IEICE TRANS. FUNDAMENTALS, VOL.E99–A, NO.1 JANUARY 2016

PAPER Special Section on Cryptography and Information Security

Cryptanalysis of the Multivariate Signature Scheme Proposed in PQCrypto 2013*

Yasufumi HASHIMOTO[†,††a)], ***Member***

SUMMARY In PQCrypto 2013, Yasuda, Takagi and Sakurai proposed a new signature scheme as one of multivariate public key cryptosystems (MPKCs). This scheme (called YTS) is based on the fact that there are two isometry classes of non-degenerate quadratic forms on a vector space with a prescribed dimension. The advantage of YTS is its efficiency. In fact, its signature generation is eight or nine times faster than Rainbow of similar size. For the security, it is known that the direct attack, the IP attack and the min-rank attack are applicable on YTS, and the running times are exponential time for the first and the second attacks and sub-exponential time for the third attack. In the present paper, we give a new attack on YTS whose approach is to use the diagonalization of matrices. Our attack works in polynomial time and it actually recovers equivalent secret keys of YTS having 140-bits security against min-rank attack in around fifteen seconds.

key words: *multivariate public key cryptosystems, signature scheme, quadratic forms, post-quantum cryptography*

1. Introduction

A Multivariate Public Key Cryptosystem (MPKC) is a cryptosystem whose public key is a set of multivariate quadratic polynomials over a finite field. It is known that the problem of solving systems of randomly chosen multivariate quadratic equations over a finite field is NP-hard [19]. Then MPKC is considered as one of candidates of public key cryptosystems which can resist against the quantum attacks. MPKC also has advantage for efficiency compared with RSA and ECC. In fact, Chen et al. [6] presented in CHES 2009 several MPKC implementations on modern x86 CPUs which are more efficient than RSA and ECC. Until now, various MPKCs have been proposed, e.g. MI [30], HFE [33], Sflash [1], l-IC [12], UOV [26], Rainbow [11], [34], TTS [36]. On the other hand, various attacks on MPKCs (e.g. the direct attacks [2], [5], [8], [10], [14], [15], the rank attacks [7], [16], [22], [24], [27], [36], the differential attacks [9], [13], [17], [18] and the UOV attacks [26], [28]) also have been proposed, and some MPKCs were shown to be insecure against (one of) these attacks [13], [14], [28], [32].

Recently in PQCrypto 2013, Yasuda, Takagi and Sakurai [37] proposed a new signature scheme as one of MPKCs. This scheme (called YTS) is based on the fact that there are two isometry classes of non-degenerate quadratic forms on a vector space with a prescribed dimension [35]. The advantage of YTS is that its signature generation is fast. In fact, it is eight or nine times faster than Rainbow of similar size. For the security, it is known that the direct attack [2], [14], [15], the IP attack [33] and the min-rank attack [36] are applicable on YTS and the running times are exponential times for the first and the second attacks and sub-exponential time for the third attack [37]. Then (at the time of PQCrypto 2013), YTS was considered to be secure enough under suitable parameter selections.

The aim in the present paper is to study the structure of YTS in detail and propose a new attack on YTS. The coefficient matrices of the quadratic forms in the central map of YTS are described by extensions of sparse smaller matrices. Then, taking two linear sums of coefficient matrices of quadratic forms in the public key and multiplying the one and the inversion of the other, the attacker gets a matrix conjugate to a matrix extended from a smaller matrix. Then, by using an approach similar to the diagonalization of this matrix, the attacker can recover partial information of the secret keys. After that, taking several elementary operations in linear algebra, the attacker can recover equivalent secret keys in polynomial time. Actually, we experimentally succeed to recover equivalent secret keys of YTS having 140-bits security against the min-rank attacks [37] in around fifteen seconds (see Sect. 5.5). This means that YTS is not secure at all and it must be repaired for practical use.

2. Notations

Throughout in this paper, we use the following notations.

q: a power of odd prime.
k: a finite field of order q.

For an integer $r \geq 1$,

$\mathrm{M}_r(k)$: the set of $r \times r$ matrices of k-entries.

$\mathrm{SM}_r(k) \subset \mathrm{M}_r(k)$: the set of symmetric matrices.

$I_r \in \mathrm{M}_r(k)$: the identity matrix.

For a matrix A,

A^t: the transpose of A.

For $1 \leq i \leq j \leq r$,

$E_{ij} \in \mathrm{SM}_r(k)$: the symmetric matrix whose (i, j) and (j, i) entries are 1 and other entries are 0, namely

Manuscript received March 17, 2015.
Manuscript revised June 16, 2015.

[†]The author is with the Department of Mathematical Sciences, University of the Ryukyus, Okinawa-ken, 903-0213 Japan.
[††]The author is with CREST, JST, Kawaguchi-shi, 332-0012 Japan.

*The preliminary version of this paper [21] was presented at the 6th International Conference on Post-Quantum Cryptography, held in Waterloo, Canada.

a) E-mail: hashimoto@math.u-ryukyu.ac.jp

DOI: 10.1587/transfun.E99.A.58

$$E_{11} := \begin{pmatrix} 1 & & \\ & & \\ & & \end{pmatrix}, \quad E_{12} := \begin{pmatrix} & 1 & \\ 1 & & \\ & & \end{pmatrix}, \ldots,$$

$$\ldots, E_{rr} := \begin{pmatrix} & & \\ & & \\ & & 1 \end{pmatrix}.$$

For $L_1 \in \mathrm{M}_{r_1}(k), \ldots, L_u \in \mathrm{M}_{r_u}(k)$,

$$L_1 \oplus \cdots \oplus L_u := \begin{pmatrix} L_1 & & \\ & \ddots & \\ & & L_u \end{pmatrix} \in \mathrm{M}_{r_1+\cdots+r_u}(k),$$
$$L_1^{\oplus u} := \underbrace{L_1 \oplus \cdots \oplus L_1}_{u} \in \mathrm{M}_{r_1 u}(k).$$

For $A = \left(a_{ij}\right)_{1\le i,j\le r_1} \in \mathrm{M}_{r_1}(k)$ and $B \in \mathrm{M}_{r_2}(k)$,

$$A \otimes B := \left(a_{ij}B\right)_{1\le i,j\le r_1} \in \mathrm{M}_{r_1 r_2}(k).$$

