IEICE TRANS. FUNDAMENTALS, VOL.E98–A, NO.1 JANUARY 2015

PAPER Special Section on Cryptography and Information Security

Cryptanalysis of the Quaternion Rainbow*

Yasufumi HASHIMOTO[†a)], ***Member***

SUMMARY Rainbow is one of signature schemes based on the problem solving a set of multivariate quadratic equations. While its signature generation and verification are fast and the security is presently sufficient under suitable parameter selections, the key size is relatively large. Recently, Quaternion Rainbow — Rainbow over a quaternion ring — was proposed by Yasuda, Sakurai and Takagi (CT-RSA'12) to reduce the key size of Rainbow without impairing the security. However, a new vulnerability emerges from the structure of quaternion ring; in fact, Thomae (SCN'12) found that Quaternion Rainbow is less secure than the same-size original Rainbow. In the present paper, we further study the structure of Quaternion Rainbow and show that Quaternion Rainbow is one of sparse versions of the Rainbow. Its sparse structure causes a vulnerability of Quaternion Rainbow. Especially, we find that Quaternion Rainbow over even characteristic field, whose security level is estimated as about the original Rainbow of at most 3/4 by Thomae's analysis, is almost as secure as the original Rainbow of at most 1/4-size.

key words: *post-quantum cryptography, multivariate public-key cryptosystems, Rainbow, quaternion ring*

1. Introduction

The multivariate public key cryptosystem (MPKC) is a family of cryptosystems based on the problem of solving a set of multivariate quadratic equations, and is expected to be a post-quantum cryptology. Rainbow [4] is one of signature schemes consisting in MPKC. This is known as a nice scheme in the sense that the signature generations and verifications are faster than RSA and ECC [2] and the security is presently sufficient under suitable parameter selections. However, the key size of Rainbow is relatively large and then reducing it is required for practical implementations.

TTS [15] and Cyclic Rainbow [11] are famous variations of Rainbow whose key sizes are smaller than those in the original Rainbow; the secret keys are smaller in the former scheme and the public keys are smaller in the latter scheme.

Recently, a new Rainbow variant was proposed by Yasuda, Sakurai and Takagi [16]. Their idea is to construct Rainbow on the quaternion ring; thus we call it Quaternion Rainbow. They claimed that the size of secret keys is about 1/4 of the same-size original Rainbow under the same security level. However, a new vulnerability emerges from the structure of the quaternion ring; in fact, Thomae [13] showed that the security of Quaternion Rainbow against rank attacks [15] is less than that expected by the authors of [16].

In the present paper, we further study the structure of Quaternion Rainbow causing its vulnerability. It is well known that there are nontrivial zero divisors in the quaternion ring over a finite field. Taking such zero divisors with several conditions as a basis of the quaternion ring, we show that Quaternion Rainbow is one of sparse versions of the Rainbow. A new vulnerability emerges from its sparse structure. Especially, when the field is of even characteristic, the quadratic forms in Quaternion Rainbow are described by balanced Oil and Vinegar type quadratic forms [3], [9], [10]. Thus the problem of recovering the secret keys of Quaternion Rainbow can be reduced to that of recovering them of the original Rainbow of at most 1/4-size by the Kipnis-Shamir attack [3], [9], [10] in polynomial time. This means that the security level of the Quaternion Rainbow over even characteristic field is almost 1/4 of that expected in [16] and about 1/3 of that estimated by Thomae [13].

2. Rainbow

Rainbow [4] is a signature scheme consisting in MPKC. Throughout this paper, we study the double-layer version of Rainbow for simplicity.

2.1 Scheme

Let q be a power of prime and k a finite field of order q. For integers $o_1, o_2, v \geq 1$, put $m := o_1 + o_2$ and $n := m + v$. The quadratic map $G : k^n \to k^m$ for Rainbow is given as follows.

$$G(x) = (g_1(x), \cdots, g_m(x)), \quad x = (x_1, \cdots, x_n)^t \in k^n,$$

where

$$g_l(x) := \sum_{(i,j)\in L_{l,1}} \alpha_{i,j}^{(l)} x_i x_j + \sum_{i\in L_{l,2}} \beta_i^{(l)} x_i + \gamma^{(l)}$$

with $\alpha_{i,j}^{(l)}, \beta_i^{(l)}, \gamma^{(l)} \in k$ and

$$L_{l,1} := \begin{cases} \{o_1 + 1 \leq i, j \leq n\} \backslash \{o_1 + 1 \leq i, j \leq m\}, \\ \qquad\qquad (1 \leq l \leq o_2), \\ \{1 \leq i, j \leq n\} \backslash \{1 \leq i, j \leq o_1\}, \\ \qquad\qquad (o_2 + 1 \leq l \leq m), \end{cases}$$

Manuscript received March 20, 2014.
Manuscript revised July 4, 2014.

[†]The author is with the Department of Mathematical Sciences, University of the Ryukyus, Okinawa-ken, 903-0213 Japan.

*The preliminary version of this paper [8] was published at the 8th International Workshop on Security (IWSEC 2013), held in Okinawa, Japan.

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

DOI: 10.1587/transfun.E98.A.144

Copyright © 2015 The Institute of Electronics, Information and Communication Engineers

$$L_{l,2} := \begin{cases} \{o_1 + 1 \le i \le n\}, & (1 \le l \le o_2), \\ \{1 \le i \le n\}, & (o_2 + 1 \le l \le m). \end{cases}$$

Note that g_l's are described by

$$g_l(x) = x^t G_l x + (\text{linear form}),$$

where

$$G_l = \begin{cases} \begin{pmatrix} 0_{o_1} & 0 & 0 \\ 0 & 0_{o_2} & * \\ 0 & * & *_v \end{pmatrix}, & (1 \le l \le o_2), \\ \begin{pmatrix} 0_{o_1} & * \\ * & *_{o_2+v} \end{pmatrix}, & (o_2 + 1 \le l \le m). \end{cases} \tag{1}$$

The (o_1, o_2, v)-Rainbow is constructed as follows.

Secret key: The secret keys consists of two invertible affine maps $S : k^n \to k^n$, $T : k^m \to k^m$ and the quadratic map $G : k^n \to k^m$ given above.

Public key: The public key is the convolution

$$F := T \circ G \circ S : k^n \to k^m$$

of three maps S, G, T, namely

$$F : k^n \xrightarrow{S} k^n \xrightarrow{G} k^m \xrightarrow{T} k^m.$$

Signature generation: For a message $y \in k^m$, the signature is given as follows.
Step 1. Compute $z := T^{-1}(y) = (z_1, \cdots, z_m)^t \in k^m$.
Step 2. Choose $r_1, \ldots, r_v \in k$ randomly.
Step 3. Find $x_{o_1+1}, \ldots, x_m \in k$ such that

$$\begin{aligned} g_1(x_1, \cdots, x_m, r_1, \cdots, r_v) &= z_1, \\ &\vdots \\ g_{o_2}(x_1, \cdots, x_m, r_1, \cdots, r_v) &= z_{o_2}. \end{aligned}$$

By the definition of G, the equations above are linear equations of $x_{o_1+1}, \ldots, x_m$. Therefore $x_{o_1+1}, \ldots, x_m$ are found by the Gaussian elimination and are independent on the choice of $x_1, \cdots, x_{o_1}$.
Step 4. For $x_{o_1+1}, \cdots, x_m$ given in Step 3, find $x_1, \cdots, x_{o_1} \in k$ such that

$$\begin{aligned} g_{o_2+1}(x_1, \cdots, x_m, r_1, \cdots, r_v) &= z_{o_2+1}, \\ &\vdots \\ g_m(x_1, \cdots, x_m, r_1, \cdots, r_v) &= z_m. \end{aligned}$$

Similar to Step 3, they can be found by the Gaussian eliminations.
Step 5. The signature for $y \in k^m$ is
$w := S^{-1}((x_1, \cdots, x_m, r_1, \cdots, r_v)^t) \in k^n$.

Signature verification: Check whether $F(w) = y$.

2.2 Major Attacks

Let $F_1, \ldots, F_m$ be $n \times n$ matrices such that the quadratic forms in the public key are given by

$$f_l(x) = x^t F_l x + (\text{linear form}), \quad (1 \le l \le m).$$

By the construction of the public key, F_l's are linear combinations of $S^t G_1 S, \ldots, S^t G_m S$. Note that, if the matrices S_1, T_1 with $SS_1 = \begin{pmatrix} *_{o_1} & * & * \\ 0 & *_{o_2} & * \\ 0 & 0 & *_v \end{pmatrix}$ and $T_1 T = \begin{pmatrix} *_{o_2} & * \\ 0 & *_{o_1} \end{pmatrix}$ are recovered, dummy signatures are generated since the coefficient matrices in $T_1(f_1(S_1 x), \ldots, f_m(S_1 x))^t$ are in the form (1). Three attacks, Kipnis-Shamir's attack, the high-rank attack and the min-rank attack, are well-known for recovering partial information S_1, T_1 of the secret keys S, T of Rainbow. We give short surveys of these attacks.

1. Kipnis-Shamir's attack. This attack was proposed by Kipnis and Shamir [10] on the Oil and Vinegar signature scheme and extended by Kipnis, Patarin and Goubin [9] on the Unbalanced Oil and Vinegar (UOV) signature scheme (see also [3] for even characteristic case). The basic idea of Kipnis-Shamir's attack is roughly described as follows.

