even if their security against Min-Rank attack is as high as 140-bit, but the public key size increases very fast. Especially for the two sets of parameters $(2053, 2053, 8)$ and $(6781, 6781, 11)$ in [YTS13], they are broken only in 1.50s and 14.77s respectively.

Table 3. $p = 3$

$p = 3$	r	8	9	10	11	12
$q = p$	attack (sec)	0.66	1.43	2.74	4.82	8.90
	Min-Rank (bit)	12	14	15	17	19
	public key (kB)	37.4	74.7	138.9	243.6	404.4
$q = p^2$	attack (sec)	1.16	2.85	6.67	11.98	24.60
	Min-Rank (bit)	25	28	31	34	38
	public key (kB)	74.9	149.4	277.8	487.1	808.7
$q = p^3$	attack (sec)	1.35	3.87	7.81	15.24	30.69
	Min-Rank (bit)	38	42	47	52	57
	public key (kB)	112.3	224.2	416.6	730.7	1,213.1
$q = p^4$	attack (sec)	1.84	4.27	8.45	18.17	36.48
	Min-Rank (bit)	50	57	63	69	76
	public key (kB)	149.8	298.9	555.5	974.3	1,617.4

Table 4. $p = 311$

$p = 311$	r	8	9	10	11	12
$q = p$	attack (sec)	0.77	1.69	3.37	10.04	16.7
	Min-Rank (bit)	66	74	82	91	99
	public key (kB)	168.5	336.3	624.9	1,096.1	1,819.6
$q = p^2$	attack (sec)	26.51	49.84	68.77	108.06	181.73
	Min-Rank (bit)	132	149	165	182	198
	public key (kB)	337.0	672.5	1,249.9	2,192.2	3,639.2

Table 5. $p = 2053$

$p = 2053$	r	8	9	10	11	12
$q = p$	attack (sec)	1.50	3.28	6.63	13.01	25.50
	Min-Rank (bit)	88	99	110	121	132
	public key (kB)	224.6	448.3	833.2	1,461.4	2,426.1

Table 6. $p = 6781$

$p = 6781$	r	8	9	10	11	12
$q = p$	attack (sec)	2.55	4.55	9.38	14.77	24.41
	Min-Rank (bit)	101	114	127	140	152
	public key (kB)	243.4	485.7	902.7	1,583.2	2,628.3

Table 7. $p = 300007$

$p = 300007$	r	8	9	10	11	12
$q = p$	attack (sec)	106.89	183.95	227.77	305.52	407.23
	Min-Rank (bit)	145	163	182	200	218
	public key (kB)	355.7	709.9	1,319.3	2,313.9	3,841.3

We further test for what set of parameters, the computation time can reach around 500s. In Table 7, we already see that ($p = 300007, q = p, r = 12$) is close to reach the 500s limit. Thus we next test the smallest $r > 2$ and the smallest odd prime, i.e., $r = 3$ and $p = 3$, see Table 8. Here we see some surprise when $\log_p q$ exceeds 12. Namely when $q = p^{13}$, the computation time has a big jump from less than 20s to more than 300s, but security against Min-Rank is only 61-bit and public key size 1.755kB only. Moreover when $q = p^{14}$, the computation even jumps to almost 500s but with security against Min-Rank attack as low as 66-bit only and public key size 1.890kB only. We then further test the smallest extension degrees $\log_p q = 2, 3, 4$, see Table 9 from which we observe similar phenomenon; namely, the computation time is already more than 500s but the security against Min-Rank attack remains as low as about 66-bit and public key size remain as small as 1.620kB.

