On the security of Cubic UOV and its variants

Yasufumi Hashimoto *

Abstract

The unbalanced oil and vinegar signature scheme (UOV) is one of signature schemes whose public key is a set of multivariate quadratic forms. Recently, a new variant of UOV called Cubic UOV was proposed at Inscrypt 2015. It was claimed that the cubic UOV was more efficient than the original UOV and its security was enough. However, an equivalent secret key of the cubic UOV can be recovered easily. In this note, we describe how to recover it.

After we posted the first version of this note, Duong et al. proposed two variants of Cubic UOV at ICISC 2016. We also explain their weakness in the second version.

Keywords. multivariate public-key cryptosystems, UOV, Cubic UOV

1 Introduction

The unbalanced oil and vinegar signature scheme (UOV) [4] is one of signature schemes whose public key is a set of multivariate quadratic forms. The signature generation of UOV is efficient since it requires only linear operations. On the other hand, the key size of UOV is relatively larger than other schemes.

Recently, a new variant of UOV called Cubic UOV was proposed at Inscrypt 2015 [6]. It was claimed that the cubic UOV was more efficient than the original UOV and its security was enough. However, an equivalent secret key of the cubic UOV can be recovered easily. In this note, we describe how to recover it.

After we posted the first version of this note, Duong et al. [2] proposed two variants of Cubic UOV at ICISC 2016. We also explain their weakness in the second version.

2 UOV

The original unbalanced oil and vinegar signature scheme (UOV) [4] is described as follows.

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

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

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

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 $y = (y_1, \dots, y_o)^t \in k^o$, first choose $u_1, \dots, u_v \in k$ randomly and find $z_1, \dots, z_o \in k$ such that

$$\begin{aligned} g_1(z_1, \dots, z_o, u_1, \dots, u_v) &= y_1, \\ &\vdots \\ g_o(z_1, \dots, z_o, u_1, \dots, u_v) &= y_o. \end{aligned}$$

Note that the above is a set of linear equations of $z_1, \dots, z_o$. The signature for y is $x = S^{-1}(z_1, \dots, z_o, u_1, \dots, u_v)^t$. It is *verified* by $F(x) = y$.

It is known that an equivalent secret key of UOV can be recovered by Kipnis-Shamir's attack [5, 4] with the complexity $\ll q^{v-o} \cdot$(polyn.). Then the parameter v must be sufficiently larger than o.

3 Cubic UOV

The Cubic UOV [6] is constructed as follows.

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 $z_1(x), \dots, z_o(x)$ and $y_1(x), \dots, y_o(x)$ by

$$\begin{aligned} z_1(x) :=& \sum_{1 \leq i \leq o} x_i \cdot (\text{linear form of } x_{o+1}, \dots, x_n) + (\text{quadratic form of } x_{o+1}, \dots, x_n), \\ z_l(x) :=& (\text{linear form of } x_1, \dots, x_n), \quad (2 \leq l \leq o), \\ y_1(x) :=& r_1 z_1(x)(1 + z_2(x)) + g_1(x), \\ y_2(x) :=& r_2 z_1(x) z_2(x) + g_2(x), \\ y_l(x) :=& r_l z_l(x)(z_{l-2}(x) + z_{l-1}(x)) + g_l(x), \quad (3 \leq l \leq o), \end{aligned}$$

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

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 $m = (m_1, \dots, m_o)^t \in k^o$, choose $u_1, \dots, u_v \in k$ randomly and compute

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

recursively. Find $\alpha_1, \dots, \alpha_o \in k$ such that

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

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

4 On the security of Cubic UOV

In this section, we propose an attack to recover an equivalent secret key.

Step 1. Let $f_1(x), \dots, f_o(x)$ be polynomials with $F(x) = (f_1(x), \dots, f_o(x))^t$. Choose a constant $c \in k^n \backslash \{0\}$ randomly and compute the difference $D_c f_i(x) := f_i(x+c) - f_i(x)$ for $i = 1, 2$. Denote by Q_i the coefficient matrix of the quadratic form $D_c f_i(x)$.

Step 2. Find $\beta \in k \backslash \{0\}$ such that the rank of $Q_1 + \beta Q_2$ is at most v.

Since

$$y_1(x) - r_1 r_2^{-1} y_2(x) = z_1(x) + (\text{cubic form of } x_{o+1}, \dots, x_n)$$

and $z_1(x)$ is a quadratic form, there exists $\beta \in k \backslash \{0\}$ such that

$$Q_1 + \beta Q_2 = S^t \begin{pmatrix} 0_o & 0 \\ 0 & *_v \end{pmatrix} S. \tag{1}$$

Such a constant β is a common solution of univariate equations derived from the condition that the rank of $Q_1 + \beta Q_2$ is at most v.

Step 3. Find a $v \times o$ matrix M such that

$$\begin{pmatrix} I_o & M^t \\ 0 & I_v \end{pmatrix} (Q_1 + \beta Q_2) \begin{pmatrix} I_o & 0 \\ M & I_v \end{pmatrix} = \begin{pmatrix} 0_o & 0 \\ 0 & *_v \end{pmatrix}$$

and put $f_i'(x) := f_i\left(\left(\begin{smallmatrix} I_o & 0 \\ M & I_v \end{smallmatrix}\right) x\right)$ for $1 \leq i \leq o$.