Let $N.M, n, m \ge 1$ be integers with $N \le M$, $n := N + M$ and $P_1, \ldots, P_m$ be public $n \times n$-matrices with k-entries. Suppose that $P_1, \ldots, P_m$ are public and are given in the forms

$$P_l = A^t \begin{pmatrix} 0_N & * \\ * & *_M \end{pmatrix} A \qquad (1 \le l \le m) \tag{2}$$

where A is an invertible $n \times n$-matrix. Kipnis-Shamir's attack is to recover an $N \times M$-matrix A_1 such that

$$A \begin{pmatrix} I_N & 0 \\ A_1 & I_M \end{pmatrix} = \begin{pmatrix} *_N & * \\ 0 & *_M \end{pmatrix}. \tag{3}$$

To do it, first take two linear sums W_1, W_2 of $P_1, \ldots, P_m$ such that W_2 is invertible and calculate $W_{12} := W_2^{-1} W_1$. Due to (2), it is easy to see that

$$W_{12} = A^{-1} \begin{pmatrix} *_N & * \\ B & *_M \end{pmatrix} A$$

where the $N \times M$-matrix B is the zero matrix when $N = M$ and is of rank $M - N$ when $M > N$. Thus, we need $O(q^{M-N} \cdot (\text{polyn.})$ operations to recover recovering A_1 with (3). See [3], [9], [10] for the algorithm and the complexity estimations of Kipnis-Shamir's attack in detail.

In Rainbow, since G_l's are given by (1), the public matrices F_l's are in the form $S^t \begin{pmatrix} 0_{o_1} & * \\ * & *_{o_2+v} \end{pmatrix} S$. Then Kipnis-Shamir's attack can recover partial information of S_1 in time $O(q^{v+o_2-o_1} \cdot (\text{polyn.}))$. Once such partial information of S_1 is given, further information of S_1 and T_1 can be recovered by several linear operations and Kipnis-Shamir's attack again.

2. The high-rank attack. The matrices $F_1, \ldots, F_m$ are linear combinations of $S^t G_1 S, \ldots, S^t G_m S$ and are of rank n

in general. Due to (1), removing the contributions of o_1-matrices $S^tG_{o_2+1}S, \ldots, S^tG_mS$ from F_l, we can get the matrix of rank $o_2 + v$. This means that the probability that the matrix $\hat{F} = c_1F_1 + \cdots + c_mF_m$ with randomly chosen $c_1, \ldots, c_m \in k$ is of rank $o_2 + v$ is q^{-o_1}. Then the attacker can find $c_1, \ldots, c_m \in k$ such that $\hat{F}$ is of rank $o_2 + v$ in time $O(q^{o_1} \cdot (\text{polyn.}))$ on average. Note that such $(c_1, \ldots, c_m) \in k^m$ gives a row vector of T_1. It is easy to see that $\hat{F}$ is in the form $S^t\begin{pmatrix} 0_{o_1} & 0 \\ 0 & *_{o_2+v} \end{pmatrix}S$, and then partial information of S_1 is easily recovered by linear operations. Once such partial information of S_1 and T_1 are recovered, further information of S_1 and T_1 can be recovered by several linear operations and the high-rank attack again.

See [5], [12], [15] for the algorithm and the complexity estimations of high-rank attack in detail.

3. The min-rank attack. Since $G_1, \ldots, G_{o_2}$ are of rank $o_2 + v$, there exist $c_1, \ldots, c_m \in k$ such that $\hat{F} = c_1F_1 + \cdots + c_mF_m$ is of rank $o_2 + v$. Choose a column vector $p \in k^m$ randomly and find $c_1, \ldots, c_m$ such that $Hp = 0$. Recall that, if $\hat{F}$ is of rank $o_2 + v$, the dimension of $\ker H$ is $n - (o_2 + v)$. Then the probability that $p \in \ker \hat{F}$ is at least q^{-o_2-v}. This means that $c_1, \ldots, c_m \in k$ with $\text{rank}\hat{F} = o_2 + v$ can be recovered in time $O(q^{v+o_2} \cdot (\text{polyn.}))$ on average. Note that such $(c_1, \ldots, c_m) \in k^n$ gives a row vector of T_1. It is easy to see that $\hat{F}$ is in the form $S^t\begin{pmatrix} 0_{o_1} & 0 \\ 0 & *_{o_2+v} \end{pmatrix}S$, and then partial information of S_1 is recovered by linear operations. Once such partial information of S_1 and T_1 are recovered, further information of S_1 and T_1 can be recovered by several linear operations and the high-rank attack again.

See [5], [12], [15] for the algorithm and the complexity estimations of min-rank attack in detail.

Other than the attacks above, the security against the Gröbner basis attacks [1], [7], the UOV-Reconciliation attacks and the Rainbow Band Separation attacks [6] have been studied. See [12] for experiments of these attacks on Rainbow with smaller n and m.

3. Quaternion Rainbow

In this section, we give a survey of Quaternion Rainbow [16].

3.1 Scheme

Let q be a power of prime and k a finite field of order q. The quaternion ring $Q(k)$ over k is defined by

$$\begin{aligned} Q(k) :=& k + ki + kj + kij \\ =& \{a_1 + a_2i + a_3j + a_4ij \mid a_1, a_2, a_3, a_4 \in k\}, \end{aligned}$$

where i, j satisfy

$$i^2 = j^2 = -1, \quad ij = -ji.$$

Notice that $Q(k)$ is non-commutative when q is odd.

For integers $\tilde{o}_1, \tilde{o}_2, \tilde{v} \geq 1$, put $\tilde{m} := \tilde{o}_1 + \tilde{o}_2$ and $\tilde{n} := \tilde{m} + \tilde{v}$. The secret quadratic map $\tilde{G} : Q(k)^{\tilde{n}} \to Q(k)^{\tilde{m}}$ of Quaternion Rainbow is defined as follows [16].

$$\tilde{g}_l(x) := \sum_{(i,j)\in\tilde{L}_{l,1}} \tilde{x}_i\tilde{\alpha}^{(l)}_{i,j}\tilde{x}_j + \sum_{i\in\tilde{L}_{l,2}} (\tilde{\beta}^{(l)}_{i,1}\tilde{x}_i + \tilde{x}_i\tilde{\beta}^{(l)}_{i,2}) + \tilde{\gamma}^{(l)}$$

where $\tilde{\alpha}^{(l)}_{i,j}, \tilde{\beta}^{(l)}_{i,1}, \tilde{\beta}^{(l)}_{i,2}, \tilde{\gamma}^{(l)} \in k$ and

$$\tilde{L}_{l,1} := \begin{cases} \{\tilde{o}_1 + 1 \leq i, j \leq \tilde{n}\} \backslash \{\tilde{o}_1 + 1 \leq i, j \leq \tilde{m}\}, & \\ & (1 \leq l \leq \tilde{o}_2), \\ \{1 \leq i, j \leq \tilde{n}\} \backslash \{1 \leq i, j \leq \tilde{o}_1\}, & \\ & (\tilde{o}_2 + 1 \leq l \leq \tilde{m}), \end{cases}$$

$$\tilde{L}_{l,2} := \begin{cases} \{\tilde{o}_1 + 1 \leq i \leq \tilde{n}\}, & (1 \leq l \leq \tilde{o}_2), \\ \{1 \leq i \leq \tilde{n}\}, & (\tilde{o}_2 + 1 \leq l \leq \tilde{m}). \end{cases}$$

Denoting

$$\begin{aligned} \tilde{x} &= x_1 + x_2i + x_3j + x_4ij, \\ \tilde{x}' &= x_1^t + x_2^ti + x_3^tj + x_4^tij \end{aligned}$$

with $x_1, x_2, x_3, x_4 \in k^{\tilde{n}}$, we can rewrite $\tilde{g}_l$ in the form

$$\tilde{g}_l(\tilde{x}) = \tilde{x}'\tilde{G}_l\tilde{x} + (\text{linear}), \tag{4}$$

where $\tilde{G}_l$ is an $\tilde{n} \times \tilde{n}$ matrix with $Q(k)$-entries given as follows.

$$\tilde{G}_l = \begin{cases} \begin{pmatrix} 0_{\tilde{o}_1} & 0 & 0 \\ 0 & 0_{\tilde{o}_2} & * \\ 0 & * & *_{\tilde{v}} \end{pmatrix}, & (1 \leq l \leq \tilde{o}_2) \\ \begin{pmatrix} 0_{\tilde{o}_1} & * \\ * & *_{\tilde{o}_2+\tilde{v}} \end{pmatrix}, & (\tilde{o}_2 + 1 \leq l \leq \tilde{m}). \end{cases} \tag{5}$$

Let $\psi : k^{4\tilde{n}} \to Q(k)^{\tilde{n}}$ and $\varphi : Q(k)^{\tilde{m}} \to k^{4\tilde{m}}$ be one-to-one maps given by

$$\begin{aligned} &\psi(a_1, a_2, a_3, a_4) = a_1 + a_2i + a_3j + a_4ij, \\ &\varphi(b_1 + b_2i + b_3j + b_4ij) = (b_1, b_2, b_3, b_4) \end{aligned}$$

for $a_1, a_2, a_3, a_4 \in k^{\tilde{n}}$ and $b_1, b_2, b_3, b_4 \in k^{\tilde{m}}$, and put $G := \varphi \circ \tilde{G} \circ \psi$.

$$G : k^{4\tilde{n}} \xrightarrow{\psi} Q(k)^{\tilde{n}} \xrightarrow{\tilde{G}} Q(k)^{\tilde{m}} \xrightarrow{\varphi} k^{4\tilde{m}}.$$

We now study the quadratic map G. Let $\tilde{G}_{l,1}, \tilde{G}_{l,2}, \tilde{G}_{l,3}, \tilde{G}_{l,4}$ $(1 \leq l \leq \tilde{m})$ be the $\tilde{n} \times \tilde{n}$ matrices with k entries such that

$$\tilde{G}_l = \tilde{G}_{l,1} + \tilde{G}_{l,2}i + \tilde{G}_{l,3}j + \tilde{G}_{l,4}ij$$

and $x := \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$ for $\tilde{x} = x_1 + x_2i + x_3j + x_4ij$. Then we have

$$\begin{aligned} \tilde{x}'\tilde{G}_lx =& (x_1^t + x_2^ti + x_3^tj + x_4^tij) \\ & \cdot (\tilde{G}_{l,1} + \tilde{G}_{l,2}i + \tilde{G}_{l,3}j + \tilde{G}_{l,4}ij) \\ & \cdot (x_1 + x_2i + x_3j + x_4ij) \end{aligned}$$

Table 1 Previous security analysis on quaternion rainbow.

