Cryptanalysis of the Birational Permutation Signature Scheme over a Non-commutative Ring

Naoki Ogura and Shigenori Uchiyama

Tokyo Metropolitan University
ogura-naoki@ed.tmu.ac.jp, uchiyama-shigenori@tmu.ac.jp

Abstract. In 2008, Hashimoto and Sakurai proposed a new efficient signature scheme, which is a non-commutative ring version of Shamir's birational permutation signature scheme. Shamir's scheme is a generalization of the OSS (Ong-Schnorr-Shamir) signature scheme and was broken by Coppersmith et al. using its linearity and commutativity. The HS (Hashimoto-Sakurai) scheme is expected to be secure against the attack of Coppersmith et al. since the scheme is based on the non-commutative structure. In this paper, we propose an attack against the HS scheme. Our proposed attack is practical under the condition that its step size and the number of steps are small. More precisely, we firstly show that the HS scheme is essentially a commutative scheme, that is, the HS scheme can be reduced to some commutative birational permutation signature scheme. Then we apply Patarin-like attack against the commutative birational permutation signature scheme. We discuss efficiency of our attack by using some experimental results. Furthermore the commutative scheme obtained from the HS scheme is the Rainbow-type signature scheme. We also discuss the security of the Rainbow-type signature scheme, and propose an efficient attack against some class of the Rainbow-type signature scheme.

Key words: non-commutative ring, birational permutation, Rainbow, Gröbner basis

1 Introduction

In 1984, a very efficient signature scheme was proposed by Ong, Schnorr and Shamir [9]. However, the OSS (Ong-Schnorr-Shamir) scheme was attacked by Pollard and Schnorr [12]. So, in 1994, Shamir [14] proposed so-called the birational permutation signature scheme as a generalization of the OSS scheme. The security of the birational permutation signature scheme is based on the hardness of the problem of finding a solution for simultaneous multivariate quadratic equations (MQ system) over an integer residue ring; we call the problem "MQ problem". The problem of deciding whether an MQ system over a finite field has a solution or not belongs to NP-complete, and quantum polynomial algorithms for solving the MQ problem are still unknown. Unfortunately, Shamir's scheme was broken by Coppersmith, Stern and Vaudenay [3] by using techniques of linear algebra. On the other hand, in 1997, Satoh and Araki [13] proposed a quaternion version of the OSS scheme. Coppersmith [2] proposed an attack against the scheme. Then, in 2008, Hashimoto and Sakurai [8] proposed a non-commutative ring version of Shamir's scheme. Since the HS scheme has a non-commutative structure, they considered that these attacks cannot be applied to their scheme. Also, they discussed the HS scheme is comparable to Shamir's scheme in efficiency.

In this paper, we propose an attack against the HS scheme. Our attack is efficient under the condition that its step size and the number of steps are small. Note that the condition would be preferable for increasing efficiency and reducing the key size. We firstly reduce the HS scheme to some commutative scheme. Then we apply Patarin-like [10] attack against the commutative birational permutation signature scheme. Also, we discuss efficiency of our attack with some experimental results. Furthermore the commutative scheme obtained from the HS scheme is the Rainbow-type [5] signature scheme. Known attacks against the Rainbow-type signature scheme are exponential time with respect to the order of the ring. In contrast, our attack is polynomial time with respect to the number of elements in the ring if the step size and the number of steps are small. Note that the attack of Coppersmith et al. can be only applied to the HS scheme under the case that its step size is one. The efficiency of our attack is comparable to that of the attack of Coppersmith et al. in that case. Moreover, we propose a practical attack against some class of the Rainbow-type signature scheme.

This paper is organized as follows. In Section 2, we will briefly introduce the HS scheme. In Section 3, we explain that the HS scheme can be considered as a scheme over an integer residue ring, that is, a commutative ring. In Section 4, we describe an attack against the HS scheme (or some Rainbow-type scheme). In Section 5, we explain an attack against these schemes under the condition that all randomnesses of the schemes are taken away. In Section 6, we give some experimental results and discuss efficiency of our attack and known attacks. In Section 7, we conclude this paper.

2 The Hashimoto and Sakurai Scheme

In this section, we describe the HS (Hashimoto and Sakurai) scheme. First of all, we explain Shamir's birational permutation scheme, which is a special class of the HS scheme. Then, we describe a concrete construction of the HS scheme.

2.1 Shamir's Birational Permutation Scheme

The HS scheme is a generalization of Shamir's birational permutation scheme. In 1993, Shamir proposed the scheme using the triangle multivariate quadratic system. We describe a concrete construction of Shamir's scheme. Let N be the product of two large primes and define $\mathbb{Z}_N := \mathbb{Z}/N\mathbb{Z}$. Note that a concrete factorization of N is not needed for signing or verification. We need only the fact that almost all elements in $\mathbb{Z}_N$ are invertible. We select an integer l such that N^l is large enough to satisfy security requirements. Then, a construction of Shamir's scheme is as the following.