Table 8. $r = 3$ and $p = 3$

$r = 3$	q	p^{10}	p^{11}	p^{12}	p^{13}	p^{14}
$p = 3$	attack (sec)	0.95	5.99	17.41	311.17	498.37
	Min-Rank (bit)	47	52	57	61	66
	public key (kB)	1.350	1.485	1.620	1.755	1.890

Table 9. $r = 3$

$r = 3$	$p = 2053, q = p^2$	$p = 149, q = p^3$	$p = 43, q = p^4$
attack (sec)	798.47	647.40	562.18
Min-Rank (bit)	66	65	65
public key (kB)	1.620	1.620	1.620

When $r = 2$, the situation is different. As it is expected that Algorithm 1 cannot always produce a correct key, we test 10, instead of 5, random instances for each set of parameters with each instance attacked twice. We then calculate the average computation time of the 20 attacks as well as the success rate, and add the success rate to the table of implementation data. We first test $p = 3$ for various extension degrees, referring to Table 10, and then for extension degree 2, 3, and 4, we find the primes reaching the 500s limit respectively, referring to Table 14. From the two tables, it is interesting to see that every success rate is no less than $\frac{1}{2}$ as expected in Assumption 2. Moreover it is surprising to see that when the computation reaches around 500s, the security against Min-Rank attack remains even lower than 50-bit and public key size remains much smaller, i.e. around 0.2kB only.

From all the above implementation data, we find that the computation time is very sensitive on the extension degree $\log_p q$ of $\mathbb{F}_q$ over $\mathbb{F}_p$, but much less sensitive on r, and least sensitive on p. If $\log_p q = 1$, i.e., $q = p$, the computation time increases slowly, but it increases very fast as $\log_p q$ increases. It seems that the best strategy of choosing parameters is: $r = 2$ and q large but p small. In addition, p should be as close as possible to but less than a power of 2. This can have high security level but also maintain small public key size as the relationship between the public key size and r is $O(r^6) = O(n^3)$, referring to Section 2. Nevertheless, this does not mean

Table 10. $r = 2$ and $p = 3$

$r = 2$	q	p^8	p^9	p^{10}	p^{11}	p^{12}	p^{13}	p^{14}	p^{15}
$p = 3$	attack (sec)	0.02	0.06	0.20	0.78	2.74	42.64	95.69	376.62
	success rate	100%	60%	60%	90%	80%	80%	70%	60%
	Min-Rank (bit)	25	28	31	34	38	41	44	47
	public key (kB)	0.120	0.135	0.150	0.165	0.180	0.195	0.210	0.225

Table 11. $r = 2$ and $p = 5$

$r = 2$	q	p^6	p^7	p^8	p^9	p^{10}	p^{11}
$p = 5$	attack (sec)	0.05	0.28	1.99	42.78	228.04	$>$ 1 hour
	success rate	80%	60%	90%	100%	80%	-
	Min-Rank (bit)	28	33	38	42	47	51
	public key (kB)	0.135	0.158	0.180	0.203	0.225	0.248

Table 12. $r = 2$ and $p = 7$

$r = 2$	q	p^5	p^6	p^7	p^8	p^9
$p = 7$	attack (sec)	0.06	0.45	4.54	136.75	$>$ 1 hour
	success rate	70%	70%	70%	80%	-
	Min-Rank (bit)	28	34	40	45	51
	public key (kB)	0.113	0.135	0.158	0.180	0.203

Table 13. $r = 2$ and $p = 43$

$r = 2$	q	p^2	p^3	p^4	p^5
$p = 43$	attack (sec)	0.01	0.31	75.34	$>$ 1 hour
	success rate	80%	80%	80%	-
	Min-Rank (bit)	22	33	44	55
	public key (kB)	0.090	0.135	0.180	0.225

Table 14. $r = 2$

$r = 2$	q	p^2	p^3	p^4
$p = 67$	attack (sec)	0.02	1.41	497.55
	success rate	90%	90%	90%
	Min-Rank (bit)	24	36	48
	public key (kB)	0.105	0.158	0.210
$p = 233$	attack (sec)	0.20	505.86	-
	success rate	80%	80%	-
	Min-Rank (bit)	31	47	-
	public key (kB)	0.120	0.180	-
$p = 4111$	attack (sec)	555.06	-	-
	success rate	80%	-	-
	Min-Rank (bit)	48	-	-
	public key (kB)	0.195	-	-

existence of practical and secure parameters because the complexity of our attack is only square of the efficiency of signature generation, referring to Proposition 4.

