On construction of signature schemes based on birational permutations over noncommutative rings

Yasufumi Hashimoto and Kouichi Sakurai

Abstract

In the present paper, we give a non-commutative version of Shamir's birational permutation signature scheme [Crypto '93, LNCS 773 (1994), pp.1-12] in terms of square matrices. The original idea to construct the multivariate quadratic signature is to hide a quadratic triangular system using two secret linear transformations. However, the weakness of the triangular system remains even after taking two transformations, and actually Coppersmith et al. broke it linear algebraically. In the non-commutative case, such linear algebraic weakness does not appear. We also give several examples of noncommutative rings to use in our scheme, the ring consisting of all square matrices, the quaternion ring and a subring of three-by-three matrix ring generated by the symmetric group of degree three. We note that the advantage of Shamir's original scheme is its efficiency. In our scheme, the efficiency is preserved enough.

[1] [2]

1 Introduction

In 1984, Ong, Schnorr and Shamir [5] suggested an efficient signature scheme in terms of the binary quadratic equation

$$x^2 + hy^2 \equiv m \bmod n, \tag{1.1}$$

where n is a composite integer with unknown factorization. Although it was considered that the security of the Ong-Schnorr-Shamir (OSS) signature scheme would be based on the difficulty of the factorization of n, Pollard and Schnorr [6] broke this scheme in

[1] This is the revised version of our manuscript presented in the first international conference on Symbolic Computation and Cryptography (SCC2008) held at Beijing, April, 2008.

[2] Keywords: Ong-Schnorr-Shamir's (OSS) signature scheme, Pollard-Schnorr's algorithm, birational permutation signature scheme, quaternion OSS, non-commutative rings, group ring

1987 by the probabilistic polynomial-time algorithm by solving (1.1) directly without factoring n.

In 1993, Shamir [9] gave an improvement of the OSS signature scheme in terms of the multi-variate quadratic forms built in a way to hide a quadratic triangular system using two secret linear transformations. However, Coppersmith, Stern and Vaudenay [2] broke it soon by reducing the multi-variate quadratic equations to binary and linear ones linear algebraically.

In 1997, Satoh and Araki [7] improved OSS in another way. They established the OSS signature scheme using the quaternion integers with the non-commutative multiplicative structure. Since Pollard-Schnorr's algorithm is based on one kind of commutative relation among the solutions of the binary quadratic equations over integers, direct non-commutative extensions of Pollard-Schnorr's algorithm is not effective to the quaternion OSS. However, their quaternion OSS was also broken by Coppersmith [1] in 1999 with some special properties of the quaternion algebra.

In this paper, we generalize Shamir's birational permutation signature scheme in terms of noncommutative ring consisting of square matrices, and discuss the security of our generalization. The weakness, in the original scheme, of the quadratic triangular system remains after taking two linear transformations. That appears in the determinants of the matrices whose entries are coefficients of the public quadratic forms. Coppersmith, Stern and Vaudenay got partial information of the second secret transformation, without any information of the first one, by solving the equations given by the determinants of such matrices. However, in the non-commutative case, such a linear algebraic discussion is not easy because the algebraic structure of the non-commutative ring is much more complicated. In fact, it is difficult to get the information of the second transformation without the first one. Furthermore, in the non-commutative linear algebra, there are no convenient tools like determinants which have the homomorphy for the multiplication ($\det(ab) = \det(a)\det(b)$) and characterize the linear independency of the row or column vectors in the matrices (cf. [3]). Even if the determinant which has all of such convenient properties could be stated, solving the equation given by the determinant would be difficult because the equation includes multi-parameters of the integers. Thus, to break our generalization, one should remove such difficulties in the non-commutative linear algebra.

However, it is not necessarily that our scheme is secure for any noncommutative ring. In fact, we think that the case of rings consisting of all square matrices is not very secure. In Section 5, we discuss the security for several examples of the noncommutative rings such like all matrix ring, quaternion algebra and a subring of three-by-three matrix ring generated by the elements of the symmetric group of degree three. We also give the way how to construct noncommutative rings like the group rings.

We note that the advantage of the original birational signature scheme is its efficiency. In Section 6, we discuss the computational task of our signature scheme and

show that it is not very different to the original scheme.

2 Ong-Schnorr-Shamir's signature scheme and its extensions

2.1 Ong-Schnorr-Shamir's signature scheme

The Ong-Schnorr-Shamir (OSS) signature scheme [5] is given as follows.

Keys. The secret keys are two primes p, q and an integer $u \in (\mathbb{Z}/pq)^\times$, and the public keys are $n := pq$ and $h := -u^{-2} \bmod n$.
Signatures. Let $m \in \mathbb{Z}/n$ be a message to be signed. The signature $(x_1, x_2) \in (\mathbb{Z}/n)^2$ is given by $x_1 := \rho^{-1}m + \rho$ and $x_2 := u(\rho^{-1}m - \rho)$, where $\rho \in (\mathbb{Z}/n)^\times$ is chosen randomly.
Verification. Verify whether $x_1^2 + hx_2^2 \equiv 4m \bmod n$.

