Efficient variant of Rainbow using sparse secret keys

Takanori Yasuda[1*], Tsuyoshi Takagi[2], and Kouichi Sakurai[1,3]
[1] *Institute of Systems, Information Technologies and Nanotechnologies, Fukuoka, Japan*
[2] *Institute of Mathematics for Industry, Kyushu University, Fukuoka, Japan*
takagi@imi.kyushu-u.ac.jp
[3] *Department of Informatics, Kyushu University, Fukuoka, Japan*
sakurai@csce.kyushu-u.ac.jp

Abstract

Multivariate Public Key Cryptosystems (MPKC) is one of candidates for post-quantum cryptography. Rainbow is an MPKC digital signature scheme, with relatively efficient encryption and decryption processes. However, the size of the secret key of Rainbow is substantially larger than that of an RSA cryptosystem for the same security level. By using sparse secret keys, the size of the secret key of Rainbow can be reduced. In addition, a method using sparse secret keys can accelerate the signature generation of Rainbow. Matrix-based Rainbow and NT-Rainbow, which we previously proposed, are variants of Rainbow using sparse secret keys. These two variants of Rainbow reduce the size of the secret key of Rainbow, and improve the efficiency of the signature generation of Rainbow. In this paper, we combine these two variants of Rainbow. As a consequence, the combined scheme realizes even smaller size of the secret key and even more efficient signature generation than those of the two variants of Rainbow. In particular, in comparison with the original Rainbow, the secret key is reduced in size by about 76% and the signature generation is sped up by about 55% at the security level of 100 bits.

Keywords: Post-quantum cryptography, Multivariate public key cryptosystems, Rainbow.

1 Introduction

Multivariate public key cryptosystems (MPKC) [1, 2] are candidates for post-quantum cryptography. Their security is based on the level of difficulty involved in finding solutions to a system of multivariate quadratic equations (MQ problem). Many MPKC schemes require secret and public keys that are larger than those of RSA and ECC. In recent years, a variety of MPKC schemes for encryption and for signatures, have been proposed. Unbalanced Oil and Vinegar (UOV) [3] is an MPKC signature scheme, whose signatures can be efficiently generated and verified. Rainbow [4] is a multilayer variant of UOV, with enhanced security. UOV and Rainbow both share the same problem of having large secret and public keys.

By using sparse secret keys, the size of the secret key of Rainbow can be reduced. Several variants of Rainbow using sparse secret keys have been proposed, e.g. Enhanced TTS[5], Matrix-based Rainbow[6], and NT-Rainbow[7]. These schemes can not only reduce the size of secret keys, but also improve the efficiency of the signature generation of Rainbow. In this paper, we propose a new variant of Rainbow into which Matrix-based Rainbow and NT-Rainbow are combined. The part which becomes sparse in the secret keys in Matrix-based Rainbow and that in NT-Rainbow are mutually exclusive. Therefore, we can combine these two schemes into a new scheme. Our proposed scheme has even smaller size of the secret key and even more efficient signature generation than those of Matrix-based Rainbow and NT-Rainbow.

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 5, number: 3, pp. 3-13

*Corresponding author: Institute of Systems, Information Technologies and Nanotechnologies, Momochihama 2–1–22, Sawara-ku, Fukuoka-shi, Fukuoka 814–0001, Japan, Tel: +81-92-852-3465, Email: yasuda@isit.or.jp

This paper analyzes the security of our scheme. In particular, we investigate the effect to our scheme for well-known attacks against Rainbow, Finally, we evaluate the security parameter of our scheme for several security levels on the basis of our security analysis and the results in [6] and [7]. We also compare the secret key length and efficiency of signature generation of our scheme with those of the corresponding Rainbow. In particular, in comparison with the original Rainbow, the size of the secret key of our scheme is reduced by about 76% and signature generation is about 55% faster at the security level of 100 bits.

2 Original Rainbow

Ding and Schmidt proposed a signature scheme called Rainbow, which is a multilayer variant of Unbalanced Oil and Vinegar [4].