[Secret-key]

1. Generate a bijective affine transformation $A : (\mathbb{Z}_N)^l \to (\mathbb{Z}_N)^l$. To be more precise, generate randomly an l-dimensional non-singular matrix A_L and an l-dimensional vector A_C over $\mathbb{Z}_N$, and set a function $A(x) = A_L x + A_C$.
2. Similarly, generate an affine transformation $B : (\mathbb{Z}_N)^{l-1} \to (\mathbb{Z}_N)^{l-1}$ (namely, a matrix B_L and a vector B_C).
3. Generate an $(l-1)$-dimensional lower triangular matrix $V = (v_{ij})_{2 \leq i \leq l,\ 1 \leq j \leq l-1}$ over $\mathbb{Z}_N$.
4. For each i from 2 to l, generate an $(i-1)$-dimensional lower triangular matrix $W_i = (w_{ij_1j_2})_{1 \leq j_1,\ j_2 \leq i-1}$ over $\mathbb{Z}_N$.

[Public-key]
Construct a map $P = B \circ G \circ A$, where $G = (g_2, \cdots, g_l) : (\mathbb{Z}_N)^l \to (\mathbb{Z}_N)^{l-1}$ is the map below.

$$g_i(x_1, \cdots, x_l) := \sum_{j \leq i-1} v_{ij} x_j x_i + \sum_{j_2 \leq j_1 \leq i-1} w_{ij_1j_2} x_{j_1} x_{j_2} \ .$$

[Signing]
We regard binary strings with length $l \cdot \lg N$ as elements in $(\mathbb{Z}_N)^l$.

1. By applying a hash function to a message, generate $m \in (\mathbb{Z}_N)^{l-1}$.
2. Compute $m' := B^{-1}(m) = (y_2, \ldots, y_l)$.
3. Select $x_1 \in \mathbb{Z}_N$ randomly.
4. Compute $\sigma' := G^{-1}(m') = (x_1, \ldots, x_l)$ by using the following inductive construction.
   For each i from 2 to l,
   $$x_i := (\sum_{j \leq i-1} v_{ij} x_j)^{-1} \cdot (y_i - \sum_{j_2 \leq j_1 \leq i-1} w_{ij_1j_2} x_{j_1} x_{j_2}) \ .$$
5. Let a signature be $\sigma := A^{-1}(\sigma')$.

[Verification]

1. By applying a hash function to a message, generate $m \in (\mathbb{Z}_N)^{l-1}$.
2. Verify that m corresponds with the element generated by applying P to the signature.

Note that v_{21} have to be an invertible element for valid signing, so we can assume that $v_{21} = 1$. Also, if some $\sum_{j \leq i-1} v_{ij} x_j$ is not invertible at the step 4, we have to be back to the step 3 and reselect x_1. A parameter N should be large enough to satisfy that almost all $\sum_{j \leq i-1} v_{ij} x_j$ is invertible.

The computational complexity of signing of the scheme is $O(l^3 \lg^2 N)$ since computing the sum $\sum_{j_2 \le j_1 \le i-1}$ is dominant. Also, the size of secret key is $O(l^3 \lg N)$.

In 1997, Coppersmith et al. [3] proposed an attack against Shamir's birational permutation scheme. The attack used some linear algebraic techniques. We describe the attack in detail at Section 6.2.

Note that the OSS (Ong-Schnorr-Shamir) scheme [9] is a special case of Shamir's scheme in the case that $l = 2$, $A(\sigma_1,\ \sigma_2) = (\sigma_1 + u\sigma_2,\ \sigma_1 - u\sigma_2)$ for some integer $u \in (\mathbb{Z}_N)^\times$, $g_2(x_1,\ x_2) = x_1 x_2$ and B is the identity map. Also, Satoh and Araki [13] proposed a quaternion version of the OSS scheme. However, the OSS scheme and the SA (Satoh-Araki) scheme were attacked by Pollard and Schnorr [12], Coppersmith [2], respectively. The HS scheme is a generalization of these schemes.

2.2 The Hashimoto and Sakurai Scheme

To avoid the attack of Coppersmith et al., the Hashimoto-Sakurai (HS) scheme used a non-commutative ring. Let N be a large prime or the product of two large primes and define $\mathbb{Z}_N := \mathbb{Z}/N\mathbb{Z}$. We select a suitable non-commutative ring R which satisfies the following conditions.

- R is a subring of the matrix ring over a residue class ring of the integer ring (of some algebraic number field) modulo N.
- If $a \in R$, then $a^t \in R$, where a^t is the transpose of a.
- R is $\mathbb{Z}_N$-free module, that is, $^\exists\{\alpha_1, \cdots, \alpha_r\} \subset R$ such that $R = \bigoplus_{i=1}^r \alpha_i \mathbb{Z}_N$.

We select an integer l such that N^{lr} is large enough to satisfy security requirements and set $n := lr$. Then, a construction of the HS scheme is as the following.