The scheme above was broken by Pollard and Schnorr [6] with the probabilistic polynomial-time algorithm. Roughly speaking, their algorithm uses the following relation among the solutions of the binary quadratic equation.

$$(x_1^2 + hy_1^2)(x_2^2 + hy_2^2) = (x_1x_2 - hy_1y_2)^2 + h(x_1y_2 + x_2y_1)^2. \tag{2.1}$$

After their attack, several extensions of OSS signature scheme were established. We consider the following two extensions, one is multivariate version called by birational permutation signature scheme [9] and the other is quaternion (noncommutative) version [7].

2.2 Birational permutation signature scheme

We first note that, while Shamir gave two kinds of signature schemes in [9], we treat one of them in this paper.

Let p, q be primes, $n = pq$ an integer. Consider the following map ($l \geq 2$).

$$(\mathbb{Z}/n)^l \xrightarrow{A} (\mathbb{Z}/n)^l \xrightarrow{G} (\mathbb{Z}/n)^{l-1} \xrightarrow{B} (\mathbb{Z}/n)^{l-1}.$$

Here A, B are invertible affine (linear) transforms and $\mathbf{g} = (g_2, \cdots, g_l) := G(\mathbf{y})$ is given as follows.

$$g_i(y_1, \cdots, y_i) := \begin{cases} y_1y_2 & (i = 2), \\ v_i(y_1, \cdots, y_{i-1})y_i + w_i(y_1, \cdots, y_{i-1}) & (i \geq 3), \end{cases}$$

where v_i is a linear form and w_i is a quadratic form defined by

$$v_i(y_1, \cdots, y_{i-1}) := \sum_{1 \le j \le i-1} v_j^{(i)} y_j,$$
$$w_i(y_1, \cdots, y_{i-1}) := \sum_{1 \le j_1, j_2 \le i-1} w_{j_1 j_2}^{(i)} y_{j_1} y_{j_2}$$

with coefficients $v_j^{(i)}, w_{j_1 j_2}^{(i)} \in \mathbb{Z}/n$.

The signature scheme is as follows.

Keys: The secret keys are A, G and B, and the public key is $F := B \circ G \circ A$.

Signatures: Let $\mathbf{m} := (m_2, \cdots, m_l)^t \in (\mathbb{Z}/n)^l$ be a message to be signed. Calculate $\mathbf{m}' = (m_2', \cdots, m_l') := B^{-1}\mathbf{m}$. Choose $y_1 \in (\mathbb{Z}/n)^\times$ randomly and determine $y_2, \cdots, y_l$ recursively by

$$y_i := \begin{cases} y_1^{-1} m_2' & (i = 2), \\ v_i(y_1, \cdots, y_{i-1})^{-1}(m_i' - w_i(y_1, \cdots, y_{i-1})) & (3 \le i \le l). \end{cases}$$

Then the signature is given by $\mathbf{x} := A^{-1}\mathbf{y}$.

Verification: Verify whether $F(\mathbf{x}) = \mathbf{m}$.

The idea of this scheme to hide the simple generation of G by two transformations A and B. However, the weakness of G remains after taking A and B. In fact, Coppersmith-Stern-Vaudenay [2] broke this scheme by reducing the problem solving multivariate quadratic equations to that doing binary quadratic and linear equations linear algebraically.

2.3 Quaternion OSS signature scheme

In 1997, Satoh and Araki [7] established the quaternion version of OSS signature scheme.

The quaternion numbers are defined by $q := q_0 + q_1 i_1 + q_2 i_2 + q_3 i_3$ where $q_0, \cdots, q_3 \in \mathbb{R}$ and $(1, i_1, i_2, i_3)$ is the basis of the quaternion algebra as a linear space over $\mathbb{R}$ determining the multiplicative rule as $i_1^2 = i_2^2 = i_3^2 = -1$, $i_1 i_2 = i_3 = -i_2 i_1$. It is well-known that there is the following one-to-one correspondence between the quaternion numbers and two-by-two complex matrices.

$$q_0 + q_1 i_1 + q_2 i_2 + q_3 i_3 \leftrightarrow \begin{pmatrix} q_0 + q_1\sqrt{-1} & q_2\sqrt{-1} + q_3 \\ -q_2\sqrt{-1} + q_3 & q_0 - q_1\sqrt{-1} \end{pmatrix}.$$

The correspondence above preserves the addition and the multiplication. Usually the transposition q^t, the complex conjugation $\bar{q}$ and the inversion q^{-1} of the quaternion number q are given as those in the corresponding matrix respectively.

The signature scheme is as follows.

Quaternion OSS signature scheme.

Let p, q be two primes, $n := pq$ and $R := \{q_0 + q_1 i_1 + q_2 i_2 + q_3 i_3 \mid q_i \in \mathbb{Z}/n\}$.

Keys. The secret keys are primes p, q and a quaternion $u \in R^\times$, and the public key is $n = pq$ and $h := -(u^t)^{-1}u^{-1}$.