First, we define parameters that determine the layer structure of Rainbow. Let t be the number of layers in Rainbow. Let $v_1, \ldots, v_{t+1}$ be a sequence of $t+1$ positive integers such that $0 < v_1 < v_2 < \cdots < v_t < v_{t+1}$. For $i = 1, \ldots, t$, the set of indices of the i-th layer in Rainbow is defined by all integers from v_i to v_{i+1}, namely $O_i = \{v_i + 1, v_i + 2, \ldots, v_{i+1} - 1, v_{i+1}\}$. The number of indices for the i-th layer, O_i is then $v_{i+1} - v_i$, and this is denoted by $o_i = v_{i+1} - v_i$. Note that the smallest integer in O_1 is $v_1 + 1$. Upon defining $V_1 = \{1, 2, \ldots, v_1\}$, and for $i = 2, 3, \ldots, t+1$, we have

$$V_i = V_1 \cup O_1 \cup O_2 \cup \cdots \cup O_{i-1} = \{1, 2 \ldots, v_i\}.$$

The number of elements in V_i is exactly v_i for $i = 1, 2, \ldots, t+1$. The sets O_i and V_i are used for the respective indices of the Oil and Vinegar variables in Rainbow. We define $n = v_{t+1}$ as the maximum number of variables used in Rainbow.

Next, let K be a finite field of order q. Rainbow consists of t layers of n variables polynomials. For $h = 1, 2, \ldots, t$, the h-th layer of Rainbow contains the following system of o_h multivariate polynomials: For $k \in O_h$,

$$g_k(x_1, \ldots, x_n) = \sum_{i \in O_h, j \in V_h} \alpha_{i,j}^{(k)} x_i x_j + \sum_{i,j \in V_h, i \le j} \beta_{i,j}^{(k)} x_i x_j + \sum_{i \in V_{h+1}} \gamma_i^{(k)} x_i + \eta^{(k)}, \tag{1}$$

where $\alpha_{i,j}^{(k)}, \beta_{i,j}^{(k)}, \gamma_i^{(k)}, \eta^{(k)} \in K$. We call the variables x_i $(i \in O_h)$ and x_j $(i \in V_j)$ Oil and Vinegar variables, respectively. The central map of Rainbow is constructed according to $G = (g_{v_1+1}, \ldots, g_n) : K^n \to K^{n-v_1}$.

Note that a system of o_h equations, $g_k(b_1, \ldots, b_{v_h}, x_{v_h+1}, \ldots, x_{v_{h+1}}) = a_k$ $(k \in O_h)$ becomes o_h linear equations in o_h variables for any $(a_{v_h+1}, \ldots, a_{v_{h+1}}) \in K^{o_h}$ and $(b_1, \ldots, b_{v_h}) \in K^{v_h}$. Therefore, once we know the values of the Oil variables in the h-th layer, we can then compute the values of the Vinegar variables in the $(h+1)$-th layer. This is the trapdoor mechanism of Rainbow.

2.1 Scheme of Rainbow

Now let us describe the key generation, signature generation, and verification processes of Rainbow.

Key Generation. The secret key consists of a central map G and two affine transformations $A_1 : K^m \to K^m$ $(m = n - v_1)$, $A_2 : K^n \to K^n$. The public key consists of the field K and the composed map $F = A_1 \circ G \circ A_2 : K^n \to K^m$, which is a system of m quadratic polynomials of n variables over K. We denote the public key by $F = (f_{v_1+1}, \ldots, f_n)^{\mathrm{T}}$, where T denotes the transpose operation. In addition, we use f_k to denote the k-th public polynomial of F for $k = v_1 + 1, \ldots, n$.

Signature Generation. Let $\mathbf{M} \in K^m$ be a message. We compute $\mathbf{A} = A_1^{-1}(\mathbf{M})$, $\mathbf{B} = G^{-1}(\mathbf{A})$ and $\mathbf{C} = A_2^{-1}(\mathbf{B})$ in that order. The signature of the message is $\mathbf{C} \in K^n$. Note that the inverse of G can be

efficiently computed. In fact, for any vector $w = (w_1, \ldots, w_m)^T \in K^m$, an element $G^{-1}(w)$ in the inverse image of w can be obtained as follows:

Step 1 Randomly choose $s'_1, \ldots, s'_{v_1} \in K$.

Step 2 For $i = 1, \ldots, t$, do the following operations:
A system $g^{(v_i+1)}, \ldots, g^{(v_i+o_i)}$ can be regarded as a multivariate quadratic system with variables $x_1, \ldots, x_{v_i+o_i}$. Upon substituting $(x_1, \ldots, x_{v_i}) = (s'_1, \ldots, s'_{v_i})$, set up a system of linear equations of o_i variables. Solve the system and obtain a solution $(x_{v_i+1}, \ldots, x_{v_i+o_i}) = (s'_{v+1}, \ldots, s'_n)$. (If the system is not regular, go back to Step 1.)

