Pacific Journal of Mathematics for Industry
a SpringerOpen Journal

ORIGINAL ARTICLE Open Access

# A security analysis of uniformly-layered rainbow defined over non-commutative rings

Takanori Yasuda[1*] and Kouichi Sakurai[1,2]

**Abstract**

Hashimoto and Sakurai proposed a signature scheme (HS scheme), whose security is based on the difficulty of integer factorization. In this paper, we redefine HS scheme as a signature scheme in Multivariate Public Key Cryptosystems (MPKC). MPKC are public key cryptosystems whose security is based on the difficulty of solving multivariate quadratic equations, and candidates for post-quantum cryptography. In this paper, we analyze the security of the extended HS scheme using technique of security analysis for MPKC. Furthermore, based on the security analysis of the extended HS scheme, we estimate secure parameters of the extended HS scheme.

**Keywords:** Public key cryptography; Multivariate public key cryptosystems; Rainbow; Post-quantum cryptography

## 1 Introduction

In 1984, Ong, Schnorr and Shamir [15] proposed an efficient signature scheme (OSS signature scheme) using a bivariate quadratic equation,

$$x^2 + hy^2 \equiv m \bmod N \tag{1}$$

where $h, m$ are integers and $N$ is a composite number whose factorization is difficult. The security of this scheme was supposed to be based on the difficulty of integer factorization. However, Pollard and Schnorr proposed an algorithm to solve the equation (1) efficiently without the factorization of $N$ [18]. Then OSS signature scheme would be extended to scheme using multivariate variables and scheme using non-commutative rings.

In 1994, Shamir [20] proposed a multivariate variant of OSS signature scheme, which is called Birational Permutation scheme. However, Coppersmith, Stern and Vaudenary [6] gave an efficient attack by observing linear combination of components of the public key. In 1997, Sato and Araki [19] proposed a new scheme extended from OSS signature scheme using quaternion algebra. Namely, $\mathbb{Z}/N\mathbb{Z}$ in OSS signature scheme is replaced by a quaternion algebra over $\mathbb{Z}/N\mathbb{Z}$. However, Coppersmith [5] gave two efficient attacks using special property of quaternion algebra. In 2008, Hashimoto and Sakurai [12] proposed a new scheme (HS scheme) including property of both Birational Permutation scheme and Sato-Araki scheme. In 2010, Uchiyama and Ogura [21] showed that this scheme is reduced to Rainbow [9], which is a signature scheme in the multivariate public key cryptosystem (MPKC), and discussed possibility of forgery in case of HS scheme with small size.

In this paper, we extend HS scheme to a signature scheme in MPKC. Therefore, the security of the extended HS scheme is no longer based on the difficulty of integer factorization. Generally, schemes in MPKC are expected to resist attacks using quantum computer, Moreover, we show that the extended HS scheme has an efficient signature generation.

On the other hand, Yasuda et al. [25] proposed another signature scheme "NC-Rainbow" in MPKC, which is an extension of a signature scheme called "Rainbow" using non-commutative rings. The paper [25] analyzed the security of NC-Rainbow for attacks against the original Rainbow, and estimated the secure parameters of NC-Rainbow.

In this paper, we analyze the security of the extended HS scheme. The attacks analyzed in this paper are 1) the attack against Birational Permutation scheme, 2) the attack against Sato-Araki scheme, and the attacks against Rainbow: 3) UOV [4,13,14], 4) MinRank [3,11,22], 5) HighRank [10,11,17], 6) direct [2,4,23], 7) Rainbow-Band-Separation (RBS) [10,16], and (8) UOV-Reconciliation (UOV-R) attacks [10,16].

*Correspondence: yasuda@isit.or.jp
[1] Institute of Systems, Information Technologies and Nanotechnologies, Fukuoka, Japan
Full list of author information is available at the end of the article

This paper is basically a journal version of the paper [24]. However, the attacks analyzed in the paper [24] are from 1) to 5) above. In this paper, we add the security analysis against the attacks 6), 7) and 8). Moreover, we present secure parameters of the extended HS scheme for several security levels.

## 2 Birational permutation scheme

In this section, we summarize the attack of Coppersmith, Stern and Vaudenary against Birational Permutation scheme [6]. We will analyze this attack in the extended HS scheme later. First, we describe Birational Permutation scheme [20].

Let $p, q$ be primes and $N = pq$. Assume that the factorization of $N$ is difficult. Let $n$ be a natural number. For $k = 2, 3, \ldots, n$, we define $g_k : (\mathbb{Z}/N\mathbb{Z})^n \to \mathbb{Z}/N\mathbb{Z}$ by a homogeneous quadratic polynomial over $\mathbb{Z}/N\mathbb{Z}$,

$$g_k(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{k-1} a_{ik} x_i x_k + \sum_{1 \le i \le j \le k-1} a_{ij} x_i x_j,$$

where $a_{ij} \in \mathbb{Z}/N\mathbb{Z}$. The central map of Birational Permutation scheme is constructed by

$$G = \left(g_2, g_3, \ldots, g_n\right) : (\mathbb{Z}/N\mathbb{Z})^n \to (\mathbb{Z}/N\mathbb{Z})^{n-1}.$$

The key generation, the signature generation and the verification of Birational Permutation scheme are described as follows.

***Key Generation.*** The secret key consists of primes $p, q$ and the central map $G$ and two affine (linear) transformations $A_1 : (\mathbb{Z}/N\mathbb{Z})^{n-1} \to (\mathbb{Z}/N\mathbb{Z})^{n-1}$, $A_2 : (\mathbb{Z}/N\mathbb{Z})^n \to (\mathbb{Z}/N\mathbb{Z})^n$. The public key consists of $N$ and the composite map $F = A_1 \circ G \circ A_2 = (f_2, f_3, \ldots, f_n) : (\mathbb{Z}/N\mathbb{Z})^n \to (\mathbb{Z}/N\mathbb{Z})^{n-1}$.

***Signature Generation.*** Let $\mathbf{M} \in (\mathbb{Z}/N\mathbb{Z})^{n-1}$ be a message. We compute $\mathbf{A} = A_1^{-1}(\mathbf{M})$, $\mathbf{B} = G^{-1}(\mathbf{A})$, $\mathbf{C} = A_2^{-1}(\mathbf{B})$ in this order. The signature of the message is $\mathbf{C} \in (\mathbb{Z}/N\mathbb{Z})^n$. Here $G^{-1}(\mathbf{A})$ stands for an element of preimage of $\mathbf{A}$ through $G$.

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

### 2.1 Attack against birational permutation scheme

It is believed that solving general equations over $\mathbb{Z}/N\mathbb{Z}$ is more difficult than that over a finite field. The security of Birational Permutation scheme was based on the difficulty of solving the problem over $\mathbb{Z}/N\mathbb{Z}$. However, Coppersmith, Stern and Vaudenary gave an efficient algorithm [6] to compute $A_2$, a part of the secret key, without solving equations over $\mathbb{Z}/N\mathbb{Z}$.