Signatures. Let $m \in$ be a message to be signed and assume that $m^t = m$. The signature $(x_1, x_2) \in R$ is given by $x_1 := \rho^{-1}m + \rho^t$ and $x_2 := u(\rho^{-1}m - \rho^t)$ where $\rho \in R^\times$ is chosen randomly.

Verification. Verify whether $x_1^t x_1 + x_2^t h x_2 = 4m$ in R.

While Pollard and Schnorr used the formula (2.1) to attack the original scheme, (2.1) holds only in commutative rings. Then the direct extension of Pollard-Schnorr's attack is not valid to the quaternion OSS. However, Coppersmith [1] broke it in 1999 by reducing the problem solving the binary quadratic form over quaternion integers to that doing binary quadratic forms over integers.

3 Non-commutative birational permutation signature schemes

In this section, we construct the non-commutative version of the birational permutation signature scheme.

Let K be an algebraic number field/$\mathbb{Q}$ with $[K : \mathbb{Q}] < \infty$, $\mathcal{O}$ the integer ring of K. Denote by p, q prime numbers or prime ideals in $\mathcal{O}$, $n = p$ or $n = pq$ and R a noncommutative subring of $\mathrm{Mat}_s(\mathcal{O}/n)$ $(s \geq 1)$ such that $a^t \in R$ for any $a \in R$. For convenience, we put $\{\alpha_1, \cdots, \alpha_r\}$ a subset of R satisfying $\{\sum_{i=1}^r m_i\alpha_i \mid m_i \in \mathbb{Z}\} = R$ and $\alpha_i \neq \sum_{j\neq i} m_j\alpha_j$ for any $1 \leq i \leq r$ and $m_j\mathbb{Z}$.

Consider the following map $(l \geq 2)$.

$$(\mathbb{Z}/n)^{rl} \xrightarrow{A} (\mathbb{Z}/n)^{rl} \xrightarrow{\phi} R^l \xrightarrow{G} R^{l-1} \xrightarrow{\psi} (\mathbb{Z}/n)^{r(l-1)} \xrightarrow{B} (\mathbb{Z}/n)^{r(l-1)},$$

Here A, B are invertible affine (linear) transforms and ϕ, ψ are projections like

$$\phi\big((y_{11}, \cdots, y_{1r}, y_{21}, \cdots, y_{lr})\big) = (y_{11}\alpha_1 + \cdots + y_{1r}\alpha_r, \cdots, y_{l1}\alpha_1 + \cdots + y_{lr}\alpha_r),$$
$$\psi\big((g_{21}\alpha_1 + \cdots + g_{2r}\alpha_r, \cdots, g_{l1}\alpha_1 + \cdots + g_{lr}\alpha_r)\big) = ((g_{21}, \cdots, g_{2r}, g_{31}, \cdots, g_{lr})),$$

and $\mathbf{g} = (g_2, \cdots, g_l) := G(\mathbf{y})$ is given as follows.

$$g_i(y_1, \cdots, y_i) := v_{i1}(y_1, \cdots, y_{i-1})^t y_i + y_i^t v_{i2}(y_1, \cdots, y_{i-1}) + w_i(y_1, \cdots, y_{i-1}),$$

where v_{i1}, v_{i2} are linear forms and w_i is a quadratic form defined by

$$v_{i\delta}(y_1, \cdots, y_{i-1}) := \sum_{1 \le j \le i-1} v_{i\delta}^{(j)} y_j, \quad (\delta = 1, 2),$$
$$w_i(y_1, \cdots, y_{i-1}) := \sum_{1 \le j_1, j_2 \le i-1} y_{j_1}^t w_{j_1 j_2}^{(i)} y_{j_2},$$

with coefficients $v_{j1}^{(i)}, v_{j2}^{(i)}, w_{j_1 j_2}^{(i)} \in R$. The signature scheme is as follows.

Signature scheme.

Keys: The secret keys are A, G and B and the public key is $F := B \circ \psi \circ G \circ \phi \circ A$.

Signatures: Let $\mathbf{m} := (m_{22}, \cdots, m_{lr})^t \in (\mathbb{Z}/n)^{r(l-1)}$ be the message to be signed. Calculate $\mathbf{m}' = (m'_{22}, \cdots, m'_{lr})^t = B^{-1}\mathbf{m}$. Choose $y_1 \in R$ randomly and determine $y_2, \cdots, y_l \in R$ recursively by solving $g_i(y_1, \cdots, y_i) = \psi^{-1}(m'_i)$. The signature is given by $\mathbf{x} = A^{-1}\big(\phi^{-1}(\mathbf{y})\big) \in (\mathbb{Z}/n\mathbb{Z})^{rl}$.

We note that solving linear equations of the type $ax + x^t b = m$ with noncommutative operations in R is not easy. However, since R is finitely generated over a commutative ring, we can solve it by the Gaussian elimination or the LU-decomposition method after writing the equation over R as equations over $\mathbb{Z}/n$.

Verification: Verify whether $F(\mathbf{x}) = \mathbf{m}$.