Result $G^{-1}(w) = (s'_1, \ldots, s'_n)$.

Verification. If $F(\mathbf{C}) = \mathbf{M}$, the signature is accepted; it is rejected otherwise.

This scheme is denoted as Rainbow$(K; v_1, o_1, \ldots, o_t)$, and we call $v_1, o_1, \ldots, o_t$ the parameters of Rainbow.

3 Matrix-based Rainbow and NT-Rainbow

In this section, we explain the idea of reduction of the size of secret key using in Matrix-based Rainbow and NT-Rainbow.

3.1 Basic Idea of Matrix-based Rainbow

The key idea underlying Matrix-based Rainbow is a modification of linear equations appearing in Step 2 of the Rainbow signature generation process. In Step 2 of the Rainbow signature generation process, for each i-th layer, we need to solve a system of linear equations described as

$$L.X = V \tag{2}$$

where L is a matrix of size $o_i \times o_i$, V is a column vector of size o_i and X is a column vector of variables of size o_i. In case of Rainbow, L is a general matrix. However, Matrix-based Rainbow uses a form of L as

$$L = \left(\begin{array}{c|c|c|c} A & 0 & \cdots & 0 \\ \hline 0 & A & \cdots & 0 \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline 0 & 0 & \cdots & A \end{array}\right) \tag{3}$$

where A is a matrix of size $o'_i \times o'_i$ for some divisor o'_i of o_i. L as in (3) can be made by taking a special and sparse set of $\alpha^{(k)}_{i,j}$'s appearing in (1). Since $\alpha^{(k)}_{i,j}$'s are part of the secret key of Rainbow, the secret key of Matrix-based Rainbow is shorter than that of Rainbow.

There is another reason why the above diagonal matrix is adopted as L for Matrix-based Rainbow. For L in (3), the system of linear equations (2) can be transformed into another system of linear equations,

$$A.X' = V' \tag{4}$$

where X', V' are matrices of size $o'_i \times (o_i/o'_i)$ corresponding to X, V, respectively. System (4) can be solved simultaneously with respect to the columns of variables in X'. If Gaussian elimination is used to solve (4), the cost of field multiplications is estimated to be $O({o'_i}^3)$. On the other hand, the cost of field multiplications to solve (2) is $O({o_i}^3)$. Therefore, Matrix-based Rainbow is more efficient at signature generation than the original Rainbow.

3.2 Basic Idea of NT-Rainbow

We focus on the terms

$$\sum_{i,j\in S_h, i\leq j} \beta_{i,j}^{(k)} x_i x_j \tag{5}$$

appearing in (1), which composes the secret key of Rainbow. Using a square matrix of size $v_h \times v_h$,

$$B = \begin{pmatrix} \beta_{1,1}^{(k)} & \beta_{1,2}^{(k)} & \cdots & \beta_{1,v_h}^{(k)} \\ 0 & \beta_{2,2}^{(k)} & * & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \beta_{v_h v_h}^{(k)} \end{pmatrix},$$

the quadratic polynomial (5) is described as

$$\mathbf{x}.B.\mathbf{x}^T \quad (\mathbf{x} = (x_1, \ldots, x_{v_h})). \tag{6}$$

However, in case of NT-Rainbow, (5) is not described by the form using an upper-triangular matrix B. For each layer of NT-Rainbow, first, a general square matrix D is prepared:

$$D = \begin{pmatrix} \delta_{1,1} & \cdots & \cdots & \delta_{1,v_h} \\ \vdots & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ \delta_{v_h,1} & \cdots & \cdots & \delta_{v_h,v_h} \end{pmatrix},$$

After that, using the circulated matrix D_l of D,

$$D_l = \begin{pmatrix} \delta_{v_h-l+1,1} & \cdots & \cdots & \delta_{v_h-l+1,v_h} \\ \delta_{v_h-l+2,1} & \cdots & \cdots & \delta_{v_h-l+2,v_h} \\ \vdots & \vdots & & \vdots \\ \delta_{v_h-l,1} & \cdots & \cdots & \delta_{v_h-l,v_h} \end{pmatrix},$$

quadratic polynomials (5) for several k are generated by the form $\mathbf{x}.D_l.\mathbf{x}^T$ for several l. In general, it is difficult to recover D from the set of these quadratic polynomials $\mathbf{x}.D_l.\mathbf{x}^T$.