For simplicity, assume that $A_2$ are linear transformations. We write $A, B$ for the matrix expression of linear parts of $A_1, A_2$, respectively, and $g_k, f_k$ $(k = 2, 3, \ldots, n)$ are denoted by

$$g_k(\mathbf{x}) = \mathbf{x}^T G_k \mathbf{x},\ f_k = \mathbf{x}^T F_k \mathbf{x} \ \left(\mathbf{x} = (x_1, \ldots, x_n)^T\right),$$

for some $F_k, G_k \in \mathbb{M}(n, \mathbb{Z}/N\mathbb{Z})$. ($T$ means the transpose operator.) Since

$$f_k(\mathbf{x}) = \sum_{l=2}^{n} a_{kl} \mathbf{x}^T B^T G_l B \mathbf{x} = \mathbf{x}^T B^T \left(\sum_{l=2}^{n} a_{kl} G_l\right) B\mathbf{x}$$

for $A = (a_{kl})$, we have

$$F_k = B^T \left(\sum_{l=2}^{n} a_{kl} G_l\right) B. \tag{2}$$

For a variable $\lambda$ and $1 \le k_1, k_2 \le n$,

$$\sum_{l=2}^{n} a_{k_1 l} G_l - \lambda \sum_{l=2}^{n} a_{k_2 l} G_j = \begin{pmatrix} * & \cdots & * & (a_{k_1 n} - \lambda a_{k_2 n}) * \\ \vdots & \ddots & \vdots & \vdots \\ * & \cdots & * & (a_{k_1 n} - \lambda a_{k_2 n}) * \\ (a_{k_1 n} - \lambda a_{k_2 n}) * & \cdots & (a_{k_1 n} - \lambda a_{k_2 n}) * & 0 \end{pmatrix}.$$

In particular, the determinant of this matrix is factored by $\left(a_{k_1 n} - \lambda a_{k_2 n}\right)^2$. From (2), the determinant of $F_{k_1} - \lambda F_{k_2}$ is factored by $\left(a_{k_1 n} - \lambda a_{k_2 n}\right)^2$. Therefore $a_{k_1 n}/a_{k_2 n}$, which is denoted by $\lambda_0$, is computed by the public key. By calculating the kernel and the image of $F_{k_1} - \lambda_0 F_{k_2}$, $(\mathbb{Z}/N\mathbb{Z})^n$ is decomposed as

$$(\mathbb{Z}/N\mathbb{Z})^n = B^{-1}\left((\mathbb{Z}/N\mathbb{Z})^{n-1} \times \{0\}\right) \oplus B^{-1}\left(\{0\}^{n-1} \times (\mathbb{Z}/N\mathbb{Z})\right) \tag{3}$$

Continuing this operation, finally we have a decomposition

$$(\mathbb{Z}/N\mathbb{Z})^n = B^{-1}\left((\mathbb{Z}/N\mathbb{Z}) \times \{0\}^{n-1}\right) \oplus \cdots \oplus B^{-1}\left(\{0\}^{n-1} \times (\mathbb{Z}/N\mathbb{Z})\right)$$

by subspaces with rank 1 over $\mathbb{Z}/N\mathbb{Z}$. By rewriting the public key by a basis along the above decomposition, one obtains a system of equations with the same form as the central map, therefore a signature is forged.

## 3 Sato-Araki scheme

In this section, we summarize two attacks of Coppersmith against Sato-Araki scheme. We will analyze these attack in the extended HS scheme later.

Sato-Araki scheme [19] uses a quaternion algebra over $\mathbb{Z}/N\mathbb{Z}$. Let $R$ be a $\mathbb{Z}/N\mathbb{Z}$-analogue of the Hamilton's quaternion algebra. Namely, $R$ is defined by

$$R = \mathbb{Z}/N\mathbb{Z} \cdot 1 \oplus \mathbb{Z}/N\mathbb{Z} \cdot i \oplus \mathbb{Z}/N\mathbb{Z} \cdot j \oplus \mathbb{Z}/N\mathbb{Z} \cdot ij,$$

and $i^2 = j^2 = -1$, $ij = -ji$. $R$ is identified with a subring of a matrix ring by the embedding homomorphism,

$$R \ni a_0 \cdot 1 + a_1 \cdot i + a_2 \cdot j + a_3 \cdot ij \longmapsto \begin{pmatrix} a_0 + a_1\sqrt{-1} & a_3 + a_2\sqrt{-1} \\ -a_3 + a_2\sqrt{-1} & a_0 - a_1\sqrt{-1} \end{pmatrix} \in \mathbb{M}\left(2, \mathbb{Z}/N\mathbb{Z}\left[\sqrt{-1}\right]\right). \quad (4)$$

Here, we identify $i$ with the imaginary unit $\sqrt{-1}$. Note that $R$ is closed by the transpose operation. Sato-Araki scheme is described as follows.

***Key Generation.*** The secret key consists of primes $p, q$ and $u \in R^\times$. The public key consists of $N = pq$ and $h := -(u^T)^{-1}u^{-1} \in R$.

***Signature Generation.*** Let $\mathbf{M} \in R$ be a message such that $\mathbf{M} = \mathbf{M}^T$. Choose $\rho \in R^\times$ randomly. We compute $\mathbf{C}_1 := \rho^{-1}\mathbf{M} + \rho^T$, $\mathbf{C}_2 := u(\rho^{-1}\mathbf{M} - \rho^T) \in R$. $(\mathbf{C}_1, \mathbf{C}_2)$ is a signature.

***Verification.*** If $\mathbf{C}_1^T\mathbf{C}_1 + \mathbf{C}_2^T h\mathbf{C}_2 = 4\mathbf{M}$ then the signature is accepted, otherwise rejected.

**Remark 3.1.** *The security of Sato-Araki scheme is based on the difficulty of solving the equation over R with respect to $X_1, X_2$,*

$$X_1^T X_1 + X_2^T h X_2 = 4\mathbf{M} \quad (5)$$

*for any $\mathbf{M} \in R$. Since the signer knows p and q, the signer can find a solution of (5) by the procedure of above signature generation.*

### 3.1 Attacks against Sato-Araki scheme

The problem of solving the equation (5) is reduced to the problem of solving a equation over $R$,

$$X^T X + h \equiv 0 \bmod N.$$

However, Coppersmith proposed two efficient attacks [5] by using special property of a quaternion algebra without the factorization of $N$.

