JSIAM Letters Vol.11 (2019) pp.45–48 ©2019 Japan Society for Industrial and Applied Mathematics JSIAM Letters

# Key recovery attack on Circulant UOV/Rainbow

Yasufumi Hashimoto[1]

[1] Department of Mathematical Sciences, University of the Ryukyus, 1 Senbaru, Nishihara-cho, Okinawa 903-0213, Japan

E-mail *hashimoto@math.u-ryukyu.ac.jp*

Received December 27, 2018, Accepted March 2, 2019

**Abstract**

UOV and Rainbow are multivariate signature schemes, which are known to be efficient and secure enough against known attacks under suitable parameter selections, and have been expected to be post-quantum cryptography. Recently, new variants of UOV and Rainbow, called Circulant UOV and Circulant Rainbow respectively, were proposed by Peng and Tang. In these variants, the signature generation is faster than the original schemes since circulant matrices appear in the process of signature generation. However, such circulant structures weaken the security. In this paper, we study the structures of these circulant variants and show that they are vulnerable against Kipnis-Shamir's attack.

**Keywords** UOV, Rainbow, Circulant UOV, Circulant Rainbow, multivariate public-key cryptosystem (MPKC)

**Research Activity Group** Algorithmic Number Theory and Its Applications

## 1. Introduction

A multivariate public key cryptosytem (MPKC) is a public key cryptosytem whose public key is a set of multivariate quadratic forms over a finite field. It has been expected that MPKCs will be post-quantum cryptography since the problem of solving a system of multivariate non-linear polynomials is NP-Hard [1,2]. The unbalanced oil and vinegar signature scheme (UOV) [3,4] and Rainbow [5] can be considered to be two of the most successful multivariate signature schemes since the signature generations are efficient and the security against known attacks are enough under suitable parameter selections. In fact, several MPKCs submitted to NIST's post-quantum cryptography standardization project [6] are based on UOV and Rainbow.

Recently, Peng and Tang proposed new variants of UOV and Rainbow called Circulant UOV [7] and Circulant Rainbow [8] respectively. In these variants, coefficients of quadratic forms in the central maps are chosen such that circulant matrices appear in the process of signature generation. Since inverting a circulant matrix is faster than inverting a random matrix, the signature generation of Circulant UOV/Rainbow is faster than the original scheme. However, such "circulant" structures weaken the security critically. In this paper, we study the structures of Circulant UOV and Circulant Rainbow carefully and conclude that equivalent secret keys can be recovered by Kipnis-Shamir's attack [4,9] in polynomial time.

## 2. UOV

We first describe the unbalanced oil and vinegar signature scheme (UOV) [3,4] and Kipnis-Shamir's attack on UOV [4,9].

Let $n$, $o$, $v \geq 1$ be integers with $v \geq o$, $n = o+v$, $q$ be a power of prime and $\mathbf{F}_q$ a finite field of order $q$. Define the quadratic map $G : \mathbf{F}_q^n \to \mathbf{F}_q^o$, $\mathbf{x} = {}^t(x_1, \ldots, x_n) \mapsto G(\mathbf{x}) = {}^t(g_1(\mathbf{x}), \ldots, g_o(\mathbf{x}))$ by

$$g_l(\mathbf{x}) = \sum_{1 \leq i \leq o} x_i \cdot (\text{linear form of } x_{o+1}, \ldots, x_n) + (\text{quadratic form of } x_{o+1}, \ldots, x_n), \ (1 \leq l \leq o),$$

where the coefficients in the right hand side are elements of $\mathbf{F}_q$. The unbalanced oil and vinegar signature scheme (UOV) is constructed as follows.

**Secret key.** An invertible affine map $S : \mathbf{F}_q^n \to \mathbf{F}_q^n$ and the quadratic map $G$ defined above.

**Public key.** The quadratic map $F := G \circ S : \mathbf{F}_q^n \to \mathbf{F}_q^o$.

**Signature generation.** For a message $\mathbf{m} = {}^t(m_1, \ldots, m_o) \in \mathbf{F}_q^o$ to be signed, choose $u_1, \ldots, u_v \in \mathbf{F}_q$ randomly, and find $(y_1, \ldots, y_o) \in \mathbf{F}_q^o$ with

$$\begin{aligned} &g_1(y_1, \ldots, y_o, u_1, \ldots, u_v) = m_1, \\ &\ldots, \quad g_o(y_1, \ldots, y_o, u_1, \ldots, u_v) = m_o. \end{aligned} \tag{1}$$

The signature for $\mathbf{m}$ is $\mathbf{z} := S^{-1t}(y_1, \ldots, y_o, u_1, \ldots, u_v)$.