In the original Rainbow, $o_h(= v_{h+1} - v_h)$ triangular matrices are needed to describe the secret key, whereas in NT-Rainbow, only one matrix D is needed. Therefore, the secret key of NT-Rainbow is shorter than that of Rainbow. Once we compute $D.\mathbf{x}^T$, the result is reused for computing $\mathbf{x}.D_l.\mathbf{x}^T$ for any l. Therefore, NT-Rainbow has an efficient signature generation.

4 A New Variant of Rainbow

Matrix-based Rainbow reduces a part of $\alpha_{i,j}^{(k)}$ in appearing (1), which composes the secret key of Rainbow. On the other hand, NT-Rainbow reduces a part of $\beta_{i,j}^{(k)}$ in appearing (1). Therefore, we can combine these two schemes. In this section, we describe the procedure of the combined scheme concretely.

4.1 Construction of the Secret Key

Here, we explain how to construct the secret key of the combined scheme of Matrix-based Rainbow and NT-Rainbow.

Let $v_1, v_2, \ldots, v_{t+1}$ be $t+1$ positive integers, as in § 2.1. For $h = 1, \ldots, t$, we write $S_h = \{1, \ldots, v_h\}$, $O_h = \{v_h + 1, \ldots, v_{h+1}\}$, and $o_h = v_{h+1} - v_h$. The number of equations and variables in the multivariate quadratic system used in the scheme is $n = v_{t+1}$ and $m = n - v_1$, respectively. Assume that for all $h = 1, \ldots, t$, o_h can be factored as $o_h = d_h o'_h$ for some positive number o'_h, d_h. In addition, for any $h = 1, \ldots, t$, it is assumed that $v_h \geq o_h$.

We first randomly generate the following matrices and vectors over K: For all $h = 1, \ldots, t$,

1. $\mathbf{a}_l^{(h)}$: matrix of size $v_h \times o'_h \quad (l = 1, \ldots, o'_h)$,
2. $\mathbf{b}_l^{(h)} \in K^{o'_h} \quad (l = 1, \ldots, o'_h)$,
3. $\mathbf{d}^{(h)} = (\delta_{i,j}^{(h)})$: matrix of size $v_h \times v_h$,
4. $B_{00}^{(v_h+l)} \in K^{v_h} \quad (l = 1, \ldots, o'_h)$,
5. $C^{(v_h+l)} \in K \quad (l = 1, \ldots, o'_h)$.

The secret key of our scheme consists of the above data. We will describe the central map $G : K^n \to K^m$ corresponding to the secret key. The central map $G = (g^{(v_1+1)}, \ldots, g^{(n)})$ is composed of quadratic polynomials $g^{(k)}$ of the form

$$g^{(k)}(\mathbf{x}) = \mathbf{x}^T A^{(k)} \mathbf{x} + B^{(k)} \mathbf{x} + C^{(k)}, \quad (\mathbf{x} = (x_1, \ldots, x_n)^T). \tag{7}$$

Here, $A^{(k)}$ is a square matrix over K of size $n \times n$ expressed by

$$A^{(v_h+l)} = \left(\begin{array}{c|c} A_0^{(v_h+l)} & 0 \\ \hline 0 & 0 \end{array} \right) \quad (h = 1, \ldots, t,\ l = 1, \ldots, o_i),$$

where $A_0^{(v_h+l)}$ $(l = 1, \ldots, o_h)$ are square matrices with size v_{h+1} of the form

$$A_0^{(v_h+l)} = \left(\begin{array}{c|c} A_{00}^{(v_h+l)} & A_{01}^{(v_h+l)} \\ \hline 0 & 0 \end{array} \right)$$

where $A_{00}^{(v_h+l)} = (c_{i,j})$ is a upper triangular matrix of size $v_h \times v_h$ defined by

$$c_{i,j} = \begin{cases} \delta_{i-l+1,j}^{(h)} + \delta_{j-l+1,i}^{(h)} & \text{if } i < j, \\ \delta_{i-l+1,i}^{(h)} & \text{if } i = j, \\ 0 & \text{otherwise,} \end{cases}$$

and $A_{01}^{(v_h+l)}$ is a matrix of size $v_h \times o_h$ defined by

$$A_{01}^{(v_h+io'_h+j)} = (\overbrace{\mathbf{0}, \ldots, \mathbf{0}}^{io'_h}, \mathbf{a}_j^{(h)}, \overbrace{\mathbf{0}, \ldots, \mathbf{0}}^{(d_h-i-1)o'_h}) \quad (0 \leq i < d_h, 0 < j \leq o'_h).$$

