Weaknesses of cubic UOV and its variants

WEAKNESSES OF CUBIC UOV AND ITS VARIANTS *

Yasufumi HASHIMOTO

Abstract

The *unbalanced oil and vinegar signature scheme* (UOV) is a signature scheme whose public key is a set of multivariate quadratic forms over a finite field. This signature scheme has been considered to be secure and efficient enough under suitable parameter selections. However, the key size of UOV is relatively large and then reducing the key size of UOV is an important issue. Recently in Inscrypt 2015, a new variant of UOV called Cubic UOV was proposed, and in ICISC 2016, two variants of Cubic UOV called CSSv and SVSv were proposed. It has been claimed that these variants were more efficient than the original UOV and were secure enough. However, the security analyses of these schemes were not enough and they can be broken easily. In the present paper, we describe the weaknesses of these schemes.

1 Introduction

A *multivariate public key cryptosystem (MPKC)* is a public key cryptosystem whose public key is a set of multivariate quadratic forms over a finite field. The MPKC is considered to be a candidate of *Post-Quantum Cryptographies* since the problem of solving a system of multivariate non-linear polynomial equations over a finite field of order 2 is NP-hard [4, 5].

The *unbalanced oil and vinegar signature scheme* (UOV) [8] is one of the most famous MPKCs. Its signature generation is simple and the security is considered to be enough under suitable parameters. On the other hand, the key size of UOV is relatively large since the number of variables should be taken sufficiently larger than twice of the number of quadratic forms. Then reducing the key size of UOV is an important issue.

Recently, a new variant of UOV called Cubic UOV was proposed in Inscrypt 2015 [10] and two variants of Cubic UOV called CSSv and SVSv were proposed in ICISC 2016 [3]. The authors of [10, 3] claimed that these schemes were secure enough and the keys were much smaller than the original UOV. However, the security analyses of these schemes in [10, 3] were not enough at all.

*Received November 30, 2017

In the present paper, we study the structure of polynomials in these schemes and describe the weaknesses these three schemes.

2 UOV

We first describe the original *unbalanced oil and vinegar signature scheme* (UOV) [8].

Let $n, o, v \geq 1$ be integers with $n := o + v$ and $v > o$ Denote by k a finite field and $q := \#k$. Define the quadratic map $G : k^n \to k^o$ by $G(x) = (g_1(x), \ldots, g_o(x))^t$ where $g_l(x)$ $(1 \leq l \leq o)$ is a quadratic polynomial in the form

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

The *secret key* of UOV is an invertible affine map $S : k^n \to k^n$ and the quadratic map $G : k^n \to k^o$. The *public key* is the quadratic map

$$F := G \circ S : k^n \to k^o.$$

To *generate a signature* of a given message $m = (m_1, \ldots, m_o)^t \in k^o$, first choose $u_1, \ldots, u_v \in k$ randomly and find $z_1, \ldots, z_o \in k$ such that

$$\begin{aligned} g_1(z_1, \ldots, z_o, u_1, \ldots, u_v) &= m_1, \\ &\vdots \\ g_o(z_1, \ldots, z_o, u_1, \ldots, u_v) &= m_o. \end{aligned} \tag{2}$$

Note that (2) is a system of o linear equations of o variables $z_1, \ldots, z_o$. Then such $z_1, \ldots, z_o$ are found by the Gaussian elimination. The signature for m is $x = S^{-1}(z_1, \ldots, z_o, u_1, \ldots, u_v)^t$. The signature is *verified* by checking $F(x) = m$.

For the security, it is known that Kipnis-Shamir's attack [9, 8] can recover an affine map $S' : k^n \to k^n$ such that

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

with the complexity $\ll q^{v-o} \cdot (\text{polyn.}) = q^{n-2o} \cdot (\text{polyn.})$. Such a map S' is enough to break UOV since the quadratic forms in

$$F \circ S' = G \circ (S \circ S')$$

is similar to (1). This means that n must be taken sufficiently larger than $2o$.

3 Cubic UOV and its variants

In this section, we describe the Cubic UOV and its variants CSSv, SVSv [10, 3].