#### 3.1.1 Coppersmith's first attack

The first attack of Coppersmith is a chosen message attack. For $i = 1, 2, 3$, let $\left(\mathbf{C}_1^{(i)}, \mathbf{C}_2^{(i)}\right)$ be signatures for messages $\mathbf{M}_i$. The following fact is the key of the attack: For $i = 1, 2, 3$,

$$\left(\mathbf{C}_1^{(i)}\right)^T u\mathbf{C}_2^{(i)} \text{ are symmetric matrices,} \quad (6)$$

where $u$ is a component of the secret key. Then these span a subspace $\left\{\delta = \delta^T \in R\right\} = \mathrm{Span}\{i, j, ij\}$ of rank 3 with high probability. One can compute $X \in R$ satisfying

$$\left(\mathbf{C}_1^{(i)}\right)^T X\mathbf{C}_2^{(i)} \text{ are symmetric matrices } (i = 1, 2, 3),$$

which is determined up to scalars. Therefore, $X$ is proportional to $u$. It is not difficult to compute $u$ from $X$.

#### 3.1.2 Coppersmith's second attack

The second attack of Coppersmith is based on the existence of the following algorithm.

**Proposition 3.1. ([1])** *Let $N$ be an odd positive integer and $f(x, y)$ a bivariate quadratic polynomial over $\mathbb{Z}/N\mathbb{Z}$. $\Delta(f)$ denotes the discriminant of $f$ defined as in [1]. If $\gcd(\Delta(f), N) = 1$, then there exists an algorithm which gives a solution to $f(x, y) = 0$ with probability $1 - \epsilon$, and requires $O(\log(\epsilon^{-1}\log N)\log^4 N)$ arithmetic operations on integers of size $O(\log N)$ bits.*

If $x, y \in R$ are written as

$$x = x_0 \cdot 1 + x_1 \cdot i + x_2 \cdot j + x_3 \cdot ij,$$
$$y = y_0 \cdot 1 + y_1 \cdot i + y_2 \cdot j + y_3 \cdot ij,$$

then the equation over $R$,

$$x^T x + y^T hy = 4\mathbf{M} \quad (7)$$

is rewritten by three quadratic equations with respect to 8 variables $x_0, x_1, \ldots, y_3$. By a simplicity of equation (7) and property of quaternion algebra, the problem of solving the system of these quadratic equations can be reduced to that of some bivariate quadratic equations. Therefore a signature can be forged from the above proposition.

## 4 Our proposal: extension of HS scheme

HS scheme [12] is a signature scheme having properties of both birational permutation scheme and Sato-Araki scheme. Since the security of HS scheme is based on the difficulty of integer factorization, the scheme defined over the ring $\mathbb{Z}/N\mathbb{Z}$. However, we want to redefine HS scheme as a scheme in MPKC. Therefore, in this section, we define HS scheme in more general fashion such that our definition involves both the original HS scheme and our proposed scheme.

### 4.1 Non-commutative rings

Let $L$ be either a field $K$ and $\mathbb{Z}/N\mathbb{Z}$. In this paper, we say that a $L$-algebra $R$ is a non-commutative ring only if

1. $R$ is a free module over $L$ with finite rank, and
2. $R$ is non-commutative.

**Example 4.1. (Quaternion algebra)** *For $a \in L^\times$, a non-commutative ring $Q_L(a)$ is defined as follows:*

$$(Set)\ Q_L(a) = L \cdot 1 \oplus L \cdot i \oplus L \cdot j \oplus L \cdot ij,$$

$$(Product)\ i^2 = a,\ j^2 = -1,\ ij = -ji.$$

*$Q_L(a)$ is a free module over L with rank 4. This is called a quaternion algebra. When $L = \mathbb{Z}/N\mathbb{Z}$ and $a = -1$, $R$ coincides with the quaternion algebra used in Sato-Araki scheme. If $L = GF(q)$ and $a = -1$, we write simply $Q_q$ instead of $Q_L(a)$. $Q_L(a)$ is embedded into a matrix ring:*

$$\iota : Q_L(a) \ni a_1 + a_2 i + a_3 j + a_4 ij \mapsto \begin{pmatrix} a_1 + a_2\sqrt{-1}a_3 + a_4\sqrt{-1} \\ -a_3 + a_4\sqrt{-1}a_1 - a_2\sqrt{-1} \end{pmatrix} \in \mathbb{M}\left(2, L\left[\sqrt{-1}\right]\right). \tag{8}$$

*If $Q_L(a)$ is identified with the image of $\iota$, any element in $Q_L(a)$ is closed by transpose operation in $Q_L(a)$. For $v = c_1 + c_2 i + c_3 j + c_4 ij \in Q_L(a)$, the main involution $v^*$ of $v$ is defined by*

$$v^* = c_1 - c_2 i - c_3 j - c_4 ij \in Q_L(a). \tag{9}$$

Let $R$ be a non-commutative ring over $L$ and $r$ its rank over $L$. Then there exists an $L$-linear isomorphism,

$$\phi : L^r \xrightarrow{\sim} R. \tag{10}$$

Using this isomorphism $\phi$, an element $\alpha \in R$ can be represented by $r$ elements in $L$.

### 4.2 HS scheme over *L*

Let $R$ be a non-commutative ring over $L$ of rank $r$ and fix $\phi$ as in (10). In the rest of this paper, assume that $R$ is realized as a subring of the matrix ring $\mathbb{M}(s, L)$ for some $s \in \mathbb{N}$, and closed by the transpose operation.

Let $\tilde{n}$ be a positive integer. HS scheme deploys non-commutative multivariate polynomials as a central map:

$$\tilde{g}_k(x_1, \ldots, x_{\tilde{n}}) = \sum_{i=1}^{k-1} x_i^T \alpha_{ik}^{(k)} x_k + \sum_{1 \le i,j \le k-1} x_i^T \alpha_{ij}^{(k)} x_j + \sum_{1 \le i \le k} \beta_i^{(k)} x_i + \gamma^{(k)} \quad (k = 2, 3, \ldots, \tilde{n}),$$

where $\alpha_{i,j}^{(k)}, \beta_i^{(k)}, \gamma^{(k)} \in R$. Note that $\tilde{g}_k$ is essentially a polynomial of $k$ variables. The central map of HS scheme is constructed by

$$\tilde{G} = \left(\tilde{g}_2, \ldots, \tilde{g}_{\tilde{n}}\right) : R^{\tilde{n}} \to R^{\tilde{n}-1}$$

The key generation, the signature generation and the verification are described as follows.

***Key Generation.*** The secret key consists of $R$, the central map $\tilde{G}$ and two affine transformations $A_1 : L^m \to L^m$ ($m = r\tilde{n} - r$), $A_2 : L^n \to L^n$ ($n = r\tilde{n}$). The public key consists of $L$ and the composed map $\tilde{F} = A_1 \circ \phi^{-\tilde{n}+1} \circ \tilde{G} \circ \phi^{\tilde{n}} \circ A_2 : L^n \to L^m$, which is a system of $m$ quadratic polynomials of $n$ variables over $L$. We denote by $\tilde{F} = \left(\tilde{f}_{r+1}, \ldots, \tilde{f}_n\right)^T$.

