On the security of Hufu-UOV

Yasufumi Hashimoto *

Abstract

In 2019, Tao proposed a new variant of UOV with small keys, called Hufu-UOV. This paper studies its security.

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

1 UOV and Hufu-UOV

We first describe the original UOV [3, 1] and Hufu-UOV [4].

1.1 UOV

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

$$\begin{aligned} g_l(\mathbf{x}) &= \sum_{1 \leq i \leq o} x_i \cdot (\text{linear form of } x_{o+1}, \ldots, x_n) + (\text{quadratic form of } x_{o+1}, \ldots, x_n) \\ &= {}^t\mathbf{x} \begin{pmatrix} 0_o & * \\ * & *_v \end{pmatrix} \mathbf{x} + (\text{linear form}), \qquad (1 \leq l \leq o) \end{aligned}$$

where the coefficients of the polynomials above are elements of $\mathbf{F}_q$. The unbalanced oil and vinegar signature scheme (UOV) [3, 1] 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

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

Since the equations in (1) are linear, $(y_1, \ldots, y_o)$ is given efficiently. 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.

Security. Major attacks on UOV are Kipnis-Shamir's attack [2, 1] and the direct attack. Kipnis-Shamir's attack is to recover an affine map $S_1 : \mathbf{F}_q^n \to \mathbf{F}_q^n$ equivalent to S and its complexity is

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

known to be $O(q^{\max(0,v-o)}\cdot(\text{polyn.}))$. The direct attack is to generate a dummy signature by solving the system of quadratic equations $F(\mathbf{x})=\mathbf{m}$ directly. It is known that its complexity is, in general, exponential of m.

1.2 Hufu-UOV

Hufu-UOV [4] is a variant of UOV whose quadratic polynomials are constructed by circulant matrices and Toeplitz matrices respectively given in the following forms.

$$\begin{pmatrix} a_0 & a_1 & \cdots & a_{n-2} & a_{n-1} \\ a_{n-1} & a_0 & \ddots & a_{n-3} & a_{n-2} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ a_2 & a_3 & \ddots & a_0 & a_1 \\ a_1 & a_2 & \cdots & a_{n-1} & a_0 \end{pmatrix}, \qquad \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-2} & a_{n-1} \\ b_1 & a_0 & \ddots & a_{n-3} & a_{n-2} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ b_{n-2} & b_{n-3} & \ddots & a_0 & a_1 \\ b_{n-1} & b_{n-2} & \cdots & b_1 & a_0 \end{pmatrix}.$$

Define the quadratic map $G(\mathbf{x})=(g_1(\mathbf{x}),\dots,g_o(\mathbf{x}))$ and the invertible linear map $S:\mathbf{F}_q^n\to\mathbf{F}_q^n$ by

$$g_l(\mathbf{x}) = {}^t\mathbf{x}\begin{pmatrix}\lambda_l A & {}^tU_l \\ U_l & W_l\end{pmatrix}\mathbf{x}, \qquad (1\le l\le o),$$
$$S(\mathbf{x}) = \begin{pmatrix} I_o & 0 \\ M & I_v\end{pmatrix}\mathbf{x},$$

where $\lambda_l\in\mathbf{F}_q$, A is an $o\times o$-Toeplitz matrix, W_l is a $v\times v$-circulant matrix and U_l, M are the first o-columns of $v\times v$-circulant matrices. Note that A and W_l can be taken to be symmetric. Then the Hufu-UOV is as follows.

Secret key. The invertible affine map $S:\mathbf{F}_q^n\to\mathbf{F}_q^n$ and the quadratic map $G:\mathbf{F}_q^n\to\mathbf{F}_q^o$ defined above, and an invertible affine map $T:\mathbf{F}_q^o\to\mathbf{F}_q^o$.

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 $\mathbf{m}\in\mathbf{F}_q^o$ to be signed, compute $\mathbf{z}=(z_1,\dots,z_o):=T^{-1}(\mathbf{m})$ and choose $u_1,\dots,u_v\in\mathbf{F}_q$ randomly. Find $(y_1,\dots,y_o)\in\mathbf{F}_q^o$ with

$$\begin{aligned} &g_1(y_1,\dots,y_o,u_1,\dots,u_v)=z_1,\\ &g_2(y_1,\dots,y_o,u_1,\dots,u_v)-\lambda_2\lambda_1^{-1}g_1(y_1,\dots,y_o,u_1,\dots,u_v)=z_2-\lambda_2\lambda_1^{-1}z_1,\\ &\quad\vdots\\ &g_o(y_1,\dots,y_o,u_1,\dots,u_v)-\lambda_o\lambda_1^{-1}g_1(y_1,\dots,y_o,u_1,\dots,u_v)=z_o-\lambda_o\lambda_1^{-1}z_1.\end{aligned} \tag{2}$$

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

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

Since the first equation in (2) is quadratic and the later $o-1$ equations are linear, one can generate the signature easily.