4 Discussions on security

4.1 The original and commutative versions

Let $\mathbf{x} \in (\mathbb{Z}/n)^l$ be the signature, $\mathbf{y} := A\mathbf{x}$, $\mathbf{g} = (g_2, \cdots, g_l) := G(\mathbf{y})$ and $\mathbf{f} = (f_2, \cdots, f_l) := B\mathbf{g}$. Denote by $G_i, F_i \in \mathrm{Mat}_l(\mathbb{Z}/n)$ matrices satisfying $g_i(\mathbf{y}) = \mathbf{y}^t G_i \mathbf{y}$ and $\mathbf{f} = B\mathbf{g}$. We have

$$f_i(\mathbf{x}) = \sum_{j=2}^{l} b_{ij} \mathbf{x}^t A^t G_j A \mathbf{x} = \mathbf{x}^t A^t \left(\sum_{j=2}^{l} b_{ij} G_j \right) A\mathbf{x} =: \mathbf{x}^t F_i \mathbf{x}, \tag{4.1}$$

where $B = (b_{ij})_{2 \le i,j \le l}$. Since

$$G_i = \begin{pmatrix} & & v_1^{(i)} \\ & W_i & \vdots \\ & & v_{i-1}^{(i)} \\ v_1^{(i)} & \cdots & v_{i-1}^{(i)} \\ & & \\ & & 0 \end{pmatrix},$$

with $W_i \in \mathrm{Mat}_{i-1}(\mathbb{Z}/n)$, we have

$$\sum_{j=2}^{l} b_{i_1 j} G_j - \lambda \sum_{j=2}^{l} b_{i_2 j} G_j$$
$$= \begin{pmatrix} & & (b_{i_1 l} - \lambda b_{i_2 l}) v_1^{(l)} \\ & * & \vdots \\ & & (b_{i_1 l} - \lambda b_{i_2 l}) v_{i-1}^{(i)} \\ (b_{i_1 l} - \lambda b_{i_2 l}) v_1^{(i)} & \cdots & (b_{i_1 l} - \lambda b_{i_2 l}) v_{i-1}^{(i)} \quad 0 \end{pmatrix}.$$

The determinant of the matrix above has a factor $(b_{i_1 l} - \lambda b_{i_2 l})^2$. Then one can get the partial information $\{b_{i_1 l} b_{i_2 l}^{-1}\}$ of secret B by taking the common divisor of $\det(F_{i_1} - \lambda F_{i_2})$ and its differentiation by λ. Other hidden information in A and B can be found little by little recursively. Using such information, one can reduce the problem solving the public polynomials $\mathbf{f} = (f_2, \cdots, f_l)$ to that doing polynomials $\mathbf{f}' = (f_2', \cdots, f_l')$ with simple forms like $\mathbf{g}$. Therefore, Pollard-Schnorr's algorithm and some elementary operations would give solutions of $\mathbf{f}(\mathbf{x}) = \mathbf{m}$. See [2] for the detail of this attack to the original birational permutation signature scheme.

For commutative R, the situation is similar. In fact, when we consider A and B as transformations of R^l and R^{l-1} respectively, (4.1) and linear algebraic operations are similar. Then one can find partial information in B by solving the equations in terms of the public matrices.

4.2 Noncommutative version

When R is noncommutative, direct extensions of the attack to the original scheme is difficult even if A, B are expressed as transformations in R^l and R^{l-1}. One of difficulties is that

$$f_i(\mathbf{x}) = \sum_{j=2}^{l} b_{ij} \mathbf{x}^t A^t G_j A \mathbf{x} \neq \mathbf{x}^t A^t \left(\sum_{j=2}^{l} b_{ij} G_j \right) A \mathbf{x},$$

namely it is difficult to express the public polynomials as the quadratic forms over R. And another difficulty is that there are few convenient tools in the linear algebra over noncommutative rings like determinants. The convenient properties of the determinant in commutative ring is (i) to characterizes the linear independency of the column and row vectors, and (ii) to satisfy the multiplicative rule $\det(ab) = \det(a)\det(b)$. In noncommutative R, there are several kinds of determinants. For example,

$$\det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} := a_{11} a_{22} - a_{11} a_{21} a_{11}^{-1} a_{12}$$

satisfies the property (i); in fact, if the determinant above is zero then $(a_{21}, a_{22}) = a_{12}a_{11}^{-1}(a_{11}, a_{12})$ and $\begin{pmatrix} a_{12} \\ a_{22} \end{pmatrix} = \begin{pmatrix} a_{11} \\ a_{21} \end{pmatrix} a_{11}^{-1}a_{12}$ (see, e.g. [3]). For $a = (a_{ij})_{1\leq i,j\leq l} \in \mathrm{Mat}_l(R)$ with larger l, the descriptions of such a determinant is much more complicated. It is easy to see that such determinants do not satisfy the multiplicative rule (ii). Then we claim that attacking with linear algebra over noncommutative ring is difficult.