***Signature Generation.*** Let $\mathbf{M} \in L^m$ be a message. We compute $\mathbf{A} = A_1^{-1}(\mathbf{M})$, $\mathbf{B} = G^{-1}(\mathbf{A})$, $\mathbf{C} = A_2^{-1}(\mathbf{B})$ in this order. The signature of the message is $\mathbf{C} \in L^n$. Here $\mathbf{B} = \tilde{G}^{-1}(\mathbf{A})$ is computed by the following procedure.

**Step 1** Choose a random element $b_1 \in R$.

**Step 2** For $k = 1, \ldots, \tilde{n}$, do the following operation recursively.

> $\tilde{g}_k$ is a non-commutative polynomial with respect to $x_1, \ldots, x_k$. By the substitution $x_1 = b_1, \ldots, x_{k-1} = b_{k-1}$ to $\tilde{g}_k$, a non-commutative polynomial $\bar{g}_k$ of one variable $x_k$ with at most 1 degree is obtained. We compute the solution $b_k \in R$ of
>
> $$\bar{g}_k(x_k) = a_k \tag{11}$$
>
> where $\mathbf{A} = (a_i) \in R^{\tilde{m}}$. (If there is no solution, return to Step 1.)

**Step 3** Set $\mathbf{B} = (b_1, \ldots, b_{\tilde{n}})$.

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

This scheme is denoted by HS($R$; $\tilde{n}$).

**Remark 4.1.** *In general, it is difficult to solve a non-commutative equation (11) directly. However, if we fix a L-basis of R then it makes a new system of (commutative) linear equations with respect to the basis, which is easy to be solved in general. If R has an efficient arithmetic operation, the equation (11) can be solved more efficiently. For example, in the case of a quaternion algebra $Q_L(a)$, its realization (8) enables to compute its arithmetic operation efficiently.*

## 5 Security analysis of the extended HS scheme

In the last section, we defined HS scheme over a non-commutative ring $R$. Here, we can take a non-commutative ring over a finite field $K$ or a ring $\mathbb{Z}/N\mathbb{Z}$. If $R$ is defined over $\mathbb{Z}/N\mathbb{Z}$, then the HS scheme becomes the original one. On the other hand, our proposed scheme is the HS scheme where $R$ is defined over a finite field $K$.

First, we analyze the security of the extended HS scheme for attacks against the original Birational Permutation scheme and Sato-Araki scheme. As such attacks, there are the attack of Coppersmith, Stern and Vaudenary (CSV) attack [6] and the attacks of Coppersmith [5] has been

analyzed [12]. These attacks can be extended those against HS scheme over $\mathbb{Z}/N\mathbb{Z}$. Moreover, the extended attacks can be changed into attacks against the extended HS scheme over $K$ easily. In this section, we analyze the security for these attacks against the extended HS scheme over $K$.

### 5.1 Security against CSV attack

In Birational Permutation scheme, only $g_n$ includes the variable $x_n$ in all the components of the central map $G = (g_2, g_3, \ldots, g_n)$. Therefore we can extract the term of $g_n$ from linear combinations of $g_2, g_3, \ldots, g_n$ by eliminating $x_n$. The components of the public key $F = (f_2, f_3, \ldots, f_n)$ are expressed as linear combinations of $g_2 \circ A_2, \ldots, g_n \circ A_2$ where $A_2$ is an affine transformation in the private key. Similarly as in the case of the central map, we can also extract the term of $g_n \circ A_2$ from the components. Then we have the decomposition (3) as we explained in § 2.1.

In HS scheme, only $\tilde{g}_n$ includes the non-commutative variable $x_n$ in all the components of the central map $\tilde{G} = (\tilde{g}_2, \tilde{g}_3, \ldots, \tilde{g}_n)$. However, from linear combinations of $\phi^{-\tilde{n}+1} \circ \tilde{G} \circ \phi^{\tilde{n}}$ we can not eliminate $x_n$ by the method in § 2.1 because the non-commutative variable $x_n$ corresponds to $r$ (commutative) variables. Therefore it is difficult to apply the CSV attack to HS scheme.

### 5.2 Security against Coppersmith's first attack

The first attack is applicable for Sato-Araki scheme because a simple relation (6) holds for a part $u$ of the secret key. However in HS scheme, a simple relation like as (6) for the secret key is not expected. Therefore it is difficult to extend this attack to HS scheme.

### 5.3 Security against Coppersmith's second attack

There exists an efficient algorithm solving a system of bivariate quadratic equations modulo $N$ (Proposition 3.1) and a system of equations appearing in Sato-Araki scheme can be reduced to some of bivariate quadratic equations modulo $N$. However HS scheme has many variables, and a system of equations appearing in the scheme is not expected to be reduced to a simple system of equations even if $L = K$. Therefore this attack is not more efficient than the direct attack which find a solution of a system of equations by XL, Gröbner basis algorithm, etc.

## 6 Reduction of Uchiyama and Ogura to Rainbow

Uchiyama and Ogura [21] pointed out that the original HS scheme which is defined over $\mathbb{Z}/N\mathbb{Z}$ can be rewritten by $\mathbb{Z}/N\mathbb{Z}$-analogue of Rainbow where the original Rainbow [9] is a multilayer variant of the Unbalanced Oil and Vinegar signature scheme [13]. This implies that the attacks against Rainbow are applicable to HS scheme.

### 6.1 Original Rainbow and its analogue

To deal with both the original Rainbow and its analogue over a finite field, we prepare Rainbow defined over $L$ which is either $K$ or $\mathbb{Z}/N\mathbb{Z}$.

At first, we define parameters which determine the layer structure of Rainbow. Let $t$ be the number of layers of Rainbow. Let $\nu_1, \ldots, \nu_{t+1}$ be a sequence of positive $t+1$ integers such that

$$0 < \nu_1 < \nu_2 < \cdots < \nu_t < \nu_{t+1}.$$

For $h = 1, \ldots, t$, the sets $V_h, O_h$ of indices of Vinegar and Oil variables of the $h$-th layer of Rainbow is defined by

$$V_h = \{1, 2 \ldots, \nu_h\}, \ O_h = \{\nu_h + 1, \nu_h + 2, \ldots, \nu_{h+1} - 1, \nu_{h+1}\}.$$

The number of elements in $O_h$ and $V_h$ are $\nu_{h+1} - \nu_h$ and $\nu_h$, respectively, and denote $o_h = \nu_{h+1} - \nu_h$. Note that the smallest integer in $O_1$ is $\nu_1 + 1$. We define $n = \nu_{t+1}$ which is the maximum number of the variables used in Rainbow.