	K-S	M-R	H-R
Original Rainbow	$q^{4\tilde{v}+4\tilde{o}_2-4\tilde{o}_1}$	$q^{4\tilde{v}+4\tilde{o}_2}$	$q^{4\tilde{o}_1}$
Y-S-T [16]	$q^{4\tilde{v}+4\tilde{o}_2-4\tilde{o}_1}$	$q^{4\tilde{v}+4\tilde{o}_2}$	$q^{4\tilde{o}_1}$
Thomae [13] ($2 \nmid q$)	$q^{4\tilde{v}+4\tilde{o}_2-4\tilde{o}_1}$	$q^{4\tilde{v}+3\tilde{o}_2}$	$q^{3\tilde{o}_1}$
Thomae [13] ($2 \mid q$)	$q^{4\tilde{v}+4\tilde{o}_2-4\tilde{o}_1}$	$q^{4\tilde{v}+\tilde{o}_2}$	$q^{3\tilde{o}_1}$

$$
\begin{aligned}
=& x^t \begin{pmatrix} \tilde{G}_{l,1} & -\tilde{G}_{l,2} & -\tilde{G}_{l,3} & -\tilde{G}_{l,4} \\ -\tilde{G}_{l,2} & -\tilde{G}_{l,1} & -\tilde{G}_{l,4} & \tilde{G}_{l,3} \\ -\tilde{G}_{l,3} & \tilde{G}_{l,4} & -\tilde{G}_{l,1} & -\tilde{G}_{l,2} \\ -\tilde{G}_{l,4} & -\tilde{G}_{l,3} & \tilde{G}_{l,2} & -\tilde{G}_{l,1} \end{pmatrix} x \cdot 1 \\
&+ x^t \begin{pmatrix} \tilde{G}_{l,2} & \tilde{G}_{l,1} & \tilde{G}_{l,4} & -\tilde{G}_{l,3} \\ \tilde{G}_{l,1} & -\tilde{G}_{l,2} & -\tilde{G}_{l,3} & -\tilde{G}_{l,4} \\ \tilde{G}_{l,4} & -\tilde{G}_{l,3} & \tilde{G}_{l,2} & -\tilde{G}_{l,1} \\ \tilde{G}_{l,3} & \tilde{G}_{l,4} & \tilde{G}_{l,1} & -\tilde{G}_{l,2} \end{pmatrix} x \cdot i \\
&+ x^t \begin{pmatrix} \tilde{G}_{l,3} & -\tilde{G}_{l,4} & \tilde{G}_{l,1} & \tilde{G}_{l,2} \\ \tilde{G}_{l,4} & \tilde{G}_{l,3} & -\tilde{G}_{l,2} & \tilde{G}_{l,1} \\ \tilde{G}_{l,1} & -\tilde{G}_{l,2} & -\tilde{G}_{l,3} & -\tilde{G}_{l,4} \\ -\tilde{G}_{l,2} & -\tilde{G}_{l,1} & -\tilde{G}_{l,4} & -\tilde{G}_{l,3} \end{pmatrix} x \cdot j \\
&+ x^t \begin{pmatrix} \tilde{G}_{l,4} & \tilde{G}_{l,3} & -\tilde{G}_{l,2} & \tilde{G}_{l,1} \\ -\tilde{G}_{l,3} & \tilde{G}_{l,4} & -\tilde{G}_{l,1} & -\tilde{G}_{l,2} \\ \tilde{G}_{l,2} & \tilde{G}_{l,1} & -\tilde{G}_{l,4} & -\tilde{G}_{l,3} \\ \tilde{G}_{l,1} & -\tilde{G}_{l,2} & -\tilde{G}_{l,3} & -\tilde{G}_{l,4} \end{pmatrix} x \cdot ij.
\end{aligned}
$$

Since $\tilde{G}_{l,1}, \tilde{G}_{l,2}, \tilde{G}_{l,3}, \tilde{G}_{l,4}$ are in the forms (5), it is easy to see that the quadratic map $G : k^{4\tilde{n}} \to k^{4\tilde{m}}$ in the $(\tilde{o}_1, \tilde{o}_2, \tilde{v})$-Quaternion Rainbow is written as G in the $(4\tilde{o}_1, 4\tilde{o}_2, 4\tilde{v})$-Rainbow. Thus, setting two invertible affine maps $S : k^{4\tilde{n}} \to k^{4\tilde{n}}$, $T : k^{4\tilde{m}} \to k^{4\tilde{m}}$ as the secret keys and $F := T \circ G \circ S : k^{4\tilde{n}} \to k^{4\tilde{m}}$ as the public key in the $(\tilde{o}_1, \tilde{o}_2, \tilde{v})$-Quaternion Rainbow, we can interpret $(\tilde{o}_1, \tilde{o}_2, \tilde{v})$-Quaternion Rainbow as a special version of the $(4\tilde{o}_1, 4\tilde{o}_2, 4\tilde{v})$-Rainbow.

3.2 Previous Security Analysis

The authors in [16] claimed that the security levels of the $(\tilde{o}_1, \tilde{o}_2, \tilde{v})$-Quaternion Rainbow and the $(4\tilde{o}_1, 4\tilde{o}_2, 4\tilde{v})$-Rainbow are same. However, Thomae [13] found that, taking linear sums of the coefficient matrices in G, one gets matrices of smaller ranks, and then the security of Quaternion Rainbow against the rank attacks is weaker than the same size original Rainbow. Table 1 summarizes the security levels estimated in [16] and [13]. Note that "K-S", "M-R" and "H-R" means the complexities of Kipnis-Shamir's attack, the min-rank attack and the high ranks respectively.

4. Proposed Security Analysis

In this section, we show that Quaternion Rainbow is one of sparse versions of Rainbow and analyze its security.

4.1 The Case of Odd Characteristic

Study the case that q is odd. Suppose that $a, b \in k$ satisfy

$$a^2 + b^2 = -4^{-1} \tag{6}$$

and put

$$\alpha := 2^{-1} + ai + bij, \qquad \bar{\alpha} := 2^{-1} - ai - bij. \tag{7}$$

It is known that there always exist $a, b \in k$ with (6) (see Lemma 2 in [13]). The following properties of $\alpha, \bar{\alpha} \in Q(k)$ are given by the Eq. (6):

$$
\begin{aligned}
&\alpha^2 = \alpha, \quad \bar{\alpha}^2 = \bar{\alpha}, \quad \alpha\bar{\alpha} = \bar{\alpha}\alpha = 0, \\
&\alpha j = j\bar{\alpha}, \quad \bar{\alpha} j = j\alpha.
\end{aligned} \tag{8}
$$

We now state the following lemma.

Lemma 1. Let k be a finite field of odd characteristic. Then, for any $(a_1, a_2, a_3, a_4) \in k^4$, there exists a unique $(b_1, b_2, b_3, b_4) \in k^4$ such that

$$a_1 + a_2 i + a_3 j + a_4 ij = b_1\alpha + b_2\bar{\alpha} + b_3\alpha j + b_4\bar{\alpha} j, \tag{9}$$

namely $\{\alpha, \bar{\alpha}, \alpha j, \bar{\alpha} j\}$ is a basis of $Q(k)$ over k.

Proof. Equation (9) holds if

$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix} = \begin{pmatrix} 2^{-1} & 2^{-1} & 0 & 0 \\ a & -a & -b & b \\ 0 & 0 & 2^{-1} & 2^{-1} \\ b & -b & a & -a \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{pmatrix}. \tag{10}$$

Due to (6), we see that the square matrix in the right hand side of the equation above is invertible. Thus the claim in this lemma holds. □

According to the properties (8) of $\alpha, \bar{\alpha}$, we can find the following multiplicative properties among the elements in the basis:

$$
\begin{aligned}
&\alpha \cdot \alpha = \alpha, \ \ \alpha \cdot \bar{\alpha} = 0, \ \ \alpha \cdot \alpha j = \alpha j, \ \ \alpha \cdot \bar{\alpha} j = 0, \\
&\bar{\alpha} \cdot \alpha = 0, \ \ \bar{\alpha} \cdot \bar{\alpha} = \bar{\alpha}, \ \ \bar{\alpha} \cdot \alpha j = 0, \ \ \bar{\alpha} \cdot \bar{\alpha} j = \bar{\alpha} j, \\
&\alpha j \cdot \alpha = 0, \ \ \alpha j \cdot \bar{\alpha} = \alpha j, \ \ \alpha j \cdot \alpha j = 0, \ \ \alpha j \cdot \bar{\alpha} j = -\alpha, \\
&\bar{\alpha} j \cdot \alpha = \bar{\alpha} j, \ \ \bar{\alpha} j \cdot \bar{\alpha} = 0, \ \ \bar{\alpha} j \cdot \alpha j = -\bar{\alpha}, \ \ \bar{\alpha} j \cdot \bar{\alpha} j = 0.
\end{aligned}
$$