7 Comparison with Y. Hashimoto's Attack

There is another attack to YTS' scheme proposed by Y. Hashimoto in PQCrypto 2014 [Has14]. We shall compare his attack and ours on several aspects including ideas, approaches, complexity and implementation.
The starting difference is the choice of the one-one correspondence ϕ_1 between $r \times r$ matrices and vectors in $\mathbb{F}_q^n = \mathbb{F}_q^{r^2}$. Our choice is, see Equation (1),

$$X \longleftrightarrow (x_{11}, \ldots, x_{1r}, x_{21}, \ldots, x_{2r}, \ldots, x_{r1}, \ldots, x_{rr})$$

while Hashimoto's is

$$X \longleftrightarrow (x_{11}, \ldots, x_{r1}, x_{12}, \ldots, x_{r2}, \ldots, x_{1r}, \ldots, x_{rr}).$$

Though this minor difference seems ignorable, it results quite different expressions of the public map

$$A_k = R^T L_k^{\oplus r} R \quad \text{and} \quad A_k = R^T (L_k \otimes I_r) R$$

respectively. Here $A \otimes B$ denotes the Kronecker product

$$A \otimes B = \begin{pmatrix} a_{11}B \cdots a_{1r}B \\ \vdots \qquad \vdots \\ a_{r1}B \cdots a_{rr}B \end{pmatrix}$$

of two matrices $A = (a_{ij})_{rr}$ and B. The two expressions are of course equivalent but lead to different approaches. Namely our expression has clear geometric interpretation after converting to the following form

$$(A_l^{-1} A_k) R^{-1} = R^{-1} L_{lk}^{\oplus r},$$

and reveals the hidden geometric structures of YTS' scheme. This leads us to a geometric approach using the theory of invariant subspaces. However, the second expression does not have such geometric meaning. Hashimoto uses an algebraic approach to deal with it. He first observes that the private key can be recovered if R is of the following special form

$$R = (Q \otimes I_r)(N_1 \oplus \cdots \oplus N_r),$$

where $Q, N_1, \ldots, N_r$ are $r \times r$ matrices, and then for general R, he develops algorithms to find an invertible P such that RP is of this form and thus recovers the private key for the general case.
Despite the above difference, both of the two approaches have some parts influenced by Kipnis and Shamir's attack to the oil-vinegar signature scheme [KS98]. In our approach, we are motivated to convert $A_k = R^T(\cdots)R$ into $A_l^{-1}A_k = R^{-1}(\cdots)R$ so that the problem can be converted into a geometric problem and be solved using the theory of invariant subspaces. In Hashimoto's attack, his method of finding the P is also analogous to Kipnis and Shamir's method to some extent.
The complexity of Hashimoto's attack is also claimed to be $O(n^4)$ $\mathbb{F}_q$ multiplications [Has14]. However implementation results show that our attack seems much faster. Hashimoto implements his attack under Windows 7, Core-i7 2.67GHz and Magma ver.2.15-10, and run 20 times to attack YTS' scheme with parameters ($p = 6781, q = p, r = 11$). He claims that he succeeds every time and the running times is between

240 to 450 seconds. Our attack to this particular set of parameters is much faster with only 14.77 seconds on average, referring to Table 6, and the time varies from 7.91 to 26.73 seconds which is not given in the table. Moreover unlike our implementation including other various parameters, Hashimoto's paper [Has14] includes only this particular set of parameters. So to have a more convincible comparison, we need to implement both attacks under the same computing environment and test the same sets of various parameters.

8 Conclusion

Yasuda, Takagi and Sakurai's signature scheme has special structure different from other MPKC and is very efficient. However, we manage to attack its structure by applying intensively the theory of invariant subspaces and recover its private key. Our attack has complexity only $O(n^4)$ which is square of the efficiency of signature generation. We further successfully implemented our algorithm and break in about 14.77 seconds a YTS' instance whose security level was claimed to be 140bit. Therefore our attack generally break efficiently Yasuda, Takagi and Sakurai's signature scheme.