Rainbow consists of $t$ layers of multivariate polynomials of $n$ variables. For $h = 1, 2, \ldots, t$, the $h$-th layer of Rainbow deploys the following system of $o_h$ multivariate polynomials:

$$g_k(x_1, \ldots, x_n) = \sum_{i \in O_h, j \in V_h} \alpha_{i,j}^{(k)} x_i x_j + \sum_{i,j \in V_h, i \le j} \beta_{i,j}^{(k)} x_i x_j + \sum_{i \in V_{h+1}} \gamma_i^{(k)} x_i + \eta^{(k)} \ (k \in O_h), \qquad (12)$$

where $\alpha_{i,j}^{(k)}, \beta_{i,j}^{(k)}, \gamma_i^{(k)}, \eta^{(k)} \in L$. Note that $g_k$ is essentially a polynomial of $\nu_h + o_h$ variables. We call variables $x_i$ $(i \in O_h)$ and $x_j$ $(i \in V_j)$ the Oil and Vinegar variable, respectively. Then the central map of Rainbow is constructed by

$$G = (g_{\nu_1+1}, \ldots, g_n) : L^n \to L^{n-\nu_1}.$$

Note that one of preimage of any element of $L^{n-\nu_1}$ through $G$ can be computed easily. For a system of $o_h$ equations for the $h$-th layer,

$$g_k(b_1, \ldots, b_{\nu_h}, x_{\nu_h+1}, \ldots, x_{\nu_{h+1}}) = a_k \ (k \in O_h)$$

becomes $o_h$ linear equations of $o_h$ variables for any $(a_{\nu_h+1}, \ldots, a_{\nu_{h+1}}) \in L^{o_h}$ and $(b_1, \ldots, b_{\nu_h}) \in L^{\nu_h}$. The values of Oil variables in the $h$-th layer obtained by solving this linear equations are utilized as that of Vinegar variables in the $(h+1)$-th layer.

We describe the key generation, the signature generation and the verification of Rainbow in the following.

***Generation.*** The secret key consists of the central map $G$ and two affine transformations $A_1 : L^m \to L^m$ $(m = n - \nu_1)$, $A_2 : L^n \to L^n$. The public key consists of $L$, which is either a field $K$ or $\mathbb{Z}/N\mathbb{Z}$, and the composed map $F = A_1 \circ G \circ A_2 : L^n \to L^m$, which is a system of $m$

quadratic polynomials of $n$ variables over $L$. We denote by $F = \left(f_{v_1+1}, \ldots, f_n\right)^{\mathrm{T}}$.

***Signature Generation.*** Let $\mathbf{M} \in L^m$ be a message. We compute $\mathbf{A} = A_1^{-1}(\mathbf{M})$, $\mathbf{B} = G^{-1}(\mathbf{A})$, $\mathbf{C} = A_2^{-1}(\mathbf{B})$ in this order. The signature of the message is $\mathbf{C} \in L^n$. Remark that $\mathbf{B} = G^{-1}(\mathbf{A})$ can be easily computed by the above property of $G$.

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

This scheme is denoted by Rainbow($L$; $v_1, o_1, \ldots, o_t$), and we call $v_1, o_1, \ldots, o_t$ a parameter of Rainbow.

### 6.2 Reduction of HS scheme to Rainbow

Uchiyama and Ogura wrote down $\phi^{-\tilde{n}+1} \circ \tilde{G} \circ \phi^{\tilde{n}}$ for HS($\mathbb{Z}/N\mathbb{Z}, \tilde{n}$) and showed the following [21].

**Proposition 6.1.** *Let $R$ be a non-commutative ring over $\mathbb{Z}/N\mathbb{Z}$ of rank $r$. Let $\tilde{F}$ be a public key of HS($R$; $\tilde{n}$). Then $\tilde{F}$ becomes a public key of Rainbow($\mathbb{Z}/N\mathbb{Z}$; $\overbrace{r, \ldots, r}^{\tilde{n}}$).*

**Remark 6.1.** *The above proposition defines a correspondent between signature schemes,*

$$\begin{array}{rccc} & HS(R;\, \tilde{n}) & \rightsquigarrow & Rainbow(\mathbb{Z}/N\mathbb{Z};\, \overbrace{r, \ldots, r}^{\tilde{n}}) \\ \textit{Secret Key:} & (A_1, \tilde{G}, A_2) & \mapsto & (A_1, \phi^{-\tilde{n}+1} \circ \tilde{G} \circ \phi^{\tilde{n}}, A_2) \\ \textit{Public Key:} & \tilde{F} & \mapsto & \tilde{F}. \end{array}$$

*Using this notation, the following correspondence holds.*

$$\begin{array}{ccc} \textit{OSS scheme} & \rightsquigarrow & Rainbow(\mathbb{Z}/N\mathbb{Z};\, 1, 1), \\ \textit{Birational Permutation scheme} & \rightsquigarrow & Rainbow(\mathbb{Z}/N\mathbb{Z};\, 1, \ldots, 1), \\ \textit{Sato-Araki scheme} & \rightsquigarrow & Rainbow(\mathbb{Z}/N\mathbb{Z};\, 4, 4). \end{array}$$

The argument of Uchiyama and Ogura in [21] is also valid for the case of HS scheme defined over field $K$. Therefore we have

**Proposition 6.2.** *Let $R$ be a non-commutative ring over $K$ of dimension $r$. Let $\tilde{F}$ be a public key of HS($R$; $\tilde{n}$). Then $\tilde{F}$ becomes a public key of Rainbow($K$; $\overbrace{r, \ldots, r}^{\tilde{n}}$).*

**Remark 6.2.** *The above proposition shows that HS scheme is another way of construction of the uniformly-layered Rainbow, where "uniformly-layered" means all components in the parameter of Rainbow are equal. If the arithmetic operation of non-commutative ring $R$ is efficient, then the signature generation of HS scheme may be more efficient than that of the corresponding Rainbow.*

### 6.3 Security analysis for attacks against Rainbow

Proposition 6.2 implies that attacks against Rainbow are applicable to the extended HS scheme over $K$. In this section, we analyze security of the extended HS scheme against well-known attacks against Rainbow.

#### *6.3.1 Attacks against Rainbow*

Here, we summarize the known attacks against Rainbow that have been reported in previous papers, and we analyze the security against each attack. The known relevant attacks against Rainbow are as follows.

(1) Direct attacks [2,23],
(2) UOV attack [13,14],
(3) MinRank attack [3,11,22],
(4) HighRank attack [10,11,17],
(5) Rainbow-Band-Separation (RBS) attack [10,16],
(6) UOV-Reconciliation (UOV-R) attack [10,16].

