JSIAM Letters Vol.2 (2010) pp.85–88 ©2010 Japan Society for Industrial and Applied Mathematics JSIAM Letters

Cryptanalysis of the birational permutation signature scheme over a non-commutative ring

Naoki Ogura[1] and Uchiyama Shigenori[1]

[1] Department of Mathematics and Information Sciences, Tokyo Metropolitan University, Tokyo 192-0397, Japan

E-mail *ogura-naoki@ed.tmu.ac.jp*

Received March 31, 2010, Accepted May 5, 2010

Abstract

In 2008, Hashimoto and Sakurai proposed a new efficient signature scheme, which is a non-commutative version of Shamir's birational permutation signature scheme. Shamir's scheme is a generalization of the Ong-Schnorr-Shamir 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 from its non-commutative structure. In this paper, we propose an attack against the HS scheme, which is practical under the condition that its step size and the number of steps are small. We discuss its efficiency by using some experimental results.

Keywords non-commutative ring, birational permutation, Rainbow, Gröbner basis, MQPKC

Research Activity Group Algorithmic Number Theory and Its Applications

1. Introduction

In 1984, the OSS signature scheme was proposed by Ong et al. [1]. Also, in 1994, Shamir [2] proposed the so-called birational permutation signature scheme as a generalization of the OSS scheme. (Indeed, Tsujii et al. [3] had already found a similar scheme in 1986.) 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 the set of NP-complete problems, and quantum polynomial algorithms for solving the MQ problem are still unknown. On the other hand, in 1997, Satoh and Araki [4] proposed a quaternion version of the OSS scheme. Unfortunately, practical attacks against these scheme were proposed [5–7]. Then, in 2008, Hashimoto and Sakurai [8] proposed a non-commutative version of Shamir's scheme. They expected that its non-commutativity makes us difficult to apply these attacks. 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, which 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 [9] attack against the commutative birational permutation signature scheme. Also, we discuss efficiency of our attack with some experimental results. Moreover, we suggest some specific parameters for the HS scheme based on our cryptanalysis.

This paper is organized as follows. In Section 2, we explain that the HS scheme can be considered as a scheme over an integer residue ring, that is, a commutative ring. In Section 3, we describe an attack against the HS scheme (or some Rainbow-type scheme). In Section 4, we show experimental results against the HS scheme. In Section 5, we suggest some possible parameters for the HS scheme based on our cryptanalysis. In Section 6, we conclude this paper.

2. Reduction to commutative case

In this section, we briefly introduce the HS scheme and explain how to reduce the HS scheme to a commutative scheme.

Let N be a large prime or the product of two large primes and define $\mathbb{Z}_N := \mathbb{Z}/N\mathbb{Z}$. We define that R is a non-commutative subring of a matrix ring over a residue class ring of an integral ring of some algebraic number field modulo N. We construct R as $\mathbb{Z}_N$-free module. Also, R has the property that $a^t \in R$ for $a \in R$, where a^t is the transpose of a. The public-key of the HS scheme is the map $P = B \circ G \circ A$, where A and B are secret bijective affine transformations. The map $G = (G_2, \ldots, G_l) : R^l \to R^{l-1}$ is defined as the following.

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

where $V_{1ij},\ V_{2ij},\ W_{ij_1j_2} \in R$. Refer to [8] about the HS scheme for more information.

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 [7] under the condition that factoring of N is infeasible. Moreover, Hashimoto and Sakurai mentioned that some non-commutative OSS scheme (which is included in the scheme above) is resistant to Coppersmith's (first) attack under the condition that factoring of N is infeasible. Though all of the HS scheme do not necessarily depend on infeasibility of factorization, we would take large N with expectation to increase its security.

Now we explain a way of reduction and define a commutative scheme obtained from the HS scheme. This reduction was partially discussed in [8]. At first we express elements in R by using a $\mathbb{Z}_N$ basis $\{\alpha_i\}_{i=1}^r$. Namely, we set as $X_i = \sum_{k_1=1}^r x_{ij}\alpha_j$ $(i = 1, \ldots, l)$, $V_{1ij} = \sum_{k_2=1}^r v_{1ijk_2}\alpha_{k_2}$ $(i = 2, \ldots, l,\ j = 1, \ldots, l-1)$, $V_{2ij} = \sum_{k_3=1}^r v_{2ijk_3}\alpha_{k_3}$ $(i = 2, \ldots, l,\ j = 1, \ldots, l-1)$ and $W_{ij_1j_2} = \sum_{k_4=1}^r w_{ij_1j_2k_4}\alpha_{k_4}$ $(i = 2, \ldots, l,\ j_1, j_2 = 1, \ldots, i-1)$, 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 a linear combination with ${\alpha_{k_1}}^t\alpha_{k_2}{}^t\alpha_{k_3}, {\alpha_{k_1}}^t\alpha_{k_2}\alpha_{k_3}$. For example,

$$X_j{}^tV_{1ij}^tX_i = \sum_{k_1,k_2,k_3\le r} x_{jk_1}v_{1ijk_2}x_{ik_3}{\alpha_{k_1}}^t\alpha_{k_2}{}^t\alpha_{k_3}.$$

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. (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.)