By using the basis $\{\alpha, \bar{\alpha}, \alpha j, \bar{\alpha} j\}$, we can rewrite the quadratic map $\tilde{G}$ in Quaternion Rainbow as follows:

$$
\begin{aligned}
&\tilde{x} = y_1\alpha + y_2\bar{\alpha} + y_3\alpha j + y_4\bar{\alpha} j, \\
&\tilde{x}' = y_1^t\alpha + y_2^t\bar{\alpha} + y_3^t\alpha j + y_4^t\bar{\alpha} j, \\
&\tilde{g}_l(\tilde{x}) = \tilde{x}'\tilde{G}_l\tilde{x} + (\text{linear form}),
\end{aligned}
$$

where y_1, y_2, y_3, y_4 are unknowns in $k^{\tilde{n}}$ and $\tilde{G}_l$ is an $\tilde{n} \times \tilde{n}$-matrix with $Q(k)$-entries given in (5). Note that, since the entries in $\tilde{G}_l$ are linear sums of $\{\alpha, \bar{\alpha}, \alpha j, \bar{\alpha} j\}$ over k, $\tilde{G}_l$ is given by

$$\tilde{G}_l = H_{l,1}\alpha + H_{l,2}\bar{\alpha} + H_{l,3}\alpha j + H_{l,4}\bar{\alpha} j,$$

where $H_{l,1}, H_{l,2}, H_{l,3}, H_{l,4}$ are $\tilde{n} \times \tilde{n}$-matrices with k-entries in the forms

$$H_{l,1}, H_{l,2}, H_{l,3}, H_{l,4}$$

$$= \begin{cases} \begin{pmatrix} 0_{\tilde{o}_1} & 0 & 0 \\ 0 & 0_{\tilde{o}_2} & * \\ 0 & * & *_{\tilde{v}} \end{pmatrix}, & (1 \le l \le \tilde{o}_2) \\ \begin{pmatrix} 0_{\tilde{o}_1} & * \\ * & *_{\tilde{o}_2+\tilde{v}} \end{pmatrix}, & (\tilde{o}_2+1 \le l \le \tilde{m}). \end{cases} \tag{11}$$

Thus $\tilde{g}_l(\tilde{x})$ is written by

$$\begin{aligned} \tilde{x}'\tilde{G}_l\tilde{x} =& (y_1^t\alpha + y_2^t\bar{\alpha} + y_3^t\alpha j + y_4^t\bar{\alpha} j) \\ & \cdot (H_{l,1}\alpha + H_{l,2}\bar{\alpha} + H_{l,3}\alpha j + H_{l,4}\bar{\alpha} j) \\ & \cdot (y_1\alpha + y_2\bar{\alpha} + y_3\alpha j + y_4\bar{\alpha} j) \\ =& (y_1^t H_{l,1} y_1 - y_4^t H_{l,2} y_3 - y_1^t H_{l,3} y_4 - y_3^t H_{l,4} y_1)\alpha \\ & + (-y_4^t H_{l,1} y_3 + y_2^t H_{l,2} y_2 - y_2^t H_{l,3} y_4 - y_3^t H_{l,4} y_2)\bar{\alpha} \\ & + (y_2^t H_{l,1} y_3 + y_3^t H_{l,2} y_1 + y_1^t H_{l,3} y_2 - y_3^t H_{l,4} y_3)\alpha j \\ & + (y_1^t H_{l,1} y_4 + y_4^t H_{l,2} y_2 - y_4^t H_{l,3} y_4 + y_2^t H_{l,4} y_1)\bar{\alpha} j. \end{aligned} \tag{12}$$

Putting $y := \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix}$, we have

$$\begin{aligned} \tilde{x}'\tilde{G}_l\tilde{x} =& y^t \begin{pmatrix} H_{l,1} & 0_{\tilde{n}} & -\frac{1}{2}H_{l,4} & -\frac{1}{2}H_{l,3} \\ 0_{\tilde{n}} & 0_{\tilde{n}} & 0_{\tilde{n}} & 0_{\tilde{n}} \\ -\frac{1}{2}H_{l,4} & 0_{\tilde{n}} & 0_{\tilde{n}} & -\frac{1}{2}H_{l,2} \\ -\frac{1}{2}H_{l,3} & 0_{\tilde{n}} & -\frac{1}{2}H_{l,2} & 0_{\tilde{n}} \end{pmatrix} y \cdot \alpha \\ & + y^t \begin{pmatrix} 0_{\tilde{n}} & 0_{\tilde{n}} & 0_{\tilde{n}} & 0_{\tilde{n}} \\ 0_{\tilde{n}} & H_{l,2} & -\frac{1}{2}H_{l,4} & -\frac{1}{2}H_{l,3} \\ 0_{\tilde{n}} & -\frac{1}{2}H_{l,4} & 0_{\tilde{n}} & -\frac{1}{2}H_{l,1} \\ 0_{\tilde{n}} & -\frac{1}{2}H_{l,3} & -\frac{1}{2}H_{l,1} & 0_{\tilde{n}} \end{pmatrix} y \cdot \bar{\alpha} \\ & + y^t \begin{pmatrix} 0_{\tilde{n}} & \frac{1}{2}H_{l,3} & \frac{1}{2}H_{l,1} & 0_{\tilde{n}} \\ \frac{1}{2}H_{l,3} & 0_{\tilde{n}} & \frac{1}{2}H_{l,2} & 0_{\tilde{n}} \\ \frac{1}{2}H_{l,1} & \frac{1}{2}H_{l,2} & -H_{l,4} & 0_{\tilde{n}} \\ 0_{\tilde{n}} & 0_{\tilde{n}} & 0_{\tilde{n}} & 0_{\tilde{n}} \end{pmatrix} y \cdot \alpha j \\ & + y^t \begin{pmatrix} 0_{\tilde{n}} & \frac{1}{2}H_{l,4} & 0_{\tilde{n}} & \frac{1}{2}H_{l,1} \\ \frac{1}{2}H_{l,4} & 0_{\tilde{n}} & 0_{\tilde{n}} & \frac{1}{2}H_{l,2} \\ 0_{\tilde{n}} & 0_{\tilde{n}} & 0_{\tilde{n}} & 0_{\tilde{n}} \\ \frac{1}{2}H_{l,1} & \frac{1}{2}H_{l,2} & 0_{\tilde{n}} & -H_{l,3} \end{pmatrix} y \cdot \bar{\alpha} j \\ =:& y^t\tilde{H}_{l,1} y \cdot \alpha + y^t\tilde{H}_{l,2} y \cdot \bar{\alpha} \\ & + y^t\tilde{H}_{l,3} y \cdot \alpha j + y^t\tilde{H}_{l,4} y \cdot \bar{\alpha} j. \end{aligned} \tag{13}$$

For $a_1, a_2, a_3, a_4 \in k^{\tilde{n}}$ and $b_1, b_2, b_3, b_4 \in k^{\tilde{m}}$, let $\psi, \psi_1 : k^{4\tilde{n}} \to Q(k)^{\tilde{n}}$ and $\varphi, \varphi_1 : Q(k)^{\tilde{m}} \to k^{4\tilde{m}}$ be the one-to-one maps as follows:

$$\begin{aligned} &\psi(a_1, a_2, a_3, a_4) = a_1 + a_2 i + a_3 j + a_4 ij, \\ &\psi_1(a_1, a_2, a_3, a_4) = a_1\alpha + a_2\bar{\alpha} + a_3\alpha j + a_4\bar{\alpha} j, \\ &\varphi(b_1 + b_2 i + b_3 j + b_4 ij) = (b_1, b_2, b_3, b_4), \\ &\varphi_1(b_1\alpha + b_2\bar{\alpha} + b_3\alpha j + b_4\bar{\alpha} j) = (b_1, b_2, b_3, b_4). \end{aligned}$$

Due to Lemma 1 and its proof, we see that there exist invertible linear transformations $U : k^{4\tilde{n}} \to k^{4\tilde{n}}$ and $V : k^{4\tilde{m}} \to k^{4\tilde{m}}$ such that

$$\psi = \psi_1 \circ U, \qquad \varphi = V \circ \varphi_1, \tag{14}$$

and U, V are explicitly described by the matrix in (10). According to (13) and (14), we have

$$T \circ \varphi \circ \tilde{G} \circ \psi \circ S = \tilde{T} \circ \tilde{H} \circ \tilde{S},$$

where

$$\begin{aligned} &\tilde{S} := U \circ S : k^{4\tilde{n}} \to k^{4\tilde{n}}, \\ &\tilde{T} := T \circ V : k^{4\tilde{m}} \to k^{4\tilde{m}} \end{aligned}$$

are invertible affine maps and

$$\tilde{H} := \varphi_1 \circ \tilde{G} \circ \psi_1 : k^{4\tilde{n}} \to k^{4\tilde{m}}$$

is a quadratic map whose coefficient matrices in the quadratic forms are given by $\tilde{H}_{l,1}, \tilde{H}_{l,2}, \tilde{H}_{l,3}, \tilde{H}_{l,4}$ $(1 \le l \le \tilde{m})$. This means that the $(\tilde{o}_1, \tilde{o}_2, \tilde{v})$-Quaternion Rainbow proposed in Sect. 3.1 is interpreted by an MPKC scheme such that $\tilde{S}, \tilde{T}$ and $\tilde{H}$ are the secret keys and $F = \tilde{T} \circ \tilde{H} \circ \tilde{S}$ is the public key.

Based on this fact, we now explain how (partial information of) the secret keys $\tilde{S}, \tilde{T}$ are recovered by the rank attacks.