[Secret-key]

1. Generate a bijective affine transformation $A : (\mathbb{Z}_N)^n \to (\mathbb{Z}_N)^n$.
2. Generate an affine transformation $B : (\mathbb{Z}_N)^{n-r} \to (\mathbb{Z}_N)^{n-r}$.
3. Generate an $(l-1)$-dimensional lower triangular matrix $V_1 = (V_{1ij})_{2 \le i \le l,\ 1 \le j \le l-1}$ over R.
4. Generate an $(l-1)$-dimensional lower triangular matrix $V_2 = (V_{2ij})_{2 \le i \le l,\ 1 \le j \le l-1}$ over R.
5. For each i from 2 to l, generate an $(i-1)$-dimensional square matrix $W_i = (W_{ij_1j_2})_{1 \le j_1,\ j_2 \le i-1}$ over R.

[Public-key]
Construct a map $P = B \circ G \circ A$, where $G = (G_2, \cdots, G_l) :\ R^l \to R^{l-1}$ is the map below.

$$G_i(X_1, \cdots, X_l) := \sum_{j \le i-1} X_j{}^t V_{1ij}^t X_i + \sum_{j \le i-1} X_i{}^t V_{2ij} X_j + \sum_{j_1, j_2 \le i-1} X_{j_1}{}^t W_{ij_1j_2} X_{j_2}\ .$$

[Signing]
We regard binary strings with length $n \lg N$ as elements in $(\mathbb{Z}_N)^n$.

1. By applying a hash function to a message, generate $m \in (\mathbb{Z}_N)^{n-r}$.
2. Compute $\dot{m} := B^{-1}(m) = (y_{21}, \ldots, y_{2r}, \cdots, y_{lr})$.
3. Compute $m' := (\sum_{j=1}^{r} y_{2j}\alpha_j, \cdots, \sum_{j=1}^{r} y_{lj}\alpha_j) = (Y_2, \cdots, Y_l)$.
4. Select $X_1 \in R$ randomly.
5. Compute $\sigma' := G^{-1}(m') = (X_1, \ldots, X_l)$ by solving the following inductive equation.

$$Y_i - \sum_{j_1, j_2 \leq i-1} X_{j_1}{}^t W_{ij_1j_2} X_{j_2} = (\sum_{j \leq i-1} X_j{}^t V_{1ij}{}^t) \cdot X_i + X_i{}^t \cdot (\sum_{j \leq i-1} V_{2ij} X_j) \ .$$

   Note that a equation $C_1X + X^tC_2 = C_3$ $(C_1,\ C_2,\ C_3 \in R)$ can be expressed as r linear equations over $\mathbb{Z}_N$ since R is $\mathbb{Z}_N$-free module.
6. Solve $(\sum_{j=1}^{r} x_{1j}\alpha_j, \cdots, \sum_{j=1}^{r} x_{lj}\alpha_j) = (X_1, \cdots, X_l)$ and set $\sigma' = (x_{11}, \cdots, x_{lr})$.
7. Let a signature be $\sigma := A^{-1}(\sigma')$.

[**Verification**]

1. By applying a hash function to a message, generate $m \in (\mathbb{Z}_N)^{n-r}$.
2. Verify that m corresponds with the element generated by applying P to the signature.

The complexity of signing of the scheme is $O(n^3 \lg^2 N)$ since computing the sum $\sum_{j_2 \leq j_1 \leq i-1}$ is dominant. [1] Also, the size of secret key is $O(l^3 r \lg N)$. So, when parameters $n = lr,\ l$ are small, we have the advantage of improving efficiency and reducing key size.

Hashimoto and Sakurai studied the security of some class of the HS scheme, which is a non-commutative version of the OSS scheme. They showed that some type of the HS scheme is resistant to Coppersmith's attack [2] under the condition that factoring of N is infeasible. Thus, we would take large N.

3 Reduction to Commutative Case

In this section, we explain how to reduce the HS scheme to a commutative scheme. This reduction was partially discussed in [8]. We explain this reduction in detail and define a commutative scheme obtained from the HS scheme.

We express elements in R by using a $\mathbb{Z}_N$ basis $\{\alpha_i\}_{i=1}^{r}$.

$$\begin{aligned}
X_i &= x_{i1}\alpha_1 + \cdots + x_{ir}\alpha_r \ (1 \leq i \leq l), \\
V_{1ij} &= v_{1ij1}\alpha_1 + \cdots + v_{1ijr}\alpha_r \ (2 \leq i \leq l,\ 1 \leq j \leq l-1), \\
V_{2ij} &= v_{2ij1}\alpha_1 + \cdots + v_{2ijr}\alpha_r \ (2 \leq i \leq l,\ 1 \leq j \leq l-1), \\
W_{ij_1j_2} &= w_{ij_1j_21}\alpha_1 + \cdots + w_{ij_1j_2r}\alpha_r \ (2 \leq i \leq l,\ 1 \leq j_1,\ j_2 \leq i-1),
\end{aligned}$$

[1] In fact, the complexity depends on the size of a matrix and the degree of a number field. The complexity $O(n^3 \lg^2 N)$ can be taken in the most efficient case.

where $x_{ik}, v_{1ijk}, v_{2ijk}, w_{ij_1j_2k} \in \mathbb{Z}_N$.