References

[Ber67] Elwyn R. Berlekamp. Factoring polynomials over finite fields. *Bell System Technical Journal*, 46:1853C1859, 1967.

[Ber70] Elwyn R. Berlekamp. Factoring polynomials over large finite fields. *Math. Comput.*, 24:713–735, 1970.

[Car54] L. Carlitz. Representations by quadratic forms in a finite field. *Duke Math J.*, 21:123–137, 1954.

[CHDY11] Weiwei Cao, Lei Hu, Jintai Ding, and Zhijun Yin. Kipnis-Shamir Attack on Unbalanced Oil-Vinegar Scheme. In F. Bao and J. Weng, editors, *ISPEC 2011*, volume 6672 of *LNCS*, pages 168–180. Springer-Verlag Berlin Heidelberg, 2011.

[Cla] Pete L. Clark. Linear algebra: Invariant subspaces. `http://math.uga.edu/~pete/invariant_subspaces.pdf`.

[DGS06] Jintai Ding, Jason E. Gower, and Dieter S. Schmidt. *Multivariate public key cryptosystems*, volume 25 of *Advances in Information Security*. Springer, 2006.

[DS05] Jintai Ding and Dieter Schmidt. Rainbow, a new multivariate polynomial signature scheme. In J. Ioannidis, A. Keromytis, and M. Yung, editors, *ACNS 2005*, volume 3531 of *LNCS*, pages 164–175. Springer-verlag Berlin Heidelberg, 2005.

[DY09] Jintai Ding and Bo-Yin Yang. Multivariate public key cryptography. In DanielJ. Bernstein, Johannes Buchmann, and Erik Dahmen, editors, *Post-Quantum Cryptography*, pages 193–241. Springer Berlin Heidelberg, 2009.

[GS03] Willi Geiselmann and Rainer Steinwandt. A short comment on the affine parts of SFLASH^{v3}. Cryptology ePrint Archive, Report 2003/220, 2003. `http://eprint.iacr.org/`.

[GSB01] Willi Geiselmann, Rainer Steinwandt, and Thomas Beth. Attacking the Affine Parts of SFLASH. In B. Honary, editor, *Cryptography and Coding 2001*, volume 2260 of *LNCS*, pages 355–359. Springer-Verlag Berlin Heidelberg, 2001.

[Has14] Yasufumi Hashimoto. Cryptanalysis of the multivariate signature scheme proposed in pqcrypto 2013. In M. Mosca, editor, *PQCrypto 2014*, volume 8772 of *LNCS*, pages 108–125. Springer International Publishing Switzerland, 2014.

[KPG99] Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced oil and vinegar signature schemes. In J. Stern, editor, *EUROCRYPT'99*, volume 1592 of *LNCS*, pages 206–222. Springer, 1999.

[KS98] Aviad Kipnis and Adi Shamir. Cryptanalysis of the oil & vinegar signature scheme. In H. Krawczyk, editor, *CRYPTO'98*, volume 1462 of *LNCS*, pages 257–267. Springer-Verlag Berlin Heidelberg, 1998.

[KU11] Kiran S Kedlaya and Christopher Umans. Fast polynomial factorization and modular composition. *SIAM Journal on Computing*, 40(6):1767–1802, 2011.

[Mac69] Jessie MacWilliams. Orthogonal matrices over finite fields. *The American Mathematical Monthly*, 76(2):152–164, 1969.

[Pat97] Jacques Patarin. The oil and vinegar signature scheme. Presented at the Dagstuhl Workshop on Cryptography, September 1997.

[Sch85] Winfried Scharlau. *Quadratic and Hermitian Forms.* Springer, 1985.

[vzGP01] J. von zur Gathen and D. Panario. Factoring polynomials over finite fields: A survey. *J. Symbolic Computation*, 31:3–17, 2001.