Next we consider the polynomials as those over integers. Let

$$\begin{aligned} \mathbf{y} =& y^{(1)}\alpha_1 + \cdots + y^{(r)}\alpha_r, & y^{(k)} \in (\mathbb{Z}/n)^l, \\ G_j =& G_j^{(1)}\alpha_1 + \cdots + G_j^{(r)}\alpha_r, & G_j^{(k)} \in \mathrm{Mat}_l(\mathbb{Z}/n). \end{aligned}$$

Then we have

$$g_i = \tilde{\mathbf{y}}^t G_i \mathbf{y} = \sum_{k_1,k_2,k_3=1}^{r} (y^{(k_1)})^t G_i^{(k_2)} y^{(k_3)} (\alpha_{k_1}^t \alpha_{k_2} \alpha_{k_3}).$$

Since R is a ring, the product $\alpha_{k_1}^t \alpha_{k_2} \alpha_{k_3}$ is written by a linear combination of $\alpha_1, \cdots, \alpha_r$. Put $c_{k_1k_2k_3}^{(k)} \in \mathbb{Z}/n$ such that $\alpha_{k_1}^t \alpha_{k_2} \alpha_{k_3} = c_{k_1k_2k_3}^{(1)}\alpha_1 + \cdots + c_{k_1k_2k_3}^{(r)}\alpha_r$. Then we have

$$\begin{aligned} g_i &= \sum_{k=1}^{r} \left[\sum_{k_1,k_2,k_3=1}^{r} c_{k_1k_2k_3}^{(k)} (y^{(k_1)})^t G_i^{(k_2)} y^{(k_3)} \right] \alpha_k \\ &= \sum_{k=1}^{r} \left[\sum_{k_1,k_3=1}^{r} (y^{(k_1)})^t \left[\sum_{k_2=1}^{r} c_{k_1k_2k_3}^{(k)} G_i^{(k_2)} \right] y^{(k_3)} \right] \alpha_k \\ &= \sum_{k=1}^{r} \left[\mathbf{y}^t G_{i,k} \mathbf{y} \right] \alpha_k, \end{aligned}$$

where

$$G_{i,k} = \left(\sum_{k_2=1}^{r} c_{k_1k_2k_3}^{(k)} G_i^{(k_2)} \right)_{1\leq k_1,k_3\leq r} = \left(\begin{pmatrix} W_{i,k}^{(k_1,k_3)} & \\ & 0 \end{pmatrix} \right)_{1\leq k_1,k_3\leq r}$$

and $W_{i,k}^{(k_1,k_3)} \in \mathrm{Mat}_i(\mathbb{Z}/n)$. In the original case, types of all matrices G_i are distinct to each other. On the other hand, in the noncommutative case, the types of $G_{i,k}$'s are same if k is same. Then, after taking the transformations A, B, the information in G is mixed and then picking up it would be difficult. However, we should be care about the choice of R because most $c_{k_1k_2k_3}^{(k)}$ might be vanished and, if so, $G_{i,k}$ would be of very simple form. Then, at the next section, we consider several examples and check the distributions of $c_{k_1k_2k_3}^{(k)}$.

5 Examples of non-commutative signatures

In this section, we give some examples of R.

5.1 $R = \mathrm{Mat}_k(\mathbb{Z}/n)$

The most naive choice of R is $R = \mathrm{Mat}_s(\mathbb{Z}/n)$. The dimension of R is $r = s^2$ and the basis of $R = \mathrm{Mat}_s(\mathbb{Z}/n)$ can be taken by $\{e_{ij}\}_{1 \le i,j \le s}$ where

$$e_{ij} := \begin{array}{c} \\ i \end{array} \begin{array}{c} \begin{array}{c} \quad j \end{array} \\ \begin{pmatrix} \cdots & \vdots \\ & 1 \\ & \end{pmatrix} \end{array}.$$

Since

$$e_{i_1 j_1} e_{i_2 j_2} = \begin{cases} e_{i_1 j_2} & (j_1 = i_2), \\ 0 & (\text{otherwise}), \end{cases}$$

it is easy to see that

$$\mathrm{Prob}_R(c \neq 0) := \frac{\#\{1 \le k_1, k_2, k_3, k \le r \mid c^{(k)}_{k_1 k_2 k_3} \neq 0\}}{\#\{1 \le k_1, k_2, k_3, k \le r\}} = \frac{1}{s^4}.$$

This means that most $c^{(k)}_{k_1 k_2 k_3}$'s are zero, and then we think that the signature scheme is not strong. In fact, the OSS signature scheme for $R = \mathrm{Mat}_s(\mathbb{Z}/n)$ can be broken easily.

An attack to OSS with $R = \mathrm{Mat}_s(\mathbb{Z}/n)$. Consider the case of $s = 2$ for simplicity. Let $h := (h_{ij})_{1 \le i,j \le 2}, m = (m_{ij})_{1 \le i,j \le 2} \in \mathrm{Mat}_2(\mathbb{Z}/n)$ be the public key and the message to be signed, and assume that $h^t = h$ and $m^t = m$. Denote by $x_1^t x_1 + x_2^t h x_2 = m$ the equation of $(x_1, x_2) \in R^2$ to be solved. Now, take

$$x_1 = \begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix}, \quad x_2 = \begin{pmatrix} b_1 & 0 \\ 0 & b_2 \end{pmatrix}.$$

Then the equation $x_1^t x_1 + x_2^t h x_2 = m$ gives the following three equations over $\mathbb{Z}/n$.

$$\begin{aligned} a_{11}^2 + h_{11} b_1^2 &= 4m_{11}, \\ a_{11} a_{12} + h_{12} b_1 b_2 &= 4m_{12}, \\ a_{12}^2 + a_{22}^2 + h_{22} b_2^2 &= 4m_{22}. \end{aligned}$$

One can solve the equations above by using the Pollard-Schnorr's algorithm twice.