The min-rank attack. Let $F_1, \ldots, F_{4\tilde{n}}$ be the coefficient matrices of the quadratic forms in the public key F. Recall that any F_l $(1 \le l \le 4\tilde{m})$ is a linear combination of $\tilde{S}^t\tilde{H}_{l,1}\tilde{S}, \tilde{S}^t\tilde{H}_{l,2}\tilde{S}, \tilde{S}^t\tilde{H}_{l,3}\tilde{S}, \tilde{S}^t\tilde{H}_{l,4}\tilde{S}$ $(1 \le l \le \tilde{m})$. Due to (11) and (13), we see that the ranks of $\tilde{H}_{l,1}, \tilde{H}_{l,2}, \tilde{H}_{l,3}, \tilde{H}_{l,4}$ for $1 \le l \le \tilde{o}_2$ are $3\tilde{v} + 3\tilde{o}_2$. Then, using the min-rank attack [15] (see also Sect. 2.2), the attacker can recover $c_1, \ldots, c_{4\tilde{m}} \in k$ such that the rank of $\hat{F} := c_1F_1 + \cdots + c_{4\tilde{m}}F_{4\tilde{m}}$ is $3\tilde{v} + 3\tilde{o}_2$ in time $O(q^{3\tilde{v}+3\tilde{o}_2} \cdot (\text{polyn.}))$. Note that $c_1, \ldots, c_{4\tilde{m}}$ are partial information of $\tilde{T}$. Since $\hat{F}$ is in the form $\tilde{S}^tP^t\begin{pmatrix} 0_{4\tilde{n}-3\tilde{v}-3\tilde{o}_2} & 0 \\ 0 & *_{3\tilde{v}+3\tilde{o}_2} \end{pmatrix}P\tilde{S}$ (where P is a permutation matrix), partial information of $\tilde{S}$ is recovered by linear operations. Once such partial information of $\tilde{S}$ and $\tilde{T}$ is recovered, further information of $\tilde{S}$ and $\tilde{T}$ can be recovered by several linear operations and the min-rank attack again.

The high-rank attack. Recall again that any F_l $(1 \le l \le 4\tilde{m})$ is a linear combination of $\tilde{S}^t\tilde{H}_{l,1}\tilde{S}, \tilde{S}^t\tilde{H}_{l,2}\tilde{S}, \tilde{S}^t\tilde{H}_{l,3}\tilde{S}, \tilde{S}^t\tilde{H}_{l,4}\tilde{S}$ $(1 \le l \le \tilde{m})$. Due to (11) and (13), we see that, removing the contributions of $3\tilde{o}_1$ matrices
$\{\tilde{S}^t\tilde{H}_{l,1}\tilde{S}, \tilde{S}^t\tilde{H}_{l,2}\tilde{S}, \tilde{S}^t\tilde{H}_{l,3}\tilde{S}\}_{\tilde{o}_2+1 \le l \le \tilde{m}}$,
$\{\tilde{S}^t\tilde{H}_{l,1}\tilde{S}, \tilde{S}^t\tilde{H}_{l,2}\tilde{S}, \tilde{S}^t\tilde{H}_{l,4}\tilde{S}\}_{\tilde{o}_2+1 \le l \le \tilde{m}}$,
$\{\tilde{S}^t\tilde{H}_{l,1}\tilde{S}, \tilde{S}^t\tilde{H}_{l,3}\tilde{S}, \tilde{S}^t\tilde{H}_{l,4}\tilde{S}\}_{\tilde{o}_2+1 \le l \le \tilde{m}}$
or $\{\tilde{S}^t\tilde{H}_{l,2}\tilde{S}, \tilde{S}^t\tilde{H}_{l,3}\tilde{S}, \tilde{S}^t\tilde{H}_{l,4}\tilde{S}\}_{\tilde{o}_2+1 \le l \le \tilde{m}}$,
from F_l, we get a matrix of rank $4\tilde{n} - \tilde{o}_1$. Then, using the high rank attack [15] (see also Sect. 2.2), the attacker can recover $c_1, \ldots, c_{4\tilde{m}} \in k$ such that the rank of $\hat{F} := c_1F_1 + \cdots + c_{4\tilde{m}}F_{4\tilde{m}}$ is $4\tilde{n} - \tilde{o}_1$ in time $O(q^{3\tilde{o}_1} \cdot (\text{polyn.}))$. Note that $c_1, \ldots, c_{4\tilde{m}}$ are partial information of $\tilde{T}$. Since $\hat{F}$ is in the form $\tilde{S}^tP^t\begin{pmatrix} 0_{\tilde{o}_1} & 0 \\ 0 & *_{4\tilde{n}-\tilde{o}_1} \end{pmatrix}P\tilde{S}$ (where P is a permutation matrix), partial information of $\tilde{S}$ is recovered by linear operations. Once such partial information of $\tilde{S}$ and $\tilde{T}$ is recovered, further information of $\tilde{S}$ and $\tilde{T}$ can be recovered by

several linear operations and the high-rank attack again.

Note that we do not have improvements of Kipnis-Shamir's attack on Quaternion Rainbow over odd characteristic field. It is still an open problem.

4.2 The Case of Even Characteristic

Study the case of even characteristic. Note that $Q(k)$ is commutative since $-1 = 1$ in even characteristic k. Let

$$\alpha := 1 + i, \qquad \beta := 1 + j.$$

Similar to the case of odd characteristic, the following lemma holds.

Lemma 2. Let k be a finite field of even characteristic. Then, for any $(a_1, a_2, a_3, a_4) \in k^4$, there exists a unique $(b_1, b_2, b_3, b_4) \in k^4$ such that

$$a_1 + a_2 i + a_3 j + a_4 ij = b_1 + b_2\alpha + b_3\beta + b_4\alpha\beta, \qquad (15)$$

namely $\{1, \alpha, \beta, \alpha\beta\}$ is a basis of $Q(k)$ over k. □

The multiplicative relations among $1, \alpha, \beta, \alpha\beta$ are as follows:

$$\begin{aligned}
&1 \cdot 1 = 1, \ \ 1 \cdot \alpha = \alpha, \ \ 1 \cdot \beta = \beta, \ \ 1 \cdot \alpha\beta = \alpha\beta,\\
&\alpha \cdot 1 = \alpha, \ \ \alpha \cdot \alpha = 0, \ \ \alpha \cdot \beta = \alpha\beta, \ \ \alpha \cdot \alpha\beta = 0,\\
&\beta \cdot 1 = \beta, \ \ \beta \cdot \alpha = \alpha\beta, \ \ \beta \cdot \beta = 0, \ \ \beta \cdot \alpha\beta = 0,\\
&\alpha\beta \cdot 1 = \alpha\beta, \ \ \alpha\beta \cdot \alpha = 0, \ \ \alpha\beta \cdot \beta = 0, \ \ \alpha\beta \cdot \alpha\beta = 0.
\end{aligned}$$

By using the basis $\{1, \alpha, \beta, \alpha\beta\}$, we can rewrite the quadratic form $\tilde{G}$ as follows:

$$\tilde{x} = y_1 + y_2\alpha + y_3\beta + y_4\alpha\beta, \quad \tilde{g}_l(\tilde{x}) = \tilde{x}^t \tilde{G}_l \tilde{x} + (\text{linear}),$$

where y_1, y_1, y_3, y_4 are unknowns in $k^{\tilde{n}}$ and $\tilde{G}_l$ is an $\tilde{n} \times \tilde{n}$-matrix with $Q(k)$-entries given in (5). Note that, since the entries in $\tilde{G}_l$ are linear sums of $\{1, \alpha, \beta, \alpha\beta\}$ over k, $\tilde{G}_l$ is given by

$$\tilde{G}_l = H_{l,1} + H_{l,2}\alpha + H_{l,3}\beta + H_{l,4}\alpha\beta,$$

where $H_{l,1}, H_{l,2}, H_{l,3}, H_{l,4}$ are $\tilde{n} \times \tilde{n}$-matrices with k-entries in the same forms of (11). Thus $\tilde{g}_l(\tilde{x})$ is written by

$$\begin{aligned}
\tilde{x}^t \tilde{G}_l \tilde{x} =& (y_1^t + y_2^t\alpha + y_3^t\beta + y_4^t\alpha\beta)\\
&\cdot (H_{l,1} + H_{l,2}\alpha + H_{l,3}\beta + H_{l,4}\alpha\beta)\\
&\cdot (y_1 + y_2\alpha + y_3\beta + y_4\alpha\beta)\\
=& y_1^t H_{l,1} y_1 \cdot 1 \qquad (16)\\
&+ (y_1^t H_{l,1} y_2 + y_2^t H_{l,1} y_1 + y_1^t H_{l,2} y_1) \cdot \alpha\\
&+ (y_1^t H_{l,1} y_3 + y_3^t H_{l,1} y_1 + y_1^t H_{l,3} y_1) \cdot \beta\\
&+ (y_1^t H_{l,1} y_4 + y_2^t H_{l,1} y_3 + y_3^t H_{l,1} y_2 + y_4^t H_{l,1} y_1\\
&\quad + y_1^t H_{l,2} y_3 + y_3^t H_{l,2} y_1 + y_2^t H_{l,3} y_1\\
&\quad + y_1^t H_{l,3} y_2 + y_1^t H_{l,4} y_1) \cdot \alpha\beta \qquad (17)
\end{aligned}$$