Then, each terms of the map G_i can be written as the following.

$$\begin{aligned} X_j{}^t V_{1ij}^t X_i &= \sum_{k_1,k_2,k_3 \le r} x_{jk_1} v_{1ijk_2} x_{ik_3} \alpha_{k_1}{}^t\alpha_{k_2}{}^t\alpha_{k_3}, \\ X_i{}^t V_{2ij} X_j &= \sum_{k_1,k_2,k_3 \le r} x_{ik_1} v_{2ijk_2} x_{jk_3} \alpha_{k_1}{}^t\alpha_{k_2}\alpha_{k_3}, \\ X_{j_1}{}^t W_{ij_1j_2} X_{j_2} &= \sum_{k_1,k_2,k_3 \le r} x_{j_1k_1} w_{ij_1j_2k_2} x_{j_2k_3} \alpha_{k_1}{}^t\alpha_{k_2}\alpha_{k_3} \ . \end{aligned}$$

Since $\alpha_{k_1}{}^t\alpha_{k_2}{}^t\alpha_{k_3},\ \alpha_{k_1}{}^t\alpha_{k_2}\alpha_{k_3} \in R$, the elements can be also expressed as the linear combination of $\{\alpha_i\}_{i=1}^r$. So the map G_i can be written as the following.

$$\sum_{k'=1}^{r} \left\{ \sum_{j \le i-1} \sum_{k_1,k_2 \le r} ({v'}_{ijk_1k_2k'} x_{ik_1} x_{jk_2}) + \sum_{j_2 \le j_1 \le i-1} \sum_{k_1,k_2 \le r} ({w'}_{ij_1j_2k_1k_2k'} x_{j_1k_1} x_{j_2k_2}) \right\} \alpha_{k'},$$

where ${}^\exists {v'}_{ijk_1k_2k'},\ {w'}_{ij_1j_2k_1k_2k'} \in R$. Hashimoto and Sakurai [8] mentioned that the representation of $\alpha_{k_1}{}^t\alpha_{k_2}\alpha_{k_3}$ as the linear combination of α_i is involved in the security of the HS scheme. However, the security of the HS scheme is related to the form of not $\alpha_{k_1}{}^t\alpha_{k_2}\alpha_{k_3}$ but ${v'}_{ijk_1k_2k'}$. So, even if $\alpha_{k_1}{}^t\alpha_{k_2}\alpha_{k_3}$ has some simple form, it is considered that the HS scheme would be secure when $V_{1ij},\ V_{2ij}$ are selected randomly [2].

We showed the HS scheme can be reduced to some commutative scheme. Based on the observation, we define the Rainbow-type [5] signature scheme as the following. Let K be a finite field or an integer residue class ring and set N be the order of K. We select two integers $r,\ l$ such that K^{lr} is large enough to satisfy security requirements and set $n := lr$. We define a function $\nu:\ \{r+1, \cdots, n\} \to \{r, 2r, \cdots, lr\}$ as $\nu(i) < i \le \nu(i) + r$.

[Secret-key]

1. Generate a bijective affine transformation $A : K^n \to K^n$.
2. Generate an affine transformation $B : K^{n-r} \to K^{n-r}$
3. For each i from $r+1$ to n, generate a $\nu(i) \times r$-matrix $V_i = (v_{ij_1j_2})_{j_1=1,\cdots,\nu(i),\ j_2=1,\dots,r}$ over K.
4. For each i from $r+1$ to n, generate a $\nu(i)$-dimensional lower triangular matrix $W_i = (w_{i,\ j_1,\ j_2})_{1 \le j_1,\ j_2 \le \nu(i)}$ over K.

[Public-key]

Construct a map $P = B \circ G \circ A$, where $G = (g_{(r+1)}, \cdots, g_n) :\ K^n \to K^{n-r}$ is the map below.

$$g_i(x_1, \cdots, x_n) := \sum_{j_1 \le \nu(i) < j_2 \le \nu(i)+r} v_{ij_1j_2} x_{j_1} x_{j_2} + \sum_{j_2 \le j_1 \le \nu(i)} w_{ij_1j_2} x_{j_1} x_{j_2} \ .$$

[2] Of course, if we consider special types such as the OSS scheme, the form of $\alpha_{k_1}{}^t\alpha_{k_2}\alpha_{k_3}$ is closely related to the security of the scheme.