**Signature verification.** The signature $\mathbf{z}$ is verified if $F(\mathbf{z}) = \mathbf{m}$ holds.

Note that, due to the definition of $G$, the equations in (1) are linear equations of $(y_1, \ldots, y_o)$. Then a signature is generated in time $O(n^3)$ on UOV. It is well-known that UOV with $o = v$ (balanced oil and vinegar signature scheme, [3]) is broken by Kipnis-Shamir's attack [4, 9]. The basic idea of Kipnis-Shamir's attack is as follows.

**Kipnis-Shamir's attack.** Suppose that $o = v$ and, for simplicity, $S$ is a linear map expressed by an $n \times n$ matrix. Let $f_1(\mathbf{x}), \ldots, f_o(\mathbf{x})$ be quadratic forms in $F(\mathbf{x})$ and $G_l$, $F_l$ $(1 \leq l \leq o)$ be the coefficient matrices of $g_l(\mathbf{x})$, $f_l(\mathbf{x})$ respectively, i.e. $g_l(\mathbf{x}) = {}^t\mathbf{x}G_l\mathbf{x} +$ (linear form of $\mathbf{x}$),

$f_l(\mathbf{x}) = {}^t\mathbf{x}F_l\mathbf{x} + (\text{linear form of } \mathbf{x})$. By the definitions of $G$, $F$, we see that

$$G_l = \begin{pmatrix} 0_o & * \\ * & *_v \end{pmatrix}, F_l = {}^tSG_lS = {}^tS \begin{pmatrix} 0_o & * \\ * & *_v \end{pmatrix} S.$$

Since

$$\begin{pmatrix} 0_o & * \\ * & *_v \end{pmatrix}^{-1} \begin{pmatrix} 0_o & * \\ * & *_v \end{pmatrix} = \begin{pmatrix} *_o & * \\ 0 & *_v \end{pmatrix},$$

we have

$$W_1^{-1}W_2 = S^{-1} \begin{pmatrix} *_o & * \\ 0 & *_v \end{pmatrix} S$$

for two linear sums $W_1$, $W_2$ of $F_1, \ldots, F_o$. It is known that an attacker can recover an invertible $n \times n$ matrix $S_1$ such that

$$SS_1 = \begin{pmatrix} *_o & * \\ 0 & *_v \end{pmatrix}$$

in polynomial time by a linear algebraic approach on $W_1^{-1}W_2$ (see [9] for the detail). Once such a matrix $S_1$ is recovered, an attacker can generate dummy signatures since

$${}^tS_1F_lS_1 = {}^t(SS_1)G_l(SS_1) = \begin{pmatrix} 0_o & * \\ * & *_v \end{pmatrix}.$$

When $v > o$, the original Kipnis-Shamir's attack [9] is not available since

$$\begin{pmatrix} 0_o & * \\ * & *_v \end{pmatrix}^{-1} \begin{pmatrix} 0_o & * \\ * & *_v \end{pmatrix} \neq \begin{pmatrix} *_o & * \\ 0 & *_v \end{pmatrix}.$$

This attack was arranged in [4] to be available also for $v > o$. However, its complexity is no longer polynomial time but $O(q^{v-o} \cdot (\text{polyn.}))$. The parameter $v$ is thus taken sufficiently larger than $o$ to construct a secure UOV.

## 3. Circulant UOV

In this section, we describe the construction of Circulant UOV (C-UOV, in short) [7], a variant of UOV.