For a monic polynomial $g(t) := c_0 + c_1 t + \cdots + c_{r-1}t^{r-1} + t^r$ of degree r,

$$C(g) := \begin{cases} (-c_0), & (r = 1), \\ \begin{pmatrix} 0 & \cdots & 0 & -c_0 \\ 1 & & 0 & -c_1 \\ & \ddots & & \vdots \\ 0 & & 1 & -c_{r-1} \end{pmatrix}, & (r \ge 2). \end{cases}$$

For matrices $A = \left(a_{ij}\right)_{1\le i,j\le r} \in \mathrm{M}_r(k)$ and $B = \left(b_{ij}\right)_{1\le i,j\le r} \in \mathrm{SM}_r(k)$,

$$\phi(A) := (a_{11}, \ldots, a_{r1}, a_{12}, \ldots, \ldots, a_{rr})^t \in k^{r^2},$$
$$\psi(B) := (b_{11}, \ldots, b_{r1}, b_{22}, \ldots, \ldots, b_{rr})^t \in k^{r(r+1)/2}.$$

3. The Signature Scheme YTS

In this section, we give a short survey of the signature scheme YTS [37].

3.1 Construction of the Scheme

In a multivariate public key cryptosystem (MPKC), the public key is a set of multivariate quadratic polynomials

$$f_1(x_1, \cdots, x_n) = \sum_{1\le i\le j\le n} a_{ij}^{(1)} x_i x_j + \sum_{1\le i\le n} b_i^{(1)} x_i + c^{(1)},$$
$$\vdots$$
$$f_m(x_1, \cdots, x_n) = \sum_{1\le i\le j\le n} a_{ij}^{(m)} x_i x_j + \sum_{1\le i\le n} b_i^{(m)} x_i + c^{(m)},$$

over a finite field. Yasuda, Takagi and Sakurai [37] proposed at PQCrypto 2013 a multivariate signature scheme using the following two functions of matrices: For an integer $r \ge 1$ and a matrix $X \in \mathrm{M}_r(k)$, let

$$U_1(X) := X^t X, \quad U_\delta(X) := X^t \begin{pmatrix} I_{r-1} & \\ & \delta \end{pmatrix} X,$$

where $\delta \in k$ is chosen such that $\delta \ne \alpha^2$ for any $\alpha \in k$. For these two functions, the following lemma holds.

Lemma 3.1: ([35], [37]) Let $r \ge 1$ be an integer. For any symmetric matrix $Y \in \mathrm{SM}_r(k)$, there exists $X \in \mathrm{M}_r(k)$ satisfying either

$$U_1(X) = Y \qquad \text{or} \qquad U_\delta(X) = Y.$$

Furthermore, such a matrix X can be found in time $O(r^4)$.

See [37] for the detail algorithm finding X. This lemma plays an important role in the process of the signature generation. The signature scheme (called YTS) of Yasuda, Takagi and Sakurai is constructed as follows.

The signature scheme YTS

Let $r \ge 1$ be an integer and put

$$n := r^2, \quad m := r(r+1)/2.$$

Secret Keys: Two invertible affine transforms $S : k^n \to k^n$ and $T : k^m \to k^m$ and an invertible matrix $B \in \mathrm{M}_r(k)$. Note that, for $x \in k^n$ and $y \in k^m$, $S(x)$ and $T(y)$ are given by

$$S(x) = S_0 x + s, \qquad T(y) = T_0 y + t \tag{1}$$

where $S_0 \in \mathrm{M}_n(k), T_0 \in \mathrm{M}_m(k)$ are invertible matrices and $s \in k^n, t \in k^m$ are vectors.

Public Keys: Two quadratic maps $V_1 := T \circ \psi \circ U_1 \circ \phi^{-1} \circ S$ and $V_\delta := T \circ \psi \circ U_\delta \circ B \circ \phi^{-1} \circ S$.

$$V_1 : k^n \xrightarrow{S} k^n \xrightarrow{\phi^{-1}} \mathrm{M}_r(k) \xrightarrow{U_1} \mathrm{SM}_r(k) \xrightarrow{\psi} k^m \xrightarrow{T} k^m$$

$$V_\delta : k^n \xrightarrow{S} k^n \xrightarrow{\phi^{-1}} \mathrm{M}_r(k) \xrightarrow{B} \mathrm{M}_r(k) \xrightarrow{U_\delta} \mathrm{SM}_r(k) \xrightarrow{\psi} k^m \xrightarrow{T} k^m$$

Signature generation: For a message $y \in k^m$, the signature is generated as follows.

Step 1. Compute $z := T^{-1}(y)$. Let $Z := \psi^{-1}(z)$.

Step 2. Find $X \in \mathrm{M}_r(k)$ satisfying either

$$U_1(X) = Z \qquad \text{or} \qquad U_\delta(BX) = Z.$$

Step 3. Let $x := \phi(X)$ and compute $w := S^{-1}(x)$. The signature for $y \in k^m$ is w.

Signature verification: Check whether

$$V_1(w) = y \quad \text{or} \quad V_\delta(w) = y$$

holds.

Thanks to Lemma 3.1, we see that Step 2 in the signature generation can be done in time $O(r^4) = O(n^2)$.

3.2 Quadratic Forms in YTS

In this subsection, we explain the structure of quadratic forms in V_1.