The direct attacks try to solve a system of equations $F(\mathbf{X}) = \mathbf{M}$ from public key $F$ and (fixed) message $\mathbf{M}$ [2,23]. By contrast, the goal of the other attacks is to find a part of the secret key. In the case of a UOV attack or HighRank attack, for example, the target Rainbow with parameters $v_1, o_1, \ldots, o_t$ is then reduced into a version of Rainbow with simpler parameters such as $v_1, o_1, \ldots, o_{t-1}$ without $o_t$. We can then break the original Rainbow with lower complexity. To carry out a reduction we need to find (a part of) a direct sum decomposition of vector space $K^n$,

$$K^n = K^{v_1} \oplus K^{o_1} \oplus \cdots \oplus K^{o_t}, \tag{13}$$

because expressing $K^n$ in an available basis enables returning the public key to the central map. In fact, if we can decompose $K^n = W \oplus K^{o_t}$ for a certain $W$ that has a coarser decomposition than (13) then the security of Rainbow($K$; $v_1, o_1, \ldots, o_t$) can be reduced to that of Rainbow($K$; $v_1, o_1, \ldots, o_{t-1}$). There are two methods for finding this decomposition:

(1) Find a simultaneous isotropic subspace of $K^n$.
Let $V$ be a vector space over $K$, and let $Q_1$ be a quadratic form on $V$. We determine that a subspace $W$ of $V$ is *isotropic* (with respect to $Q_1$) if

$$Q_1(v_1, v_2) := Q_1(v_1 + v_2) - Q_1(v_1) - Q_1(v_2) = 0.$$

for any $v_1, v_2 \in W$. In addition, we assume that $V$ is also equipped with quadratic forms $Q_2, \ldots, Q_m$. We determine that a subspace $W$ of $V$ is *simultaneously isotropic* if $W$ is isotropic with respect to all $Q_1, \ldots, Q_m$.

In Rainbow, $m$ quadratic forms on $K^n$ are defined by the quadratic parts of the public polynomials of $F$. Note that the subspace $K^{o_t}$ appearing in (13) is a simultaneous isotropic subspace of $K^n$. If we find a simultaneous isotropic subspace, the basis of $K^{o_t}$ is then obtained and

the above attack is feasible. The UOV, UOV-R and RBS attacks are classified as being of this type.

(2) Find a quadratic form with the minimum or second maximum rank.
When the quadratic part of the $k$-th public polynomial of $F$ in Rainbow is expressed as

$$\sum_{i=1}^{n}\sum_{j=i}^{n} a_{ij}^{(k)} x_i x_j,$$

we associate it with a symmetric matrix $S_k = A + A^{\mathrm{T}}$, where $A = \left(a_{ij}^{(k)}\right)$. We define

$$\mathcal{A} = \mathrm{Span}_K \left\{ S_k \,|\, k = \nu_1 + 1, \ldots, n \right\}, \tag{14}$$

which is a vector space over $K$ spanned by matrices $S_{\nu_1+1}, \ldots, S_n$. For example, if we find a matrix of rank $\nu_2 = \nu_1 + o_1$ in $\mathcal{A}$, there is a high probability that the image of this matrix coincides with $K^{\nu_1} \oplus K^{o_1}$ appearing in (13).

Therefore, we obtain the decomposition of $K^n = (K^{\nu_1} \oplus K^{o_1}) \oplus W'$ for some $W'$ that is a coarser decomposition than (13). The MinRank and HighRank attacks are classified as being of this type.

The details of abovementioned six attacks can be found in the literature [16].

### 6.4 Security against known attacks

#### 6.4.1 UOV attack

Regard $L_2$ as the part of a linear transformation of $A_2$ and place $\mathcal{O}_t = L_2^{-1}(\{0\}^{n-o_t} \times K^{o_t})$ as the subspace of $K^n$ corresponding to $K^{o_t}$ appearing in (13). The UOV attack finds a non-trivial invariant subspace of $W_{12} = W_1 W_2^{-1}$ that is included in $\mathcal{O}_t$ for invertible matrices $W_1, W_2 \in \mathcal{A}$. The analysis in [13] shows that the probability that $W_{12}$ has a non-trivial invariant subspace included in $\mathcal{O}_t$ is equal to $q^{n-2o_t}$ . This is obtained by the following lemma.

**Lemma 6.1. ([8] Lemma 3.2.4)** *Let $J : K^n \to K^n$ be an invertible linear map such that*

1. *there exist two subspace $\mathcal{O}' \subset \mathcal{V}'$ of $K^n$ where the dimensions of $\mathcal{O}'$ and $\mathcal{V}'$ are $o'$ and $\nu'$, respectively, and*
2. *$J(\mathcal{O}') \subset \mathcal{V}'$.*

*Then the probability that $J$ has a non-trivial invariant subspace in $\mathcal{O}'$ is no less than $q^{o'-\nu'}$.*

This lemma is also available for the extended HS scheme through Proposition 6.2. This means that the complexity is the same as that of the corresponding Rainbow. From the complexity of the UOV attack [13] and Proposition 6.2 we have

**Proposition 6.3.** *Let $a = \log_2(\sharp K)$. $HS(R; \tilde{n})$ has a security level of $l$ bits against the UOV attack if*

$$r\tilde{n} - 2r \geq l/a + 1.$$

**Remark 6.3.** *The UOV attack is more efficient in the case of balanced Oil and Vinegar than in the case of general Unbalanced Oil and Vinegar. Therefore, we should not choose $\tilde{n} = 2$ in the extended HS scheme, otherwise, HS scheme corresponds to a balanced Oil and Vinegar scheme.*

#### 6.4.2 MinRank attack

In the MinRank attack, we solve MinRank($\nu_2$) for $\mathcal{A}$. If there is a non-trivial $P \in \mathcal{A}$ for a $\nu \in K^n$ such that $P\nu = 0$, there is high probability that $P$ is a solution for MinRank($\nu_2$). For $\nu \in K^n$, the probability that a non-trivial $P \in \mathcal{A}$ exists such that $P\nu = 0$ is roughly $q^{-\nu_2}$. This is also true for the extended HS scheme. Therefore, from [11], we have the following proposition:

**Proposition 6.4.** *Let $a = \log_2(\sharp K)$. Assume that $r\tilde{n}$. Then $HS(R; \tilde{n})$ has a security level of $l$ bits against the MinRank attack if*

$$2r \geq l/a.$$

#### 6.4.3 HighRank attack

In the HighRank attack, we have an element $W \in \mathcal{A}$ such that $\mathrm{rank}(W) = \nu_t$. For any $W \in \mathcal{A}$, the probability that its rank is equal to $\nu_t$ is $q^{-o_t}$. This is also true for the extended HS scheme. Therefore, from [11], we have the following proposition:

**Proposition 6.5.** *Let $a = \log_2(\sharp K)$. Assume that $n \geq m$. Then $HS(R; \tilde{n})$ has a security level of $l$ bits against the HighRank attack if*

$$r \geq l/a.$$

### 6.5 Direct attacks and others

From Proposition 6.2, the public key of the extended HS scheme is exactly equal to that of the corresponding Rainbow. Therefore, the complexity against the direct attacks is estimated to be the same for the extended HS scheme as for the original Rainbow corresponding to it. Similarly, the complexities against the RBS and UOV-R attacks are estimated to be the same for the extended HS scheme as for the corresponding Rainbow.