For $1 \leq l \leq o$, let $A_l$, $B_l$ be $v \times o$- and $v \times v$- matrices respectively, $\mathbf{c}_l \in \mathbf{F}_q^n$ be a row vector and $d_l \in \mathbf{F}_q$ such that $g_l(\mathbf{x}) = {}^t\mathbf{x}\begin{pmatrix} 0_o & {}^tA_l \\ A_l & B_l \end{pmatrix}\mathbf{x} + \mathbf{c}_l\mathbf{x} + d_l$. In the original UOV, $A_l$, $B_l$, $\mathbf{c}_l$, $d_l$ are chosen randomly. On the other hand in Circulant UOV, $A_l$ and $\mathbf{c}_l$ are given as follows.

$$\begin{cases} A_1 = (\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3, \ldots, \mathbf{a}_o), \\ A_2 = (\mathbf{a}_o, \mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{o-1}), \\ A_3 = (\mathbf{a}_{o-1}, \mathbf{a}_o, \mathbf{a}_1, \ldots, \mathbf{a}_{o-2}), \\ \quad \vdots \\ A_o = (\mathbf{a}_2, \mathbf{a}_3, \mathbf{a}_4, \ldots, \mathbf{a}_o, \mathbf{a}_1), \end{cases}$$

$$\begin{cases} \mathbf{c}_1 = (c_1, c_2, c_3, \ldots, c_o, c_{o+1}^{(1)}, \ldots, c_n^{(1)}), \\ \mathbf{c}_2 = (c_o, c_1, c_2, \ldots, c_{o-1}, c_{o+1}^{(2)}, \ldots, c_n^{(2)}), \\ \mathbf{c}_3 = (c_{o-1}, c_o, c_1, \ldots, c_{o-2}, c_{o+1}^{(3)}, \ldots, c_n^{(3)}), \\ \quad \vdots \\ \mathbf{c}_o = (c_2, c_3, c_4, \ldots, c_o, c_1, c_{o+1}^{(o)}, \ldots, c_n^{(o)}), \end{cases} \quad (2)$$

where $\mathbf{a}_1, \ldots, \mathbf{a}_o \in \mathbf{F}_q^v$ are column vectors and $c_1, \ldots, c_o, c_{o+1}^{(1)}, \ldots, \ldots, c_n^{(o)} \in \mathbf{F}_q$ are constants. Note that $B_l$, $d_l$ are also random. We can easily check that, for such $A_l$, $\mathbf{c}_l$, the linear equations (1) solved in the process of signature generation of UOV are given by

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \ldots & \alpha_o \\ \alpha_o & \alpha_1 & \alpha_2 & \ldots & \alpha_{o-1} \\ \alpha_{o-1} & \alpha_o & \alpha_1 & \ldots & \alpha_{o-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_2 & \alpha_3 & \alpha_4 & \ldots & \alpha_1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ \vdots \\ y_o \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \beta_3 \\ \vdots \\ \beta_o \end{pmatrix}, \quad (3)$$

for constants $\alpha_1, \ldots, \alpha_o, \beta_1, \ldots, \beta_o \in \mathbf{F}_q$ depending on $u_1, \ldots, u_v$. The matrix in the left hand side of the equation (3) is a "circulant" matrix and is known to be inverted in time $O(n^2)$ (see, e.g. [10]), which is faster than $O(n^3)$ for a random matrix. Thus the signature generation of Circulant UOV is faster than the original UOV.

## 4. Kipnis-Shamir's attack on C-UOV

In this section, we study the security of Circulant UOV against Kipnis-Shamir's attack. For simplicity, we suppose that $S$ is a linear map expressed by an $n \times n$ matrix.

Due to (2), we see that

$$A_l = A_1P^{l-1}$$

for $1 \leq l \leq o$, where $P := \begin{pmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ 1 & & & \end{pmatrix}$ is an $o \times o$ matrix representing a cyclic permutation. We now prepare the following lemma.

**Lemma 4.1** *Let $A$ be an $v \times o$ matrix, $B_1$, $B_2$ be $v \times v$ matrices, $C$ be an $o \times o$ matrix and*

$$H_1 := \begin{pmatrix} 0_o & {}^tA \\ A & B_1 \end{pmatrix}, \quad H_2 := \begin{pmatrix} 0_o & {}^t(AC) \\ AC & B_2 \end{pmatrix}.$$

*If $H_1$ is invertible, the following (i) and (ii) hold.*

*(i)* $H := H_1^{-1}H_2 = \begin{pmatrix} *_o & * \\ 0 & *_v \end{pmatrix}$.