3.1 Cubic UOV

Let $n, o, v \geq 1$ be integers with $n := o + v$, k a finite field and $q := \#k$. For $x \in k^n$, define the polynomials $z_1(x), \ldots, z_o(x)$ and $y_1(x), \ldots, y_o(x)$ by

$$z_l(x) := \begin{cases} \sum_{1 \leq i \leq o} x_i \cdot (\text{linear form of } x_{o+1}, \ldots, x_n) \\ \quad +(\text{quadratic form of } x_{o+1}, \ldots, x_n), & (l = 1), \\ (\text{linear form of } x_1, \ldots, x_n), & (2 \leq l \leq o), \end{cases}$$

$$y_l(x) := \begin{cases} r_1 z_1(x)(1 + z_2(x)) + g_1(x), & (l = 1), \\ r_2 z_1(x) z_2(x) + g_2(x), & (l = 2), \\ r_l z_l(x)(z_{l-2}(x) + z_{l-1}(x)) + g_l(x), & (3 \leq l \leq o), \end{cases}$$

where $r_1, \ldots, r_o \in k \backslash \{0\}$, $g_1(x), g_2(x), g_3(x)$ are cubic forms of $x_{o+1}, \ldots, x_n$ and $g_4(x), \ldots, g_o(x)$ are quadratic forms of $x_{o+1}, \ldots, x_n$. Denote by $Y : k^n \to k^o$ the map $Y(x) := (y_1(x), \ldots, y_o(x))^t$.

The *secret key* of the Cubic UOV is an affine map $S : k^n \to k^n$ and the polynomial map $Y : k^n \to k^o$. The *public key* is $F := Y \circ S : k^n \to k^o$. To *generate a signature* of a given message $m = (m_1, \ldots, m_o)^t \in k^o$, first choose $u_1, \ldots, u_v \in k$ randomly and compute

$$\begin{aligned} w_1 :=& r_1^{-1} \cdot (m_1 - g_1(u_1, \ldots, u_v) - r_2^{-1} \cdot (m_2 - g_2(u_1, \ldots, u_v)), \\ w_2 :=& r_2^{-1} \cdot w_1^{-1} \cdot (m_2 - g_2(u_1, \ldots, u_v)), \\ w_l :=& r_l^{-1} \cdot (w_{l-2} + w_{l-1})^{-1} \cdot (m_l - g_l(u_1, \ldots, u_v)), \quad (3 \leq l \leq o) \end{aligned}$$

recursively. Next, find $\alpha_1, \ldots, \alpha_o \in k$ such that

$$z_l(\alpha_1, \ldots, \alpha_o, u_1, \ldots, u_v) = w_l, \quad (1 \leq l \leq o).$$

Then the signature for m is $x = S^{-1}(\alpha_1, \ldots, \alpha_o, u_1, \ldots, u_v)^{-1}$. The signature is *verified* by checking $F(x) = m$.

3.2 CSSv

Let $n, o, v \geq 1$ be integers with $n := o + v$, k a finite field and $q := \#k$. For $x \in k^n$, define the polynomials $z_1(x), \ldots, z_o(x)$ and $y_1(x), \ldots, y_o(x)$ by

$$z_l(x) := \begin{cases} (\text{quadratic form of } x_1, \ldots, x_n), & (l = 1), \\ (\text{linear form of } x_1, \ldots, x_n), & (2 \leq l \leq o), \end{cases}$$

$$y_l(x) := \begin{cases} z_1(x) + g_1(x), & (l = 1) \\ z_{l-1}(x) z_l(x) + g_l(x), & (2 \leq l \leq o). \end{cases}$$

where $g_2(x)$ is a cubic form of $x_{o+1}, \ldots, x_n$ and $g_1(x), g_3(x), \ldots, g_o(x)$ are quadratic forms of $x_{o+1}, \ldots, x_n$. Denote by $Y : k^n \to k^o$ the map $Y(x) := (y_1(x), \ldots, y_o(x))^t$.

The *secret keys* of CSSv are two invertible affine maps $S : k^n \to k^n$ and $T : k^o \to k^o$ with

$$T(y) = \begin{pmatrix} \text{linear form of } y_1, y_2, y_3, \ldots, y_n, 1 \\ \text{linear form of } y_1, y_3, \ldots, y_n, 1 \\ \vdots \\ \text{linear form of } y_1, y_3, \ldots, y_n, 1 \end{pmatrix}.$$

The *public key* is $F := T \circ Y \circ S : k^n \to k^o$. To generate a signature of $m \in k^o$, first compute $y := T^{-1}(m)$. The later process of the signature generation and the signature verification are similar to Cubic UOV (see [3] for the details).