(**0** represents a column vector.) $B^{(k)}$ is a vector in K^n expressed in the form,

$$B^{(v_h+l)} = (B_0^{(v_h+l)}, \overbrace{0,\ldots,0}^{n-v_{h+1}}) \ \ (h=1,\ldots,t, l=1,2,\ldots,o_h).$$

Here, $B_0^{(v_h+l)}$ is a vector in $K^{v_{h+1}}$ given by

$$B_0^{(v_h+l)} = (B_{00}^{(v_h+l)}, B_{01}^{(v_h+l)})$$

where $B_{01}^{(v_h+l)} \in K^{o_h}$ is defined by

$$B_{01}^{(v_h+io'_h+j)} = (\overbrace{0,\ldots,0}^{io'_h}, \mathbf{b}_j^{(h)}, \overbrace{0,\ldots,0}^{(d_h-i-1)o'_h}) \ \ (0 \le i < d_h, 0 < j \le o'_h).$$

4.2 Our Scheme

Here, we describe the key generation, the signature generation and the verification of our scheme.

• **Key generation**

Secret key $\mathbf{a}_l^{(h)}$, $\mathbf{b}_l^{(h)}$, $\mathbf{d}^{(h)}$, $B_{00}^{(v_h+l)}$, $C^{(v_h+l)}$ given in the last subsection, and two randomly chosen affine transformations $L : K^m \to K^m$ and $R : K^n \to K^n$.

Public key The public key consists of the composite map $F = L \circ G \circ R : K^n \to K^m$ for G defined in the last subsection.

• **Signature generation** Let $\mathbf{M} \in K^m$ be a message. To generate a signature $\mathbf{S}$ from $\mathbf{M}$, first compute $\mathbf{M}' = L^{-1}(\mathbf{M})$. Next compute an element $\mathbf{S}' = G^{-1}(\mathbf{M}')$ in the inverse image of $\mathbf{M}'$, and finally compute $\mathbf{S} = R^{-1}(\mathbf{S}')$. $G^{-1}(\mathbf{M}')$ is computed using the improved algorithm described above. $L^{-1}(\mathbf{M})$ and $R^{-1}(\mathbf{S}')$ can be easily computed since L and R are affine transformations, .
• **Verification** If $F(\mathbf{S}) = \mathbf{M}$, the signature is accepted. It is rejected otherwise.

We denote this scheme by MNT-Rainbow$(K; v_1, d_1 * o'_1, \ldots, d_t * o'_t)$ and call $v_1, d_1, o'_1, \ldots, d_t, o'_t$ the parameter.

5 Security Analysis for Our Scheme

Now let us analyze the security of our scheme for several attacks against Rainbow.

5.1 Security against Direct Attacks

Direct attacks [8, 9, 10, 11, 12] are the most straightforward attacks to forge a signature for a message $\mathbf{M}$ by solving the system $F(\mathbf{x}) = \mathbf{M}$ of public equations using an algorithm such as XL or a Gröbner Basis method. We experimentally compared the time taken by direct attacks against our scheme MNT-Rainbow$(GF(256); v_1, d_1 * o'_1, d_2 * o'_2)$ over against the time taken by the same attack against Rainbow$(GF(256); v_1, o_1, o_2)$ where $o_i = d_i \cdot o'_i$ $(i = 1, 2)$. The experiment used the gröbner basis implemented in Magma. The table 1 lists the results: It shows that there is no significant difference between the times of those schemes.

Table 1: Comparison of Time Taken by Direct Attacks over $GF(256)$

(v_1, o_1, o_2)	(4,3,4)	(5,3,4)	(3,4,4)
Our scheme	5.32 s	11.71 s	13.81 s
Rainbow	5.34 s	11.70 s	13.84 s
Random system	5.36 s	11.72 s	13.88 s

5.2 Security against UOV-Reconciliation attack and Rainbow-Band-Separation Attack

UOV-Reconciliation attack [13, 14] and Rainbow-Band-Separation attack [13, 14] aim to reveal the secret key using solvers of system of multivariate equations.

Tables 2 and 3 show the results of our experiments with MAGMA against UOV-Reconciliation attack and Rainbow-Band-Separation attack, respectively. These tables compare the result for our scheme with that for the original Rainbow scheme over $GF(256)$. As the tables show, UOV-Reconciliation attack and Rainbow-Band-Separation attack against our scheme cannot be significantly faster than those against the original Rainbow scheme.