[Signing]

1. By applying a hash function to a message, generate $m \in K^{n-r}$.
2. Compute $m' := B^{-1}(m) = (y_{(r+1)}, \ldots, y_n)$.
3. Select $x_1, \cdots, x_r \in K$ randomly.
4. Compute $\sigma' := G^{-1}(m') = (x_1, \ldots, x_n)$ by solving the following inductive linear equations.
   For each k from 1 to $l-1$,

$$\begin{cases} y_{kr+1} - \sum_{j_2 \le j_1 \le kr} w_{(kr+1)j_1 j_2} x_{j_1} x_{j_2} = \sum_{j_2=kr+1}^{kr+r} (\sum_{j_1=1}^{kr} v_{(kr+1)j_1 j_2} x_{j_1}) x_{j_2} \\ \vdots \\ y_{kr+r} - \sum_{j_2 \le j_1 \le kr} w_{(kr+r)j_1 j_2} x_{j_1} x_{j_2} = \sum_{j_2=kr+1}^{kr+r} (\sum_{j_1=1}^{kr} v_{(kr+r)j_1 j_2} x_{j_1}) x_{j_2} \end{cases}.$$

5. Let a signature be $\sigma := A^{-1}(\sigma')$.

[Verification]

1. By applying a hash function to a message, generate $m \in K^{n-r}$.
2. Verify that m corresponds with the element generated by applying P to the signature.

In what follows, we set N be the order of K. The complexity of signing of the scheme is $O(n^3 \lg^2 N)$ since computing the sum $\sum_{j_2 \le j_1 \le i-1}$ is dominant. Also, the size of secret key is $O(n^3 \lg N)$.

We call the scheme above the r-Rainbow scheme since Rainbow [5], which was proposed by Ding et al. in 2005, which uses similar inductive construction. However, from our standpoint, N is large and r, l are small. In contrast, N and r are small and l is large in the Rainbow scheme. So the r-Rainbow scheme is different from the original Rainbow scheme with respect to the setting of parameters.

4 Main Attack

In this section, we describe our attack in detail. We remind you of the condition that N is large and $n = rl$ is small. In what follows, we call the algorithm described in this section Algorithm A.

4.1 Our Attack (Algorithm A)

In this subsection, we explain our algorithm (Algorithm A). The Table 1 shows our algorithm of breaking the r-Rainbow scheme.

The essence of our attack is that, if $x_1, \cdots, x_r \in K$ is fixed, then the map P can be considered as an almost bijective map. Note that the idea was used at [4] for attacks against variants of HFE [11]. We can expect that almost all

Table 1. Algorithm A: our attack against the r-Rainbow scheme

```
Input: a public function $P = (P_1, \cdots, P_n)$, parameters $n, r, l$, a message $m$
Output: a valid signature for $m$
while true do
    $\{\mathrm{poly}_i\}_{i=1}^n \leftarrow$ The polynomial representations of $P_i - m_i$
    for k from 1 to r do
        $\mathrm{poly}_{(n+k)} \leftarrow$ A random linear polynomial $a_0 + a_1x_1 + \cdots a_nx_n$ $(a_i \in K)$
    end for
    $I \leftarrow$ The ideal generated by $\mathrm{poly}_1, \cdots, \mathrm{poly}_{(n+r)}$
    $\{f_1, \cdots, f_t\} \leftarrow$ A Gröbner basis of $I$
    $V \leftarrow$ The variety of $I$ (which is generated by $\{f_i\}$)
    if $V \neq \emptyset$ then
        return $\sigma \in V$ (select randomly)
    end if
end while
```

random polynomials can be a good choice, that is, V is not empty set, because the solution space of $\{poly_i\}_{i=1}^n$ has at least an r-dimensional linear space. So we can expect that Gröbner basis algorithm works very well.

We use the software Magma [15] for our implementation, and the procedure of computing a Gröbner basis in Magma is F_4 algorithm proposed by Faugére et al. [7]. If a Gröbner basis of an ideal I is determined, computing the variety of I is not so difficult.

4.2 Analysis of Algorithm A

Our algorithm uses Gröbner basis algorithm, so it would be difficult to investigate its complexity directly. Then, in order to analyze the complexity of Algorithm A, we employ Patarin's attack [10] as some approximation of Algorithm A.

At first we review the linear equations for computing G^{-1} below. For each k from 1 to $l-1$,

$$\begin{cases} y_{(kr+1)} - \sum_{j_2 \leq j_1 \leq kr} w_{(kr+1)j_1j_2} x_{j_1} x_{j_2} = \sum_{j_2=kr+1}^{kr+r} (\sum_{j_1=1}^{kr} v_{(kr+1)j_1j_2} x_{j_1}) x_{j_2} \\ \vdots \\ y_{(kr+r)} - \sum_{j_2 \leq j_1 \leq kr} w_{(kr+r)j_1j_2} x_{j_1} x_{j_2} = \sum_{j_2=kr+1}^{kr+r} (\sum_{j_1=1}^{kr} v_{(kr+r)j_1j_2} x_{j_1}) x_{j_2} \end{cases} . \tag{1}$$

Let $S^{(k)}(x)$ be the matrix below corresponding the equations (1).

$$\begin{pmatrix} \sum_{j_1=1}^{kr} v_{(kr+1)j_1(kr+1)} x_{j_1} & \cdots & \sum_{j_1=1}^{kr} v_{(kr+r)j_1(kr+1)} x_{j_1} \\ \vdots & \ddots & \vdots \\ \sum_{j_1=1}^{kr} v_{(kr+1)j_1(kr+r)} x_{j_1} & \cdots & \sum_{j_1=1}^{kr} v_{(kr+r)j_1(kr+r)} x_{j_1} \end{pmatrix} .$$