*(ii) There exists a polynomial $h_1(t)$ of degree $o$ such that $h_1(t)^2$ is a factor of the characteristic polynomial* $\det(t \cdot I_n - H)$ *and* $h_1(H) = \begin{pmatrix} 0_o & * \\ 0 & *_v \end{pmatrix}$.

**Proof** (i) Let $L_1$, $L_2$, $L_3$ be $o \times o$, $v \times o$ and $v \times v$ matrices respectively such that $H_1^{-1} = \begin{pmatrix} L_1 & {}^tL_2 \\ L_2 & L_3 \end{pmatrix}$. Since

$$H_1H_1^{-1} = H \begin{pmatrix} L_1 & {}^tL_2 \\ L_2 & L_3 \end{pmatrix} = I_n,$$

it hold ${}^tL_2A = I_o$ and $L_3A = 0$. Then we have

$$H = H_1^{-1}H_2 = \begin{pmatrix} {}^tL_2AC & * \\ L_3AC & *_v \end{pmatrix} = \begin{pmatrix} C & * \\ 0 & *_v \end{pmatrix}.$$

(ii) Let $M_1$, $M_2$ be $v \times o$ and $v \times v$ matrices respectively such that $H = \begin{pmatrix} C & M_1 \\ 0 & M_2 \end{pmatrix}$. We obtain

$${}^tM_2A = AC,$$

from the $(1,2)$-blocks of the both hand sides of the equa-

tion $H_1H = H_2$. Then, for any integer $l \geq 1$, we have

$$({}^tM_2)^l A = ({}^tM_2)^{l-1}AC = ({}^tM_2)^{l-2}AC^2 = \cdots = AC^l.$$

This means that, for the characteristic polynomial $h_1(t)$ of $C$, it holds

$$h_1({}^tM_2)A = Ah_1(C) = 0.$$

We thus conclude that the characteristic polynomial of $M_2$ has a factor $h_1(t)$, and then

$$h_1(H) = \begin{pmatrix} h_1(C) & * \\ 0 & *_v \end{pmatrix} = \begin{pmatrix} 0_o & * \\ 0 & *_v \end{pmatrix}$$

holds.

**(QED)**

Based on the lemma above, we propose the following attack on Circulant UOV.

---

**Kipnis-Shamir's attack on C-UOV.**

**Input:** The coefficient matrices $F_1$, …, $F_o$ of the quadratic forms $f_1(\mathbf{x}), \ldots, f_o(\mathbf{x})$.
**Output:** An invertible linear map $S_1 : \mathbf{F}_q^n \to \mathbf{F}_q^n$ such that $SS_1 = \begin{pmatrix} *_o & * \\ 0 & *_v \end{pmatrix}$.
**Step 1.** Take two linear sums $W_1$, $W_2$ of $F_1$, …, $F_o$ such that $W_1$ is invertible. Compute $W := W_1^{-1}W_2$.
**Step 2.** Compute the characteristic polynomial $w(t) := \det(t \cdot I_n - W)$ of $W$ and factor $w(t) = w_1(t)^2 w_2(t)$ by two polynomials $w_1(t)$, $w_2(t)$ of degree $o$ and $v - o$ respectively. If $w_2(t)$ is not square-free, go back to Step 1 and change $W_1$, $W_2$.
**Step 3.** Compute $w_1(W)$ and take an invertible $n \times n$ matrix $S'$ such that $w_1(W)S' = \begin{pmatrix} 0_o & * \\ 0 & *_v \end{pmatrix}$.
**Step 4.** Output $S_1 = S'$.

---

Due to (i) of Lemma 4.1, we see that

$$W = S^{-1}\begin{pmatrix} W_1 & * \\ 0 & *_v \end{pmatrix} S$$

for some $o \times o$ matrix $W_1$. Then there exist polynomials $w_1(t)$, $w_2(t)$ as given in Step 2. Since, if $w_2(t)$ is square-free, the characteristic polynomial $\det(t \cdot I_o - W_1)$ of $W_1$ is determined uniquely by $w_1(t)$, it holds

$$w_1(W) = S^{-1}\begin{pmatrix} 0_o & * \\ 0 & *_v \end{pmatrix} S.$$

We can easily check that $S'$ in Step 3 satisfies $SS' = \begin{pmatrix} *_o & * \\ 0 & *_v \end{pmatrix}$.

