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 $F_q$ a finite field of order $q$. Define the quadratic map $G : F_q^n \to F_q^o$, $x = \ell(x_1, \ldots, x_n) \mapsto G(x) = \ell(g_1(x), \ldots, g_o(x))$ by

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

$$= x^t \left( \begin{array}{c} 0_o \\ * \\ * \\ *_v \end{array} \right) x + (\text{linear form}), \quad (1 \leq l \leq o)$$

where the coefficients of the polynomials above are elements of $F_q$. The unbalanced oil and vinegar signature scheme (UOV) [3, 1] is constructed as follows.

Secret key. An invertible affine map $S : F_q^n \to F_q^n$ and the quadratic map $G$ defined above.

Public key. The quadratic map $F := G \circ S : F_q^n \to F_q^o$.

Signature generation. For a message $m = \ell(m_1, \ldots, m_o) \in F_q^o$ to be signed, choose $u_1, \ldots, u_v \in F_q$ randomly, and find $(y_1, \ldots, y_o) \in F_q^o$ with

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

Since the equations in (1) are linear, $(y_1, \ldots, y_o)$ is given efficiently. The signature for $m$ is $z := S^{-1}\ell(y_1, \ldots, y_o, u_1, \ldots, u_v)$.

Signature verification. The signature $z$ is verified if $F(z) = m$ 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 $S_1 : F_q^n \to F_q^n$ 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 $F(x) = m$ 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.

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

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

$$
g_l(x) = x^T \begin{pmatrix} \lambda_l A & U_l \\ I_l & W_l \end{pmatrix} x, \quad (1 \leq l \leq o),
$$

$$
S(x) = \begin{pmatrix} I_o & 0 \\ M & I_v \end{pmatrix} x,
$$

where $\lambda_l \in \mathbb{F}_q$, $A$ 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 $S : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ and the quadratic map $G : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ defined above, and an invertible affine map $T : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$.

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

**Signature generation.** For a message $m \in \mathbb{F}_q^n$ to be signed, compute $z = (z_1, \ldots, z_o) := T^{-1}(m)$ and choose $u_1, \ldots, u_v \in \mathbb{F}_q$ randomly. Find $(y_1, \ldots, y_o) \in \mathbb{F}_q$ with

$$
g_1(y_1, \ldots, y_o, u_1, \ldots, u_v) = z_1,
$$

$$
g_2(y_1, \ldots, y_o, u_1, \ldots, u_v) - \lambda_2 \lambda_1^{-1} g_1(y_1, \ldots, y_o, u_1, \ldots, u_v) = z_2 - \lambda_2 \lambda_1^{-1} z_1,
$$

$$
\vdots
$$

$$
g_o(y_1, \ldots, y_o, u_1, \ldots, u_v) - \lambda_o \lambda_1^{-1} g_1(y_1, \ldots, y_o, u_1, \ldots, u_v) = z_o - \lambda_o \lambda_1^{-1} z_1.
$$

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

**Signature verification.** The signature $z$ is verified if $F(z) = m$ 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 $\frac{1}{2} ov^2 + o^2 v$, 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-
On the security of Hufu-UOV

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 $f_1(x), \ldots, f_o(x)$ be public quadratic polynomials with $F(x) = (f_1(x), \ldots, f_o(x))$, and $g_1(x), \ldots, g_o(x)$ the quadratic polynomials with $(T \circ G)(x) = (g_1(x), \ldots, g_o(x))$. For $1 \leq l \leq o$, we write $f_l(x), g_l(x)$ by $f_l(x) = \langle A_l^T B_l \rangle x$ and $g_l(x) = \langle V_l^T U_l \rangle x$ for $o \times o$ symmetric matrices $A_l, V_l, B_l, U_l$ and $v \times v$ symmetric matrices $C_l, W_l$. By the definition of $T$ and $G$, we see that there exist $\mu_1, \ldots, \mu_o \in \mathbb{F}_q$ such that $V_l = \mu_l A$. Since $f_1(S^{-1}(x)) = g_l(x)$, we have

$$A_l - t^l B_l M - t^l M B_l + t^l M C_l M = \mu_l A, \quad B_l - C_l M = \bar{U}_l, \quad C_l = \bar{W}_l. \quad (3)$$

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 $A^c, A^c_l, B^c_l, M^c$ such that