For $X = (x_{ij})_{1\le i,j\le r} \in \mathrm{M}_r(k)$, let

$$x_j := (x_{1j}, \ldots, x_{rj})^t \in k^r,$$
$$x := \phi(X) = (x_{11}, \ldots, x_{r1}, x_{12}, \ldots, \ldots, x_{rr})^t \in k^n.$$

By the definition of U_1, we have

$$U_1(X) = X^t X = \left(x_i^t x_j\right)_{1\le i,j\le r},$$

namely the entries in $U_1(X)$ are as follows.

$$\begin{aligned}
(1,1)\text{-entry:}\quad & x_{11}x_{11} + x_{21}x_{21} + \cdots + x_{r1}x_{r1} \\
& = x^t \begin{pmatrix} I_r & & \\ & & \\ & & \end{pmatrix} x, \\
(1,2)\text{-entry:}\quad & x_{11}x_{12} + x_{21}x_{22} + \cdots + x_{r1}x_{r2} \\
& = x^t \begin{pmatrix} & \frac{1}{2}I_r & \\ \frac{1}{2}I_r & & \\ & & \end{pmatrix} x, \\
& \vdots \\
(r,r)\text{-entry:}\quad & x_{1r}x_{1r} + x_{2r}x_{2r} + \cdots + x_{rr}x_{rr} \\
& = x^t \begin{pmatrix} & & \\ & & \\ & & I_r \end{pmatrix} x,
\end{aligned}$$

Then the (i, j)-entry $u_{ij}(x)$ of $U_1(X)$ is given by

$$u_{ij}(x) = \begin{cases} x^t(E_{ij} \otimes I_r)x, & (i = j), \\ \dfrac{1}{2}x^t(E_{ij} \otimes I_r)x, & (i \neq j). \end{cases} \tag{2}$$

Thus, by the construction of the public key, the quadratic map

$$V_1(x) = (v_{11}(x), \ldots, v_{rr}(x))^t$$

is described as follows.

$$\begin{aligned}
v_{ij}(x) =& x^t S_0^t (T_{ij} \otimes I_r) S_0 x + s^t (T_{ij} \otimes I_r) S_0 x \\
& + x^t S_0^t (T_{ij} \otimes I_r) s + s^t (T_{ij} \otimes I_r) s + t_{ij},
\end{aligned} \tag{3}$$

where S_0, s are given in (1) and $T_{ij} \in \mathrm{SM}_r(k)$, $t_{ij} \in k$ are respectively derived from T_0, t.

3.3 Efficiency and Security of YTS

Based on the results in [37], we list the number of operations for signature generation/verification, the size of keys and the security against known attacks.

Signature generation: $O(n^2 \cdot \log q)$.

Signature verification: Almost same to other schemes in MPKC with the same q, m, n.

Key size: $O(n^3 \cdot \log q)$.

Security against Min-Rank attack: $O(q^{\sqrt{n}} \cdot n^3)$ for recovering T (see also [36]).

Security against IP attack: $O(q^{2n/3})$ for recovering S, T (see also [33]).

Security against Gröbner basis attack: $O(2^{m(3.31-3.62/\log_2 q)})$ for generating a dummy signature under the assumption that $\log_2 q \ll m$ and the quadratic forms in $V_1(x) - y$ or $V_\delta(x) - y$ with the public keys V_1, V_δ and a given message $y \in k^m$ is "semi-regular" (see [2], [3], [14], [15]).

4. Finding S Partially

In this section, we propose an algorithm to recover partial information of S by using the diagonalization approach.

4.1 Diagonalization

In this subsection, we give the following lemma for conjugations of matrices to explain our attack on YTS.

Lemma 4.1: Let $r, d \ge 1$ be integers, $G \in \mathrm{M}_d(k)$ and

$$g(t) := \det(t \cdot I_d - G)$$

the characteristic polynomial of G. Suppose that $g(t)$ is square free and is factored by

$$g(t) = g_1(t) \cdots g_l(t)$$

over k. Put $d_1 := \deg g_1(t), \ldots, d_l := \deg g_l(t)$. Then it holds that
(i) there exists $P \in \mathrm{M}_{rd}(k)$ such that

$$P^{-1}(G \otimes I_r)P = (C(g_1) \oplus \cdots \oplus C(g_l)) \otimes I_r, \tag{4}$$

(ii) if $P_1, P_2 \in \mathrm{M}_{rd}(k)$ satisfy

$$\begin{aligned}
& P_1^{-1}(G \otimes I_r)P_1 = P_2^{-1}(G \otimes I_r)P_2 \\
& = (C(g_1) \oplus \cdots \oplus C(g_l)) \otimes I_r,
\end{aligned}$$

there exist $B_1 \in \mathrm{M}_{rd_1}(k), \ldots, B_l \in \mathrm{M}_{rd_l}(k)$ such that

$$P_2^{-1}P_1 = B_1 \oplus \cdots \oplus B_l. \tag{5}$$

Proof. (i) Recall that the characteristic polynomial $g(t)$ of G is square free. It is known (see e.g. [23]) that, in this case, there exists $A_1 \in \mathrm{M}_d(k)$ such that

$$A_1^{-1} G A_1 = C(g).$$

Since $C(g_1) \oplus \cdots \oplus C(g_l)$ also has the same characteristic polynomial $g(t)$, there exists $A_2 \in \mathrm{M}_d(k)$ such that

$$A_2^{-1}(C(g_1) \oplus \cdots \oplus C(g_l))A_2 = C(g).$$

Thus $P := (A_1 A_2^{-1}) \otimes I_r$ satisfies (4).

(ii) It is easy to see that $B := P_2^{-1}P_1$ satisfies

$$((C(g_1) \oplus \cdots \oplus C(g_l)) \otimes I_r)B$$

$$= B((C(g_1) \oplus \cdots \oplus C(g_l)) \otimes I_r). \quad (6)$$

Divide B by $B = (B_{ab})_{1 \le a,b \le l}$, where B_{ab} is a $d_a r \times d_b r$ matrix. Then the equation (6) gives

$$(C(g_a) \otimes I_r)B_{ab} = B_{ab}(C_(g_b) \otimes I_r), \quad (7)$$

for $1 \le a, b \le l$. We now describe the diagonalization of $C(g_a) \otimes I_r$ by

$$C(g_a) = D_a^{-1}(\alpha_1^{(a)} I_r \oplus \cdots \oplus \alpha_l^{(a)} I_r)D_a, \quad (8)$$

where $\alpha_1^{(a)}, \ldots, \alpha_l^{(a)}$ are elements in an extension field of k and D_a is an invertible $d_a \times d_a$ matrix over an extension field of k. Combining (7) and (8), we have

$$(\alpha_1^{(a)} I_r \oplus \cdots \oplus \alpha_{d_a}^{(a)} I_r)(D_a B_{ab} D_b)$$
$$= (D_a B_{ab} D_b)(\alpha_1^{(b)} I_r \oplus \cdots \oplus \alpha_{d_b}^{(b)} I_r).$$

Since $g(t)$ is square free, the eigenvalues $\alpha_1^{(a)}, \ldots, \alpha_{d_a}^{(a)}$, $\alpha_1^{(b)}, \ldots, \alpha_{d_b}^{(b)}$ are distinct to each other if $a \ne b$. This means that $D_a B_{ab} D_b = 0$ and then $B_{ab} = 0$ for $a \ne b$. Thus (5) holds with $B_1 = B_{11}, \ldots, B_l = B_{ll}$. □

4.2 Finding S Partially

Using Lemma 4.1, we propose the following algorithm to recover partial information of S.