This situation is similar to the case of $s \geq 3$. In fact, one can solve the equation $x_1^t x_1 + x_2^t h x_2 = m$ by taking x_1 and x_2 as triangle and diagonal matrices respectively, and using the Pollard-Schnorr algorithm s-times. □

Of course, the discussion above does not necessarily claim that general birational permutation signature scheme with $R = \mathrm{Mat}_s(\mathcal{O}/n)$ can be broken. However, the fact that the binary case can be solved by triangle and diagonal matrices may imply that the scheme with $R = \mathrm{Mat}_k(\mathcal{O}/n)$ includes many parameters which do not contribute to the security.

5.2 Quaternion version

The notations for quaternion numbers are as in Section 2.3. Put R as follows.

$$R = \left\{ \begin{pmatrix} w & z \\ -\bar{z} & \bar{w} \end{pmatrix} \;\middle|\; w, z \in \mathbb{Z}[\sqrt{-1}]/n \right\}.$$

The basis of R is taken by $\{i_0, i_1, i_2, i_3\}$ where i_0 is the identity and i_1, i_2, i_3 satisfies the multiplicative rules $i_1^2 = i_2^2 = i_3^2 = -1$ and $i_1 i_2 = i_3 = -i_2 i_1$. It is easy to see that $i_{k_1}^t i_{k_2} i_{k_3} = \pm i_j$ for some $j = 0, \cdots, 3$. Then, for any k_1, k_2, k_3, $c_{k_1 k_2 k_3}^{(k)} = \pm 1$ holds for one of $k = 0, \cdots, 3$ and $c_{k_1 k_2 k_3}^{(k)} = 0$ otherwise. Thus we have $\mathrm{Prob}_R(c \neq 0) = 1/4$ and we think that the birational permutation signature scheme with quaternion R would be stronger than that with $R = \mathrm{Mat}_s(\mathbb{Z}/n)$.

We note that the quaternion OSS was broken by Coppersmith [1]. However, his attack is very technical and uses special properties of the quaternion algebra and those of binary quadratic equation over quaternion integers. Then we do not think that extending his attack to multivariate versions is easy. For a reference, we now give short surveys of his two kinds of attacks to the quaternion OSS (see [1] for detail).

Coppersmith's first attack. This attack requires several known pairs of messages and corresponding signatures. It is not difficult to see that if $\alpha \in R$ satisfies that $x_1^t \alpha x_2$ is symmetric for any symmetric $m \in R$ then αu is a scalar in the quaternion R. Then we see that, using 3-known signatures, one can find $\alpha \in R$ such that $\alpha = l u^{-1}$ for some $l \in \mathbb{Z}/n$ with high probability. Since $\alpha^t \alpha = l^2 h$, l^2 is known. This means that the problem solving the equation $x_1^t x_1 + x_2^t h x_2 = 4m$ to that finding $\delta \in R$ satisfying $\delta^t \delta = l^2$. Taking $\delta := c + d i_2$ $(c, d \in \mathbb{Z}/n)$, we have $\delta^t \delta = c^2 + d^2$. Since the equation $c^2 + d^2 = l^2$ can be solved by Pollard-Schnorr's algorithm, one can break the signature scheme by using $\alpha^{-1} = u\delta$ instead of the secret key u.

We note that this attack is effective to the cases where the center of R is the set of scalars and R has elements β such that both $\beta^t + \beta$ and $\beta^t \beta$ are scalars. The quaternion R $(\beta = i_2)$ and $\mathrm{Mat}_{2k}(\mathbb{Z}/n)$ $\left(\beta = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}\right)$ are examples of such R.

The second attack. Note that the second attack requires only the message m and the public key h. This attack uses the following three properties of the quaternion ring; (i) the symmetric elements of R are written by three parameters of $\mathbb{Z}/n$, (ii) any power m^k $(k \geq 2)$ of m is written by the linear combination of 1 and m, (iii) there is a $\delta = \delta(x, y) \in R$ such that $\delta^t \delta = x^2 + hy^2$ for some $h \in \mathbb{Z}/n$. Roughly speaking, these properties reduces the problem solving the quadratic equation $x_1^t x_1 + x_2^t h x_2 = 4m$ in R to that doing three quadratic equations in $\mathbb{Z}/n$. Then, using Pollard-Schnorr's algorithm three times, one can break the signature scheme.

In the next subsection, we give an example of $R \subset \mathrm{Mat}_3(\mathbb{Z}/n)$ which could not broken by Coppersmith's attacks under the assumption that factoring n is infeasible.