Due to (1), we see that the matrix M is found easily by elementary linear operations and M satisfies

$$S \begin{pmatrix} I_o & 0 \\ M & I_v \end{pmatrix} = \begin{pmatrix} *_o & * \\ 0 & *_v \end{pmatrix}.$$

Once such a matrix M is recovered, the attacker can generate dummy signatures easily, since $g_l(\left(\left(\begin{smallmatrix} *_o & * \\ 0 & *_v \end{smallmatrix}\right) x\right)$ is a polynomial of $x_{o+1}, \dots, x_n$,

$$z_1\left(\begin{pmatrix} *_o & * \\ 0 & *_v \end{pmatrix} x\right) = \sum_{1 \leq i \leq o} x_i \cdot (\text{linear form of } x_{o+1}, \dots, x_n) + (\text{quadratic form of } x_{o+1}, \dots, x_n)$$

and $z_l\left(\left(\begin{smallmatrix} *_o & * \\ 0 & *_v \end{smallmatrix}\right) x\right)$ is a linear form of $x_1, \dots, x_n$ for $2 \leq l \leq o$. □

Remark. After posting the first version of this note, Duong and Wang have presented at several places (e.g. http://www.imi.kyushu-u.ac.jp/seminars/view/2069 and http://www.math.hcmus.edu.vn/index.php?option=com_content&task=view&id=2490&Itemid=82) to claim that my attack in this section was infeasible because there were not a matrix M satisfying the condition in Step 3 with high probability. It is a foolish opinion since $M = -S_{22}^{-1} S_{21}$ satisfies the condition where S_{21}, S_{22} are respectively $v \times o$- and $v \times v$ matrices with $S = \begin{pmatrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{pmatrix}$. They further claimed that it is not available when S_{22} is taken not to be invertible. We omitted such a case because it is a minor situation and we cannot believe that there will exist a person recommending to take S in that way to enhance the security. Even if such a situation will happen, the attacker can arrange the attack quite easily (for example, permute the variables before starting the attack).

5 Duong's variants of Cubic UOV

After the first version of this note was posted, Duong et al. [2] proposed two variants of Cubic UOV. We describe their construction and discuss the security of these schemes in this section.

5.1 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 $z_1(x), \dots, z_o(x)$ and $y_1(x), \dots, y_o(x)$ by

$$\begin{aligned} z_1(x) :=& (\text{quadratic form of } x_1, \dots, x_n), \\ z_l(x) :=& (\text{linear form of } x_1, \dots, x_n), \quad (2 \leq l \leq o), \\ y_1(x) :=& z_1(x) + g_1(x), \\ y_l(x) :=& z_{l-1}(x) z_l(x) + g_l(x), \quad (2 \leq l \leq o), \end{aligned}$$

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

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

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

The *public key* is given by $F := T \circ Y \circ S : k^n \to k^o$. 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 [2] for the details).

5.2 SVSv

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

$$\begin{aligned} z_l(x) :=& (\text{linear form of } x_1, \dots, x_n), \quad (1 \leq l \leq o), \\ y_1(x) :=& z_1^2(x) + g_1(x), \\ y_l(x) :=& z_{l-1}(x) z_l(x) + g_l(x), \quad (2 \leq l \leq o), \end{aligned}$$

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

The *secret keys* of CSSv 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 [2] for the details).

SVSv2. In the second version of [2], SVSv was arranged to enhance the security against the high-rank attack. Let n, o, v, r, k, q, Y, T be as defined for SVSv. The difference between SVSv2 and SVSv is the number of variables and the choice of S. Choose an additional integer

$s \geq 1$, put $n_1 := n + s$ and change $S : k^n \to k^n$ to be an affine map $S : k^{n_1} \to k^n$. The public key is $F := T \circ Y \circ S : k^{n_1} \to k^o$.

5.3 Security of these schemes

In this subsection, we discuss the security of these schemes.

SVSv2. It is easy to see that $F(x_1, \ldots, x_n, 0, \ldots, 0)$ is a public key of SVSv. SVSv2 is a non-sense modification of SVSv. $\square$

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

$$\begin{aligned} \tilde{y}_1(x) :=& x_1^2 + g_1(x), \\ \tilde{y}_l(x) :=& x_{l-1}x_l + g_l(x), \quad (2 \leq l \leq o). \end{aligned}$$

This means that SVSv is almost same to a thin version of Tsujii's/Shamir's scheme [8, 7] proposed over 20 years ago. Then, similar to [3, 1], the attacker can recover an equivalent secret key easily. $\square$

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

$$\begin{aligned} \tilde{y}_1(x) :=& (\text{quadratic form of } x_1, \ldots, x_n, \\ \tilde{y}_2(x) :=& (\text{cubic form of } x_1, \ldots, x_n), \\ \tilde{y}_l(x) :=& x_{l-1}x_l + g_l(x), \quad (3 \leq l \leq o). \end{aligned}$$

Recall that the quadratic forms $f_2(x), \ldots, f_o(x)$ in the public key $F(x) = (f_1(x), \ldots, f_o(x))^t$ are linear sums of $\tilde{y}_1(S(Z(x))), \tilde{y}_3(S(Z(x))), \ldots, \tilde{y}_o(S(Z(x)))$. Since arbitrary linear sums of coefficient matrices of $\tilde{y}_3(x), \ldots, \tilde{y}_o(x)$ are of rank (at most) $n-1$, we can recover an equivalent secret key by the high rank attack similar to [3, 1]. $\square$

We thus conclude that Duong's variants of Cubic UOV are not secure at all.

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'93, LNCS **773** (1994), pp.435–443.

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

[3] 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).

[4] 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.

[5] A. Kipnis, A. Shamir, Cryptanalysis of the oil and vinegar signature scheme, Crypto'98, LNCS **1462** (1998), pp.257–266.

[6] X. Nie, B. Liu, H. Xiong, G. Lu, Cubic unbalance oil and vinegar signature scheme, Inscrypt'15, LNCS **9589** (2015), pp.47–56.

[7] A. Shamir, Efficient signature schemes based on birational permutations, Crypto '93, LNCS **773** (1993), pp.1–12.

[8] 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.