3.3 SVSv

Let $n, o, v, r \geq 1$ be integers with $n := o + v + r$, k a finite field and $q := \#k$. Note that $r = 2$ if q, v are even and $r = 1$ otherwise. For $x \in k^n$, define the polynomials $z_1(x), \ldots, z_o(x)$ and $y_1(x), \ldots, y_o(x)$ by

$$\begin{aligned} z_l(x) :=& (\text{linear form of } x_1, \ldots, x_n), \quad (1 \leq l \leq o), \\ y_l(x) :=& \begin{cases} z_1^2(x) + g_1(x), & (l = 1), \\ z_{l-1}(x) z_l(x) + g_l(x), & (2 \leq l \leq o), \end{cases} \end{aligned}$$

where $g_1(x), g_2(x), \ldots, g_o(x)$ are quadratic forms of $x_{o+1}, \ldots, x_n$. Denote by $Y : k^n \to k^o$ the map $Y(x) := (y_1(x), \ldots, y_o(x))^t$.

The *secret keys* of SVSv are two invertible affine maps $S : k^n \to k^n$, $T : k^o \to k^o$ and the *public key* is $F := T \circ Y \circ S : k^n \to k^o$. The signature generation and verification are similar to CSSv (see [3] for the details).

3.4 SVSv2

In the second version of [3], SVSv was arranged as follows.

Let n, o, v, r, k, q, Y, T be as defined for SVSv. Choose an integer $s \geq 1$ and put $n_1 := n + s$. The *secret keys* of SVSv2 are an affine map $S_1 : k^{n_1} \to k^n$ and the quadratic map $Y : k^n \to k^o$. The *public key* is $F := T \circ Y \circ S_1 : k^{n_1} \to k^o$. The signature generation and the signature verification are similar to the original SVSv.

4 Weaknesses Cubic UOV and its variants

In this section, we describe the weaknesses of Cubic UOV, CSSv, SVSv and SVSv2.

4.1 SVSv2

For a public key F of SVSv2, it is easy to see that $F(x_1, \ldots, x_n, 0, \ldots, 0)$ is just a public key of the original SVSv. It is a non-sense modification of SVSv. □

4.2 SVSv

Let Z be an $n \times n$ matrix with

$$(z_1(x), \ldots, z_o(x), x_{o+1}, \ldots, x_n)^t = Zx.$$

It is easy to see that

$$F = T \circ Y \circ S = T \circ \tilde{Y} \circ (Z \circ S),$$

where $\tilde{Y}(x) = (\tilde{y}_1(x), \ldots, \tilde{y}_o(x))^t$ is given by

$$\tilde{y}_l(x) := \begin{cases} x_1^2 + g_1(x), & (l = 1), \\ x_{l-1}x_l + g_l(x), & (2 \leq l \leq o). \end{cases}$$

This means that SVSv is almost same to a sparse version of Tsujii's/Shamir's scheme proposed and already broken over 20 years ago [13, 6, 11, 1]. The attacker can recover an equivalent secret key easily similar to [6, 1]. □

4.3 CSSv.

Let Z be an $n \times n$ matrix with

$$(1, z_2(x), \ldots, z_o(x), x_{o+1}, \ldots, x_n)^t = Zx.$$

It is easy to see that

$$F = T \circ Y \circ S = T \circ \tilde{Y} \circ (Z \circ S),$$

where $\tilde{Y}(x) = (\tilde{y}_1(x), \ldots, \tilde{y}_o(x))^t$ is given by

$$\tilde{y}_l := \begin{cases} (\text{quadratic form of } x_1, \ldots, x_n), & (l = 1), \\ (\text{cubic form of } x_1, \ldots, x_n), & (l = 2), \\ x_{l-1}x_l + g_l(x), & (3 \leq l \leq o). \end{cases}$$

This means that the polynomials $\tilde{y}_3, \ldots, \tilde{y}_o$ are same to $\tilde{y}_3, \ldots, \tilde{y}_o$ of SVSv. Recall that $f_2(x), \ldots, f_o(x)$ in the public key F are linear sums of $\tilde{y}_1(S(Z(x))), \tilde{y}_3(S(Z(x)))$, $\ldots, \tilde{y}_o(S(Z(x)))$. Then, removing the contribution of $\tilde{y}_1$ from $f_2(x), \ldots, f_o(x)$ by the high-rank attack [6, 1], the attacker can recover an equivalent secret key of CSSv similar to SVSv. □

4.4 Cubic UOV

Let Z be an $n \times n$ matrix as given in §4.3 and $\tilde{z}_1(x) := z_1(Z^{-1}x)$. Then we have

$$F = Y \circ S = \tilde{Y} \circ (Z \circ S),$$

where $\tilde{Y}(x) = (\tilde{y}_1(x), \ldots, \tilde{y}_o(x))^t$ is as follows.

$$\tilde{y}_l := \begin{cases} r_1\tilde{z}_1(x)(1+x_2) + g_1(x), & (l=1), \\ r_2\tilde{z}_1(x)x_2 + g_2(x), & (l=2), \\ r_l x_l(x_{l-2} + x_{l-1}) + g_l(x), & (3 \le l \le o). \end{cases} \tag{3}$$