Putting $y := \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix}$, we have

$$\begin{aligned}
\tilde{x}^t \tilde{G}_l \tilde{x} =& y^t \begin{pmatrix} H_{l,1} & 0_{\tilde{n}} & 0_{\tilde{n}} & 0_{\tilde{n}} \\ 0_{\tilde{n}} & 0_{\tilde{n}} & 0_{\tilde{n}} & 0_{\tilde{n}} \\ 0_{\tilde{n}} & 0_{\tilde{n}} & 0_{\tilde{n}} & 0_{\tilde{n}} \\ 0_{\tilde{n}} & 0_{\tilde{n}} & 0_{\tilde{n}} & 0_{\tilde{n}} \end{pmatrix} y \cdot 1\\
&+ y^t \begin{pmatrix} H_{l,2} & H_{l,1} & 0_{\tilde{n}} & 0_{\tilde{n}} \\ H_{l,1} & 0_{\tilde{n}} & 0_{\tilde{n}} & 0_{\tilde{n}} \\ 0_{\tilde{n}} & 0_{\tilde{n}} & 0_{\tilde{n}} & 0_{\tilde{n}} \\ 0_{\tilde{n}} & 0_{\tilde{n}} & 0_{\tilde{n}} & 0_{\tilde{n}} \end{pmatrix} y \cdot \alpha\\
&+ y^t \begin{pmatrix} H_{l,3} & 0_{\tilde{n}} & H_{l,1} & 0_{\tilde{n}} \\ 0_{\tilde{n}} & 0_{\tilde{n}} & 0_{\tilde{n}} & 0_{\tilde{n}} \\ H_{l,1} & 0_{\tilde{n}} & 0_{\tilde{n}} & 0_{\tilde{n}} \\ 0_{\tilde{n}} & 0_{\tilde{n}} & 0_{\tilde{n}} & 0_{\tilde{n}} \end{pmatrix} y \cdot \beta\\
&+ y^t \begin{pmatrix} H_{l,4} & H_{l,3} & H_{l,2} & H_{l,1} \\ H_{l,3} & 0_{\tilde{n}} & H_{l,1} & 0_{\tilde{n}} \\ H_{l,2} & H_{l,1} & 0_{\tilde{n}} & 0_{\tilde{n}} \\ H_{l,1} & 0_{\tilde{n}} & 0_{\tilde{n}} & 0_{\tilde{n}} \end{pmatrix} y \cdot \alpha\beta\\
=:& y^t \tilde{H}_{l,1} y \cdot 1 + y^t \tilde{H}_{l,2} y \cdot \alpha\\
&+ y^t \tilde{H}_{l,3} y \cdot \beta + y^t \tilde{H}_{l,4} y \cdot \alpha\beta. \qquad (18)
\end{aligned}$$

For $a_1, a_2, a_3, a_4 \in k^{\tilde{n}}$ and $b_1, b_2, b_3, b_4 \in k^{\tilde{m}}$, let $\psi, \psi_1 : k^{4\tilde{n}} \to Q(k)^{\tilde{n}}$ and $\varphi, \varphi_1 : Q(k)^{\tilde{m}} \to k^{4\tilde{m}}$ be the one-to-one maps as follows:

$$\begin{aligned}
&\psi(a_1, a_2, a_3, a_4) = a_1 + a_2 i + a_3 j + a_4 ij,\\
&\psi_1(a_1, a_2, a_3, a_4) = a_1 + a_2\alpha + a_3\beta + a_4\alpha\beta,\\
&\varphi(b_1 + b_2 i + b_3 j + b_4 ij) = (b_1, b_2, b_3, b_4),\\
&\varphi_1(b_1 + b_2\alpha + b_3\beta + b_4\alpha\beta) = (b_1, b_2, b_3, b_4).
\end{aligned}$$

Due to Lemma 2, we see that there exist invertible linear transformations $U : k^{4\tilde{n}} \to k^{4\tilde{n}}$ and $V : k^{4\tilde{m}} \to k^{4\tilde{m}}$ such that

$$\psi = \psi_1 \circ U, \qquad \varphi = V \circ \varphi_1, \qquad (19)$$

and U, V are explicitly given. According to (18) and (19), we have

$$T \circ \varphi \circ \tilde{G} \circ \psi \circ S = \tilde{T} \circ \tilde{H} \circ \tilde{S},$$

where

$$\begin{aligned}
&\tilde{S} := U \circ S : k^{4\tilde{n}} \to k^{4\tilde{n}},\\
&\tilde{T} := T \circ V : k^{4\tilde{m}} \to k^{4\tilde{m}}
\end{aligned}$$

are invertible affine maps and

$$\tilde{H} := \varphi_1 \circ \tilde{G} \circ \psi_1 : k^{4\tilde{n}} \to k^{4\tilde{m}}$$

is a quadratic map whose coefficient matrices in the quadratic forms are given by $\tilde{H}_{l,1}, \tilde{H}_{l,2}, \tilde{H}_{l,3}, \tilde{H}_{l,4}$ ($1 \le l \le \tilde{m}$). This means that the $(\tilde{o}_1, \tilde{o}_2, \tilde{v})$-Quaternion Rainbow proposed in Sect. 3.1 is interpreted by an MPKC scheme such that $\tilde{S}, \tilde{T}$ and $\tilde{H}$ are the secret keys and $F = \tilde{T} \circ \tilde{H} \circ \tilde{S}$ is the public key.

Based on this fact, we now explain how (partial information of) the secret keys $\tilde{S}, \tilde{T}$ are recovered by the rank attacks and the Kipnis-Shamir attack.

The min-rank attack. Let $F_1, \ldots, F_{4\tilde{n}}$ be the coefficient matrices of the quadratic forms in the public key F. These matrices are linear combinations of $\tilde{S}^t\tilde{H}_{l,1}\tilde{S}, \tilde{S}^t\tilde{H}_{l,2}\tilde{S}, \tilde{S}^t\tilde{H}_{l,3}\tilde{S}, \tilde{S}^t\tilde{H}_{l,4}\tilde{S}$ $(1 \le l \le \tilde{m})$. Due to (11) and (18), we see that $\tilde{H}_{l,1}$ $(1 \le l \le \tilde{o}_2)$ is of rank $\tilde{o}_2 + \tilde{v}$. Then there exists $c_1, \ldots, c_{4\tilde{m}} \in k$ such that $\hat{F} = c_1F_1 + \cdots + c_{4\tilde{m}}F_{4\tilde{m}}$ is of rank $\tilde{o}_2 + \tilde{v}$ and the min-rank attack [15] (see also Sect. 2.2) recovers such $c_1, \ldots, c_{4\tilde{m}} \in k$ in time $O(q^{\tilde{v}+\tilde{o}_2}\cdot(\text{polyn.})$. Note that $c_1, \ldots, c_{4\tilde{m}}$ are partial information of $\tilde{T}$. Since $\hat{F}$ is in the form $\tilde{S}^t\begin{pmatrix} *_{\tilde{o}_2+\tilde{v}} & 0 \\ 0 & 0_{4\tilde{n}-\tilde{o}_2-\tilde{v}} \end{pmatrix}\tilde{S}$, partial information of $\tilde{S}$ is recovered by linear operations. Once such partial information of $\tilde{S}$ and $\tilde{T}$ is recovered, further information of $\tilde{S}$ and $\tilde{T}$ can be recovered by several linear operations and the min-rank attack again.

The high-rank attack. The coefficient matrices F_l $(1 \le l \le 4\tilde{m})$ of the public quadratic forms are linear combinations of $\tilde{S}^t\tilde{H}_{l,1}\tilde{S}, \tilde{S}^t\tilde{H}_{l,2}\tilde{S}, \tilde{S}^t\tilde{H}_{l,3}\tilde{S}, \tilde{S}^t\tilde{H}_{l,4}\tilde{S}$ $(1 \le l \le \tilde{m})$. Due to (11) and (18), we see that, removing the contributions of $\tilde{o}_1$ matrices $\tilde{S}^t\tilde{H}_{l,4}\tilde{S}$ $(\tilde{o}_2 + 1 \le l \le \tilde{m})$ from F_l, we get a matrix of rank $4\tilde{n} - \tilde{o}_1$. Then the probability that $\hat{F} = c_1F_1 + \cdots + c_{4\tilde{m}}F_{4\tilde{m}}$ is $4\tilde{n} - \tilde{o}_1$ for randomly chosen $c_1, \ldots, c_{4\tilde{m}} \in k$ is of rank $4\tilde{n} - \tilde{o}_1$ is at least $q^{-\tilde{o}_1}$. This means that the high-rank attack [15] (see also Sect. 2.2) recovers such $c_1, \ldots, c_{4\tilde{m}} \in k$ in time $O(q^{\tilde{o}_1} \cdot (\text{polyn.})$ on average. Note that $c_1, \ldots, c_{4\tilde{m}}$ are partial information of $\tilde{T}$. Since $\hat{F}$ is in the form $\tilde{S}^t\begin{pmatrix} *_{4\tilde{n}-\tilde{o}_1} & 0 \\ 0 & 0_{\tilde{o}_1} \end{pmatrix}\tilde{S}$, partial information of $\tilde{S}$ is recovered by linear operations. Once such partial information of $\tilde{S}$ and $\tilde{T}$ is recovered, further information of $\tilde{S}$ and $\tilde{T}$ can be recovered by several linear operations and the high-rank attack again.

Kipnis-Shamir's attack. For even characteristic cases, we can improve Kipnis-Shamir's attack on Quaternion Rainbow. We now prepare the following lemma which is a minor arrangement of Kipnis-Shamir's attack discussed in Sect. 2.2.

Lemma 3. ([3], [9], [10]) Let $m, n \ge 1$ be integers and $P_1, \ldots, P_m$ be $2n \times 2n$-matrices with k-entries. If $P_1, \ldots, P_m$ are public and are given in the forms

$$P_l = A^t\begin{pmatrix} *_n & * \\ * & 0_n \end{pmatrix}A \qquad (1 \le l \le m)$$

where A is an invertible $2n \times 2n$-matrix, then Kipnis-Shamir's attack [3], [9], [10] recovers an $n \times n$-matrix A_1 such that

$$A\begin{pmatrix} I_n & A_1 \\ 0 & I_n \end{pmatrix} = \begin{pmatrix} *_n & 0 \\ * & *_n \end{pmatrix}$$

in polynomial time of n, m and $\log q$.