5.3 An example of $R \subset \mathrm{Mat}_3(\mathbb{Z}/n)$

Let

$$g_1 := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad g_2 := \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad g_3 := \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$
$$g_4 := \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad g_5 := \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

and put $R_3 := \{\sum_{i=1}^{5} a_i g_i \mid a_i \in \mathbb{Z}/n\}$. It is easy to see that R_3 is a subring of $\mathrm{Mat}_3(\mathbb{Z}/n)$ and the identity of R_3 is $I = g_1 + g_2 + g_3 - g_4 - g_5$. The set $\{I, g_1, \cdots, g_5\}$ is isomorphic to the symmetric group of degree 3. Then we see that $g_{k_1}^t g_{k_2} g_{k_3}$ is one of $g_1, \cdots, g_5$ or I and $\mathrm{Prob}_{R_3}(c \neq 0) \sim 1/3$.

We note that, for this R_3, the OSS signature scheme is secure against Coppersmith's attacks. The reason is as follows.

Against the first attack. In the quaternion case, one can find a scalar multiple of the secret key by using several known pairs of signatures and messages. However, this situation is not same in general. Because the set of $\alpha \in R$ satisfying that $x_1^t \alpha x_2$ is symmetric for any $m \in R$ includes $u^{-1}C(R)$ where $C(R)$ is the center of R. The center $C(R)$ of the quaternion R is the set of scalars, however, the center $C(R_3)$ of R_3 is $\{\gamma(a, b) := aI + b(g_4 + g_5) \mid a, b \in \mathbb{Z}/n\}$. Then a scalar multiple of the secret key is not necessarily found feasibly. Even if the scalar multiple $\alpha = lu^{-1}$ of the secret key could be found, determining $\delta \in R$ such that $\delta^t \delta = l^2$ is infeasible under the infeasibility of the factorization of n. Because, if one would find such a $\delta \in R$, he could do the square root of $(l^2)^3$ by calculating the determinant of δ. This contradicts to the infeasibility of the factorization. Then we conclude that Coppersmith's first attack is not effective.

Against the second attack. The second attack is very technical and is applicable

only to the two-by-two matrix cases. In fact, none of the properties (i)-(iii) do not hold for $R = R_3$. Then this attack is not effective to the case of $R = R_3$.

We also note that the first attack is not effective to the odd(≥ 3) dimensional matrix cases, and the second attack is not to the higher than two dimensional cases.

5.4 An idea to construct other R's

In the previous two cases, R is written by $R := \{\sum_{g\in G} a_g g \mid a_g \in \mathbb{Z}/n\}$ with the following finite non-abelian group

$$G = \begin{cases} \{\pm 1, \pm i_1, \pm i_2, \pm i_3\}, & R \text{ is quaternion,} \\ \{I, g_1, \cdots, g_5\}, & R = R_3. \end{cases}$$

This situation is generalized as follows.

Let G be a finite subset of $\mathrm{Mat}_s(\mathcal{O})$ for some algebraic number field $K(\supset \mathcal{O})$ which is isomorphic to a non-abelian group. Denote by $G' = \{g_1, \cdots, g_r\}$ a subset of G such that $g_i^t \in G'$ for any $g_i \in G'$, $\{g_1, \cdots, g_r\}$ is linearly independent over $\mathbb{Z}$ and any elements of G are written by linear combinations of $g_1, \cdots, g_r$. Put $R = R[G'] := \{\sum_{i=1}^r a_i g_i \mid a_i \in \mathbb{Z}/n\}$. Then R is a subring of $\mathrm{Mat}_k(\mathcal{O}/n)$ and can be used in our scheme. It is easy to see that $\mathrm{Prob}_R(c \neq 0) \geq 1/\#G'$, and especially if $G' = G$ then $\mathrm{Prob}_R(c \neq 0) = 1/\#G'$.

If $G = G'$, the ring $R[G]$ is isomorphic to the group ring (group algebra) of G over $\mathbb{Z}/n$. Since elements of any finite group G can be expressed as finite dimensional square matrices, the group ring can be also expressed as a subring of a matrix ring (see, e.g. [8]). We note that the ring $R[G']$ with $G' \neq G$ is constructed with the finite dimensional representation χ of G by $\{\sum_{g\in G} a_g \chi(g) \mid a_g \in \mathbb{Z}/n\}$. Then if one needs to construct $R[G']$ for a given G, he only has to do a finite dimensional representation of G.

We remark that one should be care of the construction of $R[G']$. It is known that the maximal compact group in $\mathrm{Mat}_s(\mathbb{C})$ is isomorphic to the unitary group $U(s) := \{g \in \mathrm{Mat}_s(\mathbb{C}) \mid \bar{g}^t g = I\}$ (see, e.g. [4], [10]). Then any finite group G in $\mathrm{Mat}_s(\mathbb{C})$ is expressed as a discrete subgroup of $U(s)$ up to isomorphism. Since

$$U(2) = \left\{ \rho \begin{pmatrix} w & z \\ -\bar{z} & \bar{w} \end{pmatrix} \;\middle|\; w, z, \rho \in \mathbb{C}, |\rho| = 1, |w|^2 + |z|^2 = 1 \right\}.$$

the subring $R[G']$ of $\mathrm{Mat}_2(\mathbb{C})$ has a similar expression to the quaternion R. Then we can think that the security of the signature scheme with such $R[G']$ is not very different to that with the quaternion R. In fact, OSS with such $R[G']$ can be broken by Coppersmith's attack similarly. The unitary group $U(k)$ with $k \geq 3$ does not have such a simple expression and includes many kinds of finite groups like the polyhedral groups. Then one can construct various $R[G'] \subset \mathrm{Mat}_k(\mathcal{O}/n)$ for $k \geq 3$ in this way.