Algorithm 1.

Input: Integers $r, d \ge 1$ and $m = r(r+1)/2$ matrices $F_{11}, \ldots, F_{rr} \in \mathrm{SM}_{dr}(k)$ given by

$$F_{ij} = S_0^t(G_{ij} \otimes I_r)S_0, \qquad (1 \le i \le j \le r)$$

for some $G_{ij} \in \mathrm{SM}_r(k)$ and an invertible $S_0 \in \mathrm{M}_{dr}(k)$.

Output: An integer $1 \le l \le r$, an l-tuple of positive integers $(d_1, \ldots, d_l)$ with $d_1 + \cdots + d_l = d$ and an invertible $P \in \mathrm{M}_{dr}(k)$ satisfying

$$SP = (Q \otimes I_r)(S_1 \oplus \cdots \oplus S_l) \quad (9)$$

for some invertible matrices $Q \in \mathrm{M}_d(k), S_1 \in \mathrm{M}_{d_1 r}(k), \ldots, S_l \in \mathrm{M}_{d_l r}(k)$.

Step 1. If $d = 1$, output $l = 1$, $d_1 = 1$ and $P = I_{dr}$. If not, go to the next step.

Step 2. Take two linear sums W_1, W_2 of $\{F_{ij}\}_{i,j}$ such that W_2 is invertible. Let $W := W_2^{-1}W_1$.

Step 3. Find a monic polynomial $w(t)$ of degree d such that

$$w(W) = 0.$$

Step 4. Factor $w(t)$ over k. If $w(t)$ is irreducible or has a square factor, go back to Step 2 and change W_1 and W_2. If not, let

$$w(t) = w_1(t) \cdots w_l(t)$$

be the factorization of $w(t)$ and go to the next step.

Step 5. For $1 \le u \le l$, choose a $dr \times r$ matrix Y_u such that $w_u(W)Y_u = 0$. Put

$$P := (Y_1, WY_1, \ldots, W^{d_1-1}Y_1,$$
$$Y_2, WY_2, \ldots, W^{d_2-1}Y_2,$$
$$\ldots,$$
$$Y_l, WY_l, \ldots, W^{d_l-1}Y_l) \in \mathrm{M}_{dr}(k),$$

where $d_1 := \deg w_1(t), \ldots, d_l := \deg w_l(t)$.

Step 6. If P is invertible, output

$$\{l, (d_1, \ldots, d_l), P\}.$$

If not, go back to Step 5 and change $Y_1, \ldots, Y_l$.

Since both W_1, W_2 in Step 2 are in the form $S^t(G \otimes I_r)S$ for some $G \in \mathrm{M}_r(k)$, the matrix W is given by

$$W = S^{-1}(W_0 \otimes I_r)S \quad (10)$$

for some $W_0 \in \mathrm{M}_d(k)$. Then there exists a polynomial $w(t)$ of degree d such that $w(W) = 0$ and it is the characteristic polynomial of W_0. It is known that the probability that a randomly chosen polynomial over k of degree d is irreducible is $d^{-1} + O(d^{-1}q^{-d/2})$ (see e.g. [25]) and the probability that a randomly chosen polynomial has a square factor is q^{-1} (see [31]). Then the success probability of Step 4 is considered to be about $1 - d^{-1} - O(q^{-1})$. Remark that, since $\{w(t)\}$ for such W_0 is not necessarily distributed uniformly in a polynomial ring over k, we cannot conclude here that the success probability is in this way. Table 1 shows the probabilities by 10,000 times experiments that the characteristic polynomials of such W_0's satisfy the conditions in Step 4 for $q = 31, 257, 6781$ and $d \le 15$. These probabilities are close to

$$1 - d^{-1} - q^{-1}$$

and we can consider that it is high enough in practice.

The matrix P in Step 5 is for the diagonalization of W. To show it, we now compare WP with $P((C(w_1) \oplus \cdots \oplus C(w_l)) \otimes I_r)$. It is easy to see that

$$WP = (WY_1, \ldots, W^{d_1}Y_1, \ldots,$$
$$\ldots, WY_l, \ldots, W^{d_l}Y_l).$$

On the other hand, by the definition of $C(w_i)$ given in Sect. 2,

Table 1 Success probability (%) of Step 4 in Algorithm 1 by experiments.

$q\backslash d$	2	3	4	5	6	7	8
31	50.3	62.8	71.0	77.0	79.9	83.3	83.9
257	49.9	66.3	74.8	79.6	83.0	84.7	87.2
6781	50.2	67.3	75.4	80.5	84.1	85.5	87.9