We showed the HS scheme can be reduced to some commutative scheme. Based on the observation, we define the Rainbow-type [10] 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 $\nu : \{r+1, \ldots, n\} \to \{r, 2r, \ldots, lr\}$ as $\nu(i) < i \le \nu(i)+r$.

[Secret-key]

i) Generate a bijective affine transformation $A : K^n \to K^n$.

ii) Generate an affine transformation $B : K^{n-r} \to K^{n-r}$

iii) For each i from $r+1$ to n, generate a $\nu(i)\times r$-matrix $V_i = (v_{ij_1j_2})_{j_1=1,\ldots,\nu(i),\ j_2=1,\ldots,r}$ over K.

iv) 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 $G = (g_{(r+1)}, \ldots, g_n) : K^n \to K^{n-r}$ is the map below.

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

[Signing]

i) By applying a hash function to a message, generate $m \in K^{n-r}$.

ii) Compute $m' := B^{-1}(m) = (y_{(r+1)}, \ldots, y_n)$.

iii) Select $x_1, \ldots, x_r \in K$ randomly.

iv) Compute $\sigma' := G^{-1}(m') = (x_1, \ldots, x_n)$ by solving the following inductive linear equations. For each k from 1 to $l-1$,

$$\begin{cases} y_{kr+1} - \displaystyle\sum_{j_2\le j_1\le kr} w_{(kr+1)j_1j_2}x_{j_1}x_{j_2} \\ \quad = \displaystyle\sum_{j_2=kr+1}^{kr+r}\left(\sum_{j_1=1}^{kr} v_{(kr+1)j_1j_2}x_{j_1}\right)x_{j_2}, \\ \quad \vdots \\ y_{kr+r} - \displaystyle\sum_{j_2\le j_1\le kr} w_{(kr+r)j_1j_2}x_{j_1}x_{j_2} \\ \quad = \displaystyle\sum_{j_2=kr+1}^{kr+r}\left(\sum_{j_1=1}^{kr} v_{(kr+r)j_1j_2}x_{j_1}\right)x_{j_2}. \end{cases} \tag{1}$$

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

[Verification]

i) By applying a hash function to a message, generate $m \in K^{n-r}$.

ii) 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. We call the scheme above the commutative HS scheme or the r-Rainbow scheme. Note that, Rainbow [10], which was proposed by Ding et al. in 2005, which uses similar inductive construction. However, from our perspective, N is large and r, l are small. So the scheme above is different from the original Rainbow scheme with respect to the setting of parameters.

Here, we consider the performance of the commutative HS scheme. The dominant part of the signing is computation of affine transformations, summation $\sum_{j_2\le j_1\le kr}$ and solving the linear equations (1). The total computational complexity is $O(n^3 \lg^2 N)$. The same holds for the complexity of the verification. Moreover, the size of secret-key and public-key is $O(n^3 \lg N)$. So, when parameters $n = lr$ is small, we have the advantage of improving efficiency and reducing key size.

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

Input: a public function $P = (P_1, \ldots, P_n)$, parameters n, r, l, a message m
Output: a valid signature for m

```
while true do
    {poly_i}_{i=1}^n ← The polynomial representations of P_i − m_i
    for k from 1 to r do
        poly_(n+k) ← A random linear polynomial
                     a_0 + a_1 x_1 + ··· + a_n x_n (a_i ∈ K)
    end for
    I ← The ideal generated by poly_1, ..., poly_(n+r)
    {f_1, ..., f_t} ← A Gröbner basis of I
    V ← The variety of I (which is generated by {f_i})
    if V ≠ ∅ then
        return σ ∈ V (select randomly)
    end if
end while
```

3. Attack against the HS scheme

In this section, we describe our attack in detail. We remind you of the condition that N is large and $n = rl$ is small.

3.1 Our attack

In this subsection, we explain our algorithm. Table 1 shows our algorithm of breaking the r-Rainbow scheme. The essence of our attack is that, if $x_1, \ldots, x_r \in K$ is fixed, then the map P can be considered as an almost bijective map. Note that the idea was used at [11] for attacks against variants of HFE [12]. We can expect that almost all 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 [13] for our implementation, and the the default algorithm in Magma for computing a Gröbner basis is F_4 algorithm proposed by Faugére [14]. If a lexicographical Gröbner basis of an ideal I is determined, computing the variety $V(I)$ is not so difficult.