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

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

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

the $5 \times 5$ circulant matrices $A^c, M^c$ are as follows.

$$A^c = \begin{pmatrix} 1 & 2 & y & y & 2 \\ 2 & 1 & y & y & \\ y & 2 & 1 & 2 & y \\ y & y & 2 & 1 & 2 \\ 2 & y & y & 2 & 1 \end{pmatrix}, \quad M^c = \begin{pmatrix} 3 & 2 & 0 & 1 & 1 \\ 1 & 3 & 2 & 0 & 1 \\ 1 & 1 & 3 & 2 & 0 \\ 0 & 1 & 1 & 3 & 2 \\ 2 & 0 & 1 & 1 & 3 \end{pmatrix}.$$ 

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

Due to (3), we have

$$\mu_l A^c = A^c_l - t^l B^c_l M^c - t^l M B^c_l + t^l M c_l M^c.$$ 

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

$$\mu_l A^c = A^c_l - t^l B^c_l M^c - B^c_l M^c + C_l M^c M^c \quad (4)$$

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

$$H_l := C_l M^c M^c - t^l B^c_l M^c - B^c_l M^c + A^c_l - \mu_l A^c.$$
for \(1 \leq l \leq o\)

\[
\tilde{H}_l(\delta_1, \delta_2) := (C_2 - \delta_2 C_1)H_1 - (C_1 - \delta_1 C_1)H_2 + (\delta_2 C_1 - \delta_1 C_2)H_1
\]

for \(3 \leq l \leq o\), \(\delta_2, \delta_1 \in F_q\). We have

\[
\tilde{H}_l(\delta_1, \delta_2) = (C_1^{t}B_2^{t} - C_2^{t}B_1^{t}) + \delta_2(C_1^{t}B_1^{t} - C_1^{t}B_1^{t}) + \delta_1(C_2^{t}B_2^{t} - C_2^{t}B_2^{t})M^c
\]

\[
+ (C_1 B_2^t - C_2 B_1^t) + \delta_2(C_1 B_1^t - C_1 B_1^t) + \delta_1(C_2 B_2^t - C_2 B_2^t) + M^c
\]

\[
+ (C_2 A_1^t - C_1 A_2^t) + \delta_2(C_1 A_1^t - C_1 A_1^t) + \delta_1(C_2 A_2^t - C_2 A_2^t) + (\mu_2 \delta_2 - \mu_1 \delta_1)C_2 + (\mu_2 - \mu_1 \delta_2)C_1 H^c.
\]

This means that, if \(\delta_2 = \mu_1^{-1}\mu_2\) and \(\delta_1 = \mu_1^{-1}\mu_1\) hold, the matrix equation \(\tilde{H}_l(\delta_1, \delta_2) = 0\) generates a system of linear equations of unknowns in \(M^c, A_1^t, A_2^t, A_1^t\). The number of equations and variables derived from \(\tilde{H}_3(\delta_3, \delta_2) = 0, \ldots, \tilde{H}_K(\delta_K, \delta_2) = 0\) are respectively \([\frac{n+1}{2}](K - 2)\) and \(v + [\frac{n+1}{2}] - o\)K, and then we can recover \(M\) by solving its system of linear equations if \(K \geq \frac{2n+1}{o}\) and \(\delta_2, \ldots, \delta_K\) are chosen correctly. Thus the following attack is available on Hufu-UOV.

**Step 1.** Choose \(\delta_2, \ldots, \delta_K \in F_q\) randomly.

**Step 2.** Solve the system of linear equations derived from \(\tilde{H}_3(\delta_3, \delta_2) = 0, \ldots, \tilde{H}_K(\delta_K, \delta_2) = 0\). 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 \(f_2\left(\begin{pmatrix} I_o & -M \\ I_o & 1_o \end{pmatrix} x\right), \ldots, f_m\left(\begin{pmatrix} I_o & -M \\ I_o & 1_o \end{pmatrix} x\right)\) are constant multiples of the quadratic form of \(x_1, \ldots, x_o\) in \(f_1\left(\begin{pmatrix} I_o & -M \\ I_o & 1_o \end{pmatrix} x\right)\), 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 \(q^{K-1} = q^{[\frac{2n+1}{o}] - 1}\), the complexity of this attack is \(O\left(q^{[\frac{2n+1}{o}] - 1}\cdot(\text{polyn.})\right)\). 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