9	10	11	12	13	14	15	⋯
85.8	87.0	87.8	88.4	89.7	89.5	89.9	⋯
88.1	89.5	91.2	91.2	91.6	91.9	93.4	⋯
88.6	90.1	90.5	91.5	91.8	92.9	93.7	⋯

we have

$$\begin{aligned}&P((C(w_1)\oplus\cdots\oplus C(w_l))\otimes I_r)\\ =&\Big(WY_1,\ldots,W^{d_1-1}Y_1,\\ &(-c_{0,1}I_r-c_{1,1}W-\cdots-c_{d_1-1,1}W^{d_1-1})Y_1,\\ &\quad\cdots,\\ &WY_l,\ldots,W^{d_l-1}Y_l,\\ &(-c_{0,l}I_r-c_{1,l}W-\cdots-c_{d_l-1,l}W^{d_l-1})Y_l\Big),\end{aligned}$$

where $c_{i,u}\in k$ is given by $w_u(t)=c_{0,u}+c_{1,u}t+\cdots+c_{d_u-1}t^{d_u-1}+t^{d_u}$. Since Y_u satisfies

$$w_u(W)Y_u=0,$$

two matrices WP and $P((C(w_1)\oplus\cdots\oplus C(w_l))\otimes I_r)$ coincides with each other and then it holds

$$P^{-1}WP=(C(w_1)\oplus\cdots\oplus C(w_l))\otimes I_r.$$

Since $W=S^{-1}(W_0\otimes I_r)S$, it is clear that

$$\begin{aligned}&(Q^{-1}\otimes I_r)SWS^{-1}(Q\otimes I_r)\\ &\quad=(C(w_1)\oplus\cdots\oplus C(w_l))\otimes I_r,\end{aligned}$$

where $Q\in \mathrm{M}_d(k)$ is an invertible matrix with

$$Q^{-1}W_0Q=C(w_1)\oplus\cdots\oplus C(w_l).$$

Thus, according to (ii) of Lemma 4.1, we get

$$SP=(Q\otimes I_r)(S_1\oplus\cdots\oplus S_l)$$

for some invertible matrices $S_1\in \mathrm{M}_{d_1r}(k),\ldots,S_l\in \mathrm{M}_{d_lr}(k)$. □

Complexity. Step 2 is for summations, inversions and products of matrices and checking invertibility. Then the complexity of Step 2 is $\ll d^3r^3$. Step 3 is for computing $W^2,\ldots,W^r$ and for finding d coefficients of $w(t)$. Then the complexity of Step 3 is $\ll d^3r^4$. Step 4 is for factoring a polynomial $w(t)$ of degree d. Its complexity is roughly $\ll d^3$ (see e.g. [20]). According to Table 1, we see that Step 4 is repeated less than three times on average. In Step 5, we find kernel matrices and such computations requires at most $ld^3r^3\ll d^4r^3$ operations. Step 6 is for checking the invertibility of P. Thus we conclude that the total complexity of Algorithm 4 is $\ll d^4r^3$.

5. Proposed Attack on YTS

In this section, we propose our attack on YTS, which is to recover invertible affine maps $S':k^n\to k^n$ and $T':k^m\to k^m$ such that

$$\begin{aligned}T'\left(V_1(S'x)\right)=&(U_1\circ\phi^{-1})(x)\\ =&\begin{pmatrix}x^t(E_{11}\otimes I_r)x\\ \vdots\\ x^t(E_{rr}\otimes I_r)x\end{pmatrix}.\end{aligned}\tag{11}$$

It is obvious that, once such S',T' are recovered, the attacker can generate dummy signatures for arbitrary messages.

The algorithm is as follows.

Proposed attack on YTS

Input: The public key $V_1(x)$ of YTS.
Output: Invertible affine maps $S':k^n\to k^n$ and $T':k^m\to k^m$ satisfying (11).

Step 1. Find vectors $s'\in k^n$ and $t'\in k^m$ such that $V_1(x+s')+t'$ is a set of homogeneous quadratic forms. For $1\le i\le j\le r$, let $V_{ij}\in \mathrm{M}_n(k)$ be a matrix such that $V_1(x+s')+t'=\{x^tV_{11}x,\ldots,x^tV_{rr}x\}$.

Step 2. Let $l=1$, $d_1=r$, $P=I_n$ and $F_{ij}=V_{ij}$ for $1\le i\le j\le r$.

Step 3. For $1\le i\le j\le r$ and $1\le u\le l$, let $F_{ij}^{(u)}\in \mathrm{SM}_{rd_u}(k)$ be the matrix given by

$$F_{ij}=\begin{pmatrix}F_{ij}^{(1)}&&*\\ &\ddots&\\ *&&F_{ij}^{(l)}\end{pmatrix}.$$

Use Algorithm 1 for l inputs

$$\{r,d_1,(F_{11}^{(1)},\ldots,F_{rr}^{(1)})\},\ldots,\{r,d_l,(F_{11}^{(l)},\ldots,F_{rr}^{(l)})\}$$

and get their outputs

$$\{l_1,(d_{1,1},\ldots,d_{1,l_1}),P_1\},\ldots,\{l_l,(d_{l,1},\ldots,d_{l,l_l}),P_l\}.$$

Step 4. Replace l with $l_1+\cdots+l_l$,
$(d_1,\ldots,d_l)$ with $(d_{1,1},\ldots,d_{1,l_1},d_{2,1},\ldots,\ldots,d_{l,l_l})$,
P with $P(P_1\oplus\cdots\oplus P_l)$
and F_{ij} with $(P_1\oplus\cdots\oplus P_l)^tF_{ij}(P_1\oplus\cdots\oplus P_l)$.

Step 5. If $l=r$, go to the next step. If not, go back to Step 3

Step 6. Choose (i,j) arbitrary. For $1\le a,b\le r$, let $M_{ab}\in \mathrm{M}_r(k)$ be the matrix given by

$$F_{ij}=(M_{ab})_{1\le a,b\le r}.$$

For $2\le u\le r$, choose $1\le l_u\le r$ such that both M_{l_u1},M_{l_uu} are invertible. If there are no such a pair (M_{l_u1},M_{l_uu}), try it again for another (i,j). Put

$$R_u:=M_{l_uu}^{-1}M_{l_u1}.$$

Replace F_{ij} with $(I_r\oplus R_2\oplus\cdots\oplus R_r)^tF_{ij}(I_r\oplus R_2\oplus\cdots\oplus R_r)$.

Step 7. Find an invertible $L\in \mathrm{M}_r(k)$ such that

$$(L^{\oplus r})^tF_{ij}L^{\oplus r}=D_{ij}\otimes I_r$$

for some $D_{ij}\in \mathrm{SM}_r(k)$. Let

$$\tilde{S}:=P(I_r\oplus R_2\oplus\cdots\oplus R_r)L^{\oplus r}.$$

Step 8. Find an invertible $\tilde{T}\in \mathrm{M}_m(k)$ such that

$$\tilde{T}\begin{pmatrix} D_{11} \\ \vdots \\ D_{rr} \end{pmatrix} = \begin{pmatrix} E_{11} \\ \vdots \\ E_{rr} \end{pmatrix}. \tag{12}$$

Step 9. Output affine maps $S' : k^n \to k^n$ and $T' := k^m \to k^m$ given by

$$S'x = \tilde{S}(x + s'), \quad T'y = \tilde{T}(y + t').$$

We explain in Sects. 5.1–5.3 why this attack can recover an equivalent secret key.