Also, we define $\Delta^{(k)}_{ij}(x)$ be $(i,\ j)$-cofactor of $S^{(k)}(x)$. Then, we have the following relation by Cramer's formula.

$$\begin{cases} x_{(kr+1)} = \sum_{j_3=1}^{r}(y_{(kr+j_3)} - \sum_{j_2\le j_1\le kr} w_{(kr+j_3)j_1j_2}x_{j_1}x_{j_2})\Delta^{(k)}_{1j_3}(x)/|S^{(k)}(x)| \\ \vdots \\ x_{(kr+r)} = \sum_{j_3=1}^{r}(y_{(kr+j_3)} - \sum_{j_2\le j_1\le kr} w_{(kr+j_3)j_1j_2}x_{j_1}x_{j_2})\Delta^{(k)}_{rj_3}(x)/|S^{(k)}(x)|, \end{cases} \tag{2}$$

where $|S^{(k)}(x)|$ is the determinant of $S^{(k)}(x)$. Note that $|S^{(k)}(x)|,\ \Delta^{(k)}_{ij}(x)$ are some polynomial with respect to $x = (x_1, \cdots, x_n)$ whose degree is $r,\ r-1$, respectively. Then, for i from $r+1$ to n, we can express x_i by using $x_1, \cdots, x_r$ and $y_1, \cdots, y_{(n-r)}$ as the following.

$$x_i = h^{(i)}(x_1, \cdots, x_r, y_1, \cdots, y_{(n-r)})/f^{(\nu(i))}(x_1, \cdots, x_r,\ y_1, \cdots, y_{(n-r)}),$$

where $h^{(i)}$ is some polynomial whose degree (with respect to $y_1, \cdots, y_{n-r}$) is $(r+1)^{(\nu(i)/r)-1}$ and $f^{(\nu(i))}$ is some polynomial whose degree (with respect to $y_1, \cdots, y_{n-r}$) is $(r+1)^{(\nu(i)/r)-1} - 1$ such that $f^{\nu(i)} \mid f^{\nu(i+1)}$. We can verify the relation by using (2) recursively. So we can apply Patarin's attack, that is, to find the relation between m and σ by substituting $y = B^{-1}(m),\ x = A(\sigma)$. If we assume that $x_1, \cdots, x_r$ is constant, the computational complexity of Patarin's attack is $O(n^{3r^l} \lg^2 N)$. In our situation, $l,\ r$ (and $n = lr$) are very small, so our algorithm works against the HS scheme. Note that various experiments show that Gröbner basis algorithm would work faster than Patarin's attack.

5 Randomness Contributes Security

In this section, we discuss the security of r-Rainbow scheme in the case that $x_1, \ldots, x_r$ are a constant. We call the algorithm described in this section Algorithm B. Note that l, r do not have to be small in this section.

5.1 Our Attack (Algorithm B)

Note that the assumption that $x_1, \ldots, x_r$ are a constant would be preferable because almost all public-key is a bijective map, so the scheme can be used as an encryption scheme. However, we show that the assumption causes all of the security of the scheme to be lost. The Table 2 shows our algorithm of breaking the r-Rainbow scheme under the assumption. In the Table, "$v_0 + V$" means the space of $v_0 + v$ ($^\forall v \in V$) for a vector v_0 and a linear space V. The well-known fact is that the solution space of a linear system can be expressed as the form $v_0 + V$, where v_0 is a singular solution of the system and V is the null space of the matrix corresponding to the system.

The complexity of the algorithm is $O(ln^3 \lg^2 N)$ because we only apply some linear algebraic techniques to $O(n)$-dimensional systems. So our algorithm works efficiently.

Table 2. Algorithm B: our attack against the r-Rainbow scheme

```
Input: a public function $P = (P_1, \cdots, P_n)$, parameters $n, r, l$, a message $m = (m_1, \dots, m_n)$
Output: the valid signature for $m$
$v_0 + V \leftarrow 0 + K^n$
for $k$ from 1 to $l$ do
    $\alpha$space $\leftarrow (\alpha_1, \dots, \alpha_{2n+1})$ satisfying $\sum_{i=1}^{n} \alpha_i x_i = \sum_{i=n+1}^{2n} \alpha_i y_i + \alpha_{2n+1}$ for
            $(x = v_0 + v,\ y = P(x))\ ({}^{\forall} v \in V)$
    ${v_0}' + V' \leftarrow x = {v_0}' + v'$ satisfying $\sum_{i=1}^{n} \alpha_i x_i = \sum_{i=n+1}^{2n} \alpha_i m_i + \alpha_{2n+1}$ for
            all elements in $\alpha$space
    $v_0 + V \leftarrow (v_0 + V) \cap ({v_0}' + V')$
end for
return $x \in v_0 + V$
```