6 Efficiency

The advantage of the original birational signature scheme is its efficiency, especially compared to the RSA signature (see [9]). In this section, we study the efficiency of our scheme compared to the original scheme with the same $L := lr$.

Since the public key includes $r(l-1)$ number of quadratic equations with rl variables, the efficiency of our scheme in the verification process is almost same to that of the original scheme.

On the other hand, the signing process includes the inverse operations of A, G and B. The inversions of A and B require $O\big((lr)^3\big)$-order of computational task by the Gaussian elimination and $O\big((lr)^2\big)$-order one by the LU-decomposition. Since the inversion of G is calculated by $l-1$-times of inversions of affine transforms in $\mathbb{Z}/n)^r$, the computational task of G^{-1} is $O(lr^3)$ or $O(lr^2)$-order. This means that the total computational task in the signing process is almost $O(L^2) \sim O(L^3)$ order, which is not very different to that of the original scheme.

From the discussions the above, we claim that our scheme preserves the advantage of the original scheme for the efficiency.

7 Conclusion

In this article, we construct a new signature scheme based on multivariate quadratic equations by combining Shamir's [9] and Satoh-Araki's [7] ideas and by generalizing the noncommutative situations. Although we see that the linear algebraic attack to the original scheme is not effective to our scheme, we have not completed the security proof, namely we have never proven that one cannot break our scheme unless he can solve some hard problems such like factorization problem, NP-hard (or complete) problems and so on. Then it is an open problem that which R and which properties of R assures strong security. One of criterions is $\mathrm{Prob}_R(c \neq 0)$ since, if it is bigger, the structure of the quadratic forms seems more complicated. However, it is not enough as a criterion of security because constructing a commutative R with bigger $\mathrm{Prob}_R(c \neq 0)$ is not difficult. Then we should study the relations between the security of the signature scheme and more detail distributions of $c^{(k)}_{k_1k_2k_3}$ or the algebraic structure of R. For example, if the distribution of $c^{(k)}_{k_1k_2k_3}$ has a symmetricity in some sense like commutative case, there might be attacks using the symmetricity. Conversely, if the distribution has a strong bias, there might be attacks using its bias (like the differential attack?). Other than the aboves, there might be technical attacks using special properties in the algebraic structures of R like Coppersmith's attacks to the quaternion OSS. And estimating the security against some experimental attacks like the Gröbner basis attack is an important problem. There are many things to study more for the practical use.

References

[1] D. Coppersmith, *Weakness in quaternion signatures*, Crypto'99, LNCS **1666** (1999), pp.305-314.

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

[3] I. Gelfand, S. Gelfand, V. Retakh and R.L. Wilson, *Quasideterminants*, Adv. in Math., **193** (2005), pp.56-141.

[4] S. Helgason, *Differential geometry, Lie groups and symmetric spaces*, Pure and Appl. Math. **80**, Academic Press, 1978.

[5] H. Ong, C.P. Schnorr and A. Shamir, *An efficient signature scheme based on quadratic equations*, Proc. 16th ACM Symp. Theory Comp., (1984), pp.208-216.

[6] J.M. Pollard and C.P. Schnorr, *An efficient solution of the congruence* $x^2+ky^2 \equiv m(\mathrm{mod}n)$, IEEE Trans. Inf. Theory, **IT-33** (1987), pp.702-709.

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

[8] J.P. Serre, *Linear representations of finite groups*, Graduate Texts in Mathematics, **42**, Springer, 1977.

[9] A. Shamir, *Efficient signature schemes based on birational permutations*, Advances in Cryptology - Crypto'93, LNCS **773** (1994), pp.1-12.

[10] G. Warner, *Harmonic Analysis on Semi-Simple Lie Groups I,II*, Springer, 1972.

HASHIMOTO, Yasufumi
Institute of Systems, Information Technologies and Nanotechnologies
7F 2-1-22, Momochihama, Fukuoka 814-0001, JAPAN
e-mail:hasimoto@isit.or.jp

SAKURAI, Kouichi
Institute of Systems, Information Technologies and Nanotechnologies
7F 2-1-22, Momochihama, Fukuoka, 814-0001 JAPAN
e-mail:sakurai@isit.or.jp
Department of Computer Science and Commmunication Engineering,
Kyiushu University

744 Motooka, Fukuoka, 819-0395, JAPAN
e-mail:sakurai@csce.kyushu-u.ac.jp
URL: http://itslab.csce.kyushu-u.ac.jp/index.html