5.1 Step 1

Step 1 is for recovering the contributions of the vectors s and t in the secret keys (1).

Due to (3), we have

$$\begin{aligned} &V_{ij}(x + s') \\ =&x^t S_0^t (T_{ij} \otimes I_r) S_0 x + (s + S_0 s')^t (T_{ij} \otimes I_r) S_0 x \\ &+ x^t S_0^t (T_{ij} \otimes I_r)(s + S_0 s') \\ &+ (s + S_0 s')^t (T_{ij} \otimes I_r)(s + S_0 s') + t_{ij}. \end{aligned} \tag{13}$$

Since S_0 is invertible and the linear terms of $V_{ij}(x + s')$ are given by the second and the third terms in the right hand side of (13), all linear terms of $V_{ij}(x+s')$ vanish for any i, j if and only if

$$s + S_0 s' \in \bigcap_{1 \le i,j \le r} \mathrm{Ker}(T_{ij} \otimes I_r).$$

Such a vector s' can be found by the Gaussian elimination, and once such s' is recovered, we have

$$V_{ij}(x + s') = x^t S_0^t (T_{ij} \otimes I_r) S_0 x + t_{ij}.$$

Then $t' = -t$. □

5.2 Step 2 – 5

Step 2 – 5 is for recovering $P \in \mathrm{M}_n(k)$ such that

$$S_0 P = (Q \otimes I_r)(L_1 \oplus \cdots \oplus L_r) \tag{14}$$

for some invertible $Q, L_1, \ldots, L_r \in \mathrm{M}_r(k)$.

Due to (3), we see that the first input $\{r, r, (V_{11}, \ldots, V_{rr})\}$ is available as an input of Algorithm 1 and its output $\{l, (d_1, \ldots, d_l), P\}$ satisfies that

$$S_0 P = (Q \otimes I_r)(S_1 \oplus \cdots \oplus S_l)$$

for some $Q \in \mathrm{M}_r(k)$, $S_1 \in \mathrm{M}_{d_1 r}(k), \ldots, S_l \in \mathrm{M}_{d_l r}(k)$. Since

$$\begin{aligned} P^t F_{ij} P &= (S_0 P)^t (T_{ij} \otimes I_r)(S_0 P) \\ &= (S_1 \oplus \cdots \oplus S_l)^t ((Q^t T_{ij} Q) \otimes I_r)(S_1 \oplus \cdots \oplus S_l), \end{aligned}$$

the matrix $F_{ij}^{(u)}$ $(1 \le u \le l)$ in Step 3 at the second time is given by

$$S_u^t (T'_{ij} \otimes I_r) S_u$$

for some $T'_{ij} \in \mathrm{M}_{d_u r}(k)$. Then $\{r, d_u, (F_{11}^{(u)}, \ldots, F_{rr}^{(u)})\}$ is also available as an input of Algorithm 1 and its output $\{l_u, (d_{u,1}, \ldots, d_{u,l_u}), P_u\}$ satisfies that

$$S_u P_u = (Q_u \otimes I_r)(S_{u,1} \oplus \cdots \oplus S_{u,l_u})$$

for some $Q_u \in \mathrm{M}_{d_u}(k), S_{u,1} \in \mathrm{M}_{d_{u,1} r}(k), \ldots, S_{u,l_u} \in \mathrm{M}_{d_{u,l_u} r}(k)$. Thus, repeating such operations until l becomes r, one can get P with (14). □

5.3 Step 6 – 8

Step 6 – 8 is for recovering $\tilde{S}$ and $\tilde{T}$ such that

$$\tilde{T}(V_1(\tilde{S}x)) = \begin{pmatrix} x^t (E_{11} \otimes I_r) x \\ \vdots \\ x^t (E_{rr} \otimes I_r) x \end{pmatrix}. \tag{15}$$

Recall that the matrix F_{ij} in Step 6 is given by

$$F_{ij} = P^t V_{ij} P,$$

where the matrix P satisfies (14). Then we see that the matrix F_{ij} in Step 6 is as follows.

$$\begin{aligned} F_{ij} =&P^t V_{ij} P = (S_0 P)^t (T_{ij} \otimes I_r)(S_0 P) \\ =&(L_1 \oplus \cdots \oplus L_r)^t ((Q^t T_{ij} Q) \otimes I_r) \\ &\cdot (L_1 \oplus \cdots \oplus L_r). \end{aligned}$$

This means that M_{ab} in Step 6 is a constant multiple of $L_a^t L_b$ and then R_u is a constant multiple of $L_u^{-1} L_1$. We thus obtain

$$\begin{aligned} &(I_r \oplus R_2 \oplus \cdots \oplus R_r)^t F_{ij} (I_r \oplus R_2 \oplus \cdots \oplus R_r) \\ =&\Big((1 \oplus \alpha_2 \oplus \cdots \oplus \alpha_r) Q^t T_{ij} Q \\ &\cdot (1 \oplus \alpha_2 \oplus \cdots \oplus \alpha_r)\Big) \otimes (L_1^t L_1) \\ =&(\hat{Q}^t T_{ij} \hat{Q}) \otimes (L_1^t L_1), \end{aligned}$$

where $\alpha_2, \ldots, \alpha_r \in k$ and $\hat{Q} := Q(1 \oplus \alpha_2 \oplus \cdots \oplus \alpha_r)$. Any $r \times r$ block of the matrix above is a constant multiple of $L_1^t L_1$. It is easy to see that L in Step 7 can be found by the algorithm for Lemma 3.1.