The complexities of the direct, RBS and UOV-R attacks were discussed by Petzoldt et al. [16], and we follow their data regarding the complexities of these attacks. In particular, the complexities of the direct and UOV-R attacks are equivalent.

**Table 1 Security level against attacks on the extended HS scheme over $R$ defined over $GF(256)$ and with $\tilde{n} = 3$**

| $r$ | 10 | 11 | 12 | 13 |
|---|---|---|---|---|
| UOV (bits) | 72 | 80 | 88 | 96 |
| MinRank (bits) | 160 | 176 | 192 | 218 |
| HighRank (bits) | 80 | 88 | 96 | 104 |
| Direct, UOV-R, RBS (bits) | 93 | 99 | 104 | 110 |
| Security level (bits) | 72 | 80 | 88 | 96 |

## 7 Total security and secure parameters

Based on the security analysis in the last section, we try to present secure parameters and their length for HS($R$; $\tilde{n}$) where $R$ is a non-commutative ring of rank $r$ over $K = GF(256)$. We adopt the parameters of Petzoldt et al. in [16] for estimating the security against the direct, UOV-R and RBS attacks. For other attacks, from Propositions 6.3, 6.4 and 6.5, the following criteria are used for $l$-bit security against these attacks: Let $a$ be the bit length of $q$ and $r$ the dimension of $R$. For HS($R$; $\tilde{n}$), we have $n = r\tilde{n}$, $m = r(\tilde{n} - 1)$ and we assume that $n > m$.

1. UOV attack $n - 2r \geq l/a + 1$.
2. MinRank attack $2r \geq l/a$.
3. HighRank attack $r \geq l/a$.

From the above condition of UOV attack, $\tilde{n} \geq 3$ is required in order to design a secure HS scheme. Table 1 presents the complexity against each attack for the extended HS scheme over a non-commutative ring $R$ over $GF(256)$ with $\tilde{n} = 3$. Table 1 shows that UOV attack is the strongest among all analyzed attacks.

## 8 Efficiency of HS scheme

Any non-commutative ring $R$ can be embedded in a matrix ring $\mathbb{M}(l, K)$ for some positive integer $l$. If we can choose a small $l$, the arithmetic operation of $R$ becomes efficient. In the signature generation in our proposed scheme, we have to solve several systems of linear equations of the form, $\mathcal{A}.\mathcal{X} = \mathcal{B}$ ($\mathcal{A}, \mathcal{B} \in \mathbb{M}(l, K)$) with respect to variable matrix $\mathcal{X} \in \mathbb{M}(l, K)$. If we use Gaussian elimination to solve the above linear equations, the number of field multiplication in solving the linear equations has $O(l^3)$.

On the other hand, in the signature generation in the corresponding Rainbow the number of field multiplication has $O(d^3)$ where $d$ is the dimension of $R$ because of Proposition 6.2. Thus, if $l < d$ is satisfied, the signature generation of our proposed scheme is more efficient than that of the corresponding Rainbow.

### 8.1 Efficiency in the case of group ring of dihedral group

To compare the efficiency of signature generation in HS scheme and the corresponding Rainbow, we prepare dihedral group and its realization. Let $m$ be a positive integer. $M_1 = (a_{ij}), M_2 = (b_{ij}) \in \mathbb{M}(m, K)$ is defined as

$$a_{ij} = \begin{cases} 1 & \text{if } j - i \equiv 1 \pmod m, \\ 0 & \text{otherwise,} \end{cases} \quad b_{ij} = \begin{cases} 1 & \text{if } j + i \equiv 1 \pmod m, \\ 0 & \text{otherwise.} \end{cases}$$

We write $D_m$ for the group generated by $M_1$ and $M_2$. $D_m$ is isomorphic to the dihedral group with $2m$ elements [7]. $K[D_m]$ denotes the group ring with coefficients in $K$ and associated to $D_m$, then, it is a non-commutative ring of dimension $2m-1$, realized in $\mathbb{M}(m, K)$. $K[D_m]$ is closed by a transpose operation because inverse operation on $D_m$ is closed in $D_m$. Therefore we can use $K[D_m]$ as a base ring in HS scheme. Table 2 compares the efficiency of the signature generation in HS scheme and the corresponding Rainbow. The non-commutative rings used in HS schemes in the table are chosen by $K[D_m]$ where $K = GF(256)$ and $m = 10, 11, 12, 13$. The number of layers in each HS scheme is chosen by 3, and then the corresponding Rainbow of HS($K[D_m]$; 3) becomes Rainbow($K$; $r, r, r$) with $r = 2m-1$ by Proposition 6.2. We estimate the number of multiplication of $GF(256)$ for efficiency comparison. $\mathrm{M}_{\mathrm{sig}}(\mathrm{HS}(R; 3))$ (resp. $\mathrm{M}_{\mathrm{sig}}(\mathrm{R}(GF(256); r, r, r))$) stands for the number of multiplications in the signature generation in HS($R$; 3) (resp. Rainbow($GF(256)$; $r, r, r$)). Table 2

**Table 2 Efficiency comparison of HS scheme with the corresponding Rainbow (in terms of the number of multiplications in $GF(256)$)**

| HS($R$, 3) | HS($K[D_{10}]$, 3) | HS($K[D_{11}]$, 3) | HS($K[D_{12}]$, 3) | HS($K[D_{13}]$, 3) |
|---|---|---|---|---|
| Dimension of $R$ | 19 | 21 | 23 | 25 |
| Matrix size | 10 | 11 | 12 | 13 |
| $\mathrm{M}_{\mathrm{sig}}(\mathrm{HS}(R; 3))$ | 25353 | 33233 | 42581 | 53521 |
| Corresponding Rainbow R($GF(256)$; $r, r, r$) | R(19, 19, 19) | R(21, 21, 21) | R(23, 23, 23) | R(25, 25, 25) |
| Security level (bits) | 72 | 80 | 88 | 96 |
| $\mathrm{M}_{\mathrm{sig}}(\mathrm{R}(GF(256); r, r, r))$ | 50198 | 66766 | 86618 | 110050 |
| Ratio | 50.5% | 49.8% | 49.2% | 48.6% |

shows that the signature generation of HS scheme is about 50% faster than that of the corresponding Rainbow.