Table 2: Results of the experiments with UOV-R attack over $GF(256)$

$(v_1, d_1 * o'_1, d_2 * o'_2)$	(4,4*1,1*5)	(5,5*1,2*2)	(5,5*1,1*5)
Our scheme	5.13 s	9.30 s	14.20 s
Rainbow	5.10 s	9.33 s	14.21 s

Table 3: Results of the experiments with RBS attack over $GF(256)$

$(v_1, d_1 * o'_1, d_2 * o'_2)$	(3,1*3,2*2)	(4,1*3,2*2)	(5,1*3,2*2)
Our scheme	3.57 s	7.89 s	17.48 s
Rainbow	3.57 s	7.87 s	17.46 s

5.3 Security against HighRank Attack

We can write $g^{(2)}_{v_1+1}, \ldots, g^{(2)}_n$ for the quadratic parts of the components of the central map $G = (g_{v_1+1}, \ldots, g_n)$. Each $g^{(2)}_i$ is expressed by $g^{(2)}_i(\mathbf{x}) = \mathbf{x}.T_i.\mathbf{x}^T$, $(\mathbf{x} = (x_1, \ldots, x_n))$ using a triangular matrix T_i of size n. The symmetric matrix S_i $(i = v_1 + 1, \ldots, n)$ is defined by $S_i = T_i + T_i^T$, and we can write $\mathscr{A} = \mathrm{Span}_K\{S_{v_1+1}, \ldots, S_n\}$.

The HighRank attack[15, 13, 16] finds a matrix in $\mathscr{A}$ with the maximal rank (not full rank), and it spends most of its times in this process. The computation has the following steps.

Step 1 Choose $M \in \mathscr{A}$ randomly.
Step 2 Determine whether M is regular. If M is regular, then return to Step 1
Output M.

The complexity of HighRank attack against our scheme is the same as that of Matrix-based Rainbow. From the security analysis in [6], we have the following proposition.

Proposition 1. *If $q > 2$ and $v_t > o_t + o'_t - d_t$ then the complexity of HighRank attack against our scheme is $q^{o'_t - d_t + 1} \cdot n^3/12$* **m**.

Here, **m** denotes the field multiplication.

5.4 Security against MinRank Attack

We use the same notation as in the last subsection. MinRank attack [15, 5, 17] finds a matrix in $\mathscr{A}$ with the minimal rank (not equal to zero), and it spends most of its times in this process.

The complexity of MinRank attack against our scheme is the same as that of Matrix-based Rainbow. From the security analysis in [6], we have the following proposition.

Proposition 2. *The complexity of a MinRank attack against our scheme is* $q^{v_1} \cdot m(n^2/2 - m^2/6)$ **m**.

5.5 Security against UOV Attack

The space spanned by the variables $x_{v_t+1}, \ldots, x_n$ is a simultaneously isotropic space with respect to $g^{(2)}_{v_1+1}, \ldots, g^{(2)}_n$. Here, a subspace W of a vector space V with a quadratic form g is said to be isotropic if $v_1, v_2 \in V \Rightarrow g(v_1, v_2) = 0$.

The UOV attack[18, 19, 10] finds the simultaneously isotropic space by using the following steps.

Step 1 Randomly choose $M_1, M_2 \in \mathscr{A}$ such that M_2 is regular.
Step 2 Compute a proper invariant subspace W of $M_{1,2} = M_1 M_2^{-1}$. If there is no invariant subspace, return to Step 1.
Output W.

Considering the construction of $\alpha^{(k)}_{i,j}$'s in our scheme, the probability that $M_{1,2}$ has an invariant subspace is equal to $1/q^{n-2o_t}$. Therefore, the complexity of the UOV attack is $q^{n-2o_t-1}o_t^3$ field multiplication[19].

6 Examples and Comparison

Using our security analysis and the result of Petzoldt et al. [14], we have that $\mathscr{S}_1 =$ MNT-Rainbow$(GF(256);$ $18, 14*1, 1*14)$ corresponds to the security levels of 80-bits, and $\mathscr{S}_2 =$ MNT-Rainbow(GF(256);31, $19*1, 2*12)$ corresponds to the security levels of 100-bits. $\mathscr{S}_1$ and $\mathscr{S}_2$ have the same security as Rainbow$(GF(256); 18, 14, 14)$ and Rainbow$(GF(256); 31, 19, 24)$, respectively. We compare the secret key lengths and the efficiencies of the signature generation of our scheme and the original Rainbow for these parameters. Table 4 compares the secret key sizes, and Table 5 compares the efficiencies of the signature generation. In Table 5, the time taken by a C-Language implementation. We used gcc and an Intel Core i5 2.67GHz CPU with 4GB RAM.