5.2 Remark on Algorithm B

In this subsection, we describe some background of Algorithm B theoretically. We first assume that $x_1, \dots, x_{ir}$ $(i < l)$ are a constant. Because of the assumption, $g_{ir+1}(x), \dots, g_{ir+r}(x)$ are polynomials whose degree is 1, that is, linear. So $(B^{-1}(m))_{(i-1)r+1} = g_{ir+1}(A(\sigma)), \dots, (B^{-1}(m))_{(i-1)r+r} = g_{ir+r}(A(\sigma))$ are linear equations with respect to $m_i,\ \sigma_j$. That is, we can expect that the r linear independent equations below can be found.

$$\sum_{i=1}^{n} \alpha_i m_i = \sum_{i=n+1}^{2n} \alpha_i \sigma_i + \alpha_{2n+1} \tag{3}$$

Since the equation (3) corresponds to $y_{(i-1)r+1} = g_{ir+1}(x), \dots, y_{(i-1)r+r} = g_{ir+r}(x)$, considering only x's satisfying (3) for fixed m corresponds to considering the space of g_i under the condition that $x_{ir+1}, \dots, x_{ir}$ are a constant. That is, reducing the space of x by using (3) for a fixed m, we can determine the signature σ inductively.

6 Consideration on Algorithm A

In this section, we give some discussion for Algorithm A. Firstly, we remark on efficiency of Algorithm A by using some experiments. Secondly, we compare Algorithm A to known attacks. Finally, the security of the HS scheme might be recovered by taking parameters carefully.

6.1 Efficiency of Algorithm A

In this section, we give some experiments against the HS scheme / the r-Rainbow scheme. Table 3, 4 are experimental results of our attack.

Table 3. Experimental Results against the r-Scheme

r	2	2	2	2	3	3	4
l	3	4	5	6	3	4	3
N	140	140	140	140	140	140	140
time[s]	0.02	0.08	1.1	169	0.08	2.1	11

Table 4. Experimental Results against the r-Rainbow scheme for $r = 2,\ l = 4$

$\lg N$	100	110	120	130	140	150
time[s]	0.24	0.25	0.26	0.27	0.28	0.29

These tables show that our attack is practical if $r,\ l$ are small. However, if r or l is large, our attack would not be applicable. For example, for the parameters $r = 2,\ l = 7$, we have $(r * l)^{r^l} \approx 2^{487}$, so our attack would be impractical against the r-Rainbow scheme in this case.

6.2 Previous Attack

In this subsection, we briefly review known attacks against Shamir's birational permutation scheme and the Rainbow scheme. We remark that our attack would be more efficient than previous attacks under our situation.

Attack against Shamir's Scheme In 1997, Coppersmith, Stern and Vaudenay [3] proposed an attack against Shamir's birational permutation scheme. The CSV (Coppersmith-Stern-Vaudenay) attack uses essentially the following structure. For each i from 2 to l, the map $g_i(\boldsymbol{x}) = \boldsymbol{x}^t \bar{g_i} \boldsymbol{x}$ corresponds to the matrix $\bar{g_i}$ as the following.

$$\bar{g_i} = \begin{pmatrix} w_{11} & w_{21}/2 \cdots & w_{(i-1)1}/2 & v_{i1}/2 & 0 \cdots 0 \\ w_{21}/2 & w_{22} & \vdots & \vdots & \vdots \quad \vdots \\ \vdots & \ddots & \vdots & \vdots & \vdots \quad \vdots \\ w_{(i-1)1}/2 & \cdots \quad \cdots & w_{(i-1)(i-1)} & v_{i(i-1)}/2 & 0 \cdots 0 \\ v_{i1}/2 & \cdots \quad \cdots & v_{i(i-1)}/2 & 0 & 0 \cdots 0 \\ 0 & \cdots \quad \cdots & 0 & 0 & 0 \cdots 0 \\ \vdots & & \vdots & \vdots & \vdots \ddots \vdots \\ 0 & \cdots \quad \cdots & 0 & 0 & 0 \cdots 0 \end{pmatrix}.$$

Then, for $P = (p_2, \cdots, p_l)$, the map p_i corresponds to the matrix $\bar{p_i} := A^t(\sum_{j=2}^{l} b_{ij}\bar{g_j})A$, where $B = (b_{ij})_{2 \leq i,j \leq l}$. So if $\lambda = b_{k_1 l}/b_{k_2 l}$, the determinant of $\bar{p_{k_1}} - \lambda \bar{p_{k_2}}$ equals 0. That is, we can obtain $b_{k_1 l}/b_{k_2 l}$ by solving the univariate equation [3] . The

[3] In fact, we only have to find a double root of the univariate equation.

similar step can be continued inductively. Finally, we have a matrix $\tilde{B}$ which behaves in the same way to B. We can compute a matrix $\tilde{A}$, which is almost same as A, by investigating the kernel of $P\tilde{B}^{-1}$.