3.2 Analysis of our algorithm

Our algorithm uses Gröbner basis algorithm, so it would be difficult to investigate its complexity directly. Then, in order to analyze the complexity of our algorithm, we employ Patarin's attack [9] as some approximation of our algorithm.

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

$$x_{(kr+1)} = \sum_{j_3=1}^{r} \left(y_{(kr+j_3)} - \sum_{j_2 \le j_1 \le kr} w_{(kr+j_3)j_1j_2} x_{j_1} x_{j_2} \right) \times \frac{\Delta_{1j_3}^{(k)}(x)}{|S^{(k)}(x)|}$$

$$\vdots$$

$$x_{(kr+r)} = \sum_{j_3=1}^{r} \left(y_{(kr+j_3)} - \sum_{j_2 \le j_1 \le kr} w_{(kr+j_3)j_1j_2} x_{j_1} x_{j_2} \right) \times \frac{\Delta_{rj_3}^{(k)}(x)}{|S^{(k)}(x)|}, \quad (2)$$

where $|S^{(k)}(x)|$ is the determinant of $S^{(k)}(x)$. Note that $|S^{(k)}(x)|, \Delta_{ij}^{(k)}(x)$ are some polynomial with respect to $x = (x_1, \ldots, x_n)$ whose degree is $r, r-1$, respectively. Here, we assume that $y_1, \ldots, y_r$ is a linear combination of $x_1, \ldots, x_r$. For i from $r+1$ to n, we can express x_i by using $x_1, \ldots, x_r$ and $y_1, \ldots, y_{(n-r)}$ as the following.

$$x_i = \frac{h^{(i)}(y_1, \ldots, y_{(n)})}{f^{(\nu(i))}(y_1, \ldots, y_{(n)})},$$

where $h^{(i)}$ is some polynomial whose degree (with respect to $y_1, \ldots, y_n$) is $(r+1)^{(\nu(i)/r)} - 1$ and $f^{(\nu(i))}$ is some polynomial whose degree (with respect to $y_1, \ldots, y_{n-r}$) is $(r+1)^{(\nu(i)/r)}$ 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 $y = B^{-1}(m), x = A(\sigma)$. The computational complexity of deducing some relations is $O(n^{3(r+1)} \lg^2 N)$. 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.

Table 2. Experimental results against the r-Rainbow 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 3. 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

4. Experimental results

In this section, we give some experiments against the r-Rainbow scheme. Tables 2, 3 are experimental results of our attack. We used the computer with 2GHz CPU (AMD Opteron 246), 4GB memory, and 160GB hard disk. For our implementation, we employed Magma V2.15-3. We showed that the complexity of our attack is $O(n^{3(r+1)} \lg^2 N)$. So our attack would be practical if n^r can be polynomial to $r, l, \lg N$, for example, r can be regarded as a constant. In fact, Tables 2 and 3 suggest that

Table 4. Specific parameters for the r-Rainbow scheme with $N = 65537 (\simeq 2^{16})$.

r	5	6	7	7	8	9
l	5	3	2	4	3	2
security[bit]	80			112		
sig[bit]	400	288	224	448	384	288
sk[kB]	8.44	3.40	1.57	11.48	7.39	3.06
pk[kB]	13.71	4.45	1.64	17.84	10.16	3.34
keygen[ms]	0.75	0.33	0.19	0.95	0.62	0.28
signing[ms]	7.92	3.16	1.43	10.73	6.89	2.78
verification[ms]	7.88	3.08	1.36	11.08	7.14	2.81

our attack is practical if r, l satisfying $(rl)^{(r+1)} \leq 2^{18}$. However, if r or l is large, our attack would be impractical. For example, for the parameters $r = 4, l = 11$, we have $n^{3(r+1)} \approx 2^{82}$, so our attack would not be efficient against the r-Rainbow scheme in this case.

5. Selection of parameters

In this subsection, we remark on the security of the HS scheme and suggest specific parameters for the HS scheme. We analyzed the complexity of our attack against the HS scheme in Section 3. This shows that our attack is efficient under the condition that $(rl)^{(r+1)} \leq 2^{18}$, that is, the parameters r, l are small. In contrast, many attacks against the Rainbow-type scheme were proposed. These attacks are collectively called "rank attack". For more information, see [15]. The complexity of rank attack is $O(N^r n^4 \lg^2 N)$. This shows that rank attack is efficient under the condition that the parameters N, r are small.

We propose specific parameters for the HS scheme as follows. The columns "sig", "pk" and "sk" mean the size of signature, public-key and secret-key, respectively. The security of these parameters is based on above cryptanalysis. For example, for the parameters $r = 5, l = 5, N = 65537$, we have $n^{3(r+1)} \simeq 2^{83.6}, N^r n^4 \simeq 2^{98.6}$. So we consider the HS scheme corresponding to the parameter satisfies almost 80 bit security, that is, it would achieve the similar security level to 1024 bit RSA. The bit sizes of signature, public-key and secret-key are taken as possible maximum sizes based on the commutative HS scheme. The columns "keygen", "signing" and "verification" are experimental results implemented on Magma. Although these discussions are very roughly, this might be a certain guideline for setting parameters for the HS scheme or the Rainbow-type scheme.