The number of parameters in the secret key of Hufu-UOV is about $\frac{3}{2}ov$. It is much smaller than $\frac{1}{2}ov^2+o^2v$, which is a round number of the parameters in the secret key of the original UOV. This situation is similar to the public key. For the security, Tao [4] claimed that Hufu-

UOV is almost as secure as the original UOV against the known attacks. However, it is not true. We propose an attack on Hufu-UOV in the next section.

2 Proposed attack

Let $f_1(\mathbf{x}),\dots,f_o(\mathbf{x})$ be public quadratic polynomials with $F(\mathbf{x})=(f_1(\mathbf{x}),\dots,f_o(\mathbf{x}))$, and $\bar{g}_1(\mathbf{x}),\dots,\bar{g}_o(\mathbf{x})$ the quadratic polynomials with $(T\circ G)(\mathbf{x})=(\bar{g}_1(\mathbf{x}),\dots,\bar{g}_o(\mathbf{x}))$. For $1\le l\le o$, we write $f_l(\mathbf{x}),g_l(\mathbf{x})$ by $f_l(\mathbf{x})={}^t\mathbf{x}\begin{pmatrix}A_l & {}^tB_l\\ B_l & C_l\end{pmatrix}\mathbf{x}$ and $\bar{g}_l(\mathbf{x})={}^t\mathbf{x}\begin{pmatrix}\bar{V}_l & {}^t\bar{U}_l\\ \bar{U}_l & \bar{W}_l\end{pmatrix}\mathbf{x}$ for $o\times o$ symmetric matrices $A_l,\bar{V}_l$, $v\times o$ matrices $B_l,\bar{U}_l$ and $v\times v$ symmetric matrices $C_l,\bar{W}_l$. By the definition of T and G, we see that there exist $\mu_1,\dots,\mu_o\in\mathbf{F}_q$ such that $\bar{V}_l=\mu_lA$. Since $f_l(S^{-1}(\mathbf{x}))=\bar{g}_l(\mathbf{x})$, we have

$$A_l-{}^tB_lM-{}^tMB_l+{}^tMC_lM=\mu_lA,\quad B_l-C_lM=\bar{U}_l,\quad C_l=\bar{W}_l. \tag{3}$$

Recall that $M,\bar{U}_l,\mu_l,A$ are secret and A_l,B_l,C_l are public. Furthermore, note that A_l is an $o\times o$ symmetric Toeplitz matrix, C_l is a $v\times v$ symmetric circulant matrix and B_l is the first o column of a $v\times v$ circulant matrix. It is easy to see that there exist $v\times v$ circulant matrices A^c,A_l^c,B_l^c,M^c such that

$$A=(I_o,0)A^c\begin{pmatrix}I_o\\0\end{pmatrix},\quad A_l=(I_o,0)A_l^c\begin{pmatrix}I_o\\0\end{pmatrix},\quad B_l=B_l^c\begin{pmatrix}I_o\\0\end{pmatrix},\quad M=M^c\begin{pmatrix}I_o\\0\end{pmatrix}.$$

For example, if $o=2,v=5$ and

$$A=\begin{pmatrix}1&2\\2&1\end{pmatrix},\qquad M=\begin{pmatrix}3&2\\1&3\\1&1\\0&1\\2&0\end{pmatrix},$$

the 5×5 circulant matrices A^c,M^c are as follows.

$$A^c=\left(\begin{array}{cc|ccc}1&2&y&y&2\\2&1&2&y&y\\\hline y&2&1&2&y\\y&y&2&1&2\\2&y&y&2&1\end{array}\right),\qquad M^c=\left(\begin{array}{cc|ccc}3&2&0&1&1\\1&3&2&0&1\\1&1&3&2&0\\0&1&1&3&2\\2&0&1&1&3\end{array}\right).$$

Remark that A^c cannot be fixed uniquely and the number of unknowns in A^c is $\lceil\frac{v+1}{2}\rceil-o$. At the present time, we remain such unfixed parameters to be unknowns.

