On the security of Cubic UOV

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.

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

1 Introduction

The unbalanced oil and vinegar signature scheme (UOV) [1] 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 [3]. 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.

2 UOV

The original unbalanced oil and vinegar signature scheme (UOV) [1] is described.

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 $G(x) = (g_1(x), \ldots, g_o(x))^t$ where $g_l(x)$ $(1 \leq l \leq o)$ is a quadratic polynomial in the form

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

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*

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

signature of a given message $y = (y_1, \ldots, y_o)^t \in k^o$, first choose $u_1, \ldots, u_v \in k$ randomly and find $z_1, \ldots, z_o \in k$ such that

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

Note that the above is a set of linear equations of $z_1, \ldots, z_o$. The signature for y is $x = S^{-1}(z_1, \ldots, z_o, u_1, \ldots, u_v)^t$. 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 [2, 1] 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 [3] 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 $z_1(x), \ldots, z_o(x)$ and $y_1(x), \ldots, y_o(x)$ by

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

where $r_1, \ldots, r_o \in k \backslash \{0\}$, $g_1(x), g_2(x), g_3(x)$ are cubic forms of $x_{o+1}, \ldots, x_n$ and $g_4(x), \ldots, g_n(x)$ 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 $m = (m_1, \ldots, m_o)^t \in k^o$, choose $u_1, \ldots, u_v \in k$ randomly and compute

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

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

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

The signature for m is $x = S^{-1}(\alpha_1, \ldots, \alpha_o, u_1, \ldots, u_v)^{-1}$. 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 $f_1(x), \ldots, f_o(x)$ be polynomials with $F(x) = (f_1(x), \ldots, f_o(x))^t$. Choose $c \in k^n$ 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

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

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 $1 \le i \le o$.

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 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 $x_{o+1}, \ldots, x_n$,

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

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

Acknowledgment. This work was supported by CREST, JST and JSPS Grant-in-Aid for Young Scientists (B) no. 26800020.

References

[1] 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.

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

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