7 Conclusion

We presented a variant of Rainbow, that has a smaller secret key and faster signature generation process compared with the original. We analyzed the security of our scheme against known attacks such as direct attacks. In addition, we presented an explicit parameter of our scheme for several security levels. Our test proves that our scheme is 55% faster than Rainbow at generating the signatures and has a 76% smaller key at a security level of 100 bits.

Acknowledgments

This work was supported by "Strategic Information and Communications R&D Promotion Programme (SCOPE), no. 0159-0172," Ministry of Internal Affairs and Communications, Japan. The first author is supported by Grant-in-Aid for Young Scientists (B), Grant number 24740078.

Table 4: Secret Key Lengths of Schemes over $GF(256)$

Parameter $(v_1, d_1 * o'_1, d_2 * o'_2)$	$(18, 14*1, 1*14)$	$(31, 19*1, 2*12)$
Security Level	80 bits	100 bits
Rainbow (Byte)	23680	89026
Matrix-based Rainbow (Byte)	19975	56674
NT-Rainbow (Byte)	15242	53663
Our scheme (Byte)	11537	21311
Ratio (Our scheme/Rainbow)	48.7%	23.9%

Table 5: Efficiencies of Signature Generation of Schemes over $GF(256)$

Parameter $(v_1, d_1 * o'_1, d_2 * o'_2)$	$(18, 14*1, 1*14)$	$(31, 19*1, 2*12)$
Rainbow	188 μs	651 μs
Matrix-based Rainbow	138 μs	423 μs
NT-Rainbow	129 μs	443 μs
Our scheme	96 μs	294 μs
Ratio (Our scheme/Rainbow)	51.1%	45.2%

References

[1] J. Ding, J. E. Gower, and D. S. Schmidt, *Multivariate Public Key Cryptosystems*, ser. Advances in Information Security. Springer, 2006, vol. 25.

[2] C. Wolf, "Introduction to multivariate quadratic public key systems and their applications," in *Proc. of the 2006 Yet Another Conference on Cryptography (YACC'06), Porquerolles Island, France*, June 2006, pp. 44–55.

[3] J. Patarin, "The oil and vinegar signature scheme," in Dagstuhl Workshop on Cryptography, 1997.

[4] J. Ding and D. Schmidt, "Rainbow, a new multivariable polynomial signature scheme," in *Proc. of the 3rd International Conference on Applied Cryptography and Network Security (ACNS'05), New York, New York, USA, LNCS*, vol. 3531. Springer-Verlag, June 2005, pp. 164–175.

[5] B.-Y. Yang and J.-M. Chen, "Building secure tame like multivariate public-key cryptosystems: The new tts," in *Proc. of the 10th Australasian Conference on Information Security and Privacy (ACISP'05), Brisbane, Australia, LNCS*, vol. 3574. Springer-Verlag, July 2005, pp. 518–531.

[6] T. T. Takanori Yasuda, Jintai Ding and K. Sakurai, "A variant of rainbow with shorter secret key and faster signature generation," in *Proc. of the 1st ACM workshop on Asia public-key cryptography (AsiaPKC'13), Hangzhou, China*. ACM, May 2013, pp. 57–62.

[7] T. Yasuda, T. Takagi, and K. Sakurai, "Efficient variant of rainbow without triangular matrix representation," in *Proc. of the 2nd Information & Communication Technology -EurAsia Conference (ICT-EurAsia'14), Bali, Indonesia, LNCS*, vol. 8407. Springer-Verlag, April 2014, pp. 532–541.

[8] E. D. Daniel J. Bernstein, Johannes Buchmann, *Post Quantum Cryptography*. Springer Berlin Heidelberg, 2008.

[9] B.-Y. Yang and J.-M. Chen, "All in the xl family, theory and practice," in *Proc. of the 7th International Conference on Information Security and Cryptology (ICISC'04), Seoul, Korea, LNCS*, vol. 3506. Springer-Verlag, December 2005, pp. 67–86.