The complexity of the CSV attack is $O(l^5 \lg^2 N)$, so the attack is practical. Comparing the complexity of Algorithm A and the CSV attack, Algorithm A is more efficient than the attack. Besides it would be difficult to generalize the CSV attack against the r-Rainbow scheme. For example, we consider that computing the determinant of $\bar{p_{k_1}} - \lambda_1 \bar{p_{k_2}} - \lambda_2 \bar{p_{k_3}} - \cdots \lambda_r \bar{p_{k_r}}$ is a kind of generalization of the CSV attack. However, the attack is inefficient since we have to solve some multivariate systems.

Attack against the Rainbow Scheme Many attacks, for example, [1], [6], against the Rainbow scheme were proposed. These attacks are collectively called Rank Attack. Rank Attack is essentially used the fact that the dimension of kernel of $\bar{g}_i$ is $n - \nu(i)$ or the dimension of the image is $\nu(i)$. However, the complexity of Rank Attack is exponential time with respect to $r \lg N$ since we have to search subspaces of the image of $\bar{g}_i$ or the kernel of $\bar{g}_i$. So these attack are not practical against the r-Rainbow scheme if N is large.

6.3 Selection of Parameters

In this subsection, we remark on the security of the HS scheme and the r-Rainbow scheme. We cryptanalyzed the HS scheme / r-Rainbow scheme under the condition that N is huge but $r,\ l$ are very small. In contrast, Rank Attack can be applied to these schemes under the condition that l is large but $N,\ r$ are small. So these schemes would be secure in the case that $N,\ l$ are not small and r is large. More concrete cryptanalysis against the r-Rainbow scheme is our future work.

7 Conclusion

We proposed an attack against the HS (Hashimoto-Sakurai) scheme, which uses a non-commutative ring. Our attack is practical under the condition that parameters $r,\ l$ are small. Note that our attack is more efficient than the attack proposed by Coppersmith et al. when $r = 1$. We discussed efficiency of our attack by using some experiments. In our proposed attack, firstly we reduce the HS scheme to some commutative scheme. Then, we select r linear equations randomly, and solve a public-key relation with added these equations by using Gröbner bases algorithm. Also, we defined the commutative scheme obtained from the HS scheme as the Rainbow type signature scheme. We showed that these schemes are insecure if $x_1, \ldots, x_r$ are a constant.

However, not all the HS scheme are broken, namely, our algorithm would not work efficiently in the case that r, l are large. Investigating security of the scheme for all parameters is our future work.

References

1. O. Billet and H. Gilbert. "Cryptanalysis of rainbow." *Security and Cryptography for Networks*, LNCS 4116, pp. 336-347, Springer (2006)
2. D. Coppersmith. "Weakness in quaternion signatures." *Crypto '99*, LNCS 1666, pp. 305-314, Springer (1999)
3. D. Coppersmith, J. Stern and S. Vaudenay. "The security of the birational permutation signature scheme." *J. Cryptology*, 10, pp. 207-221 (1997)
4. N. T. Coutois, M. Daum and P. Felke. "On the Security of HFE, HFEv- and Quartz." *PKC2003*, LNCS 2567, pp. 337-350, Springer (2002)
5. J. Ding and D. Schmidt. "Rainbow, a New Multivariable Polynomial Signature Scheme." *Applied Cryptography and Network Security*, LNCS 3531, pp. 164-175, Springer (2005)
6. J. Ding, B-Y Yang, C-H O. Chen, M-S Chen and C-M Cheng. "New Differential-Algebraic Attacks and Reparametrization of Rainbow." *Applied Cryptography and Network Security*, LNCS 5037, pp. 242-257, Springer (2006)
7. J-C Faugère. "A new efficient algorithm for computing Gr"obner bases (F_4)." *J. Pure and Applied Algebra*, Vol. 139, No. 1-3, pp. 61-68 (1999)
8. Y. Hashimoto and K. Sakurai. "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. *Cryptology ePrint*, `http://eprint.iacr.org/2008/340`
9. H. Ong, C.P. Schnorr and A. Shamir. "An efficient signature scheme based on quadratic equations." *Proc. 16th ACM Symp. Theory Comp.*, pp. 208-216 (1984)
10. J. Patarin. "Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88." *CRYPTO '95*, LNCS 963, pp. 248-261, Springer (1995)
11. J. Patarin. "Hidden Field Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of asymmetric algorithms." *EUROCRYPT '96*, LNCS 1070, pp. 33-48, Springer (1996)
12. J.M. Pollard and C.P. Schnorr. "An efficient solution of the congruence $x^2 + ky^2 \equiv m(\pmod{n})$." *IEEE Trans. Inf. Theory*, IT-33, pp. 702-709 (1987)
13. T. Satoh and K. Araki. "On construction of signature scheme over a certain non-commutative ring." *IEICE Trans. Fundamentals*, E80-A, pp. 702-709 (1987)
14. A. Shamir. "Efficient signature schemes based on birational permutations." *Crypto '93*, LNCS 773, pp. 1-12, Springer (1994)
15. Magma, `http://magma.maths.usyd.edu.au/magma/`