## 9 Concluding remarks

We analyzed the security of the extended HS scheme, and presented secure parameters of the extended HS scheme. The attacks we analyzed the security are the attack of Coppersmith, Stern and Vaudenary for Birational Permutation scheme, two attacks of Coppersmith for Sato-Araki scheme and attacks against Rainbow. Based on the security analysis, we estimate secure parameters of the extended HS scheme. If a non-commutative ring used in the extended HS scheme is chosen by the group ring associated to dihedral group, the speed of the signature generation can be accelerated by about 50% in comparison with the corresponding Rainbow.

**Acknowledgments**
This work has been supported by "Strategic Information and Communications R&D Promotion Programme (SCOPE), no. 0159-0172", Ministry of Internal Affairs and Communications, Japan.

**Author details**
[1]Institute of Systems, Information Technologies and Nanotechnologies, Fukuoka, Japan. [2]Kyushu University, Fukuoka, Japan.

Received: 1 April 2014 Accepted: 7 May 2014
Published online: 11 September 2014

**References**

1. Adleman, LM., Estes, DR., McCurley, KS.: Solving bivariate quadratic congruences in random polynomial time. Math. Comput. **48**, 17–28 (1987)
2. Bernstein, DJ., Buchmann, J., Dahmen, E.: Post Quantum Cryptography. Springer, Berlin Heidelberg (2009)
3. Billet, O., Gilbert, H.: Cryptanalysis of rainbow. In: *SCN'06 Springer LNCS 4116*, pp. 336–347. Springer, Berlin Heidelberg, (2006)
4. Braeken, A., Wolf, C., Preneel, B.: A study of the security of unbalanced oil and vinegar signature schemes. In: *CT-RSA'05 Springer LNCS 3376*, pp. 29–43. Springer, Berlin Heidelberg, (2005)
5. Coppersmith, D.: Weakness in quaternion signatures. In: *CRYPTO'99 Springer LNCS 1666*, pp. 305–314. J. Cryptology'01, (2001)
6. Coppersmith, D., Stern, J., Vaudenay, S.: The security of the birational permutation signature scheme. J. Cryptology. **10**, 207–221 (1997)
7. Dummit, DS., Foote, RM.: Abstract Algebra. John Wiley & Sons, Inc. (2006)
8. Ding, J., Gower, JE., Schmidt, DS.: Multivariate Public Key Cryptosystems, Advances in Information Security 25. Springer, New York (2006)
9. Ding, J., Schmidt, D.: Rainbow, a new multivariable polynomial signature scheme. In: *ACNS'05 Springer LNCS 3531*, pp. 164–175. Springer, Berlin Heidelberg, (2005)
10. Ding, J., Yang, B-Y., Chen, C-HO., Chen, M-S., Cheng, CM.: New differential-algebraic attacks and reparametrization of rainbow. In: *Springer LNCS 5037*, pp. 242–257. Springer, Berlin Heidelberg, (2008)
11. Goubin, L., Courtois, NT.: Cryptanalysis of the TTM cryptsystem. In: *ASIACRYPT'00 Springer LNCS 1976*, pp. 44–57. Springer, Berlin Heidelberg, (2000)
12. Hashimoto, Y., Sakurai, K.: On construction of signature schemes based on birational permutations over noncommutative. presented at the 1st International Conference on Symbolic Computation and Cryptography (SCC2008) held in Beijin, April 2008. *ePrint*. http://eprint.iacr.org/2008/340
13. Kipnis, A., Patarin, L., Goubin, L.: Unbalanced oil and vinegar schemes. In: *EUROCRYPT'99, Springer LNCS 1592*, pp. 206–222. Springer, Berlin Heidelberg, (1999)
14. Kipnis, A., Shamir, A.: Cryptanalysis of the oil and vinegar signature scheme. In: *CRYPTO'98. Springer LNCS 1462*, pp. 257–266. Springer, Berlin Heidelberg, (1998)
15. Ong, H., Schnorr, CP., Shamir, A.: An efficient signature scheme based on quadratic equations. In: *Proc. 16th ACM Symp. Theory Comp*, pp. 208–216. Springer, Berlin Heidelberg, (1984)
16. Petzoldt, A., Bulygin, S., Buchmann, J.: Selecting parameters for the rainbow signature scheme. In: *PQCrypto'10, Springer LNCS 6061*, pp. 218–240. Springer, Berlin Heidelberg, (2010)
17. Petzoldt, A., Bulygin, S., Buchmann, J.: CyclicRainbow - a multivariate signature scheme with a partially cyclic public key based on rainbow. In: *INDOCRYPT'10, Springer LNCS 6498*, pp. 33–48. Springer, Berlin Heidelberg, (2010)
18. Pollard, JM., Schnorr, CP.: An efficient solution of the congruence $x^2 + ky^2 \equiv m \pmod{n}$. IEEE Trans. Inf. Theory. **IT-33**, 702–709 (1987)
19. Satoh, T., Araki, K.: On construction of signature scheme over a certain noncommutative ring. IEICE Trans. Fundamentals. **E80-A**, 702–709 (1997)
20. Shamir, A.: Efficient signature schemes based on birational permutations. In: *CRYPTO'93, Springer LNCS 773*, pp. 1–12. Springer, Berlin Heidelberg, (1994)
21. Uchiyama, S., Ogura, N.: Cryptanalysis of the birational permutation signature scheme over a non-commutative ring. JSIAM Lett. **2**, 85–88 (2010). *ePrint* http://eprint.iacr.org/2009/245
22. Yang, B-Y., Chen, J-M.: Building secure tame like multivariate public-key cryptosystems: the new TTS. In: *ACISP'05, Springer LNCS 3574*, pp. 518–531. Springer, Berlin Heidelberg, (2005)
23. Yang, B-Y., Chen, J-M.: All in the XL family, theory and practice. In: *ICISC'04, Springer LNCS 3506*, pp. 67–86. Springer, Berlin Heidelberg, (2005)
24. Yasuda, T., Sakurai, K.: A security analysis of uniformly-layered rainbow — revisiting Sato-Araki's non-commutative approach to Ong-Schnorr-Shamir signature towards PostQuantum paradigm. In: *PQCrypto'11, Springer LNCS 7071*, pp. 275–294. Springer, Berlin Heidelberg, (2011)
25. Yasuda, T., Sakurai, K., Takagi, T.: Reducing the key size of rainbow using non-commutative rings. In: *CT-RSA f12, Springer LNCS vol. 7178*, pp. 68–83. Springer, Berlin Heidelberg, (2012)

doi:10.1186/s40736-014-0001-1
**Cite this article as:** Yasuda and Sakurai: **A security analysis of uniformly-layered rainbow defined over non-commutative rings.** *Pacific Journal of Mathematics for Industry* 2014 **6**:1.