Since $L^t (L_1^t L_1) L = \beta I_r$ for some $\beta \in k$, the matrix D_{ij} in Step 7 is given by

$$D_{ij} = \beta \hat{Q}^t T_{ij} \hat{Q}.$$

By the definition of T_{ij}, we see that

$$\begin{pmatrix} D_{11} \\ \vdots \\ D_{rr} \end{pmatrix} = \beta T_0 \begin{pmatrix} \hat{Q}^t E_{11} \hat{Q} \\ \vdots \\ \hat{Q}^t E_{11} \hat{Q} \end{pmatrix}.$$

The entries in the right hand side are $r \times r$ symmetric matrices and any $r \times r$ symmetric matrix is expressed by a linear combination of $E_{11}, \ldots, E_{rr}$. Then there exists $T_1 \in \mathrm{M}_m(k)$ such that

$$\begin{pmatrix} \hat{Q}^t E_{11} \hat{Q} \\ \vdots \\ \hat{Q}^t E_{rr} \hat{Q} \end{pmatrix} = T_1 \begin{pmatrix} E_{11} \\ \vdots \\ E_{rr} \end{pmatrix}.$$

The matrix T_1 is known as the "symmetric square" of $\hat{Q}$ and the determinant of T_1 is a power of that of $\hat{Q}$ (its proof is complicated; see the discussions in Chap. 2 of [29]). Thus, there always exists $\tilde{T} = (\beta T_0 T_1)^{-1}$ satisfying (12) and such $\tilde{T}$ can be found by the Gaussian elimination. □

5.4 Total Complexity of the Attack

Step 1 uses the Gaussian elimination for linear equation of $n = r^2$ variables. Then its complexity is $\ll r^6$. In Step 2–5, we use Algorithm 1 at most $r-1$ times. Then its complexity is $\ll r \cdot d^4 r^3 \ll r^8$. In Step 6, we take inversions and multiplications of $r \times r$ matrices $r-1$ times for R_u's and take $2m$ multiplications of special type $n \times n$ matrices for replacing F_{ij}. Then the complexity of Step 6 is $\ll r^7$. In Step 7, we use the algorithm for Lemma 3.1 with $O(r^4)$ operations. In Step 8, we take the Gaussian elimination for m variables. Then its complexity is $\ll r^6$.

We thus conclude that the total complexity of our attack is $\ll r^8 = n^4$.

5.5 Experiments

In this subsection, we describe the results of experiments of our attack for $q = 6781$ and $r \leq 15$. These experiments are done under Windows 7, Core-i7 2.67GHz and Magma ver.2.15-10 [4]. For every experiments, we succeeded to recover equivalent secret keys S', T'. The results are given in Table 2. In this table, "Sec. (bits)" means the security level (bits) of YTS against the min-rank attack or the Gröbner basis attack described in Sect. 3.3, and "Attack (s)" means the average of the running times (seconds) of our attack to recover S', T' by 100 times experiments.

According to Table 2, we see that running times in practice seem around r^7. The paper [37] claimed that YTS of $(q, r) := (6781, 11)$ was secure enough since it had more than 140 bits security. However, Table 2 shows that it is not secure at all.

Table 2 Experiments of our attack for $q = 6781$.

r	5	6	7	8	9	10	11	12	13	14	15
n	25	36	49	64	81	100	121	144	169	196	225
m	15	21	28	36	45	55	66	78	91	105	120
Sec. (bits)	45.4	63.5	84.7	108.9	133.6	147.2	160.8	174.2	187.7	201.0	214.4
Attack (s)	0.04	0.17	0.53	1.41	3.36	7.43	14.7	28.9	63.6	95.5	163

6. Conclusion

In PQCrypto 2013, a new multivariate signature scheme YTS [37] was presented. Its signature generation is fast enough and its structure is quite different to other known MPKCs. Then YTS had been expected as a new idea to build secure and efficient MPKCs. However, the present paper shows that YTS is not secure at all. YTS must be repaired for practical use.

Acknowledgment

The author is partially supported by JSPS Grant-in-Aid for Young Scientists (B) no. 26800020. He would like to thank anonymous reviewers for reading the previous draft carefully and giving helpful comments.

References

[1] M.-L. Akkar, N.T. Courtois, R. Duteuil, and L. Goubin, "A fast and secure implementation of Sflash," Public Key Cryptography — PKC 2003, Lecture Notes in Computer Science, vol.2567, pp.267–278, Springer, 2002.

[2] M. Bardet, J.C. Faugère, B. Salvy, and B.Y. Yang, "Asymptotic expansion of the degree of regularity for semi-regular systems of equations," MEGA'05, 2005.

[3] L. Bettale, J.-C. Faugère, and L. Perret, "Solving polynomial systems over finite fields," Proc. 37th International Symposium on Symbolic and Algebraic Computation, ISSAC'12, pp.67–74, 2012.

[4] W. Bosma, J. Cannon, and C. Playoust, "The magma algebra system I: The user language," J. Symb. Comput., vol.24, no.3-4, pp.235–265, 1997.

[5] C. Bouillaguet, H.-C. Chen, C.-M. Cheng, T. Chou, R. Niederhagen, A. Shamir, and B.-Y. Yang, "Fast exhaustive search for polynomial systems in $\mathbb{F}_2$," Cryptographic Hardware and Embedded Systems, CHES 2010, Lecture Notes in Computer Science, vol.6225, pp.203–218, Springer, 2010.

[6] A.I.-T. Chen, M.-S. Chen, T.-R. Chen, C.-M. Cheng, J. Ding, E.L.-H. Kuo, F.Y.-S. Lee, and B.-Y. Yang, "SSE implementation of multivariate PKCs on modern x86 CPUs," Cryptographic Hardware and Embedded Systems — CHES 2009, Lecture Notes in Computer Science, vol.5747, pp.33–48, Springer, 2009.

[7] D. Coppersmith, J. Stern, S. Vaudenay, "Attacks on the birational permutation signature schemes," Crypto'93, LNCS, vol.773, pp.435–443, 1994.

[8] N. Courtois, A. Klimov, J. Patarin, and A. Shamir, "Efficient algorithms for solving overdefined systems of multivariate polynomial equations," Advances in Cryptology — EUROCRYPT 2000, Lecture Notes in Computer Science, vol.1807, pp.392–407, Springer, 2000.