Note that we discussed not the original HS scheme but the r-Rainbow scheme (the commutative HS scheme) only. So we need to promote research about constructing good non-commutative ring for the HS scheme. For example, the parameter $N = 65537$ is small prime, so we cannot use non-commutative OSS scheme. On the other hand, efficiency, especially key size, should be considered on. Finding how to generate keys for the original HS scheme is challenging future work.

6. Conclusion

We proposed an attack against the Hashimoto-Sakurai scheme. Our proposed attack is a polynomial-time algorithm with respect to its input sizes $r, l, \lg N$ under the condition that $n^r = (rl)^r$ is a polynomial in n and $\lg N$. Also, we discussed its efficiency of the attack and showed that it is practical if $(rl)^{(r+1)} \leq 2^{18}$ by using some experiments. In our 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. Note that not all the HS scheme are broken, namely, our algorithm would not work efficiently if $(rl)^{(r+1)}$ is large. It implies that the scheme would be secure in the case that N, l are not small and r is large, for example, the case that $(rl)^{(r+1)} > 2^{27}$ and $N^r (rl)^4 \geq 2^{80}$. Investigating security of the scheme for the HS scheme with specific parameters is our future work.

References

[1] H. Ong, C. P. Schnorr and A. Shamir, An efficient signature scheme based on quadratic equations, in: Proc. of 16th ACM Symp. Theory Comp., pp. 208–216, 1984.

[2] A. Shamir, Efficient signature schemes based on birational permutations, in: Proc. of Crypto '93, 1994; Lect. Notes in Comput. Sci., Vol. 773, pp. 1-12, Springer-Verlag, 1993.

[3] S. Tsujii, K. Kurosawa, T. Itoh, A. Fujioka and T. Matsumoto, A public-key cryptosystem based on the difficulty of solving a system of non-linear equations (in Japanese), IEICE Trans. Inf. & Syst., **J69-D** (1986), 1963–1970.

[4] T. Satoh and K. Araki, On construction of signature scheme over a certain non-commutative ring, *IEICE Trans. Fundamentals*, **E80-A** (1997), 40–45.

[5] J. M. Pollard and C. P. Schnorr, An efficient solution of the congruence $x^2 + ky^2 \equiv m(\pmod n)$, IEEE Trans. Inform. Theory, **33** (1987), 702–709.

[6] D. Coppersmith, J. Stern and S. Vaudenay, The security of the birational permutation signature scheme, J. Cryptology, **10** (1997), 207–221.

[7] D. Coppersmith, Weakness in quaternion signatures, in: Proc. of Crypto '99, Lect. Notes in Comput. Sci., Vol. 1666, pp. 305–314, Springer-Verlag, 1999.

[8] Y. Hashimoto and K. Sakurai, On construction of signature schemes based on birational permutations over noncommutative rings, presented at the 1st Int. Conf. on Symbolic Computation and Cryptography (SCC2008) held in Beijing, April 2008; Cryptology ePrint, http://eprint.iacr.org/2008/340+.

[9] J. Patarin, Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88, in: Proc. of CRYPTO '95, Lect. Notes in Comput. Sci., Vol. 963, pp. 248–261, Springer-Verlag, 1995.

[10] J. Ding and D. Schmidt, Rainbow, a new multivariable polynomial signature scheme, Lect. Notes in Comput. Sci., Vol. 3531, pp. 164–175, Springer-Verlag, 2005.

[11] N. T. Coutois, M. Daum and P. Felke, On the security of HFE, HFEv- and Quartz, in: Proc. of PKC2003, Lect. Notes in Comput. Sci., Vol. 2567, pp. 337–350, Springer-Verlag, 2003.

[12] J. Patarin, Hidden Field Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of asymmetric algorithms, in: Proc. of EUROCRYPT '96, Lect. Notes in Comput. Sci., Vol. 1070, pp. 33–48, Springer-Verlag, 1996.

[13] Magma, http://magma.maths.usyd.edu.au/magma/.

[14] J-C Faugère, A new efficient algorithm for computing Gröbner bases (F_4), J. Pure Appl. Algebra, **139** (1999), 61–68.

[15] J. Ding, B-Y Yang, C-H O. Chen, M-S Chen and C-M Cheng, New differential-algebraic attacks and reparametrization of Rainbow, Lect. Notes in Comput. Sci., Vol. 5037, pp. 242–257, Springer-Verlag, 2008.