The attack above is in polynomial time since it includes only basic linear operations. Table 1 describes the results of experiments of Kipnis-Shamir's attack against Circulant UOV on Magma [11] ver.2.22-3 on Windows 8.1, Core(TM)i7-4800MQ, 2.70GHz for the parameters selected in [7] as 80-, 100- and 120-bit security parameters. Note that, in these parameters, the numbers $m$ of quadratic forms in $F$ do not coincide with $o$ since the "minus" is applied on Circulant UOV (see §5 of [7]). It is easy to see that the "minus" does not disturb Kipnis-Shamir's attack. Due to the results in this table, we can conclude that Circulant UOV is not secure at all against Kipnis-Shamir's attack.

Table 1. Kipnis-Shamir's attack on Circulant UOV.

| $q$ | $n$ | $m$ | $o$ | $v$ | Time | (Security) |
|---|---|---|---|---|---|---|
| 31 | 99 | 33 | 34 | 65 | 0.59s | (80bit) |
| 31 | 123 | 41 | 43 | 80 | 1.64s | (100bit) |
| 31 | 156 | 52 | 53 | 103 | 6.54s | (128bit) |

Remark that further discussions are required in the case that the field $\mathbf{F}_q$ is of even characteristic. When $q$ is even, the coefficient matrices $F_1, \ldots, F_o$ cannot be symmetric and then an attacker uses $F_l + {}^tF_l$ instead of $F_l$ itself. Such matrices are symmetric and also skew-symmetric. It is known, for two $n \times n$ skew-symmetric matrices $R_1, R_2$, that the matrices $R_1, R_2$ are not invertible if $n$ is odd and the minimal polynomial of $R_1^{-1}R_2$ is of degree $n/2$ if $n$ is even (see, e.g. [12–14]). This means that the attack proposed in this section is not directly available for even characteristic cases, and we must arrange it to be available also for even characteristic cases in the future.

We also remark that, if $A_1$ is not of full-rank, Step 1 of our attack always fails since $W_1^{-1}$ does not exist. However, in such a case, an attacker can recover partial information of $S$. When the rank of $A_1$ is, for example, $o - 1$, there exist an invertible $o \times o$ matrix $D$ and a $v \times (o-1)$ matrix $A'$ such that $A_1 = (0, A')D$ and then $F_1 = {}^tS\begin{pmatrix} {}^tD & \\ & I_v \end{pmatrix}\begin{pmatrix} 0_1 & \\ & *_{n-1} \end{pmatrix}\begin{pmatrix} D & \\ & I_v \end{pmatrix}S$ holds. We can recover an $n \times n$ matrix $S_0$ with $\begin{pmatrix} D & \\ & I_v \end{pmatrix}SS_0 = \begin{pmatrix} *_1 & * \\ 0 & *_{n-1} \end{pmatrix}$ by elementary linear operations on $F_1$. It is easy to see that, once such an $S_0$ is given, one can reduce the problem of recovering an equivalent key of $(o, v)$-UOV to that of $(o-1, v)$-UOV by taking the lower-right $(n-1) \times (n-1)$ minor matrices of ${}^tS_0F_1S_0$, …, ${}^tS_0F_oS_0$. This means that the attacker can recover an equivalent key by applying our attack on such smaller size matrices.

## 5. Rainbow and Circulant Rainbow

Rainbow [5] is a multi-layer version of UOV. We now describe a 2-layer version.

Let $o_1$, $o_2$, $v$, $n$, $m \geq 1$ be integers with $n = o_1 + o_2 + v$, $m = o_1 + o_2$. Define the quadratic map $G : \mathbf{F}_q^n \to \mathbf{F}_q^m$ by

$$g_l(\mathbf{x}) = \begin{cases} \sum_{1 \leq i \leq o_1} x_i \cdot (\text{linear form of } x_{o_1+1}, \ldots, x_n) \\ \quad +(\text{quadratic form of } x_{o_1+1}, \ldots, x_n), \\ \quad (1 \leq l \leq o_1), \\ \sum_{1 \leq i \leq o_2} x_{o_1+i} \cdot (\text{linear form of } x_{m+1}, \ldots, x_n) \\ \quad +(\text{quadratic form of } x_{m+1}, \ldots, x_n), \\ \quad (o_1 + 1 \leq l \leq m). \end{cases}$$

The signature scheme Rainbow is constructed as follows.