Due to (3), we have

$$\mu_lA^c=A_l^c-{}^tB_l^cM^c-{}^tM^cB_l^c+{}^tM^cC_lM^c.$$

Since the multiplication between circulant matrices is commutative, the equation above is written by

$$\mu_lA^c=A_l^c-{}^tB_l^cM^c-B_l^{ct}M^c+C_l{}^tM^cM^c \tag{4}$$

for $1\le l\le o$. Let

$$H_l:=C_l{}^tM^cM^c-{}^tB_l^cM^c-B_l^{ct}M^c+A_l^c-\mu_lA^c$$

for $1 \leq l \leq o$ and

$$\bar{H}_l(\delta_l, \delta_2) := (C_2 - \delta_2 C_1)H_l - (C_l - \delta_l C_1)H_2 + (\delta_2 C_l - \delta_l C_2)H_1$$

for $3 \leq l \leq o$, $\delta_2, \delta_l \in \mathbf{F}_q$. We have

$$\begin{aligned}\bar{H}_l(\delta_l, \delta_2) =& ((C_l{}^t B_2^c - C_2{}^t B_l^c) + \delta_2(C_1{}^t B_l^c - C_l{}^t B_1^c) + \delta_l(C_2{}^t B_1^c - C_1{}^t B_2))M^c \\ &+ ((C_l B_2^c - C_2 B_l^c) + \delta_2(C_1 B_l^c - C_l B_1^c) + \delta_l(C_2 B_1^c - C_1 B_2))^t M^c \\ &+ (C_2 A_l^c - C_l A_2^c) + \delta_2(C_l A_1^c - C_1 A_l^c) + \delta_l(C_1 A_2^c - C_2 A_1^c) \\ &+ ((\mu_l \delta_2 - \mu_2 \delta_l)C_1 + (\mu_1 \delta_l - \mu_l)C_2 + (\mu_2 - \mu_1 \delta_2)C_l)A^c.\end{aligned}$$

This means that, if $\delta_2 = \mu_1^{-1}\mu_2$ and $\delta_l = \mu_1^{-1}\mu_l$ hold, the matrix equation $\bar{H}_l(\delta_l, \delta_2) = 0$ generates a system of linear equations of unknowns in M^c, A_1^c, A_2^c, A_l^c. The number of equations and variables derived from $\bar{H}_3(\delta_3, \delta_2) = 0, \ldots, \bar{H}_K(\delta_K, \delta_2) = 0$ are respectively $\lceil \frac{v+1}{2} \rceil (K-2)$ and $v + (\lceil \frac{v+1}{2} \rceil - o)K$, and then we can recover M by solving its system of linear equations if $K \geq \frac{2v+1}{o}$ and $\delta_2, \ldots, \delta_K$ are chosen correctly. Thus the following attack is available on Hufu-UOV.

Step 1. Choose $\delta_2, \ldots, \delta_K \in \mathbf{F}_q$ randomly.

Step 2. Solve the system of linear equations derived from $\bar{H}_3(\delta_3, \delta_2) = 0, \ldots, \bar{H}_K(\delta_K, \delta_2) = 0$. If there exists a solution, fix M by its solution. If not, go back to Step 1 and choose another $(\delta_1, \ldots, \delta_K)$.

Step 3. If the quadratic forms of $x_1, \ldots, x_o$ in $f_2\left(\begin{pmatrix} I_o & \\ -M & I_v \end{pmatrix}\mathbf{x}\right), \ldots, f_m\left(\begin{pmatrix} I_o & \\ -M & I_v \end{pmatrix}\mathbf{x}\right)$ are constant multiples of the quadratic form of $x_1, \ldots, x_o$ in $f_1\left(\begin{pmatrix} I_o & \\ -M & I_v \end{pmatrix}\mathbf{x}\right)$, output M as the correct secret key. If not, go back to Step 1 and choose another $(\delta_2, \ldots, \delta_K)$.

Since the number of candidates of $(\delta_2, \ldots, \delta_K)$ are $q^{K-1} = q^{\lceil \frac{2v+1}{o} \rceil - 1}$, the complexity of this attack is $O\left(q^{\lceil \frac{2v+1}{o} \rceil - 1} \cdot (\text{polyn},)\right)$. It is much less than the complexities of the Kipnis-Shamir's attack and the direct attack on the original UOV.

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

References

[1] A. Kipnis, J. Patarin, L. Goubin, Unbalanced oil and vinegar signature schemes, Eurocrypt'99, LNCS **1592** (1999), 206–222, extended in `http://www.goubin.fr/papers/OILLONG.PDF`, 2003.

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

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

[4] C. Tao, A Method to Reduce the Key Size of UOV Signature Scheme, https://eprint.iacr.org/2019/473.