On the security of Circulant UOV/Rainbow

Yasufumi Hashimoto *

Abstract

Circulant UOV and Circulant Rainbow are new variants of UOV (unbalanced oil and vinegar signature scheme) and Rainbow respectively. In this short report, we study the security of these new variants Circulant UOV and Circulant Rainbow.

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

1 Introduction

The unbalanced oil and vinegar signature scheme (UOV) [7, 3] and Rainbow [2] are multivariate signature schemes, considered to secure and efficient enough under suitable parameter selections. In fact, several variants of these two schemes are submitted to NIST's post-quantum cryptography standardization project [6]. Recently in [9, 8], new variants of UOV and Rainbow were proposed. They are called Circulant UOV and Circulant Rainbow respectively, since circulant matrices appear in the process of signature generation. It is known that inverting circulant matrices are faster than doing random matrices, and then the signature generation of these circulant variants are faster than the original schemes. However, such "circulant" structures weaken the security critically. In this short report, we study the security of Circulant UOV/Rainbow and conclude that these two circulant variants are not secure against Kipnis-Shamir's attack [4, 3].

2 UOV

We first describe the unbalanced oil and vinegar signature scheme (UOV) [7, 3] and Kipnis-Shamir's attack on UOV [4, 3].

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

$$\begin{aligned} g_l(x_1, \ldots, x_n) = &\sum_{1 \leq i \leq o} x_i \cdot (\text{linear form of } x_{o+1}, \ldots, x_n) \\ &+ (\text{quadratic form of } x_{o+1}, \ldots, x_n), \end{aligned}$$

for $1 \leq l \leq o$, where the coefficients in the right hand side are elements of $\mathbb{F}_q$. The unbalanced oil and vinegar signature scheme (UOV) is constructed as follows.

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

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

*Department of Mathematical Science, University of the Ryukyus, e-mail: hashimoto@math.u-ryukyu.ac.jp

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

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

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

Signature verification. Check whether $F(\mathbf{z}) = \mathbf{m}$.

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. For the security of UOV, we should discuss Kipnis-Shamir's attack [4, 3] given below.

Kipnis-Shamir's attack. It is well-known that UOV with $o = v$ (balanced oil and vinegar signature scheme, [7]) is broken by Kipnis-Shamir's attack [4]. The basic idea is as follows.

Let G_l, F_l $(1 \leq l \leq o)$ be $n \times n$ symmetric matrices with

$$\begin{aligned} g_l(\mathbf{x}) &= {}^t\mathbf{x} G_l \mathbf{x} + (\text{linear form of } \mathbf{x}), \\ f_l(\mathbf{x}) &= {}^t\mathbf{x} F_l \mathbf{x} + (\text{linear form of } \mathbf{x}). \end{aligned}$$

By the definitions of the quadratic maps G, F, we see that the matrices G_l, F_l are written by

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

It is easy to see that, if $o = v$, it holds

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

Then, for two linear sums W_1, W_2 of $F_1, \ldots, F_o$, we have

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

This means that there exists an invertible $n \times n$ matrix S_1 with

$$S_1^{-1}W_1^{-1}W_2S_1 = \begin{pmatrix} *_o & * \\ 0 & *_v \end{pmatrix},$$

and such a matrix S_1 satisfies

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

Since

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

the matrix S_1 is enough to generate dummy signatures of UOV. It is known that S_1 can be recovered in polynomial time (see [4] for the detail).

When $v > o$, the original Kipnis-Shamir's attack [4] 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 to be available also for $v > o$ in [3]. However, its complexity is no longer polynomial time but $O(q^{v-o} \cdot (\text{polyn.}))$. Thus v is taken sufficiently larger than o for the original UOV.

3 Circulant UOV

Circulant UOV [9] is a variant of UOV constructed as follows.

For $1 \leq l \leq o$, let A_l, B_l be $v \times o$ and $v \times v$ matrices respectively, $\mathbf{c}_l \in \mathbb{F}_q^n$ a row vector and $d_l \in \mathbb{F}_q$ 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.