Remark that Kipnis-Shamir's attack [9], [10] is usually applied for symmetric matrices. When k is of odd characteristic, the coefficient matrix of a quadratic form can be taken as a symmetric matrix and then it can be applied directly. On the other hand, when k is of even characteristic, the coefficient matrix of most quadratic forms cannot be taken as a symmetric matrix in general and the diagonal entries are zero. The book [3] gives a nice idea (see also [14]) to cover this point that one replaces the coefficient matrix P_l into $\hat{P}_l := P_l + P_l^t$. It is obvious that $\hat{P}_l$ is symmetric and then Kipnis-Shamir's attack is also available for even characteristic cases. See pp.80–84 of [3] for Kipnis-Shamir's attack on even characteristic field in detail.

The situation of Quaternion Rainbow over even characteristic is similar. Since the smaller matrices $H_{l,1}, H_{l,2}, H_{l,3}, H_{l,4}$ $(1 \le l \le \tilde{m})$ are not symmetric, the bigger matrices $\tilde{H}_{l,1}, \tilde{H}_{l,2}, \tilde{H}_{l,3}, \tilde{H}_{l,4}$ $(1 \le l \le \tilde{m})$ and the public matrices F_l $(1 \le l \le 4\tilde{m})$ are not symmetric. However, by taking $\hat{F}_l := F_l + F_l^t$, we can use symmetric matrices for Kipnis-Shamir's attack for Quaternion Rainbow over even characteristic field as follows.

Equation (18) tells that any linear sum of $\tilde{H}_{l,1}, \tilde{H}_{l,2}, \tilde{H}_{l,3}, \tilde{H}_{l,4}$ $(1 \le l \le \tilde{m})$ is in the form $\begin{pmatrix} *_{2\tilde{n}} & * \\ * & 0_{2\tilde{n}} \end{pmatrix}$. Then, due to Lemma 3, Kipnis-Shamir's attack [3], [9], [10] recovers a $2\tilde{n} \times 2\tilde{n}$ matrix M_1 such that

$$\tilde{S}\begin{pmatrix} I_{2\tilde{n}} & M_1 \\ 0 & I_{2\tilde{n}} \end{pmatrix} = \begin{pmatrix} *_{2\tilde{n}} & 0 \\ * & *_{2\tilde{n}} \end{pmatrix}$$

in polynomial time. Put

$$F_l^{(1)} := \begin{pmatrix} I_{2\tilde{n}} & 0 \\ M_1^t & I_{2\tilde{n}} \end{pmatrix}\hat{F}_l\begin{pmatrix} I_{2\tilde{n}} & M_1 \\ 0 & I_{2\tilde{n}} \end{pmatrix}.$$

Since

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\begin{pmatrix} * & * \\ * & 0 \end{pmatrix}\begin{pmatrix} * & 0 \\ * & * \end{pmatrix} = \begin{pmatrix} * & * \\ * & 0 \end{pmatrix},$$
$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\begin{pmatrix} * & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} * & 0 \\ * & * \end{pmatrix} = \begin{pmatrix} * & 0 \\ 0 & 0 \end{pmatrix}, \tag{20}$$

any $F_l^{(1)}$ is in the form $\begin{pmatrix} *_{2\tilde{n}} & * \\ * & 0_{2\tilde{n}} \end{pmatrix}$ and we can find $2\tilde{m}$ linear sums $F_1^{(2)}, \ldots, F_{2\tilde{n}}^{(2)}$ of $F_1^{(1)}, \ldots, F_{4\tilde{n}}^{(1)}$ in the forms $\begin{pmatrix} *_{2\tilde{n}} & 0 \\ 0 & 0_{2\tilde{n}} \end{pmatrix}$ by the Gaussian eliminations. Note that $F_l^{(2)}$ $(1 \le l \le 2\tilde{m})$ is a linear sum of $\begin{pmatrix} I_{2\tilde{n}} & 0 \\ M_1^t & I_{2\tilde{n}} \end{pmatrix}\tilde{S}^t\tilde{H}_{l,1}\tilde{S}\begin{pmatrix} I_{2\tilde{n}} & M_1 \\ 0 & I_{2\tilde{n}} \end{pmatrix}$ and $\begin{pmatrix} I_{2\tilde{n}} & 0 \\ M_1^t & I_{2\tilde{n}} \end{pmatrix}\tilde{S}^t\tilde{H}_{l,2}\tilde{S}\begin{pmatrix} I_{2\tilde{n}} & M_1 \\ 0 & I_{2\tilde{n}} \end{pmatrix}$ $(1 \le l \le \tilde{m})$.

Equation (18) tells that the upper left block of any linear sum of $\tilde{H}_{l,1}, \tilde{H}_{l,2}$ $(1 \le l \le \tilde{m})$ is in the form $\begin{pmatrix} *_{\tilde{n}} & * \\ * & 0_{\tilde{n}} \end{pmatrix}$. Then, due to Lemma 3, Kipnis-Shamir's attack recovers an $\tilde{n} \times \tilde{n}$ matrix M_2 such that

$$\tilde{S}\begin{pmatrix} I_{2\tilde{n}} & M_1 \\ 0 & I_{2\tilde{n}} \end{pmatrix}\begin{pmatrix} I_{\tilde{n}} & M_2 & 0 \\ 0 & I_{\tilde{n}} & 0 \\ 0 & 0 & I_{2\tilde{n}} \end{pmatrix} = \begin{pmatrix} *_{\tilde{n}} & 0 & 0 \\ * & *_{\tilde{n}} & 0 \\ * & * & *_{2\tilde{n}} \end{pmatrix} \tag{21}$$

in polynomial time. Put

$$F_l^{(3)} := \begin{pmatrix} I_{\tilde{n}} & 0 & 0 \\ M_2^t & I_{\tilde{n}} & 0 \\ 0 & 0 & I_{2\tilde{n}} \end{pmatrix}\begin{pmatrix} I_{2\tilde{n}} & 0 \\ M_1^t & I_{2\tilde{n}} \end{pmatrix}F_l^{(2)}\begin{pmatrix} I_{2\tilde{n}} & M_1 \\ 0 & I_{2\tilde{n}} \end{pmatrix}\begin{pmatrix} I_{\tilde{n}} & M_2 & 0 \\ 0 & I_{\tilde{n}} & 0 \\ 0 & 0 & I_{2\tilde{n}} \end{pmatrix}$$

$(1 \le l \le 2\tilde{m})$. We see that any $F_l^{(3)}$ is in the form $\begin{pmatrix} *_{\tilde{n}} & * & 0 \\ * & 0_{\tilde{n}} & 0 \\ 0 & 0 & 0_{2\tilde{n}} \end{pmatrix}$

and we can find $\tilde{m}$ linear sums $F_1^{(4)}, \ldots, F_{\tilde{m}}^{(4)}$ of $F_1^{(3)}, \ldots, F_{2\tilde{m}}^{(3)}$ in the forms $\begin{pmatrix} *_{\tilde{n}} & 0 \\ 0 & 0_{3\tilde{n}} \end{pmatrix}$ by the Gaussian eliminations. Since the upper left blocks of $F_l^{(4)}$ $(1 \le l \le \tilde{m})$ is a linear sums of $\tilde{S}_1^t H_{l,1} \tilde{S}_1$ $(1 \le l \le \tilde{m})$ with an $\tilde{n} \times \tilde{n}$ invertible matrix $\tilde{S}_1$, the quadratic forms derived from $F_1^{(4)}, \ldots, F_{\tilde{n}}^{(4)}$ correspond to those in the $(\tilde{o}_1, \tilde{o}_2, \tilde{v})$-Rainbow.

Now let $\tilde{F}(x) = (\tilde{f}_1(x), \ldots, \tilde{f}_{4\tilde{m}}(x))$ be the quadratic map given by

$$\tilde{f}_l(x) := \begin{cases} x^t F_l^{(4)} x + (\text{linear}), & (1 \le l \le \tilde{m}), \\ x^t F_l^{(3)} x + (\text{linear}), & (\tilde{m}+1 \le l \le 2\tilde{m}), \\ x^t F_l^{(1)} x + (\text{linear}), & (2\tilde{m}+1 \le l \le 4\tilde{m}) \end{cases}$$

$$= \begin{cases} x^t \begin{pmatrix} *_{\tilde{n}} & 0 \\ 0 & 0_{3\tilde{n}} \end{pmatrix} x + (\text{linear}), \\ \qquad\qquad (1 \le l \le \tilde{m}), \\ x^t \begin{pmatrix} *_{\tilde{n}} & * & 0 \\ * & 0_{\tilde{n}} & 0 \\ 0 & 0 & 0_{2\tilde{n}} \end{pmatrix} x + (\text{linear}), \\ \qquad\qquad (\tilde{m}+1 \le l \le 2\tilde{m}), \\ x^t \begin{pmatrix} *_{2\tilde{n}} & * \\ * & 0_{2\tilde{n}} \end{pmatrix} x + (\text{linear}), \\ \qquad\qquad (2\tilde{m}+1 \le l \le 4\tilde{m}). \end{cases}$$

Since $\tilde{F} = \hat{T}^{-1} \circ F \circ \hat{S}^{-1}$ with two invertible affine maps $\hat{S} : k^{4\tilde{n}} \to k^{4\tilde{n}}$ derived from M_1, M_2 and $\hat{T} : k^{4\tilde{m}} \to k^{4\tilde{m}}$ derived from the maps $\{F_l^{(1)}\} \mapsto \{F_l^{(2)}\}, \{F_l^{(3)}\} \mapsto \{F_l^{(4)}\}$, inverting $\tilde{F}$ is equivalent to doing F. In order to find $x = (x_1, \ldots, x_{4\tilde{n}})$ with $\tilde{F}(x) = z$ for given $z = (z_1, \ldots, z_{4\tilde{m}})$, we compute as follows.