[9] J. Ding and J.E. Gower, "Inoculating multivariate schemes against differential attacks," Public Key Cryptography — PKC 2006, Lecture Notes in Computer Science, vol.3958, pp.290–301, Springer, 2006.

[10] J. Ding, J.E. Gower, D. Schmidt, C. Wolf, and Z. Yin, "Complexity estimates for the F_4 attack on the perturbed matsumoto-imai cryptosystem," Cryptography and Coding, Lecture Notes in Computer Science, vol.3796, pp.262–277, Springer, 2005.

[11] J. Ding and D. Schmidt, "Rainbow, a new multivariable polynomial signature scheme," Applied Cryptography and Network Security, Lecture Notes in Computer Science, vol.3531, pp.164–175, Springer, 2005.

[12] J. Ding, C. Wolf, and B.-Y. Yang, ℓ-invertible cycles for Multivariate Quadratic (MQ) public key cryptography, PKC'07, LNCS, vol.4450, pp.266–281, 2007.
[13] V. Dubois, P.-A. Fouque, A. Shamir, and J. Stern, "Practical cryptanalysis of SFLASH," Crypto'07, LNCS, Vol.4622, pp.1–12, 2007.
[14] J.-C. Faugére, "A new efficient algorithm for computing Gröbner bases (F_4)," J. Pure Appl. Algebra., vol.139, no.1-3, pp.61–88, 1999.
[15] J.-C. Faugère and A. Joux, "Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases," Advances in Cryptology — CRYPTO 2003, Lecture Notes in Computer Science, vol.2729, pp.44–60, Springer, 2003.
[16] J.C. Faugère, F. Levy-dit-Vehel, and L. Perret, "Cryptanalysis of MinRank," Crypto'08, LNCS, vol.5157, pp.280–296, 2008.
[17] P.-A. Fouque, L. Granboulan, and J. Stern, "Differential cryptanalysis for multivariate schemes," Advances in Cryptology — EUROCRYPT 2005, Lecture Notes in Computer Science, vol.3494, pp.341–353, Springer, 2005.
[18] P.A. Fouque, G. Macario-Rat, L. Perret, and J. Stern, "Total break of the ℓ-IC signature scheme," PKC'08, LNCS, vol.4939, pp.1–17, 2008.
[19] M.R. Garey and D.S. Johnson, Computers and Intractability, A Guide to the Theory of NP-completeness, W.H. Freeman, 1979.
[20] J.V.Z. Gathen and D. Panario, "Factoring polynomials over finite fields: A survey," J. Symb. Comput., vol.31, no.1-2, pp.3–17, 2001.
[21] Y. Hashimoto, "Cryptanalysis of the multivariate signature scheme proposed in PQCrypto 2013," Post-Quantum Cryptography, Lecture Notes in Computer Science, vol.8772, pp.108–125, Springer, 2014.
[22] S. Hasegawa, and T. Kaneko, "An attacking method for a public-key cryptosystem based on the difficulty of solving a system of non-linear equations (in Japanese)," Proc. 10th SITA, vol.JA5-3, 1987.
[23] R. Horn and C. Johnson, Matrix Analysis, Cambridge University Press, Cambridge, 1985.
[24] X. Jiang, L. Hu, J. Ding, and S. Sun, "On the Kipnis-Shamir method solving the MinRank problem," Proc. IWSEC'10 (Short Papers), pp.1–13, 2010.
[25] R. Lidl and H. Niederreiter, Finite Fields, Addison-Wesley, 1983.
[26] A. Kipnis, J. Patarin, and L. Goubin, "Unbalanced oil and vinegar signature schemes," Advances in Cryptology — EUROCRYPT'99, Lecture Notes in Computer Science, vol.1592, pp.206–222, Springer, 1999.
[27] A. Kipnis and A. Shamir, "Cryptanalysis of the HFE public key cryptosystem by relinearization," Advances in Cryptology — CRYPTO'99, Lecture Notes in Computer Science, vol.1666, pp.19–30, Springer, 1999.
[28] A. Kipnis and A. Shamir, "Cryptanalysis of the oil and vinegar signature scheme," Advances in Cryptology — CRYPTO'98, Lecture Notes in Computer Science, vol.1462, pp.257–266, Springer, 1998.
[29] M. Marcus, Finite Dimensional Multilinear Algebra, Pure and Applied Mathematics, vol.23, Marcel Dekker, New York, 1973.
[30] T. Matsumoto and H. Imai, "Public quadratic polynomial-tuples for efficient signature-verification and message-encryption," Eurocrypt'88, LNCS, vol.330, pp.419–453, 1988.
[31] Morrison, Random polynomials over finite fields, 1999.
[32] J. Patarin, "Cryptanalysis of the Matsumoto and Imai public key scheme of eurocrypt'88," Advances in Cryptology — CRYPT0'95, Lecture Notes in Computer Science, vol.963, pp.248–261, Springer, 1995.
[33] J. Patarin, "Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms," Advances in Cryptology — EUROCRYPT'96, Lecture Notes in Computer Science, vol.1070, pp.33–48, Springer, 1996.
[34] A. Petzoldt, S. Bulygin, and J. Buchmann, "CyclicRainbow — A multivariate signature scheme with a partially cyclic public key," Progress in Cryptology — INDOCRYPT 2010, Lecture Notes in Computer Science, vol.6498, pp.33–48, Springer, 2010.
[35] W. Scharlau, Quadratic and Hermitian Forms, Springer, 1987.
[36] B.-Y. Yang and J.-M. Chen, "Building secure tame-like multivariate public-key cryptosystems: The new TTS," Information Security and Privacy, Lecture Notes in Computer Science, vol.3574, pp.518–531, Springer, 2005.
[37] T. Yasuda, T. Takagi, and K. Sakurai, "Multivariate signature scheme using quadratic forms," Post-Quantum Cryptography, Lecture Notes in Computer Science, vol.7932, pp.243–258, Springer, 2013.

Yasufumi Hashimoto received the Ph.D. degree in mathematics from Kyushu university, Fukuoka, Japan, in 2006. He is currently an assistant professor of Department of Mathematical Sciences, University of the Ryukyus. His research interests include cryptography, number theory and representation theory.