$$\begin{cases} A_1 = (\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3, \ldots, \mathbf{a}_o), \\ A_2 = (\mathbf{a}_o, \mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{o-1}), \\ A_3 = (\mathbf{a}_{o-1}, \mathbf{a}_o, \mathbf{a}_1, \ldots, \mathbf{a}_{o-2}), \\ \quad \vdots \\ A_o = (\mathbf{a}_2, \mathbf{a}_3, \mathbf{a}_4, \ldots, \mathbf{a}_o, \mathbf{a}_1), \end{cases} \quad \begin{cases} \mathbf{c}_1 = (c_1, c_2, c_3, \ldots, c_o, c_{o+1}^{(1)}, \ldots, c_n^{(1)}), \\ \mathbf{c}_2 = (c_o, c_1, c_2, \ldots, c_{o-1}, c_{o+1}^{(2)}, \ldots, c_n^{(2)}), \\ \mathbf{c}_3 = (c_{o-1}, c_o, c_1, \ldots, c_{o-2}, c_{o+1}^{(3)}, \ldots, c_n^{(3)}), \\ \quad \vdots \\ \mathbf{c}_o = (c_2, c_3, c_4, \ldots, c_o, c_1, c_{o+1}^{(o)}, \ldots, c_n^{(o)}), \end{cases} \tag{2}$$

where $\mathbf{a}_1, \ldots, \mathbf{a}_o \in \mathbb{F}_q^v$ are column vectors and $c_1, \ldots, c_o, c_{o+1}^{(1)}, \ldots, \ldots, c_n^{(o)} \in \mathbb{F}_q$ are constants. Note that B_l and d_l are chosen randomly. 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

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

where $\alpha_1, \ldots, \alpha_o, \beta_1, \ldots, \beta_o \in \mathbb{F}_q$. It is known that the matrix in the left hand side of the equation above is inverted in time $O(n^2)$ [5], which is smaller than $O(n^3)$ for the original UOV. Thus the signature generation of Circulant UOV is faster than that of the original UOV.

4 Kipnis-Shamir's attack on Circulant UOV

In this section, we explain why Circulant UOV is vulnerable against Kipnis-Shamir's attack.

Due to (2), we see that

$$A_l = A_1 P^{l-1}$$

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. It is easy to check that

$$\begin{pmatrix} 0_o & (A_1C_1)^t \\ A_1C_1 & B_1' \end{pmatrix}^{-1} \begin{pmatrix} 0_o & (A_1C_2)^t \\ A_1C_2 & B_2' \end{pmatrix} = \begin{pmatrix} *_o & * \\ 0 & *_v \end{pmatrix}$$

for $o \times o$ matrices C_1, C_2 and $v \times v$ matrices B_1', B_2', if C_1 is invertible. This means that

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

even if $v > o$. This situation is almost the same to the original UOV with $o = v$. Thus the attacker can recover an $n \times n$ matrix S_1 satisfying $SS_1 = \begin{pmatrix} *_o & * \\ 0 & *_v \end{pmatrix}$ in polynomial time similarly to the

Table 1: Running times of 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)

original UOV with $o = v$ [4].

Table 1 describes the results of experiments of Kipnis-Shamir's attack against Circulant UOV on Magma [1] ver.2.22-3 on Windows 8.1, Core(TM)i7-4800MQ, 2.70GHz for the parameter selections given in [9] as 80-, 100- and 120-bit security parameters. In this table, the numbers m of quadratic forms in F do not coincide with o since the "minus" is used on Circulant UOV (see §5 of [9]). Note 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.

5 Rainbow and Circulant Rainbow

Rainbow is a multi-layer version of UOV (see, e.g. [2] for the detail) and Circulant Rainbow [8] can be constructed similarly. The original Rainbow has been considered to be secure enough against known attacks including Kipnis-Shamir's attack under a suitable parameter selections. However, due to §4, we can easily check that Kipnis-Shamir's attack is also available on Circulant Rainbow and it recovers an equivalent secret key in polynomial time. We thus conclude that Circulant Rainbow is also insecure similar to Circulant UOV.

Acknowledgment. The author was supported by JST CREST no.JPMJCR14D6 and JSPS Grant-in-Aid for Scientific Research (C) no. 17K05181.

References

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

[2] J. Ding, D. Schmidt, Rainbow, a new multivariate polynomial signature scheme, ACNS'05, LNCS **3531** (2005), pp.164–175.

[3] A. Kipnis, J. Patarin, L. Goubin, Unbalanced oil and vinegar signature schemes, Eurocrypt'99, LNCS **1592** (1999), pp.206–222, extended in citeseer/231623.html, 2003-06-11.

[4] A. Kipnis, A. Shamir, Cryptanalysis of the oil and vinegar signature scheme, Crypto'98, LNCS **1462** (1998), pp.257–267.

[5] I. Kra, S. R. Simanca, On circulant matrices, Notices AMS, **59** (2012), pp. 368-377.

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

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

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

[9] Z. Peng, S. Tang, Circulant UOV: a new UOV variant with shorter private key and faster signature generation, KSII Transactions on Internet and Information Systems, **12** (2018), pp. 1376-1395.