**Secret key.** Two invertible affine maps $S : \mathbf{F}_q^n \to \mathbf{F}_q^n$, $T : \mathbf{F}_q^m \to \mathbf{F}_q^m$ and the quadratic map $G$ defined above.
**Public key.** The quadratic map $F := T \circ G \circ S : \mathbf{F}_q^n \to \mathbf{F}_q^o$.

**Signature generation.** For a message $\mathbf{m} \in \mathbf{F}_q^m$ to be signed, let $\mathbf{w} = {}^t(w_1, \ldots, w_m) := T^{-1}(\mathbf{m})$. Choose $u_1$, $\ldots$, $u_v \in \mathbf{F}_q$ randomly and find $(y_{o_1+1}, \ldots, y_m) \in \mathbf{F}_q^{o_2}$ with

$$\begin{aligned} &g_{o_1+1}(y_1, \ldots, y_m, u_1, \ldots, u_v) = w_{o_1+1}, \\ &\ldots, \quad g_m(y_1, \ldots, y_m, u_1, \ldots, u_v) = w_m. \end{aligned} \tag{4}$$

After that, find $(y_1, \ldots, y_{o_1}) \in \mathbf{F}_q^{o_1}$ with

$$\begin{aligned} &g_1(y_1, \ldots, y_m, u_1, \ldots, u_v) = w_1, \\ &\ldots, \quad g_{o_1}(y_1, \ldots, y_m, u_1, \ldots, u_v) = w_{o_1}. \end{aligned} \tag{5}$$

The signature for $\mathbf{m}$ is $\mathbf{z} := S^{-1}{}^t(y_1, \ldots, y_m, u_1, \ldots, u_v)$.

**Signature verification.** The signature $\mathbf{z}$ is verified if $F(\mathbf{z}) = \mathbf{m}$ holds.

Note that (4) is a system of $o_2$ linear equations of $o_2$ variables $y_{o_1+1}$, $\ldots$, $y_m$ and (5) is a system of $o_1$ linear equations of $o_1$ variables $y_1$, $\ldots$, $y_{o_1}$.

The coefficient matrices $G_1$, $\ldots$, $G_m$ of $g_1(\mathbf{x})$, $\ldots$, $g_m(\mathbf{x})$ are written by

$$G_j = \begin{cases} \begin{pmatrix} 0_{o_1} & {}^tA_j \\ A_j & B_j \end{pmatrix}, & (1 \le j \le o_1), \\ \begin{pmatrix} 0_{o_1} & 0 & 0 \\ 0 & 0_{o_2} & {}^tC_j \\ 0 & C_j & D_j \end{pmatrix}, & (o_1 + 1 \le j \le m), \end{cases}$$

where $A_j$, $B_j$, $C_j$, $D_j$ are $(o_2+v)\times o_1$-, $(o_2+v)\times(o_2+v)$-, $v \times o_2$- and $v \times v$- matrices respectively. Similarly to UOV, the coefficient matrices $F_1$, $\ldots$, $F_m$ of $f_1(\mathbf{x})$, $\ldots$, $f_m(\mathbf{x})$ are given by

$$F_j = {}^tS \begin{pmatrix} 0_{o_1} & * \\ * & *_{o_2+v} \end{pmatrix} S$$

and then the complexity of Kipnis-Shamir's attack on the original Rainbow is $O(q^{o_2+v-o_1} \cdot (\text{polyn.}))$.

In Circulant Rainbow [8], the matrices $A_j, C_j$ above are chosen similarly to (2), and then the systems of linear equations (4), (5) in the signature generation are also written by circulant matrices similar to (3). The signature generation of Circulant Rainbow is thus faster than that of the original Rainbow.

However, similarly to Circulant UOV, the attacker can recover an invertible linear map $S_1 : \mathbf{F}_q^n \to \mathbf{F}_q^n$ such that $SS_1 = \begin{pmatrix} *_{o_1} & * \\ 0 & *_{o_2+v} \end{pmatrix}$ by Kipnis-Shamir's attack given in §4. It is easy to see that, once such an $S_1$ is recovered, the attacker can recover further information of $S$ and $T$, which is sufficient to generate dummy signatures for arbitrary messages (see, e.g. [15]). We thus conclude that Circulant Rainbow is also insecure.