Step 1. Find $x_1, \ldots, x_{\tilde{n}}$ such that $\tilde{f}_1(x) = z_1, \ldots, \tilde{f}_{\tilde{m}}(x) = z_{\tilde{m}}$.
Step 2. For $x_1, \ldots, x_{\tilde{n}}$ given in Step 1, find $x_{\tilde{n}+1}, \ldots, x_{2\tilde{n}}$ such that $\tilde{f}_{\tilde{m}+1}(x) = z_{\tilde{m}+1}, \ldots, \tilde{f}_{2\tilde{m}}(x) = z_{2\tilde{m}}$.
Step 3. For $x_1, \ldots, x_{2\tilde{n}}$ given in Step 1 and 2, find $x_{2\tilde{n}+1}, \ldots, x_{4\tilde{n}}$ such that $\tilde{f}_{2\tilde{m}+1}(x) = z_{2\tilde{m}+1}, \ldots, \tilde{f}_{4\tilde{m}}(x) = z_{4\tilde{m}}$.

Once $x_1, \ldots, x_{\tilde{n}}$ are fixed, $\tilde{f}_{\tilde{m}+1}(x) = z_{\tilde{m}+1}, \ldots, \tilde{f}_{2\tilde{m}}(x) = z_{2\tilde{m}}$ are linear equations of $\tilde{n}$ variables $x_{\tilde{n}+1}, \ldots, x_{2\tilde{n}}$. Furthermore, once $x_1, \ldots, x_{2\tilde{n}}$ are fixed, $\tilde{f}_{2\tilde{m}+1}(x) = z_{2\tilde{m}+1}, \ldots, \tilde{f}_{4\tilde{m}}(x) = z_{4\tilde{m}}$ are linear equations of $2\tilde{n}$ variables $x_{2\tilde{n}+1}, \ldots, x_{4\tilde{n}}$. Then Step 2 and 3 are computed by the Gaussian eliminations in polynomial time. Recall that finding a solution of $\tilde{f}_1(x) = z_1, \ldots, \tilde{f}_{\tilde{m}}(x) = z_{\tilde{m}}$ is equivalent to generating a dummy signature of the $(\tilde{o}_1, \tilde{o}_2, \tilde{v})$-Rainbow. then the $(\tilde{o}_1, \tilde{o}_2, \tilde{v})$-Quaternion Rainbow over even characteristic field is as secure as the $(\tilde{o}_1, \tilde{o}_2, \tilde{v})$ original Rainbow. Recall Sect. 2.2 that we need $O(q^{\tilde{v}+\tilde{o}_2-\tilde{o}_1} \cdot (\text{polyn.}))$ operations to recover partial information of the secret keys of the $(\tilde{o}_1, \tilde{o}_2, \tilde{v})$-Rainbow by Kipnis-Shamir's attack for generating dummy signatures. Thus we conclude that the complexity of the $(\tilde{o}_1, \tilde{o}_2, \tilde{v})$-Quaternion Rainbow over even characteristic field against Kipnis-Shamir's attacks is $q^{\tilde{v}+\tilde{o}_2-\tilde{o}_1} \cdot (\text{polyn.})$.

5. Conclusion

In the present paper, we show that Quaternion Rainbow is one of sparse versions of Rainbow (see (13) and (18)) and estimate the security of Quaternion Rainbow against Kipnis-Shamir's attack [3], [9], [10] and the rank attacks [15]. Table 2 summarizes the complexities of the $(\tilde{o}_1, \tilde{o}_2, \tilde{v})$ Quaternion Rainbow.

Table 2 Comparisons of the security analysis on quaternion rainbow.

	K-S	M-R	H-R
Original Rainbow	$q^{4\tilde{v}+4\tilde{o}_2-4\tilde{o}_1}$	$q^{4\tilde{v}+4\tilde{o}_2}$	$q^{4\tilde{o}_1}$
Y-S-T [16]	$q^{4\tilde{v}+4\tilde{o}_2-4\tilde{o}_1}$	$q^{4\tilde{v}+4\tilde{o}_2}$	$q^{4\tilde{o}_1}$
Thomae [13] $(2 \nmid q)$	$q^{4\tilde{v}+4\tilde{o}_2-4\tilde{o}_1}$	$q^{4\tilde{v}+3\tilde{o}_2}$	$q^{3\tilde{o}_1}$
Proposed $(2 \nmid q)$	$q^{4\tilde{v}+4\tilde{o}_2-4\tilde{o}_1}$	$q^{3\tilde{v}+3\tilde{o}_2}$	$q^{3\tilde{o}_1}$
Thomae [13] $(2 \mid q)$	$q^{4\tilde{v}+4\tilde{o}_2-4\tilde{o}_1}$	$q^{4\tilde{v}+\tilde{o}_2}$	$q^{3\tilde{o}_1}$
Proposed $(2 \mid q)$	$q^{\tilde{v}+\tilde{o}_2-\tilde{o}_1}$	$q^{\tilde{v}+\tilde{o}_2}$	$q^{\tilde{o}_1}$

Due to the forms (13) and (18) of the quadratic forms in Quaternion Rainbow, we see that the securities of Quaternion Rainbow against these attacks for both odd and even characteristic cases are weaker than expected by the authors of [16]. Especially, the Quaternion Rainbow over even characteristic field is almost as secure as the original Rainbow of $1/4$ size. Thus, Quaternion Rainbow is less practical than the original Rainbow. We consider that such vulnerabilities emerge from less randomness of the distribution of coefficients in quadratic forms and then preserving its randomness will be required to build secure and efficient schemes.

The authors of [16] recently claimed in [17] that, the security levels against Gröbner basis attack, the UOV-Reconciliation attack and the Rainbow Band Separation attack of Quaternion Rainbow on odd characteristic field are almost same to those of the original Rainbow, and then Quaternion Rainbow of odd characteristic is almost as secure as the original Rainbow in practice. However, their claim that the security levels of Quaternion Rainbow and the original Rainbow against such attacks are almost same has no evidence (at least in [17]). Moreover, further attacks using the forms (13) might be proposed in the near future. Therefore, to check whether their claim in [17] is true, we need to await developments of security analysis for some years ahead.

References

[1] 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.
[2] A.I.T. Chen, M.S. Chen, T.R. Chen, C.M. Chen, J. Ding, E.L.H. Kuo, F.Y.S. Lee, and B.Y. Yang, "SSE Implementation of Multivariate PKCs on Modern x86 CPUs," CHES'09, Lect. Notes Comput. Sci. 5747, pp.33–48, 2009.
[3] J. Ding, J.E. Gower, and D.S. Schmidt, Multivariate public key cryptosystems, Springer, Heidelberg, 2006.
[4] J. Ding and D. Schmidt, "Rainbow, a new multivariate polynomial signature scheme," ACNS'05, Lect. Notes Comput. Sci. 3531, pp.164–175, 2005.
[5] J. Ding and B. Yang, "Multivariate public key cryptography," Post-Quantum Cryptography, pp.193–241, 2009.
[6] J. Ding, B. Yang, C. Chen, M. Chen, and C. Cheng, "New differential-algebraic attacks and reparametrization of rainbow," ACNS'08, Lect. Notes Comput. Sci. 5037, pp.242–257, 2008.

[7] J.C. Faugère, "A new efficient algorithm for computing Grobner bases (F_4)," J. Pure and Applied Algebra 139 pp.61–88, 1999.
[8] Y. Hashimoto, "Cryptanalysis of the Quaternion Rainbow," IWSEC'13, Lect. Notes Comput. Sci. 8231, pp.244–257, 2013.
[9] A. Kipnis, J. Patarin, and L. Goubin, "Unbalanced oil and vinegar signature schemes," Eurocrypt'99, Lect. Notes Comput. Sci. 1592, pp.206–222, 1999. extended in citeseer/231623.html, 2003-06-11.
[10] A. Kipnis and A. Shamir, Cryptanalysis of the Oil and Vinegar signature scheme, Crypto'98, Lect. Notes Comput. Sci. 1462, pp.257–267, 1998.
[11] A. Petzoldt, S. Bulygin, and J. Buchmann, "CyclicRainbow — A multivariate signature scheme with a partially cyclic public key," Indocrypt'10, Lect. Notes Comput. Sci. 6498, pp.33–48, 2010.
[12] A. Petzoldt, S. Bulygin, and J. Buchmann, "Selecting parameters for the Rainbow signature scheme," PQC'10, Lect. Notes Comput. Sci. 6061, pp.218–240, 2010.
[13] E. Thomae, "Quo Vadis Quaternion? Cryptanalysis of Rainbow over non-commutative rings," SCN'12, Lect. Notes Comput. Sci. 7485, pp.361–363, 2012.
[14] C. Wolf, A. Braeken, and B. Preneel, "On the security of stepwise triangular systems," Des., Codes Cryptogr., vol.40, pp 285–302, 2006.
[15] B.Y. Yang and J.M. Chen, "Building secure tame-like multivariate public-key cryptosystems: The new TTS," ACISP'05, Lect. Notes Comput. Sci. 3574, pp.518–531, 2005.
[16] T. Yasuda, K. Sakurai, and T. Takagi, Reducing the Key Size of Rainbow using Non-commutative Rings, CT-RSA'12, Lect. Notes Comput. Sci. 7178, pp.68–83, 2012.
[17] T. Yasuda, T. Takagi, K. Sakurai, "Security of multivariate signature scheme using non-commutative rings," IEICE Trans. Fundamentals, vol.E97-A, no.1, pp.245–252, Jan. 2014.

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.