[WP05a] Christopher Wolf and Bart Preneel. Equivalent Keys in HFE, C^*, and Variations. In E. Dawson and S. Vaudenay, editors, *Mycrypt 2005*, volume 3715 of *LNCS*, pages 33–49. Springer-Verlag Berlin Heidelberg, 2005.

[WP05b] Christopher Wolf and Bart Preneel. Taxonomy of public key schemes based on the problem of multivariate quadratic equations. Cryptology ePrint Archive, Report 2005/077, http://eprint.iacr.org/2005/077/, 2005.

[YTS13] Takanori Yasuda, Tsuyoshi Takagi, and Kouichi Sakurai. Multivariate signature scheme using quadratic forms. In P. Gaborit, editor, *PQCrypto 2013*, volume 7932 of *LNCS*, pages 243–258. Springer, 2013.

[ZT15] Wenbin Zhang and Chi How Tan. Algebraic Cryptanalysis of Yasuda, Takagi and Sakurais Signature Scheme. In J. Lee and J. Kim, editors, *Information Security and Cryptology - ICISC 2014*, volume 8949 of *LNCS*, pages 53–66. Springer International Publishing, 2015.

A A Brief Introduction of the Theory of Invariant Subspaces

In this section, we introduce the theory of invariant subspaces. We give here only a very brief introduction which will be used in the paper, referring to [Cla] for a complete theory.

Let $\mathbb{F}$ be a finite field, V a nontrivial finite dimensional vector space over $\mathbb{F}$, and $T : V \to V$ a linear map. A subspace $U \subseteq V$ is called an *invariant subspace* of T if $T(U) \subseteq U$. And a *proper invariant subspace* is an invariant subspace which is neither the zero subspace nor the whole space V.

For a vector $v \in V$, the invariant subspace, denoted $\langle v|T\rangle$, generated by v under T is the linear subspace spanned by $v, Tv, T^2v, \ldots$. It is minimal in the sense that if U is an invariant subspace containing v, then $\langle v|T\rangle \subseteq U$. If we have k linear maps $T_1, \ldots, T_k : V \to V$, we can obviously define the invariant subspace generated by v under $T_1, \ldots, T_k$, and denote it $\langle v|T_1, \ldots, T_k\rangle$.

There is interesting and deep relationship between invariant subspaces of T and the characteristic polynomial, denoted f_T, of T.

Proposition 5. *For any polynomial $f(x) \in \mathbb{F}[x]$, the kernel* $\ker f(T)$ *and the image $f(T)(V)$ of $f(T)$ both are invariant subspaces of T.*

Given a vector $v \in V$, a polynomial f_v is called the *local minimal polynomial* of T at v, if $f_v(T)(v) = 0$ and for any polynomial g such that $g(T)(v) = 0$, $f_v|g$. Such f_v exists and $f_v|f_T$. v is called a prime vector if f_v is irreducible.
For a prime, i.e., irreducible, factor g of f_T, we shall call $\ker g(T)$ a *prime* invariant subspace of T. Prime invariant subspaces have the following property.

Proposition 6. *If g is a prime factor of f_T, then $g = f_v$ for any nonzero $v \in$* $\ker g(T)$*.*

For each prime vector v, $\langle v|T\rangle$ contains no proper invariant subspaces, and thus may be regarded as a minimal invariant subspace. Furthermore the prime invariant subspace $\ker g(T)$ can be decomposed as a direct sum of some such minimal invariant subspaces, but such decomposition is not unique.
Suppose f_T is decomposed as

$$f_T = f_1^{s_1} \cdots f_r^{s_r}$$

with each f_i irreducible and $f_i \neq f_j$ if $i \neq j$. Then each $\ker f_i^{s_i}(T)$ is called a primary invariant subspace of V and V can be decomposed as the direct sum of all primary invariant subspaces

$$V = \bigoplus_{i=1}^{r} \ker f_i^{s_i}(T).$$

Each primary invariant subspace can be decomposed further, cf. [Cla].
Prime invariant subspaces will be the *key* in our attack to YTS' scheme. They have the property that any proper invariant subspace must contain a prime vector, or equivalently intersects nontrivially with a prime invariant subspace. So to find vectors in the desired invariant subspaces, we may search them in prime invariant subspaces rather than in the whole space. This significantly reduces the searching range and thus may amount to fast attacks.