Choose a constant $c \in k^n \backslash \{0\}$ randomly, take the difference

$$Df_i(x) := f_i(x+c) - f_i(x)$$

for $i = 1, 2$ and let Q_i the coefficient matrix of the quadratic form $D_i f(x)$. Since

$$\begin{aligned} \tilde{y}_1(x) - r_2^{-1}r_1\tilde{y}_2(x) =& r_1\tilde{z}_1 + (g_1(x) - r_2^{-1}r_1 g_2(x)) \\ =& (\text{quadratic form of } x_1, \ldots, x_n) \\ & + (\text{cubic form of } x_{o+1}, \ldots, x_n), \end{aligned}$$

we see that

$$Q_1 - r_2^{-1}r_1 Q_2 = (ZS)^t \begin{pmatrix} 0_o & \\ & *_v \end{pmatrix} (ZS),$$

namely there exists $\beta \in k \backslash \{0\}$ such that the rank of $Q_1 - \beta Q_2$ is at most v. Once such a β is found, the attacker can recover an $n \times n$ matrix S_1 with

$$(ZS)S_1 = \begin{pmatrix} *_o & * \\ 0 & *_v \end{pmatrix}$$

easily. After that, recovering an $n \times n$ matrix $S_2 = \begin{pmatrix} *_o & * \\ 0 & *_v \end{pmatrix}$ such that $F \circ S_1 \circ S_2$ is as given in (3) is an elementary problem in the undergraduate linear algebra. □

Remark 1. After we described our attack on Cubic UOV in the e-print [7], Duong and Wang (e.g. [2, 14]) claimed that our attack did not work. However, their opinions were based on elementary mistakes. We heard that they already admitted that they were completely wrong and withdrew their work.

Remark 2. Our attacks on CSSv, SVSv and SVSv2 were presented in the second version of our e-print [7] posted in May 2017. At ICISC 2017 held in November - December 2017, Shim et al. [12] presented almost the same attacks even though the submission deadline was in September 2017 and they cited our e-print.

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

References

[1] D. Coppersmith, J. Stern, S. Vaudenay, Attacks on the birational permutation signature schemes, Crypto 1993, Springer LNCS **773** (1994), pp.435–443.

[2] D.H. Duong, Two polynomial time attacks against CUOV scheme, Seminar, Ho Chi Minh, Vietnam, May 2017, `http://www.math.hcmus.edu.vn/index.php?option=com_content&task=view&id=2490&Itemid=82`.

[3] D.H. Duong, A. Petzoldt, Y. Wang, T. Takagi, Revisiting the cubic UOV signature scheme, ICISC 2016, Springer LNCS **10157** (2016), pp.223–238 (ver. 1), `https://eprint.iacr.org/2016/1079` (ver. 2).

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

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

[6] S. Hasegawa, T. Kaneko, An attacking method for a public-key cryptosystem based on the difficulty of solving a system of non-linear equations (in Japanese), Proc. 10th SITA. **JA5-3** (1987).

[7] Y. Hashimoto, On the security of Cubic UOV and its variants, `https://eprint.iacr.org/2016/788`, 2016.

[8] A. Kipnis, J. Patarin, L. Goubin, Unbalanced oil and vinegar signature schemes, Eurocrypt 1999, Springer LNCS **1592** (1999), pp.206–222, `http://www.goubin.fr/papers/OILLONG.PDF` (extended).

[9] A. Kipnis, A. Shamir, Cryptanalysis of the oil and vinegar signature scheme, Crypto 1998, Springer LNCS **1462** (1998), pp.257–266.

[10] X. Nie, B. Liu, H. Xiong, G. Lu, Cubic unbalance oil and vinegar signature scheme, Inscrypt 2015, Springer LNCS **9589** (2015), pp.47–56.

[11] A. Shamir, Efficient signature schemes based on birational permutations, Crypto 1993, Springer LNCS **773** (1993), pp.1–12.

[12] K.-A. Shim, N. Koo, C.-M. Park, Security analysis of improved Cubic UOV signature schemes, ICISC 2017, Springer LNCS **10779** (2017), pp. 310-324.

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

[14] Y. Wang, Two polynomial-time attacks on CUOV signature scheme, Seminar, Kyushu University, April 2017, `http://www.imi.kyushu-u.ac.jp/seminars/view/2069`.

Department of Mathematical Sciences
Faculty of Science
University of the Ryukyus
Nishihara-cho, Okinawa 903-0213
JAPAN