## 6. Conclusion

Circulant UOV [7] and Circulant Rainbow [8] are new variants of UOV [3, 4] and Rainbow [5]. These variants use "circulant" structures in the quadratic forms to accelerate the signature generations of UOV and Rainbow. However, as described in §4, such circulant structures weaken the security critically, especially against Kipnis-Shamir's attack [4, 9]. This situation is similar to ELSA, another fast variant of Rainbow proposed at Asiacrypt 2017 [16] and broken at IWSEC 2018 [17]. We thus consider that we must study the security quite carefully when we attempt to improve the efficiency of these schemes.

## Acknowledgments

The author would like to thank the anonymous reviewer(s) for reading the previous draft carefully and giving helpful comments. He was supported by JST CREST no. JPMJCR14D6 and JSPS Grant-in-Aid for Scientific Research (C) no. 17K05181.

## References

[1] A.S. Fraenkel and Y. Yesha, Complexity of problems in games, graphs and algebraic equations, Discrete Appl. Math., **1** (1979), 15–30.

[2] M.R. Garey and D.S. Johnson, Computers and Intractability: A Guide to the Theory of NP-completeness, W. H. Freeman, New York, 1979.

[3] J. Patarin, The Oil and Vinegar Signature Scheme, the Dagstuhl Workshop on Cryptography, 1997.

[4] A. Kipnis, J. Patarin and L. Goubin, Unbalanced oil and vinegar signature schemes, in: Proc. of EUROCRYPT '99, J. Stern ed., LNCS, Vol. 1592, pp. 206–222, Springer, Berlin, Heidelberg, 1999, extended in `http://www.goubin.fr/papers/OILLONG.PDF`, 2003.

[5] J. Ding and D. Schmidt, Rainbow, a new multivariate polynomial signature scheme, in: Proc. of ACNS 2005, J. Ioannidis et al. eds., LNCS, Vol. 3531, pp. 164–175, Springer, Berlin, Heidelberg, 2005.

[6] NIST, Post-quantum cryptography standardization, `https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization`.

[7] Z. Peng and S. Tang, Circulant UOV: a new UOV variant with shorter private key and faster signature generation, KSII T. Internet Info., **12** (2018), 1376–1395.

[8] Z. Peng and S. Tang, Circulant Rainbow: A new Rainbow variant with shorter private key and faster signature generation, IEEE Access, **5** (2007), 11877 – 11886.

[9] A. Kipnis and A. Shamir, Cryptanalysis of the oil and vinegar signature scheme, in: Proc. of CRYPTO '98, H. Krawczyk ed., LNCS, Vol. 1462, pp. 257–267, Springer, Berlin, Heidelberg, 1998.

[10] I. Kra and S. R. Simanca, On circulant matrices, Notices of the AMS, **59** (2012), 368–377.

[11] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput., **24** (1997), 235–265.

[12] A. Cayley, Sur les determinants gauches (On skew determinants), J. Reine Angew. Math, **38** (1847), 93–96.

[13] D.Z. Doković, On the product of two alternating matrices, Amer. Math. Monthly, **98** (1991), 935–936.

[14] O. Taussky and H. Zassenhaus, On the similarity transformation between a matrix and its transpose, Pacific J. Math., **9**, (1959), 893–896.

[15] B.Y. Yang and J.M. Chen, Building secure tame-like multivariate public-key cryptosystems: the new TTS, in: Proc. of ACISP '05, C. Boyd et al. eds, LNCS, Vol. 3574, pp. 518–531, Springer, Berlin, Heidelberg, 2005.

[16] K.-A. Shim, C.-M. Park and N. Koo, An existential unforgeable signature scheme based on multivariate quadratic equations, in: Proc. of ASIACRYPT '17, T. Takagi et al. eds, LNCS, Vol. 10624, pp. 37–64, Springer, Cham, 2017.

[17] Y. Hashimoto, Y. Ikematsu and T. Takagi, Chosen message attack on multivariate signature ELSA at Asiacrypt 2017, in: Proc. of IWSEC '18, A. Inomata et al. eds, LNCS, Vol. 11049, pp. 3–18, Springer, Cham, 2018.