B Attacking the Affine Parts

In this section, we show that if the central map of the bipolar construction is quadratic homogeneous and its variables take value in $\mathbb{F}_q$ with $q > 2$, then the affine parts of the two secret affine maps L, R can be either recovered or illuminated easily. That is, they do not enhance the security at all. Such phenomenon has been investigated for SFLASH in [GSB01, GS03] and also for YTS' scheme in [Has14]. The method is indeed just letting the linear part of the public key be zero and then solving the resulted linear system. It is therefore unnecessary to use affine instead of linear maps for the two secret maps L, R whenever the central map is quadratic homogeneous.
Let $q > 2$ be a power of a prime p where p can be 2 or an odd prime. Assume that $F = (f_1, \ldots, f_m) : \mathbb{F}_q^n \to \mathbb{F}_q^m$ is quadratic homogeneous, i.e. each $f_k(x)$ has nonzero terms of degree two only. Let L, R be two invertible affine maps and $\bar{F} = L \circ F \circ R$. Assume $R(x) = R_0(x + r) = R_0x + R_0r$, $L(y) = L_0y + l$, then

$$\bar{F}(x) = L(F(R(x))) = L_0 \cdot F(R_0(x + r)) + l.$$

Assume we do not know L, R, F but we know $\bar{F}$, and we want to find the affine parts l, r of L, R respectively.
We first write

$$\bar{F}(x) = (x^T A_1 x, \ldots, x^T A_m x)^T + Bx + C,$$

where A_i is an $n \times n$ matrix which can be symmetric or not, B is an $m \times n$ matrix and $C \in \mathbb{F}_q^m$. By assumption, these matrices are known.

$$\bar{F}(x-r) = \begin{pmatrix} x^T A_1 x \\ \vdots \\ x^T A_m x \end{pmatrix} + (B - \begin{pmatrix} r^T(A_1 + A_1^T) \\ \vdots \\ r^T(A_m + A_m^T) \end{pmatrix})x + (\begin{pmatrix} r^T A_1 r \\ \vdots \\ r^T A_m r \end{pmatrix} - Br + C).$$

Compare this equation with

$$\bar{F}(x-r) = L(F(R(x-r))) = L_0 \cdot F(R_0 x) + l.$$

Since F is quadratic homogeneous and $q > 2$, $L_0 \cdot F(R_0 x)$ is quadratic homogeneous — this may not hold if $q = 2$ since $x^T x = x$. Hence we must have

$$L_0 \cdot F(R_0 x) = (x^T A_1 x, \ldots, x^T A_m x)^T,$$

$$B - \begin{pmatrix} r^T(A_1 + A_1^T) \\ \vdots \\ r^T(A_m + A_m^T) \end{pmatrix} = 0,$$

$$l = (r^T A_1 r, \ldots, r^T A_m r)^T - Br + C.$$

The middle equation is an overdetermined linear system of n unknowns and mn equations, and r is a solution to it. As there are much more equations than unknowns, the probability that it has a unique solution is almost one. If it has a unique solution then the original r is recovered; if there are more than one solutions, we can pick a solution r' and calculate correspondingly

$$l' = (r'^T A_1 r', \ldots, r'^T A_m r')^T - Br' + C,$$

and then we have

$$\bar{F}(x - r') - l' = L_0 \cdot F(R_0 x)$$

which involves only the linear parts of L, R and illuminates their affine parts.

We remark that when this approach is applied to higher degree, the resulted system for r is no longer linear but of high degree, because the coefficients of the linear term x contain high degree terms of r. So the situation for high degree is more complicated and needs more sophisticated study.