[10] A. Braeken, C. Wolf, and B. Preneel, "A study of the security of unbalanced oil and vinegar signature schemes," in *Topics in Cryptology - CT-RSA 2005, The Cryptographers' Track at the RSA Conference 2005, San Francisco, California, US, LNCS*, vol. 3376. Springer-Verlag, February 2005, pp. 29–43.

[11] S. Bulygin, A. Petzoldt, and J. Buchmann, "Towards provable security of the unbalanced oil and vinegar

signature scheme under direct attacks," in *Proc. of the 11th International Conference on Cryptology in India (INDOCRYPT'10), Hyderabad, India, LNCS*, vol. 6498. Springer-Verlag, December 2010, pp. 17–32.

[12] J.-C. Faugére and L. Perret, "On the security of UOV," in *Proc. of the 1st International Conference on Symbolic Computation and Cryptography (SCC'08), Beijing, China*, ser. LMIB, April 2008, pp. 103–109.

[13] J. Ding, B.-Y. Yang, C.-H. O. Chen, M.-S. Chen, and C.-M. Cheng, "New differential-algebraic attacks and reparametrization of rainbow," in *Proc. of the 6th International Conference on Applied Cryptography and Network Security (ACNS'08), New York, New York, USA, LNCS*, vol. 5037. Springer-Verlag, June 2008, pp. 242–257.

[14] S. B. Albrecht Petzoldt and J. Buchmann, "Selecting parameters for the rainbow signature scheme," in *Proc. of the 3rd International Workshop on Post-Quantum Cryptography (PQCrypto'10), Darmstadt, Germany, LNCS*, vol. 6061. Springer-Verlag, May 2010, pp. 218–240.

[15] L. Goubin and N. T. Courtois, "Cryptanalysis of the ttm cryptosystem," in *Advances in Cryptology, Proc. of the 6th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT'00), Kyoto, Japan, LNCS*, vol. 1976. Springer-Verlag, December 2000, pp. 44–57.

[16] S. B. Albrecht Petzoldt and J. Buchmann, "Cyclicrainbow - a multivariate signature scheme with a partially cyclic public key based on rainbow," in *Progress in Cryptology - INDOCRYPT'10, Proc. of the 11th International Conference on Cryptology in India, Hyderabad, India, LNCS*, vol. 6498. Springer-Verlag, December 2010, pp. 33–48.

[17] O. Billet and H. Gilbert, "Cryptanalysis of rainbow," in *Proc. of the 5th International Conference on Security and Cryptography for Networks (SCN'06), Maiori, Italy, LNCS*, vol. 4116. Springer-Verlag, September 2006, pp. 336–347.

[18] A. Kipnis and A. Shamir, "Cryptanalysis of the oil and vinegar signature scheme," in *Advances in Cryptology - CRYPTO'98, Proc. of the 18th Annual International Cryptology Conference, Santa Barbara, California, USA, LNCS*, vol. 1462. Springer-Verlag, August 1998, pp. 257–266.

[19] J. P. Aviad Kipnis and L. Goubin, "Unbalanced oil and vinegar signature schemes," in *Advances in Cryptology - EUROCRYPT'99, Proc. of the 1999 International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, LNCS*, vol. 1592. Springer-Verlag, May 1999, pp. 206–222.

Author Biography

Takanori Yasuda received the PhD. degrees in mathematics from Kyushu University in 2007. He was a postdoctal fellow in Osaka City University from 2007 through 2008, in Kyushu University from 2008 through 2011. He is currently a researcher in Institute of Systems, Information Technologies and Nanotechnologies. His current research interests are pairing cryptography, multivariate public-key cryptosystem, and automorphic representations.

Tsuyoshi Takagi received the B.Sc. and M.Sc. degrees in mathematics from Nagoya University in 1993 and 1995, respectively. He had engaged in the research on network security at NTT Laboratories from 1995 to 2001. He received the Dr.rer.nat. degree from Technische Universität Darmstadt in 2001. He was an Assistant Professor at Technische Universität Darmstadt until 2005, and was a Professor at Future University Hakodate until 2010. He is currently a Professor in the Institute of Mathematics for Industry at Kyushu University. His current research interests are information security and cryptography.

Kouichi Sakurai is Professor of Department of Computer Science and Communication Engineering, Kyushu University, Japan since 2002. He received B.E., M.E., and D.E. of Mathematics, Applied Mathematics, and Computer Science from Kyushu University in 1982, 1986, and 1993, respectively. He is interested in cryptography and information security.